apdcat
Autoritat Catalana de Protecció de Dades

Las autoridades de protección de datos y el Reglamento de inteligencia artificial

Nuevos roles y responsabilidades

Autoría: Daniel Duro Millan y Tatiana Bianca Vulpe beneficiarios de las dos becas de formación en materia de protección de datos personales para el año 2024, convocadas mediante Resolución de 10 de mayo de 2024 (DOGC n.º 9165, de 17/5/2024).

Coordinación APDCAT: Joana Marí Cardona, delegada de protección de datos y responsable de Proyectos Estratégicos, y Guillem López Sanz, responsable de Relaciones Institucionales y Organización.

Generalitat de Catalunya

apdcat
Autoritat Catalana de Protecció de Dades

Índice

Abreviaturas

AEPD: Agencia Española de Protección de Datos

APD: autoridad de control de protección de datos

APDCAT: Autoridad Catalana de Protección de Datos

APDF: autoridad de protección de derechos fundamentales

AVM: autoridad de vigilancia del mercado

CEPD: Comité Europeo de Protección de Datos

DD. FF.: derechos fundamentales

DOUE: Diario Oficial de la Unión Europea

EM: Estados miembros

FRA: Agencia Europea de Derechos Fundamentales

IA: inteligencia artificial

NIS2: Directiva (UE) 2022/2555, relativa a las destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión

NVS: notificación de violación de seguridad

RD: Real Decreto

RGPD: Reglamento General de Protección de Datos

RIA: Reglamento de Inteligencia Artificial

RMD: Reglamento de Mercados Digitales

RSD: Reglamento de Servicios Digitales

RT: responsable del tratamiento

RVM: Reglamento de Vigilancia de Mercado

SIA: sistema de inteligencia artificial

TFUE: Tratado de Funcionamiento de la UE

TJUE: Tribunal de Justicia de la Unión Europea

UE: Unión Europea

1. Introducción

Tatiana Bianca Vulpe y Daniel Duro Millan

Las palabras del P. Ovidius Naso siguen siendo plenamente vigentes: *Datae leges, ne fortis omnia posset* —las leyes tienen como finalidad evitar la arbitrariedad de los fuertes. A lo largo de la historia, las normas jurídicas han servido para limitar los abusos de poder y garantizar el equilibrio social. En la era digital, esta necesidad se traslada al ámbito tecnológico, donde el desarrollo de sistemas y modelos de inteligencia artificial (IA) plantea desafíos éticos y jurídicos que requieren una regulación clara y efectiva. Hoy, más que nunca, es esencial contar con un marco normativo que impida que se vulneren los derechos fundamentales, asegurando una IA alineada con los valores y principios europeos.

En esta línea, el 12 de julio de 2024 se publicó en el Diario Oficial de la Unión Europea (DOUE) el Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, en adelante RIA). Esta disposición, con efecto normativo directo, supone un paso significativo en la regulación y supervisión de tecnologías emergentes en Europa, como la IA. El RIA se fundamenta principalmente en el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que habilita a la Unión a adoptar medidas para garantizar el establecimiento y el funcionamiento del mercado interior, respetando los principios de subsidiariedad y proporcionalidad; también se basa en el artículo 16 del mismo tratado, que constituye el fundamento jurídico de la protección de datos.

Sin embargo, la redacción del RIA ha estado marcada por las divergencias entre los diferentes actores implicados. Esto se ejemplifica en los conflictos de intereses y sobre el alcance normativo que surgieron a lo largo del proceso legislativo. Algunos cambios significativos entre la propuesta inicial y la definitiva son los siguientes:

- La incorporación de 91 nuevos considerandos, destinados a precisar aspectos que generan inquietud, como la biometría.
- La incorporación de los conceptos *modelo* y *sistema de IA de uso general* en relación con los sistemas de IA generativa, dados los riesgos significativos de futuro que presentan.[1]

[1] La inclusión de los modelos y sistemas de IA de uso general no estaba previsto inicialmente en el RIA, ni en la propuesta de la Comisión Europea ni en la orientación general del Consejo. Esta incorporación fue impulsada principalmente por la irrupción de ChatGPT, desarrollado por OpenAI, que evidenció la necesidad de regular este tipo de modelos también llamados *fundacionales* o *de propósito general*. Los modelos de IA de uso general se caracterizan por ser entrenados con grandes volúmenes de datos mediante diversos métodos de aprendizaje, como el aprendizaje autosupervisado, el no supervisado o por refuerzo. A pesar de su relevancia en el desarrollo de la IA, estos modelos no constituyen por sí solos sistemas de IA completos, puesto que necesitan otros elementos para ser operativos, como una interfaz de usuario o mecanismos de integración en aplicaciones específicas (considerando 97 RIA).

- La introducción del concepto de riesgo sistémico.[2]
- La adición de nuevos anexos.
- El reconocimiento del derecho a obtener una explicación de decisiones individuales (art. 86 RIA), en línea con el artículo 22 y el considerando 71 del Reglamento General de Protección de Datos (RGPD).
- El derecho a presentar una reclamación ante una autoridad de vigilancia de mercado (art. 85 RIA), novedad que permite a los particulares dirigirse directamente a estas autoridades.

En este contexto, la solución adoptada finalmente ha sido establecer un marco normativo que garantice la intervención pública, pero con un grado de flexibilidad que permita adaptar las obligaciones en función de la importancia y el impacto de los riesgos asociados. Así, el RIA adopta un enfoque basado en el riesgo (art. 26 y 27 RIA) y clasifica los sistemas de IA en cuatro categorías de riesgo diferentes: (i) riesgo inaceptable (art. 5 RIA); (ii) alto riesgo (art. 6 y anexos I y III RIA); (iii) riesgo limitado o de transparencia (obligaciones de transparencia de acuerdo con el art. 50 RIA); i (iv) riesgo mínimo o nulo.[3]

El objetivo principal del RIA es mejorar el funcionamiento del mercado interior y promover la adopción de una IA centrada en el ser humano y fiable, y garantizar, al mismo tiempo, un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea, incluidos la democracia y el Estado de Derecho (considerandos 1, 2, 6, 7, 27 y 28; y art. 40.3 RIA). Además, el RIA se concibe como una norma abierta y dinámica, diseñada para adaptarse a los avances tecnológicos y a los nuevos retos que pueda plantear el uso de la IA. A tal fin, incluye múltiples elementos sujetos a desarrollos futuros y contempla facultades de modificación para la Comisión Europea; de esta forma, asegura su flexibilidad y capacidad de adaptación a la evolución del sector y a las necesidades reguladoras emergentes. Aunque inicialmente parecería que estas modificaciones se podían hacer sin control parlamentario, los artículos 97.8 y 112.1 del RIA clarifican que solo entrarán en vigor si el Parlamento Europeo y el Consejo no formulan objeciones en un plazo de tres meses, garantizando así un cierto control legislativo.

