El impacto del Reglamento de Inteligencia Artificial en las Administraciones públicas*

The impact of the Artificial Intelligence Act on public administrations

Agustí Cerrillo i Martínez
Catedrático de Derecho Administrativo
Universitat Oberta de Catalunya

https://doi.org/10.36151/RJIB.2024.26.03

Resumen: La reciente aprobación del Reglamento de Inteligencia Artificial abre la puerta a un nuevo escenario en la Unión Europea para el desarrollo y la utilización de esta tecnología disruptiva. Las Administraciones públicas están llamadas a tener un papel protagonista como proveedoras y responsables del despliegue de la inteligencia artificial y como garantes del cumplimiento de la norma europea. En este artículo se hace una primera aproximación al contenido del Reglamento de Inteligencia Artificial desde la perspectiva de las Administraciones públicas españolas.

* Este artículo es resultado del proyecto de investigación «Personalización de servicios públicos, sesgos e inteligencia artificial: Hacia la consolidación de los derechos digitales en la administración» del Programa Estatal de I+D+i Orientada a los Retos de la Sociedad (PID2020-115774RB-I00). El autor quiere agradecer los comentarios realizados por el professor Miquel PEGUERA.

Palabras clave: inteligencia artificial, Administración pública, Unión Europea, transformación digital.

Resum: La recent aprovació del Reglament d'intel·ligència artificial obre la porta a un nou escenari a la Unió Europea per al desenvolupament i la utilització d'aquesta tecnologia disruptiva. Les administracions públiques estan cridades a tenir un paper protagonista com a proveïdores i responsables del desplegament de la intel·ligència artificial i com a garants del compliment de la norma europea. En aquest article es fa una primera aproximació al contingut del Reglament d'intel·ligència artificial des de la perspectiva de les administracions públiques espanyoles.

Paraules clau: intel·ligència artificial, Administració pública, Unió Europea, transformació digital.

Abstract: The recent approval of the Artificial Intelligence Act opens the door to a new scenario in the European Union for the development and use of this disruptive technology. Public administrations are expected to play a leading role as providers and deployers of artificial intelligence and as guarantors of compliance with the European regulation. This article provides a first overview of the content of the Artificial Intelligence Act from the perspective of Spanish public administrations.

Key words: Artificial intelligence, Public administration, European Union, digital transformation.

I. LA INTELIGENCIA ARTIFICIAL Y LAS ADMINISTRACIONES PÚBLICAS

Las Administraciones públicas están inmersas en un proceso de transformación digital propiciado, entre otros motivos, por la irrupción de la inteligencia artificial (en adelante, IA). Gracias al uso de la IA, las Administraciones públicas están sentando las bases de un nuevo modelo de Administración pública, la administración digital, basado en el uso intensivo e innovador de la tecnología para la apertura a la ciudadanía, la recopilación y el análisis de datos y la prestación de servicios inclusivos, eficientes, resilientes, sostenibles y centrados en las personas.[1]

El uso de la IA en las Administraciones públicas puede reportar numerosos beneficios, mas, como se ha ido constatando, también puede generar múltiples riesgos llegando a poner en entredicho los principios de funcionamiento de las Administraciones públicas o vulnerando los derechos de la ciudadanía.[2]

---

1 CERRILLO I MARTÍNEZ, A. «Presentación», en CERRILLO I MARTÍNEZ, A. *La transformación digital de la Admistración local*. Madrid: Fundación Democracia y Gobierno Local, 2021.

2 GAMERO CASADO, E.; PÉREZ GUERRERO, F. L. *Inteligencia artificial y sector público. Retos, límites y medios*. Valencia: Tirant lo Blanch, 2023.

Para prevenir estas situaciones, dar respuesta a los problemas que puedan surgir y, en última instancia, promover el desarrollo de una IA centrada en las personas y respetuosa con los principios del Estado de Derecho y del funcionamiento de las Administraciones públicas, en los últimos años se han empezado a aprobar distintas normas jurídicas. La mayoría de estas normas tienen un carácter principial y, por ello, su eficacia e impacto puede ser limitado.[3]

Junto a estas normas, recientemente se ha aprobado el Reglamento de Inteligencia Artificial (en adelante RIA).[4] Como veremos a continuación, esta norma está llamada a mejorar el funcionamiento del mercado interior y promover la adopción de los sistemas de IA centrados en el ser humano y fiables.[5] Asimismo, el RIA ha de promover una participación activa de las Administraciones públicas en el uso de la IA en tanto sean desarrolladoras y usuarias de sistemas de IA pero también como garantes del cumplimiento del RIA.

Ante la reciente aprobación del RIA y a la espera de poder llevar a cabo estudios más detallados y pausados sobre su contenido y el impacto que tendrá en el funcionamiento y la actividad de las Administraciones públicas, este artículo persigue llevar a cabo una primera aproximación a su contenido desde la perspectiva de las Administraciones públicas españolas que permita identificar los elementos que estas deberán tener en cuenta cuando automaticen su funcionamiento y la prestación de servicios públicos a través del uso de sistemas de IA y también determinar los recursos de que deberán disponer para poderlo llevar a cabo de manera adecuada.

Con esta finalidad, en primer lugar, expondremos el contexto en el que se aprueba el Reglamento de Inteligencia Artificial. En segundo lugar, identificaremos el concepto de inteligencia artificial y la tipología de sistemas de IA que incorpora el RIA. A continuación, analizaremos las obligaciones que incluye el RIA para las Administraciones públicas cuando desarrollen, pongan en servicio o utilicen sistemas de inteligencia artificial. En cuarto lugar,

---

3 VELASCO RICO, C. I. «Marco regulatorio de los sistemas algorítmicos y de Inteligencia Artificial: El papel de la Administración», en VALCÁRCEL FERNÁNDEZ, P. *Actas XVIII Congreso de la Asociación Española de Derecho Administrativo*. Madrid: Instituto Nacional de Administración Pública, 2024.

4 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.º 300/2008, (UE) n.º 167/2013, (UE) n.º 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) (en adelante, RIA).

5 Artículo 1 RIA.

identificaremos las funciones y potestades que el Reglamento de Inteligencia Artificial atribuye a los Estados miembros en relación con la garantía del cumplimiento de las obligaciones previstas en el mismo. Por último, concluiremos con algunas reflexiones finales.

II. EL CONTEXTO DE LA REGULACIÓN EUROPEA DE LA INTELIGENCIA ARTIFICIAL

En la última década, la Unión Europea ha desempeñado un papel de catalizador de la investigación y el desarrollo de los sistemas de IA y de regulador del uso de estas tecnologías con la finalidad de garantizar un diseño y un uso acorde con los valores de la Unión y respetuosa con los derechos fundamentales.

Para ello, en 2018, la Comisión impulsó una iniciativa europea sobre la IA que, entre otras finalidades, preveía «[g]arantizar el establecimiento de un marco ético y jurídico apropiado, basado en los valores de la Unión y en consonancia con la Carta de los Derechos Fundamentales de la UE».[6] Desde el primer momento, la estrategia europea sobre IA se centró en el ser humano reconociendo que «la IA no es un fin en sí mismo, sino un medio que debe servir a las personas con el objetivo último de aumentar su bienestar». De este modo, se ha venido reconociendo que «las aplicaciones de IA no solo deben ajustarse a la ley, sino también respetar unos principios éticos y garantizar que su implementación evite daños involuntarios».[7]

Para avanzar en esta dirección, inicialmente, se promovió la adopción de unas directrices éticas que fuesen aplicadas por desarrolladores, proveedores y usuarios de la IA en el mercado interior. A tal efecto se creó un grupo de expertos de alto nivel sobre la IA que presentó en marzo de 2019 las *Directrices éticas para una IA fiable*. Según este documento, para materializar y lograr una IA fiable es necesaria la concurrencia de los siguientes siete requisitos: la acción y supervisión humanas; la solidez técnica y seguridad; la gestión de la privacidad y de los datos; la transparencia; la diversidad, no discriminación y equidad; el bienestar social y medioambiental, y la rendición de cuentas.

---

6 COMISIÓN EUROPEA. *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones 'Inteligencia artificial para Europa' COM(2018) 237 final* (2018).

7 COMISIÓN EUROPEA. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Generar confianza en la inteligencia artificial centrada en el ser humano COM/2019/168 final* (2019).