Por otra parte, es importante destacar que el RIA no agota la regulación de la IA, sino que forma parte de un marco normativo más amplio. Por este motivo, la aplicación debe ser integrada con otras normativas del derecho digital europeo (como el RGPD, el RSD, el RMD

---

[2] Este concepto se integra en la regulación de los modelos de IA de uso general, ya que se reconoce como uno de los riesgos potenciales que pueden conllevar. Esto incluye "cualquier efecto negativo real o razonablemente previsible en relación con accidentes graves, perturbaciones de sectores críticos y consecuencias graves para la salud y la seguridad públicas, cualquier efecto negativo real o razonablemente previsible sobre los procesos democráticos y la seguridad pública y económica o la difusión de contenidos ilícitos, falsos o discriminatorios" (considerando 110 RIA). Es importante destacar que estos riesgos sistémicos se intensifican a medida que aumenta la capacidad y el alcance de los modelos, pudiendo manifestarse a lo largo de todo su ciclo de vida.

[3] Los sistemas de IA que presentan un riesgo mínimo o nulo no están regulados, pero los proveedores y responsables de despliegue pueden adherirse a códigos de conducta voluntarios.

o el NIS2) y, también, con las normativas sectoriales específicas que sean relevantes, como las que afectan al sector financiero o a los dispositivos médicos (Barrio Andrés 2024). En este contexto, la protección de los datos personales, como derecho fundamental, adquiere un papel central a lo largo de todas las fases de desarrollo y uso de los sistemas de IA que, en muchos casos, utilizan datos personales.[4]

Por lo tanto, no es de extrañar que las autoridades de protección de datos asuman un papel central dentro del nuevo marco regulador establecido por el RIA. Estas entidades, que ya ejercían una función clave en la supervisión del tratamiento de datos personales bajo el RGPD,[5] ahora amplían sus responsabilidades para incluir nuevas bajo el RIA. Teniendo en cuenta este escenario, este trabajo se propone analizar:

- El rol de las autoridades de protección de datos en el RIA, examinando si las competencias asignadas suponen una ampliación de sus competencias o si, por el contrario, constituyen una evolución natural de las atribuciones ya establecidas por el RGPD.

- Su designación como autoridades de protección de derechos fundamentales, con las implicaciones que esto conlleva en la protección de los derechos individuales en el contexto de la IA.

En resumen, se pretende comprender mejor los mecanismos de gobernanza establecidos por el RIA y el papel central que juegan las autoridades de protección de datos. Esto sin entrar a considerar otras funciones o competencias que puedan ser asumidas en caso de que, de acuerdo con el esquema de gobernanza previsto en el RIA, se pueda ser designado como AVM.

[4] Uno de los principales retos es la prevención de riesgos, como los ataques de inversión de modelos o la identificación indebida de personas, que pueden producirse tanto durante la recopilación inicial de los datos como en las fases de aprendizaje y despliegue de los sistemas de IA (Keber 2024). Por eso, resulta fundamental asegurar que los sistemas cumplan los principios del RGPD y que exista una autoridad competente que evalúe factores como el coste de la identificación, el tiempo necesario para llevarla a cabo y los avances tecnológicos que puedan facilitar la reidentificación de datos personales, incluso si inicialmente parecen anonimizados.

[5] Las autoridades de protección de datos han estado activas durante mucho tiempo y colaboran en foros internacionales en materias relacionadas con los sistemas de IA (Asamblea Global de Privacidad, Grupo Internacional sobre Protección de Datos en Tecnologías, etc.).
EDPB. *Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial*. Julio 2024. Disponible en: edpb_statement_202403_dpasroleaiact_es.pdf

2. El rol de las autoridades de protección de datos en el RIA

Tatiana Bianca Vulpe

En el contexto de la adopción creciente de sistemas de IA en la Unión Europea, el RIA establece un marco normativo que busca equilibrar el desarrollo tecnológico con la protección de los derechos fundamentales, uno de ellos siendo la protección de datos. En este marco, tal y como se apuntaba en la introducción, las autoridades de protección de datos juegan un papel esencial para asegurar que el uso de las tecnologías que incorporen IA respete plenamente las normas vigentes en materia de protección de datos personales.

En esta línea, es importante analizar cómo el RIA amplía y concreta las funciones de estas autoridades para abordar los retos específicos que plantea la implementación de estas tecnologías emergentes, a la vez que mantiene su independencia y competencias; así, garantiza la preservación de los derechos de los ciudadanos en un entorno cada vez más digitalizado y global.

Los considerandos 10, 45, 69 y 157 del RIA proporcionan un contexto inicial para interpretar este reglamento en materia de protección de datos, así como para comprender el papel de las autoridades de protección de datos. En particular, durante todo el análisis hay que tener en cuenta los siguientes aspectos:

- El RIA no pretende afectar a la aplicación del Derecho de la Unión vigente que regula el tratamiento de datos personales, incluidas las funciones y atribuciones de las autoridades competentes. Tampoco afecta a las obligaciones de los proveedores y responsables de despliegue de sistemas de IA, en su rol de responsables o encargados del tratamiento, en la medida en que el diseño, desarrollo o uso de sistemas de IA impliquen el tratamiento de datos personales. Además, los interesados siguen manteniendo todos los derechos y garantías previstas en el RGPD (considerando 10).

- El RIA no debe afectar a las prácticas prohibidas por el Derecho de la Unión, incluido el Derecho de la Unión en materia de protección de datos (considerando 45). Esto significa que cualquier uso de sistemas de IA debe respetar las leyes europeas vigentes, especialmente en lo que respecta a la protección de los datos personales y la privacidad de los ciudadanos.

- El derecho a la protección de datos personales debe garantizarse a lo largo de todo el ciclo de vida del sistema de IA. En este sentido, los principios de minimización de datos y de protección de datos desde el diseño y, por defecto, establecidos en el Derecho de la Unión en materia de protección de datos, serán de aplicación cuando se traten datos personales (considerando 69).

- Además, el RIA se entiende sin perjuicio de las competencias, funciones, poderes e independencia de las autoridades de protección de datos (considerando 157). Esto asegura que estas autoridades sigan ejerciendo plenamente sus responsabilidades sin interferencias, para garantizar que los derechos de los individuos en materia de protección de datos se preserven en todo momento, incluso con la implementación de nuevas tecnologías de IA.

- Cuando sea necesario para su mandato, las autoridades de protección de datos también tendrán acceso a cualquier documentación creada en virtud del presente Reglamento (157). Este es un punto importante, porque los operadores deberán facilitar la documentación creada en virtud de este Reglamento a las autoridades de protección de datos cuando estas actúen en relación con el RGPD.

En esta línea, el CEPD ha subrayado que, siempre que un modelo o sistema de IA implique el tratamiento de datos personales, entraría en el ámbito de supervisión de las autoridades nacionales de protección de datos pertinentes.[6] En este sentido, es importante tener claro el concepto de datos personales en contraposición al concepto de datos anónimos.

Además, debe tenerse en cuenta que la existencia y el uso de sistemas de IA es previa al RIA, y que las autoridades de protección de datos ya habían abordado esta materia en relación con el RGPD. La APDCAT, por ejemplo, ya se ha pronunciado en este ámbito haciendo énfasis en obligaciones como la protección de datos desde el diseño, la aplicación de los principios de protección de datos o las evaluaciones de impacto.[7] Por otra parte, en el desarrollo de los modelos con inteligencia artificial, esta autoridad también ha recomendado que se apliquen mecanismos de aprendizaje federado "de modo que las personas que tienen los datos (individuos, entidades, etc.) pueden entrenar el modelo de forma distribuida, sin que tengan que ceder los datos a una entidad que centraliza el entrenamiento."[8]

Para abordar adecuadamente el análisis normativo, resulta imprescindible precisar primero el concepto de *sistema de IA*. El artículo 3.1 del RIA define un sistema de IA como “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”.

Este artículo debe relacionarse con el considerando 12 del RIA. Según este considerando, podemos decir que un sistema de IA es un software que se distingue de los enfoques tradicionales basados en reglas predefinidas por humanos. A diferencia de estos, un sistema de IA está diseñado para operar con varios niveles de autonomía y tiene una capacidad de inferencia que le permite alcanzar objetivos, tanto de forma explícita como implícita. Además, el sistema debe disponer de capacidad de autoaprendizaje, lo que implica la posibilidad de modificar su comportamiento mientras se utiliza, de acuerdo con la lógica aplicada, el conocimiento adquirido y las estrategias previamente establecidas. Esta

---

[6] EDPB. *Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial.* Julio 2024. Disponible en: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_es

[7] Autoridad Catalana de Protección de Datos (APDCAT). *Inteligencia Artificial: Decisiones Automatizadas en Cataluña.* 2020. Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/intelligencia_artificial/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf

[8] Autoridad Catalana de Protección de Datos (APDCAT). *La privacidad desde el diseño y la privacidad por defecto. Guía para desarrolladores* Junio 2024. Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD.pdf

característica es fundamental, puesto que permite a los sistemas de IA evolucionar y adaptarse a nuevas situaciones, lo que los diferencia claramente de los sistemas de programación estática basados en normas fijas.

Es especialmente relevante tener en cuenta esta definición, puesto que los sistemas que no cumplan estas características esenciales quedarían, en principio, fuera del ámbito de aplicación del RIA. Dicho de otro modo: si hablamos de sistemas automatizados sustentados exclusivamente en normas preestablecidas por personas, sin capacidad de inferencia o aprendizaje autónomo, no estaríamos ante un sistema de IA en el sentido estricto del RIA; por tanto, su uso se escaparía del alcance regulador de este marco jurídico (Fernández Hernández 2024).

Así pues, en los siguientes apartados se analizan las diversas menciones que hace el RIA sobre las autoridades de protección de datos, ya sea en términos de habilitaciones o exigencias. Además, a fin de adquirir el contexto necesario, se recomienda leer el anexo de este trabajo, que trata sobre la identificación biométrica remota.

2.1. Recepción de notificaciones sobre el uso de sistemas de identificación biométrica remota *en tiempo real* (art. 5.4 y considerandos 36 y 38 RIA)

"Sin perjuicio de lo dispuesto en el apartado 3, **todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará** a la autoridad de vigilancia del mercado pertinente y **a la autoridad nacional de protección de datos** de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles". (art. 5.4 RIA)

Aplicable a partir del 2 de febrero de 2025.

El considerando 36 del RIA dispone que cada uso de un sistema de identificación biométrica remota en tiempo real debe notificarse a la autoridad de vigilancia del mercado pertinente, así como a la autoridad nacional de protección de datos. El artículo 5.4 del RIA detalla esta notificación y estipula que, sin perjuicio de lo dispuesto en el apartado 3 del mismo artículo, cualquier uso de un sistema de identificación biométrica remota en tiempo real en espacios de acceso público, con fines de garantía del cumplimiento del Derecho, debe notificarse a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos; la notificación debe incluir como mínimo la información especificada en el apartado 6 y excluir datos operativos sensibles. Teniendo en cuenta que los Estados miembros no están obligados a nombrar una autoridad nacional de vigilancia del mercado antes del 2 de agosto de 2025, se entiende que en el período comprendido entre el 2 de febrero de 2025 y esa fecha (o si lo hacen en plazo) solo existe la obligación de notificar a las autoridades de protección de datos.

En el Estado existen varias autoridades de protección de datos: la Agencia Española de Protección de Datos (AEPD), la Autoridad Catalana de Protección de Datos (APDCAT), la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía. Por tanto, se podría considerar razonable que la notificación se efectuase directamente a la autoridad de protección de datos competente, según quien despliegue el sistema de identificación biométrica. Por ejemplo, el ámbito de actuación de la APDCAT, tal y como se dispone en el artículo 3 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, comprende los ficheros y tratamientos efectuados por las instituciones públicas, la Administración de la Generalitat y los entes locales, entre otros. Así, si un sistema es utilizado por fuerzas de seguridad de Cataluña, la notificación debería presentarse ante la APDCAT.

Queda claro que cada autoridad debe disponer de la información necesaria para ejercer sus funciones dentro de su ámbito competencial. Sin embargo, para evitar duplicidades o vacíos en la supervisión, especialmente en situaciones en las que no sea claro a quién debe notificarse (por ejemplo, en casos de colaboración entre los cuerpos y fuerzas de seguridad de varios territorios), sería recomendable disponer de mecanismos de coherencia entre las diferentes autoridades. Esta coherencia garantizaría que la información sobre el uso de estos sistemas sea accesible para todas las partes pertinentes y que, indirectamente, los derechos de las personas se protegieran de forma coherente.

Es importante tener presente que esta notificación se enmarca en el contexto de excepciones a prácticas prohibidas, reguladas en el artículo 5 del RIA. Cualquier uso, entendido en un sentido amplio, de sistemas de identificación biométrica remota en tiempo real que requiera notificación se enmarca dentro de un contexto de excepcionalidad, regido por criterios de necesidad, proporcionalidad y respeto a los derechos fundamentales.

Las prácticas prohibidas no deben entenderse como una lista cerrada, ya que el artículo 112 del RIA exige que, cada año, la Comisión Europea revise “la necesidad de modificar la lista del anexo III y la lista de prácticas de IA prohibidas previstas en el artículo 5”. Además, de acuerdo con el artículo 96.1.*b* del RIA, la Comisión, como ya lo ha hecho recientemente, debe aprobar directrices sobre la implementación de las prácticas prohibidas por el artículo 5 del RIA. Estas directrices no solo deben servir para ayudar a los proveedores y responsables del despliegue a la hora de garantizar el cumplimiento del RIA, sino que también deben funcionar como una guía para orientar a las autoridades competentes en virtud del RIA.[9]

En este contexto analizado, la notificación a las autoridades de protección de datos proporciona de forma indirecta una garantía adicional para asegurar que estas prácticas cumplen con las normas de protección de datos. Aunque el RIA no detalla una actuación posterior de estas autoridades, la notificación permite un seguimiento exhaustivo y una intervención efectiva, en caso de indicios de irregularidades sobre las competencias que estas autoridades ya tenían atribuidas en el marco del RGPD; no se puede olvidar que la

[9] No debe perderse de vista que estas directrices no son vinculantes y que, por tanto, cualquier interpretación del Reglamento debe pasar por el Tribunal de Justicia de la Unión Europea (TJUE).

biometría era ya una cuestión que trataban las autoridades de protección de datos[10] o el Comité Europeo de Protección de datos (CEPD), integrado por todas las autoridades de control nacionales europeas.