Posteriormente, la Comisión llegó a la conclusión de que era necesario profundizar en esta dirección y, para ello, avanzar hacia la adopción de una nueva legislación específica sobre IA a nivel europeo que complementase la posible adaptación de la legislación vigente a la evolución tecnológica.[8] Igualmente, en octubre de 2020, el Parlamento Europeo adoptó una resolución sobre aspectos éticos de la IA, donde recomendó a la Comisión que revisase la legislación vigente de la Unión aplicable a la IA de acuerdo con las recomendaciones que formulaba.[9]

De este modo, en abril de 2021, la Comisión presentó 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).[10]

La tramitación de esta propuesta se ha prolongado por tres años y ha sido compleja. No solo ha sido complicado el proceso de elaboración de la norma por la multitud de actores que, de manera directa o indirecta, han participado o influido en él, sino también por la dificultad de regular un ámbito en rápida evolución, en el que no existen prácticamente referentes y en el que es difícil evaluar *ex ante* el impacto y los efectos que podrá tener la regulación adoptada. Como muestra de todo ello, podemos recordar el impacto que tuvo en la elaboración de la norma la aparición en noviembre de 2022 de ChatGPT, una muestra de la inteligencia artificial generativa, que hasta ese momento poco reflejo tenía en el articulado de la propuesta de RIA.[11]

Durante la tramitación de la propuesta de RIA, el Parlamento Europeo, el Consejo y la Comisión adoptaron la Declaración conjunta sobre los Derechos y Principios Digitales para la Década Digital con el fin de fijar unos compromisos políticos comunes, recordar los derechos más importantes en el contexto de la transformación digital, guiar a los responsables de las políticas cuando reflexionen sobre su concepción de la transformación digi-

---

8 COMISIÓN EUROPEA. *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza COM(2020) 65 final* (2020).

9 PARLAMENTO EUROPEO. *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas* (2020).

10 COM(2021) 206 final.

11 Sobre cómo la inteligencia artificial generativa ha incidido en los conceptos y principios en que se basa el RIA, véase HELBERGER, N.; DIAKOPOULOS, N. «ChatGPT and the AI Act». *Internet Policy Review*, núm. 12 (2023).

tal y servir de referencia a las empresas y otros agentes a la hora de desarrollar e implantar nuevas tecnologías.[12]

Siguiendo todos estos antecedentes, a la hora de regular la IA, la Unión Europea ha hecho una apuesta por trasladar el modelo de IA centrado en el ser humano al Reglamento de Inteligencia Artificial, de manera que llegue a «ser un líder mundial en el desarrollo de IA segura, digna de confianza y ética».[13]

Finalmente, el texto fue aprobado el 13 de marzo de 2024 por el pleno del Parlamento y el 21 de mayo siguiente por el Consejo publicándose en el Diario Oficial de la Unión Europea el 12 de julio de 2024.[14]

El resultado ha sido una norma extensa como se desprende del hecho de estar conformada por 113 artículos acompañados de 13 anexos e introducidos por 180 considerandos.[15] Asimismo, como advierte PEGUERA, «[e]l RIA es sin duda un reglamento complejo, ambicioso y a la vez revelador de difíciles equilibrios de intereses, que muestra la voluntad política de la UE de ser pionera en la regulación de la IA a nivel mundial y de fijar los estándares para otras jurisdicciones».[16]

El RIA es una norma que tiene por objetivo mejorar el funcionamiento del mercado interior en relación con estas tecnologías a partir de la definición de los requisitos que deben cumplir para poder ser puestas en el mercado

---

12 Diario Oficial de la Unión Europea, C 23, de 23 de enero de 2023.

13 Considerando 8 RIA. En esta dirección, el Consejo Europeo, en su Reunión extraordinaria de 1 y 2 de octubre de 2020 concluía que «La UE tiene que ser un líder mundial en el desarrollo de inteligencia artificial segura, digna de confianza y ética».

14 Aunque el RIA entró en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea será aplicable veinticuatro meses después. No obstante, el RIA prevé que los capítulos I y II serán aplicables a los seis meses; el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 a los doce meses, y el artículo 6, apartado 1, y las obligaciones correspondientes a los treinta y seis meses (artículo 113 RIA).
En particular, a los efectos de este trabajo, resulta de interés advertir que el RIA prevé que los proveedores y los responsables del despliegue de los sistemas de IA de alto riesgo destinados a ser utilizados por las autoridades públicas adoptarán las medidas necesarias para cumplir los requisitos y obligaciones del presente Reglamento a más tardar a los seis años a partir de la fecha de su entrada en vigor (artículo 111.2 RIA).

15 El RIA prevé que, a los cinco años a partir de la fecha de entrada en vigor y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del RIA y a los siete años evaluará su ejecución (artículo 112 RIA).

16 PEGUERA POCH, M. *Algunos aspectos del consenso interinstitucional en torno al Reglamento de IA*, en CERRILLO I MARTÍNEZ, A.; DI LASCIO, F.; MARTÍN DELGADO, I.; VELASCO RICO, C. I. *Inteligencia Artificial y Administraciones Públicas: una triple visión en clave comparada*. Madrid: Iustel, 2024 (en prensa).

o en servicio y ser utilizadas en la Unión Europea.[17] Para ello, el RIA define un marco jurídico uniforme a nivel europeo que regula el desarrollo, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA evitando las divergencias que puedan obstaculizar la libre circulación, fragmentar el mercado o generar inseguridad jurídica.[18] Este marco no solo se propone respetar los valores de la Unión Europea sino, en particular, desarrollarse de acuerdo con el modelo de IA centrada en el ser humano, que sea fiable, garantice la protección de la salud, la seguridad y los derechos fundamentales, la democracia, el Estado de Derecho y la protección del medio ambiente y apoye la innovación.[19]

Con estas finalidades, el RIA establece las normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión. Asimismo, fija unas prohibiciones de determinadas prácticas de IA; dispone los requisitos específicos y obligaciones para los operadores de los sistemas de IA de alto riesgo; define las normas de transparencia aplicables a determinados sistemas de IA y las normas armonizadas para la introducción en el mercado de modelos de IA de uso general. Por último, define las normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento y las medidas en apoyo de la innovación.[20]

III. LOS SISTEMAS DE IA EN EL RIA

La IA ha sido definida de manera muy diversa y su concepto está estrechamente relacionado a la disciplina y la aproximación que se realice. Por ello, uno de los aspectos que ha experimentado cambios significativos entre la propuesta y el texto finalmente aprobado es el relativo a la definición de

---

17 Artículo 1.1 RIA. Diversos autores se han mostrado críticos con el planteamiento de base del RIA. Véase, por todos, EDWARDS, L. *Regulating AI in Europe: four problems and four solutions*. London: Ada Lovelace Institute, 2022.
Además, deben tenerse en cuenta otras normas aprobadas por la Unión Europea y que incidirán en estas mismas finalidades desde el Reglamento (UE) 2023/988 relativo a la seguridad general de los productos a los Reglamentos (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital (Reglamento de Mercados Digitales) y 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales (Reglamento de Servicios Digitales).

18 Considerando 3 RIA.

19 Considerando 1 y artículo 1.1 RIA.

20 Artículo 1.2 RIA.

sistema de IA, aspecto que resulta fundamental para poder determinar adecuadamente el alcance de la regulación contenida en el RIA.[21]

1. Los sistemas de IA

El RIA incluye una definición de sistema de inteligencia artificial amplia.[22] Esta definición es acorde con el concepto propuesto a nivel internacional, por ejemplo, por la OCDE o el Consejo de Europa.[23] Según el RIA un sistema de IA es «un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales».[24]

2. La tipología de sistemas de IA en el RIA

La regulación que lleva a cabo el RIA sobre los sistemas de IA y, en particular, su introducción en el mercado, parte de la identificación de los riesgos —es decir, la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio—,[25] que su uso puede entrañar para intereses públicos y los derechos fundamentales.[26]

---

21 Como advierte PEGUERA, «la definición de IA que ofrece el Reglamento no pretende, por tanto, ser académica o descriptiva, sino una definición funcional a los efectos de fijar los límites de la acción legislativa» (PEGUERA POCH, M. «La propuesta de Reglamento de IA: Una intervención legislativa insoslayable en contexto de incertidumbre», en PEGUERA POCH, M. *Perspectivas regulatorias de la inteligencia artificial en la Unión Europea*. Madrid: Reus, 2023).

22 A pesar de su objeto, no todos los sistemas de IA se someten a los dictados del RIA. Entre otras exclusiones, cabe considerar que el RIA no se aplica cuando el responsable del despliegue sean personas físicas que utilicen los sistemas de IA con una finalidad puramente personal de carácter no profesional (artículo 2.10 RIA). Tampoco se aplica a los sistemas desarrollados con fines militares, de defensa o de seguridad nacional (artículo 2.3 RIA). Considerando 24 RIA en relación con el artículo 4.2 TFUE, título V, capítulo 2 TFUE. Asimismo, no se aplica a los sistemas o modelos de IA, desarrollados específicamente con fines únicamente de investigación y desarrollo científico (artículo 2.6 RIA). Por último, entre las exclusiones de la aplicación del RIA también se encuentran los sistemas de IA divulgados con licencias libres y código abierto (artículo 2.12 RIA).

23 En esta dirección, resulta de interés la lectura de la Recomendación del Consejo sobre Inteligencia Artificial adoptada en 2019 y actualizada en 2024 o del Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y derechos humanos, democracia y Estado de Derecho adoptado en mayo de 2024 que han definido un sistema de IA de la misma manera que el RIA.

24 Artículo 3.1 RIA.

25 Artículo 3.2) RIA.

26 Considerando 5 RIA. Como advierte MANTELERO, «el borrador de la IA Act adopta claramente un enfoque minimalista en cuanto a la salvaguarda del individuo y la sociedad en un escenario

A partir de este análisis de los riesgos que puedan generar los sistemas de IA y en función de su alcance e intensidad, el reglamento determina los requisitos que deben reunir y las obligaciones que deben cumplir los distintos operadores en relación con el sistema de IA y se determinan sus responsabilidades para garantizar el cumplimiento de estas obligaciones.[27]

A) Las prácticas prohibidas

El RIA identifica un primer conjunto de sistemas que pueden generar unos riesgos que se consideran inasumibles por invadir de forma especialmente grave los derechos y las libertades de las personas, por ejemplo, por afectar a su vida privada, provocar la sensación de estar bajo una vigilancia constante o disuadir del ejercicio de sus derechos, como la libertad de reunión. También por poder ser tan imprecisos que puedan generar resultados erróneos, sesgados, discriminatorios o excluyentes de determinadas personas o colectivos.[28]

En particular, el RIA prohíbe la introducción en el mercado, la puesta en servicio o la utilización de los siguientes sistemas de IA:[29]

a) sistemas de IA que utilicen técnicas subliminales, manipuladoras o engañosas. El uso de estos sistemas se prohíbe cuando tengan el objetivo o efecto de alterar el comportamiento de una persona o un colectivo, mermando su capacidad para tomar decisiones informadas, haciendo que tomen decisiones que no tomarían provocándole, o sea razonablemente probable que le pueda provocar, perjuicios considerables socavando su autonomía y su capacidad de elegir libremente;[30]

---

impulsado por la IA, centrándose únicamente en los casos más peligrosos, es decir, en las aplicaciones prohibidas y de alto riesgo» (MANTELERO, A. *La IA Act: Contexto, límites y retos de una ley de primera generación,* en PEGUERA POCH, M. *Perspectivas regulatorias de la inteligencia artificial en la Unión Europea*. Madrid: Reus, 2023).

27 Considerando 26 RIA. De todos modos, no puede desconocerse las fronteras difusas que existen entre las distintas categorías identificadas en el RIA y los solapamientos que pueden existir en relación con determinados sistemas de IA (SUNDE, I. M. «AI-based Law Enforcement Online: The Impact of the European Artificial Intelligence Act (AIA)». *Bergen Journal of Criminal Law & Criminal Justice*, núm. 10 (2022)).

28 Como recuerda PEGUERA, «la delimitación de los sistemas de IA que se quieren prohibir en la UE ha sido uno de los grandes caballos de batalla en la tramitación legislativa» (PEGUERA POCH, M. *La propuesta de Reglamento de IA: Una intervención legislativa insoslayable en contexto de incertidumbre*, en PEGUERA POCH, M. *Perspectivas regulatorias de la inteligencia artificial en la Unión Europea*, *op. cit.*).

29 Artículo 5.1 RIA.

30 Considerando 29 RIA.

b) sistemas de IA que exploten las vulnerabilidades de personas o colectivos por su edad, discapacidad, situación social o económica. El uso de estos sistemas se prohíbe cuando tengan la finalidad o el efecto de alterar sustancialmente su comportamiento provocándole o pudiéndole provocar de manera razonable perjuicios a ella o a otra persona;

c) sistemas de IA de puntuación ciudadana que evalúen o clasifiquen a personas o a colectivos en función de su comportamiento social o de sus características personales. El uso de estos sistemas se prohíbe cuando pueda resultar en un trato perjudicial o desfavorable en contextos sociales distintos a aquel en el que se obtuvieron los datos o que sea injustificado o desproporcionado respecto a su comportamiento;

d) sistemas de IA de elaboración de perfiles o de evaluación de los rasgos y características de la personalidad que permitan evaluar o predecir el riesgo de que una persona cometa un delito excepto cuando los sistemas se utilicen como apoyo a la valoración humana;

e) sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes de internet o de circuitos cerrados de televisión;

f) sistemas de IA para inferir las emociones de una persona física en lugares de trabajo y centros educativos. El RIA exceptúa aquellos casos en los que el sistema sea utilizado por motivos médicos o de seguridad;

g) sistemas de categorización biométrica para deducir o inferir datos sensibles como la raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida u orientación sexual de las personas;

h) sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con el fin de garantizar el cumplimiento del Derecho.[31] Esta prohibición se exceptúa en los casos en los que el uso de estos sistemas de IA sea necesario para confirmar la identidad de las personas para buscar víctimas de determinados delitos (secuestro, trata de seres humanos o explotación sexual de seres humanos) o personas desaparecidas; prevenir amenazas específicas e inminentes

[31] En relación con estos sistemas, véase, entre otros, COTINO HUESO, L. *Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos*. Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2023.

para la vida, la seguridad física o atentados terroristas; o localizar o identificar personas sospechosas de haber cometido algún delito grave de entre los recogidos en el anexo II RIA castigados con penas superiores a cuatro años.[32] En estos casos, deberán cumplirse las garantías y condiciones previstas, haberse realizado una evaluación de impacto relativa a los derechos fundamentales, registrado el sistema en la base de datos de la UE y obtenido una autorización de una autoridad judicial o administrativa independiente.

B) Los sistemas de IA de alto riesgo

En segundo lugar, el RIA identifica otros sistemas de IA que define como de alto riesgo que son aquellos cuyo uso pueda tener un efecto perjudicial considerable en la salud, la seguridad y los derechos fundamentales de las personas.[33]

Acorde con el principio de proporcionalidad, la idea que subyace al RIA es que sean catalogados como de alto riesgo únicamente aquellos sistemas que tengan un efecto perjudicial considerable.[34]

En particular, la determinación de los sistemas de IA que deben considerarse como de alto riesgo se hace sobre la base de un doble criterio.[35]

Por un lado, el RIA considera como sistemas de IA de alto riesgo aquellos sistemas que cumplen con dos condiciones: (1) son componentes de seguridad de productos de acuerdo con los actos legislativos de armonización de la Unión identificados en el anexo I[36] o el propio sistema de IA es un producto de los contemplados en dichos actos legislativos y (2) el producto

---

[32] La lista de delitos incluidos en el anexo II se basa en la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros.

[33] En relación con estos riesgos resulta interesante observar cómo únicamente se vinculan a la salud, la seguridad y los derechos fundamentales si bien en el artículo 1 RIA se incluye, al referirse a los derechos fundamentales consagrados en la Carta, «la democracia, el Estado de Derecho y la protección del medio ambiente».

[34] Considerando 46.

[35] Artículo 6 RIA. Como advierte el propio RIA, «que un sistema de IA sea clasificado como un sistema de IA de alto riesgo en virtud del presente Reglamento no debe interpretarse como indicador de que su uso sea lícito con arreglo a otros actos del Derecho de la Unión o del Derecho nacional» (considerando 63).

[36] Por ejemplo, máquinas, juguetes, ascensores, equipo y sistemas de protección para uso en atmósferas potencialmente explosivas, equipos radioeléctricos, equipos a presión, equipos de embarcaciones de recreo, instalaciones de transporte por cable, aparatos que queman combustibles gaseosos, productos sanitarios, productos sanitarios para diagnóstico in vitro, automoción y aviación.

del que sea componente de seguridad el sistema de IA o el propio sistema de IA como producto deba someterse a una evaluación de la conformidad por un organismo de evaluación de la conformidad de terceros para su introducción en el mercado o puesta en servicio de acuerdo con los actos legislativos de armonización de la Unión identificados en el anexo I.[37]

Por otro lado, el RIA también considera como sistemas de IA de alto riesgo los sistemas que se incluyan en alguno de los ocho ámbitos y se encuentren dentro de las distintas prácticas identificadas en el anexo III.[38] Como rápidamente se podrá advertir, muchos de estos usos pueden tener lugar en el desarrollo de la actividad de las Administraciones públicas:

1) biometría (sistemas de identificación biométrica remota, sistemas de categorización biométrica y sistemas de reconocimiento de emociones);
2) gestión y funcionamiento de infraestructuras críticas (tráfico, agua, gas o electricidad);
3) educación y formación profesional (por ejemplo, la gestión del acceso o admisión a la educación; la evaluación de los resultados de aprendizaje; la evaluación del nivel de educación adecuado o el seguimiento y la detección de comportamientos prohibidos por estudiantes en pruebas);
4) empleo, gestión de trabajadores y acceso al autoempleo (sistemas destinados a la contratación o selección de personas; la toma de decisiones que afecten a las condiciones de las relaciones de trabajo o a la promoción o rescisión);
5) acceso de las personas a servicios esenciales públicos y privados (como servicios esenciales de asistencia sanitaria, la evaluación y clasificación de las llamadas de emergencia, el establecimiento de prioridades en el envío de servicios de situaciones de emergencia o el triaje de pacientes en servicios de asistencia sanitaria urgente);
6) garantía del cumplimiento del Derecho (evaluación del riesgo de que una persona sea víctima de delitos; polígrafos; evaluación de la fiabilidad de las pruebas; evaluación de rasgos y características de la personalidad o comportamientos delictivos; elaboración de perfiles durante la detección, investigación o enjuiciamiento de delitos);

[37] Artículo 6.1 RIA.
[38] Artículo 6.2 RIA.

7) migración, asilo y control fronterizo (como polígrafos, evaluación del riesgo para la seguridad, la salud o la migración regular; valoración de solicitudes de asilo, visado o permiso de residencia; detección, reconocimiento o identificación a personas), y
8) administración de justicia y procesos democráticos (ayuda a la autoridad judicial en la investigación e interpretación de los hechos o la ley; resolución alternativa de litigios; sistemas utilizados para influir en el resultado de una elección o referéndum o en el comportamiento electoral de las personas).