Concretamente, como texto relevante que conviene mencionar, el CEPD aprobó las Directrices 5/2022, sobre el uso de la tecnología de reconocimiento facial, adoptadas en fecha 26 de mayo de 2023, después de la consulta pública. En el apartado 12, dicen: "Aunque las dos funciones (autenticación e identificación) son distintas, ambas se refieren al tratamiento de datos biométricos relacionados con una persona física identificada o identificable y, por lo tanto, constituyen un tratamiento de datos personales y, más concretamente, un tratamiento de categorías especiales de datos personales".

En último término, la identificación mediante sistemas de IA no es posible sin una base de datos de referencia que contenga datos biométricos a efectos de comparación. La utilización de la IA posibilita un tratamiento más sofisticado de los datos biométricos, lo que permite no solo la identificación, sino también obtener inferencias sobre determinados aspectos o patrones de comportamiento de la persona, con los consiguientes riesgos para sus derechos. Este punto es especialmente relevante porque estamos ante categorías especiales de datos, tal y como se establece en el artículo 9.1 del Reglamento (UE) 2016/679, el artículo 10 de la Directiva (UE) 2016/680 y el artículo 10.1 del Reglamento (UE) 2018/1725. Así, el tratamiento de datos biométricos encaminados a identificar de forma unívoca a una persona física está sujeto al régimen específico del RGPD en categorías especiales de datos.

Sin embargo, sería deseable una mayor claridad sobre algunos aspectos clave de esta notificación, a fin de garantizar una aplicación coherente y eficaz de la normativa. En primer lugar, aunque el artículo hace referencia a que la notificación debe excluir datos operativos sensibles, no se aportan detalles concretos sobre qué elementos son imprescindibles, más allá de una remisión. Por ejemplo, sería importante definir si es necesario incluir información sobre los objetivos del uso, el alcance temporal, geográfico y personal o las medidas de seguridad implementadas. Esta falta de claridad puede generar inconsistencias en la práctica. En segundo lugar, también es preciso aclarar los plazos en los que debe efectuarse esta notificación. El RIA no determina si debe presentarse antes del uso del sistema, inmediatamente después de utilizarlo o si hay un período específico para presentarla. Sí lo prevén directrices recientes [11] relativas a prácticas prohibidas, donde se concreta lo siguiente: la notificación debe realizarse después de cada uso, para poder informar sobre el número de autorizaciones y su resultado. Aunque proporciona mayor concreción, no tenemos una definición precisa, lo que puede resultar problemático, especialmente en contextos donde el tiempo es crítico, en situaciones de urgencia o en casos excepcionales. El establecimiento de plazos claros contribuiría a garantizar una

[10] Como, por ejemplo, la APDCAT, en el dictamen emitido en la consulta 21/2020, o en el informe 1/2022.

[11] Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

coherencia efectiva entre las autoridades implicadas y aseguraría que la supervisión se realice en tiempo real o en un período razonable.

2.2. Presentación de informes anuales a la Comisión, en relación con las notificaciones sobre el uso de sistemas de identificación en tiempo real (art. 5.6 RIA y considerando 36)

"Las autoridades nacionales de vigilancia del mercado y l**as autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho** con arreglo al apartado 4 **presentarán a la Comisión informes anuales sobre dicho uso**. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o una autoridad administrativa independiente cuya decisión sea vinculante en relación con las solicitudes de autorización de conformidad con el apartado 3, así como su resultado". (art. 5,6 RIA)

Aplicable a partir del 2 de febrero de 2025.

Vinculado con lo desarrollado en el punto anterior de este trabajo, las autoridades nacionales de protección de datos de los Estados miembros que reciban notificaciones sobre el uso de sistemas de identificación biométrica remota en tiempo real, en espacios de acceso público, con fines de garantía del cumplimiento del Derecho, tienen la obligación de presentar informes anuales a la Comisión Europea, que deben incluir información sobre el número de decisiones adoptadas. Este sistema plantea varios retos prácticos y conceptuales.

Un aspecto a mencionar es que, en este apartado, el RIA hace uso del plural ('las autoridades nacionales de protección de datos') cuando se refiere a las autoridades de protección de datos, mientras que en el contexto de la recepción de la notificación utiliza el singular ('la autoridad nacional de protección de datos'). En principio, el uso del singular o plural en el RIA no tiene por qué tener una implicación jurídica significativa, ya que podría tratarse simplemente de una cuestión de redacción sin intención de introducir diferencias prácticas. Sin embargo, teniendo en cuenta el contexto del Estado español, donde coexisten diferentes autoridades, esta diferencia terminológica podría abrir la puerta a interpretaciones más amplias. Así, debe entenderse que todas las autoridades competentes según el territorio o el ámbito material afectado por el sistema de identificación biométrica— deben redactar el informe correspondiente. No obstante, queda pendiente concretar cómo se vehicularía el envío formal de los informes a la Comisión Europea.

Asimismo, el hecho de que cada autoridad que ha recibido notificaciones presente un informe en el marco del artículo 5.6 del RIA genera dudas sobre las posibles duplicidades en los informes. Por ejemplo, si varias autoridades (autoridades de vigilancia de mercado y autoridades de protección de datos) reciben notificaciones sobre el mismo uso, será necesario definir si cada una de ellas debe presentar un informe independiente a la Comisión, o si se

concentrarán en una única autoridad para facilitar una presentación unificada. La falta de claridad en ese punto podría generar una duplicidad de datos o una carga administrativa innecesaria, dificultando el objetivo de supervisión efectiva. Además, como ya se apunta en las directrices de la Comisión respecto a las prácticas prohibidas, de momento las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos son libres de decidir si quieren presentar informes individuales o un informe conjunto por Estado miembro.

El informe previsto en el artículo 5.6 del RIA representa una novedad dentro del nuevo marco regulador para las autoridades de protección de datos y se diferencia significativamente del informe regulado por el artículo 59 del RGPD. Mientras que este último tiene un carácter público y el contenido está claramente definido, el informe del RIA al que nos referimos todavía no tiene un desarrollo concreto. Además, la redacción de estos informes anuales depende de la disponibilidad de directrices y modelos establecidos por la Comisión Europea; esto limita la acción de las autoridades, puesto que el marco regulador todavía no está completamente definido, aunque el artículo 5 del RIA ya está vigente. Por otra parte, solo el informe de las autoridades nacionales de protección de datos cubriría el período comprendido entre el 2 de febrero de 2025 y el 2 de agosto de 2025, ya que el RIA no exige a los Estados miembros que designen una autoridad nacional de vigilancia del mercado antes de esa fecha.