A pesar de su inclusión en la relación recogida en los párrafos anteriores, puede no considerarse de alto riesgo, excepto cuando elabore perfiles de las personas, aquel sistema de IA que no plantee un riesgo importante de causar un perjuicio a la salud, la seguridad o los derechos fundamentales, incluido el caso en que no influya sustancialmente en el resultado de la toma de decisiones. Se entiende que así será cuando el sistema esté destinado a realizar una tarea de procedimiento limitada, a mejorar el resultado de una actividad humana previamente realizada, a detectar patrones de toma de decisiones o desviaciones con respecto a patrones de toma de decisiones anteriores y no esté destinado a sustituir la valoración humana previamente realizada sin una revisión humana adecuada, ni a influir en ella, o a realizar una tarea preparatoria para una evaluación que sea pertinente.[39] En estos casos, el proveedor deberá documentar su evaluación antes de introducir el sistema de IA en el mercado o ponerlo en servicio.[40]

A fin de poder adaptarse a la evolución que vayan experimentando los sistemas de IA, la Comisión tiene atribuida una capacidad para modificar o suprimir las condiciones anteriores a través de la adopción de actos delegados siempre y cuando no se reduzca el nivel global de protección de la salud, la seguridad y los derechos fundamentales.[41] También para añadir o modificar los casos de uso de sistemas de IA de alto riesgo dentro de los ámbitos fijados de acuerdo con distintos criterios como la finalidad prevista, la medida en que se utilice o sea probable que se utilice el sistema, la naturaleza y cantidad de datos tratados y utilizados por el sistema, su grado

---

39 Artículo 6.3 RIA.

40 Artículo 6.4 RIA.

41 Apartados 5, 6 y 7 del artículo 6 RIA.
Al respecto se prevé que una vez al año la Comisión evaluará la necesidad de modificar la lista del anexo III y la lista de prácticas de IA prohibidas. También que cada cuatro años la Comisión evaluará la necesidad de ampliar los ámbitos enumerados en el anexo III o de añadir nuevos ámbitos (artículo 112 RIA).

de autonomía, la medida en que haya causado un perjuicio o problemas importantes y su intensidad o capacidad de afectar a varias personas, la existencia de un desequilibrio de poder, la facilidad para corregir o revertir el resultado, la probabilidad de que el sistema sea beneficioso y la magnitud del beneficio y la medida en que se prevean vías de recurso efectivas en relación con los riesgos o para prevenir o reducirlos.[42] Asimismo, la Comisión podrá suprimir casos de alto riesgo cuando ya no planteen riesgos para la salud, la seguridad o los derechos fundamentales y no se reduzca el nivel general de protección.[43]

Cuando un sistema de IA es clasificado como de alto riesgo debe cumplir determinados requisitos para evitar que puedan causar riesgos inaceptables para intereses públicos:[44]

1. Sistema de gestión de riesgos.[45] El proveedor debe establecer, implantar, documentar y mantener un sistema de gestión de riesgos entendido como un proceso iterativo continuo que sea planificado y ejecutado durante todo el ciclo de vida y que, entre otros, permita la determinación y el análisis de los riesgos conocidos y previsibles que pueda plantear el sistema de IA de alto riesgo cuando se utilice conforme a la finalidad prevista o cuando se le dé un uso indebido razonablemente previsible, pero también la estimación o evaluación de otros riesgos que puedan surgir, así como la adopción de medidas adecuadas para su gestión.
2. Gobernanza y calidad de los datos.[46] Como advierte el propio RIA, «los datos de alta calidad y el acceso a datos de alta calidad desempeñan un papel esencial a la hora de proporcionar una estructura y garantizar el funcionamiento de muchos sistemas de IA».[47] En particular,

---

42 Artículo 7.2 RIA.

43 Artículo 7.2 RIA.

44 Considerando 46 y artículo 8 RIA.

45 Artículo 9 RIA.

46 Artículo 10 RIA.

47 Considerando 67 RIA. En relación con esta cuestión no pueden desconocerse las iniciativas impulsadas en los últimos años por la Unión Europea para fomentar la calidad y la reutilización de los datos. La Estrategia Europea de Datos en febrero de 2020 [COM(2020) 66 final] persigue convertir a la Unión Europea en *un modelo de referencia de una sociedad empoderada por los datos para tomar mejores decisiones* a través de la creación de un espacio único europeo de datos que ha de ser «como un mercado interior de datos en el que estos puedan utilizarse independientemente de su ubicación física de almacenamiento en la Unión de conformidad con el Derecho aplicable, lo que, entre otras cosas, podría resultar fundamental para el rápido desarrollo de las tecnologías de inteligencia artificial». Véase al respecto CERRILLO I MARTÍNEZ, A. «Reutilización de la información del sector público e inteligencia artificial», en GAMERO CASADO, E. *Inteligencia artificial y sector público. Retos, límites y medios*. Valencia: Tirant lo Blanch, 2023.

el RIA dispone que se deben cumplir los criterios de calidad en los conjuntos de datos de entrenamiento, validación y prueba y adoptar las medidas necesarias para que sean pertinentes y representativos, estén completos, carezcan de errores y no contengan sesgos. Asimismo, prevé que deben adoptarse las prácticas adecuadas de gestión y gobernanza de datos para lograr que los conjuntos de datos para el entrenamiento, la validación y la prueba sean de alta calidad. Por último, el RIA reconoce que si los sistemas de IA han sido entrenados y probados con datos que reflejan el entorno geográfico, conductual, contextual o funcional específico en el que esté previsto su uso se presumirá que cumplen los requisitos previstos.[48]

3. Documentación técnica.[49] Con carácter previo a la introducción en el mercado o puesta en servicio de un sistema de IA, se redactará una documentación técnica en la que se demuestre el cumplimiento de los requisitos de manera clara y completa para que las autoridades competentes y los organismos notificados puedan evaluar su conformidad.
4. Registro automático de acontecimientos (archivo de registro).[50] Los sistemas de IA deben permitir el registro automático de acontecimientos a lo largo del ciclo de vida del sistema para garantizar la trazabilidad de su funcionamiento así como la vigilancia poscomercialización para la detección de situaciones que puedan dar lugar a que el sistema presente un riesgo o a una modificación sustancial.
5. Transparencia.[51] El sistema de IA de alto riesgo debe diseñarse con un nivel de transparencia suficiente para que los responsables del despliegue puedan interpretar y usar correctamente los resultados de salida. Asimismo, los sistemas de IA de alto riesgo deben acompañarse de unas instrucciones de uso con información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible sobre la identidad y los datos de contacto del proveedor; las características, capacidades y limitaciones del funcionamiento del sistema de IA (finalidad prevista, nivel de precisión, solidez y ciberseguridad, información que permita interpretar los resultados de salida); los cambios en el sistema de IA y su funcionamiento predeterminados por el provee-

---

48 Artículo 42.1 RIA.

49 Artículo 11 RIA. Véase al respecto lo que dispone el anexo IV en relación con la información que como mínimo debe contener la documentación técnica.

50 Artículo 12 RIA.

51 Artículo 13 RIA.

dor; las medidas de supervisión humana; los recursos informáticos y de hardware necesarios, la vida útil prevista del sistema de IA de alto riesgo y las medidas de mantenimiento y cuidado necesarias para garantizar el correcto funcionamiento del sistema; una descripción de los mecanismos incluidos en el sistema de IA de alto riesgo que permita a los responsables del despliegue recabar, almacenar e interpretar correctamente los archivos de registro.

6. Supervisión humana.[52] Los sistemas de IA de alto riesgo deben diseñarse para que puedan ser vigilados de manera efectiva por personas con el fin de prevenir o reducir al mínimo los riesgos que puedan surgir para la salud, la seguridad o los derechos fundamentales. La supervisión humana debe ser proporcional a los riesgos, el nivel de autonomía y el contexto en el que se utilice el sistema de IA y se concretará bien en medidas integradas inicialmente en el sistema, bien en medidas que puedan ser utilizadas por el responsable del despliegue, bien en ambos tipos de medidas. Para garantizar la supervisión humana, es necesario que el sistema de IA permita que el responsable del despliegue pueda entender adecuadamente las capacidades y limitaciones del sistema de IA y vigilar su funcionamiento; ser consciente de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida; interpretar correctamente los resultados de salida; decidir no usar el sistema o descartar, invalidar o revertir sus resultados de salida; intervenir en su funcionamiento o interrumpir el sistema pulsando un botón de parada.
7. Fiabilidad.[53] Los sistemas de IA de alto riesgo deben diseñarse para que gocen de un nivel adecuado de precisión, solidez y ciberseguridad que deben mantener durante todo su ciclo de vida. En esta dirección, las instrucciones de uso deben informar sobre los niveles de precisión y los parámetros para medirla. Asimismo, deberán cumplir las medidas técnicas y organizativas para que sean resistentes respecto a errores o fallos que puedan surgir. Por último, deben comprender medidas técnicas para garantizar la ciberseguridad de manera que sean resistentes a los intentos de terceros no autorizados de alterar su uso, resultados o funcionamiento. En relación con esta cuestión, el RIA prevé que si los sistemas de IA cuentan con un certificado o de-

[52] Artículo 14 RIA.
[53] Artículo 15 RIA.

claración de conformidad en virtud de un esquema de ciberseguridad se presumirá que cumplen con los requisitos de ciberseguridad.[54]

Como veremos posteriormente, corresponde a los proveedores del sistema de IA de alto riesgo velar por el cumplimiento de los requisitos anteriores.[55] Para ello, los proveedores seguirán el procedimiento de evaluación de la conformidad.[56] Los certificados expedidos por los organismos notificados serán válidos por un periodo que no excederá de cuatro (sistemas del anexo III) o cinco años (sistemas del anexo I) y se redactarán en la lengua que puedan entender fácilmente las autoridades del Estado miembro en que esté establecido el organismo.[57] Si el organismo notificado observa que el sistema ya no cumple con los requisitos suspenderá o retirará el certificado o le impondrá restricciones. En el caso de que los sistemas de IA de alto riesgo sean conformes con las normas armonizadas cuyas referencias se publiquen en el Diario Oficial de la Unión Europea se presumirá que son conformes con los requisitos anteriores.[58]

Por último, un sistema de IA puede ser introducido en el mercado o puesto en servicio sin contar con la evaluación de conformidad por un periodo de tiempo limitado, cuando sea autorizado por las autoridades de vigilancia del mercado si concurren motivos excepcionales de seguridad pública o con el fin de proteger la vida y salud de las personas, el medio ambiente o activos fundamentales de la industria y de las infraestructuras.[59]

C) Los modelos de IA de uso general

En tercer lugar, el RIA identifica los sistemas de IA de uso general que se basan en un modelo de IA de uso general.[60] Un modelo de IA de uso general es aquel modelo de IA que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas distintas.[61]

---

54 Artículo 42.2 RIA.
55 Artículo 16.a) RIA.
56 En relación con esta cuestión, véase lo dispuesto en el artículo 43 RIA.
57 Artículo 44 RIA.
58 Artículo 40 RIA.
59 Artículo 46 RIA.
60 Artículo 3.66) RIA.
61 Artículo 3.63) RIA. Las dificultades para definir los modelos de IA de uso general han sido puestos de manifiesto por distintos autores como GUTIERREZ, C. I.; AGUIRRE, A.; UUK, R.; BOINE, C. C.; FRANKLIN, M. «A proposal for a definition of general purpose artificial intelligence systems». *Digital Society*, núm. 2 (2023) o MOREIRA, N. A.; FREITAS, P. M.; NOVAIS, P. «The AI Act Meets

Los modelos de IA de uso general están entrenados con grandes volúmenes de datos a través de métodos diversos, como el aprendizaje autosupervisado, no supervisado o por refuerzo.[62] Precisamente, la especial configuración de los modelos de IA de uso general y la diversidad de tareas que pueden desarrollar determina que sean objeto de una atención especial en el RIA y que sus proveedores tengan atribuidas unas funciones y responsabilidades particulares a lo largo de la cadena de valor del sistema.

En esta dirección, el RIA dispone que los proveedores de modelos de IA de uso general deben elaborar la documentación técnica del modelo para la Oficina de IA y las autoridades nacionales competentes; información y documentación para los proveedores de sistemas de IA que quieran integrar el modelo de IA de uso general en sus sistemas de IA con el fin de que puedan entender bien las capacidades y limitaciones del modelo de IA de uso general y cumplir sus obligaciones, y un resumen suficientemente detallado del contenido utilizado para el entrenamiento del modelo de IA de uso general para el público. También deben establecer directrices para cumplir legislación europea en materia de derechos de autor y derechos afines.[63]

El RIA dispone que alguna de estas obligaciones de transparencia no debe cumplirse cuando los modelos de IA se divulguen con arreglo a una licencia libre y de código abierto, es decir, que puedan ser compartidos abiertamente y los usuarios puedan usarlos o modificarlos libremente.[64]

Para demostrar el cumplimiento de las obligaciones, los proveedores de modelos de IA de uso general pueden utilizar códigos de buenas prácticas.[65] Asimismo, si los modelos de IA de uso general cumplen las normas armonizadas europeas, el RIA prevé una presunción del cumplimiento de dichas obligaciones.[66]

Por último, cuando, entre otras condiciones, los modelos de IA de uso general tengan capacidades de gran impacto será considerado que presentan riesgos sistémicos (por ejemplo, accidentes graves, perturbaciones de sectores críticos, consecuencias graves para la salud y la seguridad públicas, efectos negativos reales o razonablemente previsibles sobre procesos de-

---

General Purpose AI: The Good, The Bad and The Uncertain», en MONIZ, N.; VALE, Z.; CASCALHO, J.; SILVA, C.; SEBASTIÃO, R. *EPIA Conference on Artificial Intelligence*. Cham: Springer, 2023.

62 Considerando 97.

63 Artículo 53 RIA.

64 Considerando 102.

65 En relación con el artículo 56 RIA.

66 Artículo 53.4 RIA.

mocráticos o la difusión de contenidos ilícitos, falsos o discriminatorios).[67] En estos casos, el proveedor debe notificarlo a la Comisión sin demora.[68] Asimismo, deberá cumplir unas obligaciones específicas como evaluar los modelos de acuerdo con los protocolos y herramientas normalizadas que se prevean para detectar y mitigar los riesgos sistémicos, evaluar y mitigar los posibles riesgos que puedan derivarse a escala europea, comunicar la información sobre incidentes graves y las posibles medidas correctoras y velar por que se establezca un nivel adecuado de ciberseguridad.[69] Los proveedores también podrán recurrir a códigos de buenas prácticas para demostrar el cumplimiento de estas obligaciones.

D) Sistemas de IA que pueden generar riesgos específicos

En cuarto lugar, el RIA identifica otros sistemas de IA que pueden generar otros riesgos específicos como la suplantación, el engaño o la manipulación de las personas. Como advierte PEGUERA, no nos encontramos en sentido estricto ante una categoría específica de riesgo, ya que estos sistemas pueden ser o no ser de alto riesgo.[70] En relación con estos sistemas de IA, el RIA prevé determinadas obligaciones de transparencia con el fin de que las personas usuarias o destinatarias de los resultados de estos sistemas de IA puedan ser conscientes de que están tratando con sistemas de IA o de que un determinado contenido ha sido generado de manera artificial.[71]

En particular, el RIA incluye en esta categoría los sistemas de IA destinados a interactuar directamente con personas físicas; los sistemas de IA, incluidos los de uso general, que generen contenido sintético de audio, imagen, vídeo o texto; los sistemas de IA de reconocimiento de emociones; los sistemas de IA de categorización biométrica, y los sistemas de IA que generen o manipulen imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación.[72]

---

67 Artículo 51 RIA y considerando 110.

68 Artículo 52 RIA.

69 Artículo 53.4 RIA en relación con el artículo 56 RIA.

70 PEGUERA POCH, M. «La propuesta de Reglamento de IA: Una intervención legislativa insoslayable en contexto de incertidumbre», en PEGUERA POCH, M. *Perspectivas regulatorias de la inteligencia artificial en la Unión Europea, op. cit.*

71 Véase al respecto CERRILLO I MARTÍNEZ, A. «Artículo 50. Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA», en COTINO HUESO, L.; SIMÓN CASTELLANO, P. *El Reglamento de Inteligencia Artificial*. Cizur Menor: Aranzadi, 2024.

72 El RIA prevé que cada cuatro años la Comisión evaluará la necesidad de modificar la lista de sistemas de IA que requieren medidas de transparencia adicionales (artículo 112 RIA).

E) Otros sistemas de IA

Por último, el RIA reconoce otros sistemas de IA que no generarán riesgos significativos. De hecho, tal y como se ha puesto de manifiesto, lo más habitual será que los sistemas de IA que utilicen las Administraciones públicas no se encuentren entre los sistemas expuestos anteriormente.

El hecho de que estos sistemas no generen riesgos no quiere decir que no deban diseñarse, desarrollarse o utilizarse de una manera ética y fiable y que puedan cumplir con lo previsto en el RIA.

En esta dirección, el RIA invita a los proveedores y responsables del despliegue de sistemas de IA que no son de alto riesgo a crear códigos de conducta que fomenten la aplicación voluntaria de la totalidad o parte de los requisitos aplicables a los sistemas de IA de alto riesgo adaptados al menor riesgo planteado.[73] Entre otros aspectos, los códigos de conducta deben integrar los elementos aplicables establecidos en las Directrices éticas de la Unión para una IA fiable; la evaluación y reducción al mínimo de las repercusiones de los sistemas de IA en la sostenibilidad medioambiental; la promoción de la alfabetización en materia de IA; la facilitación de un diseño inclusivo y diverso de los sistemas de IA, y la evaluación y prevención de los perjuicios de los sistemas de IA para las personas vulnerables o los colectivos de personas vulnerables, la accesibilidad para las personas con discapacidad y la igualdad de género.

IV. LAS ADMINISTRACIONES PÚBLICAS COMO PROVEEDORAS Y USUARIAS DE SISTEMAS DE INTELIGENCIA ARTIFICIAL

El RIA no regula específicamente el uso de los sistemas de IA en las Administraciones públicas.[74]

No obstante, sí define las obligaciones que deben cumplir los distintos operadores relacionados con el desarrollo y uso de los sistemas de IA (proveedores y responsables del despliegue, importadores, distribuidores, representantes autorizados).[75] En la medida en que las Administraciones

---

[73] Asimismo, el artículo 95 RIA prevé que la Oficina de IA y los Estados miembros fomenten y faciliten la elaboración de códigos de conducta.

[74] A lo largo de estas páginas nos referimos de manera genérica a Administraciones públicas en el bien entendido que el RIA se refiere a «autoridades públicas, instituciones, órganos u organismos de la Unión».

[75] Si bien no es objeto de atención en este trabajo, se debe tener presente que el RIA también se aplica a proveedores y responsables del despliegue establecidos en terceros países cuando los resultados de salida de los sistemas de IA se utilicen en la Unión (artículo 2.1.c).

públicas diseñen o utilicen sistemas de IA, es evidente que se verán afectadas por lo dispuesto en la norma europea.

El nivel de aplicación del RIA a las Administraciones públicas variará en función de que estas sean las que diseñen y desarrollen los sistemas de IA o simplemente, como será más habitual, utilicen sistemas de IA desarrollados por terceros.