Este sistema de aplicación progresiva puede justificarse por la complejidad y la evolución constante de la inteligencia artificial. Como apunta Quadra-Salcedo (2024), es prácticamente imposible regular con precisión desde el inicio todo el alcance, las posibilidades y riesgos que plantea esta tecnología. Por tanto, parece razonable sentar unas bases iniciales, que se puedan ajustar y desarrollar a medida que se consolide y se entienda mejor la tecnología. Esto permitirá abordar nuevos retos y adaptar las normas a las circunstancias cambiantes. Sin embargo, esta aproximación progresiva también plantea incertidumbres. Cuando la Comisión establezca el contenido específico de los informes, todavía quedará abierta la posibilidad de ampliar o modificar la información exacta que deberá incluirse, lo que podría requerir ajustar las prácticas de notificación y los informes respectivos de forma continua.

2.3. Acceso a documentación sobre el uso de sistemas de identificación biométrica remota en diferido, documentada en el expediente policial pertinente (art. 26.10 RIA).

"No obstante lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación cuya finalidad sea la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello, el responsable del despliegue de un sistema de IA de alto riego de identificación biométrica remota en diferido solicitará, ex ante o sin demora indebida y a más tardar en un plazo de cuarenta y ocho horas, a una autoridad judicial o administrativa cuyas decisiones sean vinculantes y estén sujetas a revisión judicial, una autorización para utilizar ese sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso sobre la base de hechos objetivos y verificables vinculados directamente al delito. Cada utilización deberá limitarse a lo que resulte estrictamente necesario para investigar un delito concreto.

(...)

Con independencia de la finalidad o del responsable del despliegue, **se documentará toda utilización de tales sistemas de IA de alto riesgo en el expediente policial pertinente y se pondrá a disposición, previa solicitud,** de la autoridad de vigilancia del mercado pertinente y **de la autoridad nacional de protección de datos, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho.** El presente párrafo se entenderá sin perjuicio de los poderes conferidos por la Directiva (UE) 2016/680 a las autoridades de control.

(...)" (art. 26.10 RIA)

Aplicable a partir del 2 de agosto de 2026.

El artículo 26 del RIA recoge las obligaciones de los responsables de despliegue de sistemas de IA de alto riesgo. Este responsable se define como una persona física o jurídica, o una autoridad pública, organismo o entidad, que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional (art. 3.4 RIA).

Antes de entrar en el análisis, es importante realizar dos consideraciones previas. En primer lugar, cabe destacar que las obligaciones recogidas en el artículo 26 no son las únicas que recaen sobre los responsables del despliegue, ya que también existen otras relevantes fuera de este artículo. Por ejemplo, el artículo 27, que se introdujo en una fase avanzada del proceso legislativo, impone a ciertos responsables del despliegue de sistemas de IA de alto riesgo la obligación de realizar una evaluación del impacto que el uso de estos sistemas puede tener sobre los derechos fundamentales.

Por otra parte, el RIA no altera las obligaciones que otras normativas de la Unión Europea o de legislaciones nacionales impongan a los responsables del despliegue, como queda explícito en el artículo 26.2 del RIA. Por ejemplo, y como ya se ha mencionado previamente, si el uso de sistemas de IA implica el tratamiento de datos personales, el responsable del despliegue también debe asumir el rol de responsable o encargado del tratamiento y cumplir las normativas aplicables en materia de protección de datos personales (considerando 10).

En concreto, el artículo 26.10 del RIA aborda las obligaciones de documentación y supervisión de usos de sistemas de IA de alto riesgo para la identificación biométrica remota en diferido. Cualquier utilización de estos sistemas debe quedar registrada en los expedientes policiales pertinentes, con el fin de garantizar una trazabilidad adecuada y posibilitar la supervisión por parte de las autoridades competentes. Esta documentación debe estar disponible, previa solicitud, para la autoridad de vigilancia del mercado pertinente y la autoridad nacional de protección de datos, excluida explícitamente la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho.

El RIA distingue entre los sistemas de identificación biométrica remota en tiempo real y en diferido, en función de si la captura de datos biométricos, la comparación y la identificación se producen con o sin un retraso significativo, tal y como se explica en apartados previos.[12]

Dado el carácter altamente intrusivo de los sistemas de identificación biométrica, conviene tener presente que, aparte del RIA, estos sistemas están sometidos a una serie de garantías impuestas por el Derecho de la Unión en materia de protección de datos y que el legislador europeo del RIA ha querido establecer de forma expresa una serie de garantías adicionales, para evitar que el despliegue de los sistemas de identificación biométrica remota en diferido pueda dar lugar a una vigilancia indiscriminada (considerando 95).

En este sentido, cabe destacar que el artículo 26.10 del RIA presenta numerosas similitudes con la regulación de los sistemas de identificación biométrica remota en tiempo real, establecida en los artículos 5.2 a 5.7 (desarrollados en los apartados 2.1 y 2.2 de este trabajo). Así, desde una perspectiva sistemática, la regulación del uso policial de los sistemas de identificación biométrica en diferido se ha elevado al artículo 26, puesto que, aunque el legislador europeo quiere limitar su uso e impedir su aplicación indiscriminada, no ha optado por convertir esta práctica en una prohibición absoluta, sino que la somete a condiciones y requisitos estrictos (López 2024).

No obstante, ninguno de los dos supuestos define de forma suficientemente precisa el contenido exacto de los informes o registros a mantener o facilitar. Esta falta de concreción genera un vacío normativo, que puede dar lugar a interpretaciones divergentes y a dificultades prácticas en la aplicación efectiva del RIA, hasta que la Comisión publique las directrices correspondientes.

La única referencia (indirecta) que tenemos es en el considerando 93 del RIA, sobre la información que debe constatar el responsable del despliegue en relación con los interesados:

- Los responsables del despliegue de sistemas de IA de alto riesgo incluidos en el anexo III, que tomen o ayuden a tomar decisiones relacionadas con personas físicas, están obligados a informar a los afectados que están expuestos al uso de sistemas de IA de alto riesgo. Esta información debe incluir la finalidad prevista y el tipo de decisiones que se toman, así como garantizar el derecho de la persona afectada a una explicación de acuerdo con el RIA. Por tanto, podría extraerse que sería conveniente acreditar en los expedientes el contenido de esta información, y cómo se ha hecho efectiva.

- Por lo que respecta a los sistemas de IA de alto riesgo utilizados con fines de aplicación del Derecho, se aplica el artículo 13 de la Directiva (UE) 2016/680. Este precepto establece que debe ponerse a disposición del interesado información adicional o facilitarle, en caso de tratamiento de datos personales por parte de las autoridades competentes en materia de prevención, investigación, detección o

[12] En el anexo de este artículo se expone brevemente esta diferencia.

enjuiciamiento de infracciones penales, así como en la ejecución de sanciones penales.[13] Por tanto, sería conveniente dejar también constancia en los expedientes de esta información adicional.

Así pues, uno de los principales retos identificados es la ausencia de directrices específicas sobre el contenido que debería incluir la documentación en los expedientes policiales. Esta carencia de precisión no solo puede dificultar la labor de supervisión de las autoridades, sino que también podría llevar a una aplicación inconsistente entre Estados miembros, o incluso entre autoridades en un mismo estado.