1. Las obligaciones de las Administraciones públicas como proveedoras de sistemas de IA

Las Administraciones públicas serán consideradas como proveedoras de sistemas de IA cuando desarrollen un sistema de IA, o se desarrolle un sistema de IA para ellas, y lo introduzcan en el mercado[76] o lo pongan en servicio[77] previo pago o gratuitamente.

A) Las obligaciones en relación con los sistemas del alto riesgo

Cuando la Administración pública actúe como proveedora de sistemas de IA, con independencia de si es o no quien ha diseñado o desarrollado el sistema, debe cumplir con distintas obligaciones.[78]

Así, el proveedor debe asegurarse de que el sistema cumple plenamente con todos los requisitos aplicables para lo que desarrollará una evaluación de conformidad que se realizará a partir de un control interno.[79] Además, debe redactar una declaración UE de conformidad en la que constará que el sistema cumple con los requisitos previstos para los sistema de IA de alto riesgo.[80] Asimismo, el proveedor colocará el marcado CE con el que se indica que el sistema de IA es conforme con los requisitos establecidos.[81]

---

76 De acuerdo con el RIA, la introducción en el mercado se refiere a la primera comercialización en el mercado de la Unión de un sistema de IA (artículo 3 RIA).

77 Según el RIA, la puesta en servicio consiste en el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista, es decir, «el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica» (artículo 3 RIA).

78 Artículo 16 RIA.

79 Artículos 8.2 y 43 RIA.

80 Artículo 47 RIA. El anexo V identifica la información que debe contener la declaración UE de conformidad.

81 El marcado CE estará sujeto a los principios establecidos en el Reglamento (CE) 765/2008 y se utilizará el marcado digital colocándose de manera visible, legible e indeleble. Si no es posible, se colocará en el embalaje (artículo 48 RIA).

El proveedor también debe registrar los sistemas de IA en la base de datos de la UE.[82]

Asimismo, el proveedor de sistemas de IA de alto riesgo deberá establecer el sistema de gestión de la calidad para garantizar el cumplimiento del RIA que, de manera proporcional al tamaño de la organización del proveedor, debe integrar: una estrategia para el cumplimiento de la normativa; las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño y el desarrollo del sistema de IA de alto riesgo; los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que se ejecutarán; las especificaciones técnicas que se aplicarán; los sistemas y procedimientos de gestión de datos; el sistema de gestión de riesgos; el establecimiento, aplicación y mantenimiento de un sistema de vigilancia poscomercialización; los procedimientos asociados a la notificación de un incidente grave; la gestión de la comunicación con las autoridades nacionales competentes, los organismos notificados, otros operadores, los clientes u otras partes interesadas; los sistemas y procedimientos para llevar un registro de toda la documentación e información pertinente; la gestión de los recursos; un marco de rendición de cuentas.[83]

Además, el proveedor debe establecer un sistema de vigilancia poscomercialización que sea proporcional a la naturaleza de los sistemas de IA y a los riesgos que puedan entrañar.[84] Este sistema debe permitir recopilar, documentar y analizar de manera activa y sistemática los datos que faciliten los responsables del despliegue durante la vida útil del sistema de IA. Este sistema se basará en un plan de vigilancia.

---

82 A estos efectos, se prevé que la base de datos de la UE será creada y mantenida por la Comisión en colaboración con los Estados miembros (artículo 71 RIA) en la que el proveedor deberá registrarse, así como también el sistema de IA antes de introducirlo en el mercado o ponerlo en servicio. No obstante, en el caso de los sistemas de IA relativos a infraestructuras críticas (punto 2 anexo III) se registrarán a nivel nacional (artículo 49, apartados 1 y 5, RIA). La obligación de registro también la deberán cumplir los responsables de despliegue de sistemas de IA de alto riesgo recogidos en el anexo III que sean Administraciones públicas (artículo 49 apartado 3 RIA). El anexo VII identifica la información que debe presentarse para la inscripción en el registro de sistemas de IA de alto riesgo.

83 Artículo 17 RIA y anexo VI. En el caso de que los proveedores de sistemas de IA de alto riesgo estén sujetos a obligaciones relativas a los sistemas de gestión de la calidad o una función equivalente con arreglo al derecho de la Unión podrán incluir los aspectos relativos a los sistemas de IA como parte de los sistemas de gestión de la calidad.

84 Artículo 72 RIA.

En el caso de que se produzca un incidente grave, el proveedor del sistema de IA de alto riesgo debe notificarlo a las autoridades de vigilancia del mercado de manera inmediata, a más tardar quince días después de que se tenga conocimiento del incidente.[85] Cuando el sistema no sea conforme al RIA, los proveedores deberán adoptar las medidas correctoras necesarias para que sea conforme, se retire del mercado, se desactive o se recupere; y demostrar la conformidad a los requisitos a solicitud de la autoridad nacional competente.

Junto a estas obligaciones, el proveedor también debe informar en el sistema o en su embalaje o documentación que lo acompañe de su nombre y contacto; conservar la documentación durante diez años (por ejemplo, la documentación técnica, la relativa al sistema de gestión de calidad, a los cambios aprobados o a la declaración de conformidad); o conservar los archivos de registro generados cuando estén bajo su poder durante un periodo adecuado de al menos seis meses, y velar por el cumplimiento de los requisitos de accesibilidad.

B) Las obligaciones en relación con sistemas que generen riesgos específicos

En relación con los sistemas de IA que puedan generar riesgos específicos de suplantación o engaño, el proveedor deberá cumplir determinadas obligaciones de transparencia que deben facilitar a las personas destinatarias información clara, distinguible y accesible.[86] Estas obligaciones deben cumplirse con independencia de si el sistema sea considerado como de alto riesgo o no y si, en consecuencia, se deben cumplir con otros requisitos u obligaciones.

En el caso de los sistemas de IA destinados a interactuar directamente con personas, el proveedor debe garantizar que estas personas estén informadas de que están interactuando con un sistema de IA. No obstante, si esta situación puede ser evidente para una persona *razonablemente informada, atenta y perspicaz* no será necesario informar. Tampoco cuando estos sistemas sean utilizados para detectar, prevenir, investigar o enjuiciar delitos si así está autorizado por una ley.

En el supuesto de los sistemas de IA, incluidos los de uso general, que generen contenido sintético de audio, imagen, vídeo o texto, el proveedor

---

85 Artículo 73 RIA.
86 Artículo 50 RIA.

debe velar por que los resultados de salida estén marcados en un formato legible por máquina para permitir detectar que han sido creados o manipulados de manera artificial. Esta obligación tampoco se aplicará a los sistemas que sean utilizados para detectar, prevenir, investigar o enjuiciar delitos si así está autorizado por una ley.

2. Las obligaciones de las Administraciones públicas como responsables del despliegue

En segundo lugar, las Administraciones públicas en la medida en que utilicen un sistema de IA bajo su propia autoridad serán consideradas responsables de despliegue.[87]

A) Las obligaciones en relación con los sistemas del alto riesgo

El RIA reconoce un papel fundamental a los responsables del despliegue.

Desde un punto de vista general, el responsable del despliegue debe adoptar medidas técnicas y organizativas adecuadas para garantizar que utiliza el sistema de IA de alto riesgo conforme a las instrucciones de uso.[88] También debe encargar a personas que tengan la competencia, formación y autoridad necesarias la supervisión humana del sistema de IA. Igualmente, en la medida en que ejerza control sobre los datos, el responsable del despliegue debe asegurarse de que son pertinentes y suficientemente representativos para la finalidad prevista. Asimismo, el responsable del despliegue debe vigilar el funcionamiento del sistema de IA de acuerdo con las instrucciones de uso. También conservará los archivos de registro que los sistemas generen, por un plazo de al menos seis meses. Por último, el responsable del despliegue debe cooperar con las autoridades competentes.

Asimismo, en el caso de los sistemas de IA de alto riesgo recogidos en el anexo III, el responsable del despliegue es el encargado de informar a las personas físicas a las que puedan afectar los resultados del sistema de IA de alto riesgo de que están expuestas al uso de estos sistemas de IA en la toma de decisiones o en la ayuda en la toma de decisiones relacionadas

---

87 Artículo 3.4) RIA. Pero cuando un responsable del despliegue ponga su nombre en el sistema, o lo modifique sustancialmente, será considerado como proveedor y estará sujeto a sus mismas obligaciones (artículo 25 RIA).

88 Artículo 26 RIA.

con personas físicas lo cual tendrá una dimensión especial en el caso de las Administraciones públicas.[89]

Asimismo, el responsable del despliegue debe facilitar una explicación clara y significativa acerca del papel que el sistema de IA ha tenido en el proceso de toma de decisiones y los principales elementos de la decisión adoptada cuando la decisión se base principalmente en los resultados de salida de determinados sistemas de IA de alto riesgo incluido en el anexo III y produzca efectos jurídicos o afecte significativamente de modo similar a dichas personas, de manera que consideren que tiene un efecto perjudicial en su salud, su seguridad o sus derechos fundamentales.[90]

Por último, cuando el responsable del despliegue de un sistema de IA de alto riesgo de los recogidos en el anexo III sea una Administración pública se establecen obligaciones específicas.

En primer lugar, la Administración pública —o la entidad privada que preste servicios públicos— deberá realizar una evaluación de impacto en los derechos fundamentales.[91] Esta evaluación consistirá en una descripción de los usos del sistema de IA y sus finalidades; una descripción del tiempo y la frecuencia del uso del sistema de IA; las categorías de personas y colectivos afectados; los riesgos de perjuicio específicos que puedan afectarles; una descripción de la aplicación de medidas de supervisión humana; las medidas a adoptar si se materializan los riesgos. Realizada la evaluación, el responsable del despliegue notificará los resultados a la autoridad de vigilancia del mercado.

---

89 Artículo 26.11 RIA.

90 Artículo 86.1 RIA.

91 Cabe advertir que el apartado 1 artículo 27 limita la obligación de realizar la evaluación de impacto relativa a los derechos fundamentales a los sistemas de IA de alto riesgo previstos en el anexo III excepto los utilizados en las infraestructuras críticas. Asimismo, se emplaza a las entidades públicas a contar con la participación de representantes de colectivos de personas que probablemente se vean afectados por el sistema de IA, expertos independientes u organizaciones de la sociedad civil (considerando 96). En última instancia, se debe observar que en determinados supuestos otros sujetos, además de las Administraciones públicas, deben llevar a cabo esta evaluación de impacto (por ejemplo, en relación con sistemas de IA destinados a ser utilizados para evaluar la solvencia de personas físicas o establecer su calificación crediticia o para la evaluación de riesgos y la fijación de precios de los seguros de vida y de salud).
En relación con la evaluación de impacto en los derechos fundamentales de los sistemas de IA resulta de interés MANTELERO, A. *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*. The Hague: Asser Press, 2022.

En segundo lugar, la Administración pública deberá registrarse y registrar el sistema de IA de alto riesgo en la base de datos de la UE antes de su puesta en servicio o uso.[92]

B) Las obligaciones en relación con sistemas que generen riesgos específicos

En el caso de los sistemas de IA de reconocimiento de emociones y en el de los de categorización biométrica, el responsable del despliegue debe informar a las personas expuestas a ellos y además deben tratar sus datos personales de acuerdo con lo dispuesto en el Reglamento General de Protección de Datos y el Reglamento (UE) 2018/1725 y la Directiva (UE) 2016/680. Esta obligación no se aplicará en el caso de sistemas que sean utilizados para detectar, prevenir, investigar o enjuiciar delitos si así está autorizado por una ley.

Por último, en el supuesto de sistemas de IA que generen o manipulen imágenes o contenidos de audio o vídeo que constituyan una ultrasuplantación, el RIA prevé que el responsable del sistema debe hacer público que los contenidos han sido creados o manipulados artificialmente. Además de la excepción prevista en los casos anteriores respecto a los sistemas que sean utilizados para detectar, prevenir, investigar o enjuiciar delitos si así está autorizado por una ley, en este caso la obligación de transparencia se limitará en los supuestos en que el contenido forme parte de una obra creativa, satírica, artística o de ficción. También cuando el contenido manipulado se publique con el fin de informar al público sobre asuntos de interés público y haya sido sometido a un proceso de revisión humana o de control editorial.

V. LAS ADMINISTRACIONES PÚBLICAS COMO GARANTES DEL CUMPLIMIENTO DEL RIA

El RIA identifica distintas funciones para garantizar su cumplimiento atribuyendo su ejecución en algunos casos a las instituciones comunitarias y en otras a los Estados miembros. De este modo, algunas Administraciones públicas también acabarán teniendo reconocido un papel fundamental en

[92] Artículo 49.3 RIA. El anexo VII identifica la información que debe presentarse para la inscripción en el registro de sistemas de IA de alto riesgo.

relación con el cumplimiento del RIA que se concretará en función de las competencias que tengan atribuidas.[93]

Por un lado, el RIA prevé el establecimiento de una gobernanza de la IA a nivel europeo que permita tanto coordinar y apoyar su aplicación a escala nacional, como desarrollar capacidades a escala de la Unión e integrar a las partes interesadas en el ámbito de la IA.[94] La gobernanza de la IA está conformada por distintos órganos como la Oficina de IA a través de la que la Comisión desarrollará sus conocimientos y capacidades en materia de IA,[95] el Comité Europeo de Inteligencia Artificial compuesto por un representante de cada Estado miembro y que prestará tanto a los Estados como a la Comisión asesoramiento y asistencia para facilitar la aplicación del RIA,[96] el foro consultivo formado por una selección de actores de la industria, empresas emergentes, sociedad civil y académicos para proporcionar conocimientos técnicos y asesorar al Comité y la Comisión,[97] y el grupo de expertos científicos independientes para apoyar las actividades de garantía del cumplimiento del RIA.[98] Por último, también se prevé la designación de estructuras de apoyo a los ensayos de IA de la Unión.[99]

Junto a esta gobernanza a nivel europeo, el RIA también regula diversos aspectos relativos a la gobernanza estatal de la IA.

En esta dirección, el RIA prevé que cada Estado miembro debe nombrar las autoridades nacionales competentes y, en particular, una autoridad notificante y una autoridad de vigilancia del mercado.[100] Estas autoridades deben actuar de manera independiente, imparcial y sin sesgos y deben disponer de los recursos técnicos, financieros y humanos adecuados para poder desarrollar sus funciones de manera efectiva y de los poderes de ejecución previstos en la legislación europea.

---

93 En relación con la incidencia del RIA en la distribución de competencias entre el Estado y las Comunidades Autónomas, véase CERRILLO I MARTÍNEZ, A.; VELASCO RICO, C. I. «El Reglamento de IA de la UE y competencias autonómicas», en GARCÍA ROCA, J.; CARMONA CONTRERAS, A.; MOYA MALAPEIRA, D. *Informe Comunidades Autónomas 2023*. Barcelona: Observatorio de Derecho Público, 2024.

94 Considerando 148. La Comisión elaborará directrices sobre la aplicación práctica del RIA (artículo 96 RIA). Asimismo, se le otorgan poderes para adoptar actos delegados (artículo 97 RIA).

95 Artículo 64 RIA.

96 Artículos 65 y 66 RIA.

97 Artículo 67 RIA.

98 Artículo 68 RIA.

99 Artículo 84 RIA.

100 Artículo 3.48) RIA en relación con el artículo 70 RIA. En relación con las autoridades de vigilancia del mercado, véase lo dispuesto, entre otros, en el Reglamento (UE) 2019/1020 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativo a la vigilancia del mercado y la conformidad de los productos.

Por un lado, cada Estado miembro debe nombrar una autoridad notificante que será la responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión.[101] Estas actividades de evaluación y supervisión pueden ser realizadas por un organismo nacional de acreditación.

Por otro lado, cada Estado miembro debe designar como mínimo una autoridad de vigilancia del mercado encargada de supervisar la aplicación y ejecución del RIA de acuerdo con lo previsto en el Reglamento (UE) 2019/1020.[102] Entre otras funciones, las autoridades de vigilancia del mercado deben evaluar el sistema de IA que pueda presentar un riesgo que afecte a la salud, la seguridad o los derechos fundamentales y cuando se detecte deberá informar a las autoridades encargadas de proteger los derechos fundamentales. Si constata que el sistema de IA no cumple con los requisitos y obligaciones exigirá al operador que adopte las medidas correctoras oportunas e informará al organismo notificado correspondiente y, si el incumplimiento va más allá del territorio estatal, informará a la Comisión y al resto de Estados miembros.[103] En el caso de que el operador no adopte las medidas correctoras, la autoridad de vigilancia del mercado adoptará las medidas provisionales adecuadas para prohibir o restringir la comercialización del sistema de IA o su puesta en servicio y lo notificará a la Comisión y a los demás Estados miembros. Cuando la autoridad de vigilancia del mercado concluya que el sistema de IA de alto riesgo presenta un riesgo para la salud, la seguridad de las personas, los derechos fundamentales u otros aspectos de protección del interés público solicitará al proveedor que adopte las medidas adecuadas para que el sistema de IA no presente el riesgo de lo que deberán informar los Estados miembros inmediatamente a la Comisión y al resto de Estados miembros.[104]

Las autoridades de vigilancia del mercado también son las competentes para tramitar el procedimiento relativo a los sistemas de IA clasificados por el proveedor como no de alto riesgo. En particular, se dispone que cuando tenga motivos suficientes de que dicho sistema sí que es de alto riesgo debe realizar una evaluación del sistema de IA y si constata que efectiva-

---

101 Artículo 3.19) RIA en relación con el artículo 28 RIA. No se analiza el procedimiento de notificación (artículos 29 y 30), ni los requisitos y obligaciones operativas y otros aspectos relativos a los organismos notificados previstos en el RIA (artículos 31 a 39).

102 Artículos 3.26) y 74 RIA.

103 Artículo 79 RIA.

104 Artículo 82 RIA.

mente es de alto riesgo solicitará al proveedor para que adopte las medidas necesarias para que el sistema cumpla con los requisitos y obligaciones previstos.[105]

Por último, las autoridades de vigilancia del mercado son las competentes para exigir a los proveedores que subsanen los incumplimientos del RIA observados en relación como las obligaciones relacionadas con la colocación del marcado CE, la elaboración de la declaración UE de conformidad, el registro en la base de datos de la UE o la disponibilidad de documentación técnica.[106] En el caso que el incumplimiento persista, estas autoridades podrán adoptar las medidas necesarias para restringir o prohibir la comercialización del sistema de IA.

Más allá de las funciones atribuidas a las autoridades notificantes y de vigilancia del mercado, el RIA reconoce otras funciones que deberán desarrollar los Estados miembros a través de sus Administraciones públicas u organismos públicos pertinentes que supervisan la aplicación del Derecho de la Unión que protege los derechos fundamentales (por ejemplo, organismos de igualdad o autoridades de protección de datos).[107] Estas autoridades deben ser designadas e incluidas en una lista pública que se notificará a la Comisión y demás Estados miembros.