Tal y como sucede con los sistemas en tiempo real, analizados en los apartados 2.1 y 2.2 de este trabajo, en el artículo 26.10 no queda claro cómo debe gestionarse la coherencia entre las diversas autoridades implicadas, como las autoridades nacionales de protección de datos y las autoridades de vigilancia del mercado.

2.4. Recepción de informes anuales sobre el uso de sistemas de identificación biométrica remota en diferido (art. 26.10 RIA)

"No obstante lo dispuesto en la Directiva (UE) 2016/680, en el marco de una investigación cuya finalidad sea la búsqueda selectiva de una persona sospechosa de haber cometido un delito o condenada por ello, el responsable del despliegue de un sistema de IA de alto riego de identificación biométrica remota en diferido solicitará, ex ante o sin demora indebida y a más tardar en un plazo de cuarenta y ocho horas, a una autoridad judicial o administrativa cuyas decisiones sean vinculantes y estén sujetas a revisión judicial, una autorización para utilizar ese sistema, salvo cuando se utilice para la identificación inicial de un posible sospechoso sobre la base de hechos objetivos y verificables vinculados directamente al delito. Cada utilización deberá limitarse a lo que resulte estrictamente necesario para investigar un delito concreto.

(...)

Los responsables del despliegue presentarán informes anuales a la autoridad de vigilancia del mercado pertinente y **a la autoridad nacional de protección de datos sobre el uso que han hecho de los sistemas de identificación biométrica remota en diferido**, quedando excluida la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho. Los informes podrán agregarse de modo que cubran más de un despliegue.

(...)" (art. 26.10 RIA)

Aplicable a partir del 2 de agosto de 2026.

[13] En España hay que tener en cuenta el artículo 21 de la LO 7/2021.

Los responsables del despliegue deben presentar informes anuales a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos, sobre el uso que hayan hecho de los sistemas de identificación biométrica remota en diferido, excluyendo la divulgación de datos operativos sensibles relacionados con la garantía del cumplimiento del Derecho.

La obligación de que los responsables del despliegue presenten informes anuales a las autoridades de vigilancia del mercado y de protección de datos podría considerarse como medida esencial para garantizar la adecuada transparencia y supervisión del uso de los sistemas de identificación biométrica remota en diferido. Esta medida permite a las autoridades competentes, como la APDCAT, supervisar cómo se utilizan estos sistemas, asegurar que se cumplan las normativas establecidas y detectar posibles irregularidades a la hora de implementarlos o utilizarlos.

Un aspecto relevante de esta obligación es que los informes pueden ser agregados para cubrir más de un despliegue. Esta opción puede facilitar la gestión administrativa a los responsables del despliegue, especialmente si han hecho múltiples usos de los sistemas en diferentes contextos. Al mismo tiempo, la agregación podría simplificar el proceso de revisión de las autoridades de vigilancia y protección de datos, ofreciendo una visión más global del uso de estos sistemas en un período determinado. Sin embargo, la agregación también plantea retos: es crucial que no comprometa la capacidad de supervisión de las autoridades, asegurando que los informes agregados sean suficientemente detallados para identificar posibles abusos o desviaciones de la normativa. Sería recomendable que los informes agregados incluyeran datos clave sobre cada despliegue, como la finalidad específica, el alcance geográfico, las condiciones de uso y las medidas de control implementadas.

En todo caso, la presentación de informes anuales se convierte en una herramienta clave para reforzar la responsabilidad de los responsables del despliegue, así como garantizar que los sistemas de identificación biométrica remota en diferido no se utilizan de forma abusiva ni vulneran los derechos fundamentales. Además, estos informes anuales podrían ser útiles para analizar el impacto acumulado de estos sistemas, detectar tendencias en su uso y ajustar las actuaciones futuras según las necesidades y riesgos identificados.

2.5. Participación en espacios controlados de pruebas para la IA (art. 57.10 RIA)

"Las autoridades nacionales competentes velarán por que, **en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes que proporcionen o respalden el acceso a los datos, las autoridades nacionales de protección de datos** y las demás autoridades nacionales o competentes **estén ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y competencias**." (art. 57.10 RIA)

Aplicable a partir del 2 de agosto de 2026.

El artículo 57 del RIA establece la creación de espacios controlados de pruebas para la IA (o *sandboxes*), con el objetivo de fomentar la innovación y facilitar el desarrollo, entrenamiento, prueba y validación de sistemas de IA innovadores, antes de introducirlos en el mercado. Los Estados miembros tendrán que establecer, como mínimo, un espacio controlado de pruebas operativo antes del 2 de agosto de 2026, bajo la supervisión de las autoridades competentes nacionales.

Aunque los *sandboxes* inicialmente surgieron como entornos regulados de experimentación centrados principalmente en el sector de empresas de tecnologías financieras (*fintech*), recientemente han comenzado a aparecer espacios similares diseñados específicamente para la IA en diferentes partes del mundo (Arellano Toledo 2024). Un ejemplo cercano es "el entorno controlado de pruebas" establecido por el Gobierno del Estado con el Real Decreto 817/2023, de 8 de noviembre. Este decreto regula un espacio de pruebas dedicado a garantizar que la propuesta del RIA se cumple. En esta línea, se puede constatar que el Gobierno del Estado español se ha adelantado a las exigencias del artículo 57 del RIA. Aunque aparentemente esto pueda parecer positivo, puede provocar una falta de coherencia entre los requisitos establecidos por el RIA y los que prevé el RD. Un ejemplo es que el artículo 3.2 del RD hace referencia tanto a los proveedores como a los usuarios, mientras que el RIA (tal y como se observa en los considerandos 138 y 139 y en el artículo 57) se limita a mencionar a los proveedores y proveedores potenciales, dejando al margen a los usuarios (equivalencia responsables del despliegue, según el RIA). Además, el artículo 3.8 del RD distingue entre dos tipos de usuarios (solicitantes y participantes) y, en el artículo 3.7, entre proveedores solicitantes y participantes.

Así, en cuanto a los llamados *sandbox*, se establecen cuatro categorías diferentes que no aparecen exactamente de la misma manera en el RIA. Estas divergencias, junto con otras cuestiones, como las diferencias en los tipos de sistemas de IA regulados, podrían hacer necesaria una revisión o modificación de los marcos legales nacionales, para garantizar su armonización y adecuación a la normativa comunitaria (Arellano Toledo, 2024). Ello, sin contar con la posibilidad de que la Comisión, mediante sus actos ejecutivos, establezca disposiciones más precisas sobre los tipos y el número de participantes que pueden hacer uso de los espacios de pruebas.

Por otra parte, en las guías y recomendaciones elaboradas hasta ahora por la AEPD[14] y la CNMC,[15] así como por otras autoridades, también se pone de manifiesto una actitud favorable respecto a la implementación de este tipo de proyectos, que se consideran una oportunidad para promover la innovación, mientras se reducen los posibles impactos de la

[14] AEPD. *Requisitos para Auditorías de Tratamientos que incluyan IA,* 2021.
AEPD. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*, 2020.
AEPD. *Tratamientos que incluyen Inteligencia Artificial (IA). Mapa de referencia,* 2022.

[15] CNMC. Informe sobre el proyecto de Real Decreto 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, 2023.

IA sobre la ciudadanía.[16] Este enfoque debería asegurar que la asignación de competencias se formalizara mediante normas con valor legal y que se desplieguen medidas de protección adecuadas. Además, tiene especial importancia respetar principios como la limitación en el tratamiento de datos y la transparencia, restringiendo el alcance de los proyectos a objetivos específicos, explícitos y legítimos (Arellano Toledo 2024).

Uno de los puntos más delicados, vinculados a la interacción con el RGPD, es la limitación de finalidades, que exige una evaluación más precisa del uso de sistemas de IA destinados a objetivos concretos. Esto tiene como objetivo evitar que el entrenamiento o diseño inicial de un sistema interfiera con su uso posterior, para finalidades diferentes o incompatibles. Este mismo principio se aplica a los sistemas de IA que, siendo utilizados para objetivos compatibles, necesitan identificar claramente la base legal que sustenta el tratamiento y llevar a cabo las acciones necesarias para validarlo, si es necesario (Arellano 2024).

En lo que se refiere a las autoridades de protección de datos, el artículo 57.10 las menciona directamente al indicar que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales (o estén bajo la supervisión de otras autoridades nacionales o competentes que proporcionen o apoyen el acceso a los datos), estas autoridades deben estar ligadas al funcionamiento del espacio controlado para la IA e involucradas en la supervisión de estos aspectos, según sus funciones y competencias. Esto es un indicador del papel activo que desempeñan las autoridades de protección de datos en estos entornos. Pero, ¿cuál es el alcance real de esa vinculación al funcionamiento del espacio? No queda claro.

El artículo 57 del RIA no vuelve a referirse explícitamente a las autoridades de protección de datos, sino que utiliza el término genérico *autoridades competentes* para regular el funcionamiento del entorno de pruebas. Esta formulación podría generar inseguridad jurídica y requerir futuras aclaraciones sobre si *autoridades competentes* es lo mismo que *autoridades nacionales competentes*.

Independientemente de si se consideran o no autoridades competentes en este contexto, en cualquier caso las autoridades de protección de datos deben estar vinculadas al funcionamiento del espacio controlado de pruebas para la IA y participar en la supervisión de estos aspectos, tal y como se apunta anteriormente.

Según el enfoque adoptado, el siguiente listado podría conllevar nuevas funciones para las autoridades de protección de datos o, como mínimo, una mejor inferencia/definición de lo que debería implicar su vinculación al funcionamiento y supervisión:

- En primer lugar, en el espacio controlado de pruebas, las autoridades competentes deben proporcionar orientación, supervisión y apoyo para determinar los riesgos, especialmente para los derechos fundamentales, la salud y la seguridad. Esto incluye evaluar las pruebas y medidas de mitigación, así como su eficacia en relación con las

[16] Estas guías presentan ejemplos de usos razonables de sistemas de inteligencia artificial, justificados por el interés público, como por ejemplo proyectos de ciudades inteligentes (*smartcities*) o el control de fronteras.

obligaciones y requisitos del RIA y, cuando proceda, otras disposiciones del Derecho de la Unión y nacional supervisadas en el espacio controlado de pruebas (art. 57.6 RIA).

- En segundo lugar, las autoridades competentes deben proporcionar a los proveedores y potenciales proveedores orientaciones sobre las expectativas en materia de regulación y la forma de cumplir los requisitos y obligaciones establecidos en el RIA. Si el proveedor o potencial proveedor del sistema de IA lo solicita, la autoridad competente también debe aportar una prueba escrita de las actividades realizadas con éxito en el espacio controlado de pruebas, así como un informe de salida que detalle las actividades realizadas y los resultados y aprendizajes correspondientes. Los proveedores pueden utilizar esta documentación para demostrar que cumplen con el RIA, mediante el proceso de evaluación de la conformidad o las actividades de vigilancia del mercado pertinentes (art. 57.7 RIA).

- En tercer lugar, los espacios controlados de pruebas para la IA no afectan a las facultades de supervisión o correctoras de las autoridades competentes que los supervisan, ni siquiera a nivel regional o local. Cualquier riesgo considerable para la salud, seguridad y derechos fundamentales detectado durante el proceso de desarrollo y prueba de estos sistemas de IA requerirá una mitigación adecuada. Si no es posible mitigarlos, las autoridades nacionales competentes están facultadas para suspender temporal o permanentemente el proceso de prueba, o la participación en el espacio controlado de pruebas, y deben informar a la Oficina de IA de esta decisión. Con el objetivo de apoyar la innovación en materia de IA en la Unión, estas autoridades ejercen sus facultades de supervisión dentro de los límites del derecho pertinente y utilizan su potestad discrecional para aplicar disposiciones jurídicas relacionadas con un proyecto específico de espacio controlado de pruebas para la IA (art. 57.11 RIA).

Otros apartados indican que los espacios controlados de pruebas para la IA deben diseñarse e implementarse de forma que, cuando proceda, faciliten la cooperación transfronteriza entre las autoridades nacionales competentes. Estas autoridades deben coordinar sus actividades y cooperar en el marco del Consejo de IA, informando sobre el establecimiento de un espacio controlado de pruebas a la Oficina de IA y al Consejo de IA, a los que pueden solicitar apoyo y orientación. Además, deben presentar informes anuales que proporcionen información sobre el progreso y los resultados de la implementación de estos espacios, incluyendo mejores prácticas, incidentes, enseñanzas extraídas y recomendaciones sobre su configuración y, en su caso, sobre la aplicación y posible revisión del Reglamento.

Sin embargo, el apartado a analizar con más detalle es el número 12, especialmente teniendo en cuenta que el RIA no debería interferir en las competencias sancionadoras de las autoridades de protección de datos. Este apartado establece que según el Derecho de la Unión y nacional en materia de responsabilidad, los proveedores y potenciales proveedores que participen en el espacio controlado de pruebas para la IA son responsables de cualquier daño infligido a terceros, como resultado de la experimentación llevada a cabo en el espacio. Sin embargo, siempre que los proveedores potenciales respeten el plan específico y las condiciones de su participación, y sigan de buena fe las orientaciones proporcionadas

por la autoridad nacional competente, las autoridades no impondrán multas administrativas por infracciones del RIA. En los casos en que otras autoridades competentes responsables de otras disposiciones del Derecho de la Unión y nacional hayan participado activamente en la supervisión del sistema de IA y hayan proporcionado orientaciones para su cumplimiento, tampoco se impondrán multas administrativas en relación con estas disposiciones.

Según el RGPD, las autoridades de protección de datos tienen la potestad de imponer sanciones administrativas en caso de incumplimiento de la normativa de protección de datos. Si el RIA establece una posible exención de sanciones administrativas, esta debería ser interpretada con cautela para no contradecir las atribuciones legales de estas autoridades. En particular, el artículo 57.12 del RIA genera dudas, puesto que podría ser interpretado como una limitación o interferencia en las funciones de las autoridades de protección de datos. Sin embargo, esta interpretación no es inequívoca y habría que valorarla caso por caso.