Entre las funciones previstas en el RIA que pueden ser realizadas por las Administraciones públicas cabe traer a colación las siguientes:

> En primer lugar, la alfabetización en materia de IA. A lo largo del RIA destaca la importancia que se da a las capacidades, los conocimientos y la comprensión del funcionamiento del RIA por parte de los distintos operadores en función de sus respectivos derechos y obligaciones.[108]
>
> En segundo lugar, el apoyo a la innovación.[109] En particular, el RIA prevé que los Estados miembros deben impulsar el establecimiento de espacios controlados de pruebas para la IA con el fin de facilitar la innovación, el desarrollo, la prueba y la validación

---

105 Artículo 80 RIA.

106 Artículo 83 RIA.

107 Considerando 157. A estas autoridades el RIA les atribuye «la facultad de solicitar cualquier documentación creada o conservada con arreglo al presente Reglamento y de acceder a ella, en un lenguaje y formato accesibles, cuando el acceso a dicha documentación sea necesario para el cumplimiento efectivo de sus mandatos, dentro de los límites de su jurisdicción. La autoridad u organismo público pertinente informará sobre cualquier solicitud de este tipo a la autoridad de vigilancia del mercado del Estado miembro que corresponda» (artículo 77.1 RIA).

108 Artículos 3.56) y 4 RIA. Más allá de las Administraciones públicas, de acuerdo con el último de los preceptos citados, todos los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar la alfabetización en materia de IA de su personal.

109 Considerando 15 RIA. A pesar de ello, no debe olvidarse que quedan fuera del ámbito de aplicación del RIA los sistemas desarrollados específicamente con fines de investigación y desarrollo científicos.

de los sistemas de IA.[110] Estos espacios tienen por objetivo mejorar la seguridad jurídica; apoyar el intercambio de mejores prácticas mediante la cooperación con las autoridades que participan en el espacio controlado de pruebas para la IA; fomentar la innovación y la competitividad; contribuir a un aprendizaje normativo basado en datos contrastados, y facilitar y acelerar el acceso al mercado de los sistemas de IA. Además, también se prevé la posibilidad de que los proveedores potenciales de sistemas de IA de alto riesgo puedan realizar pruebas en condiciones reales fuera de espacios controlados de pruebas cuando se cumplan determinadas condiciones como haber elaborado un plan de la prueba que se haya presentado a la autoridad de vigilancia del mercado competente.[111]

En tercer lugar, la concienciación y comunicación de información dirigidas a las pymes, incluidas las empresas emergentes, que sean proveedores o responsables del despliegue de sistemas de IA, ofreciéndoles, entre otros, acceso prioritario a los espacios controlados de pruebas para la IA o canales de comunicación específicos con las pymes para apoyarlas durante toda su trayectoria de desarrollo en relación con la aplicación del RIA[112].

Además, las Administraciones públicas tienen atribuida la potestad sancionadora frente a los incumplimientos del RIA. En esta dirección, el RIA reconoce esta potestad, que estará sujeta a las garantías procesales adecuadas, y fija unos límites máximos para la imposición de las multas administrativas dejando a cada Estado miembro el establecimiento del régimen sancionador cuya aprobación deben comunicar a la Comisión.[113]

En particular, el RIA prevé los siguientes límites para las sanciones:[114]

– la realización de las prácticas prohibidas estará sujeta a multas administrativas de hasta 35 millones de euros o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total, si esta cuantía fuese superior;
– el incumplimiento de cualquiera de las obligaciones de los proveedores, representantes autorizados, importadores, distribuidores y responsables del despliegue, así como los requisitos y obligaciones de los organismos notificados y las obligaciones de transparencia de los proveedores y responsables del despliegue con arreglo al artículo 50,

110 Artículo 57 RIA.

111 Artículo 60 RIA. Al respecto, resulta de interés traer a colación el 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.

112 Considerando 143.

113 Artículo 99. El RIA también prevé que los Estados miembros deben informar cada año a la Comisión de las multas administrativas que hayan impuesto.

114 Además, el RIA prevé que la Comisión podrá imponer multas a los proveedores de modelos de IA de uso general (artículo 101 RIA). En este caso, no podrán superar el 3 % de su volumen de negocios mundial total anual o de 15 millones de euros, si esta cifra es superior.

estará sujeto a multas administrativas de hasta 15 millones de euros o, si el infractor es una empresa, de hasta el 3 % de su volumen de negocios mundial total, si esta cuantía fuese superior;

– la presentación de información inexacta, incompleta o engañosa a organismos notificados o a las autoridades nacionales competentes en respuesta a una solicitud estará sujeta a multas administrativas de hasta 7,5 millones de euros o, si el infractor es una empresa, de hasta el 1 % del volumen de negocios mundial total, si esta cuantía fuese superior.

El RIA establece que, en el caso de las pymes, incluidas las empresas emergentes, las multas podrán ser por el porcentaje o el importe, según cuál de ellos sea menor.

Para imponer la multa y su cuantía, las Administraciones públicas deben tener en cuenta las circunstancias pertinentes de la situación de que se trate así como la naturaleza, la gravedad y la duración de la infracción y de sus consecuencias; si otras autoridades de vigilancia del mercado han impuesto ya multas administrativas al mismo operador por la misma infracción o de otros actos legislativos nacionales o de la Unión; el tamaño, el volumen de negocios anual y la cuota de mercado del operador que comete la infracción; cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso; el grado de cooperación con el fin de subsanar la infracción y mitigar sus posibles efectos adversos; el grado de responsabilidad del operador; la forma en que las autoridades nacionales competentes tuvieron conocimiento de la infracción; la intencionalidad o negligencia en la infracción; las acciones emprendidas por el operador para mitigar los perjuicios sufridos por las personas afectadas.

Por último, el RIA prevé que las Administraciones públicas pueden desarrollar funciones de control. En particular, se prevé que deben habilitar vías de recurso efectivas para las personas físicas y jurídicas cuyos derechos y libertades se vean perjudicados por el uso de sistemas de IA. En particular, deberá articularse la posibilidad de presentar una reclamación ante la autoridad de vigilancia del mercado por parte de cualquier persona física o jurídica que considera que se ha incumplido el RIA.[115] En relación con estas infracciones se aplicarán las garantías y, en particular, las medi-

[115] Artículo 85 RIA. Al respecto, debe destacarse que el RIA prevé la aplicación de lo previsto en la Directiva (UE) 2019/1937 respecto a la denuncia de infracciones y a la protección de las personas que denuncien tales infracciones (artículo 87 RIA).

das de protección a las personas denunciantes que prevé la Directiva (UE) 2019/1937.[116]

VI. REFLEXIONES FINALES

El RIA tendrá un impacto significativo en el desarrollo y uso de la IA en las próximas décadas y ha de contribuir a que esta tecnología disruptiva esté al servicio de las personas y su bienestar, proteja la salud, la seguridad y los derechos fundamentales, la democracia, el Estado de Derecho y el medio ambiente y apoye la innovación.

Como hemos tenido oportunidad de constatar a lo largo de estas páginas, las Administraciones públicas están llamadas a tener un papel relevante en la aplicación del RIA. No solo como proveedoras y responsables del despliegue de sistemas de IA. También como responsables de garantizar su cumplimiento por la galaxia de actores que de manera directa o indirecta intervendrán en el desarrollo y en la utilización de la IA a medida que vaya avanzando la transformación digital.

De este modo, en los próximos años, las Administraciones públicas no solo han de ser protagonistas de su proceso de transformación digital sino también pueden contribuir al desarrollo y extensión de la IA entre las empresas y la sociedad. En esta dirección ya se han ido produciendo diversas iniciativas como, por ejemplo, las que se recogen en la Estrategia de Inteligencia Artificial 2024 de reciente aprobación.[117]

No obstante, a pesar del protagonismo de las Administraciones públicas en la aplicación del RIA y el impacto que la norma europea puede tener en su funcionamiento o en la toma de decisiones públicas y la prestación de servicios públicos, no podemos desconocer que el RIA no es una norma pensada para las Administraciones públicas. Por ello, será necesario que las Administraciones públicas dispongan de unas normas ajustadas a los principios que guían su funcionamiento y que garanticen de manera adecuada los derechos de las personas cuando se relacionan con ellas. Por ello, será necesario incorporar en la legislación de régimen jurídico y de procedimiento administrativo las normas en que se concreten los requisitos, las obliga-

---

116 En relación con esta cuestión, téngase en cuenta lo previsto en la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

117 Otros países han avanzado en la misma dirección tal y como se desprende de VAN NOORDT, C.; MEDAGLIA, R.; TANGI, L. «Policy initiatives for Artificial Intelligence-emonabled government: An analysis of national strategies in Europe». *Public Policy and Administration*, núm. 0 (2023).

ciones y los procedimientos de las Administraciones públicas en tanto que proveedoras y responsables del despliegue de sistemas de IA.

Si bien el RIA prevé un amplio margen de seis años a partir de su entrada en vigor para que las Administraciones públicas puedan adoptar las medidas necesarias para cumplir los requisitos y obligaciones previstos en él, ello no es obstáculo para que si las Administraciones públicas quieren efectivamente ejercer el papel que les corresponde en el proceso de transformación digital vayan adoptando las normas y medidas necesarias.[118]

[118] Artículo 111.2 RIA.