Es importante remarcar que el hecho de que se formule una recomendación genérica en el marco de un espacio controlado de pruebas no puede entenderse como una exención automática de responsabilidad o sanción. Habrá que analizar cada situación concreta para determinar hasta qué punto estas recomendaciones se han aplicado de forma efectiva y adecuada al caso en cuestión. Este extremo es especialmente relevante cuando la autoridad que investigue una posible infracción no coincida con la que ha participado en el espacio de pruebas, y pueda verse eventualmente condicionada por el criterio de esta última.

En cualquier caso, conviene recordar los principios de no interferencia en las competencias, funciones, poderes e independencia de las autoridades de protección de datos (considerandos 10, 45, 69 y 157 del RIA), tal y como ya se ha expuesto en la introducción de este apartado.

2.6. Designación como autoridad de vigilancia del mercado (art. 74.8 RIA)

"En el caso de los sistemas de IA de alto riesgo enumerados en el anexo III del presente Reglamento, punto 1, en la medida en que los sistemas se utilicen a los efectos de la garantía del cumplimiento del Derecho, la gestión de fronteras y la justicia y la democracia, y **en el caso de los sistemas de IA de alto riesgo enumerados en el anexo III, puntos 6, 7 y 8, del presente Reglamento, los Estados miembros designarán como autoridades de vigilancia del mercado** a efectos del presente Reglamento bien **a las autoridades de control encargadas de la protección de datos competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680**, bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680. Las actividades de vigilancia del mercado no afectarán en modo alguno a la independencia de las autoridades judiciales ni interferirán de otro modo en sus actividades en el ejercicio de su función judicial."

Aplicable a partir del 2 de agosto de 2026.

En la definición 26 del artículo 3, el RIA define a las autoridades de vigilancia de mercado con una remisión al Reglamento 2019/1020: "la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020". Además, tal y como dispone el considerando 156 del RIA, estas autoridades deben disponer de todos los poderes de ejecución establecidos en el RIA y en el RVM.

Según el artículo 3.4 del Reglamento 2019/1020, la autoridad de vigilancia del mercado se define como "la autoridad designada por un Estado miembro, de conformidad con el artículo 10, responsable de efectuar la vigilancia del mercado en el territorio de ese Estado miembro". En el mismo artículo 3, la vigilancia del mercado se define como las actividades y medidas adoptadas por estas autoridades para garantizar que los productos cumplan los requisitos de la legislación de armonización de la Unión y velen por la protección del interés público amparado por esta legislación. Esta concepción contrasta con la naturaleza de las autoridades de control de protección de datos, que según el artículo 51 del RGPD, supervisan la aplicación del Reglamento para salvaguardar los derechos y libertades fundamentales en relación con el tratamiento de datos y facilitar la libre circulación de estos datos en la UE.

A priori, pues, aunque parezca que las autoridades de vigilancia del mercado y las autoridades de protección de datos responden a lógicas distintas, no puede perderse de vista la estrecha relación entre IA y datos personales. Por tanto, el artículo 74.8 del RIA, que insta (u obliga) a los Estados miembros a designar como autoridades de vigilancia del mercado de IA a las autoridades de protección de datos u otros órganos que cumplan unas condiciones determinadas, parece un acierto. Además, el Comité Europeo de Protección de Datos, en la "Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial", pone de manifiesto la adecuación de esta designación, dado que las autoridades de protección de datos ya tienen experiencia y conocimientos especializados. Esta designación debe venir acompañada de los recursos económicos y humanos necesarios para asegurar una implementación efectiva.[17]

Aunque no se analizará en este trabajo, debe tenerse presente que el RIA confiere a las AVM una serie de poderes y funciones que podrían asimilarse a los recogidos en el RGPD, ya que, aunque no se categoricen de este modo, se pueden identificar poderes de investigación, poderes correctores y poderes de autorización y consultivos. A modo de ejemplo, en relación con los poderes de investigación, el RIA (y el RVM) regula diferentes tipos de accesos a información y documentación determinada. Algunos ejemplos concretos relativos a posibles solicitudes de accesos a información o documentación que tendrán las AVM[18] son los siguientes:

[17] En este sentido, es interesante mencionar el artículo 15 del RVM, que dictamina que los Estados miembros pueden autorizar a las AVM a reclamar a los operadores económicos pertinentes la totalidad de los costes de sus actividades, en relación con casos de incumplimientos.

[18] Este listado no comprende todos los accesos y solo es ilustrativo.

- Declaración UE de conformidad (art. 18.1.*e* y art. 47 RIA).[19]
- Información y documentación según el RVM (art. 14.4 RVM).
- Información y documentación de sistemas de IA de alto riesgo (art. 18.1.*a*, art. 21, art. 22.3.*c*, art. 23.6, art. 26.6, art. 74.13 y art. 75.3 RIA).
- Documentación de las autoridades garantes de cumplimiento del Derecho, de inmigración o de asilo, cuando sean proveedoras de sistemas de IA de alto riesgo (art. 78.2 y 3 RIA).
- Información de sistemas de IA de uso general (art. 53.1.*a*, art. 54.3.*b* RIA y art. 75.3 RIA).
- Documentación del sistema de gestión de la calidad (art. 18.1.*b* y art. 17 RIA).
- Modificaciones y decisiones de los organismos notificados (art. 18.1.*c* y art 18.1.*d* RIA).
- Base de datos de la UE (art. 49.4 RIA).

Es importante destacar que, en virtud del artículo 58.1.*e* del RGPD, las autoridades de protección de datos ya disponen del poder de obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a la información necesaria para desempeñar sus funciones de supervisión y control.

Una conclusión que puede extraerse de que una autoridad de protección de datos sea designada como AVM es que las principales novedades no se encuentran tanto en el acceso a la información —ya previsto en el RGPD y reforzado por el considerando 157 del RIA—, sino en la posibilidad de imponer sanciones en virtud del RIA y de organizar espacios de pruebas (*sandboxes*) en el sentido del artículo 57 del mismo reglamento, con las consecuencias específicas que esto conlleva.

En cuanto al acceso a la información, la cuestión relevante no es tanto si pueden acceder, sino con qué fundamento jurídico legitiman su solicitud de acceso en cada caso concreto o con qué finalidad acceden (por ejemplo, investigación/sanción según el RIA o según el RGPD).

[19] El anexo V del RIA establece los elementos que debe contener, como mínimo, la declaración UE de conformidad: (i) Los datos identificativos del sistema de IA: nombre, tipo y cualquier referencia unívoca que permita trazar el producto; (ii) El nombre y la dirección del proveedor o de su representante autorizado; (iii) La afirmación de que la DUEC se expide bajo la responsabilidad exclusiva del proveedor; (iv) La declaración de conformidad con el RIA y, en su caso, con el resto de normativa de armonización de la Unión; (v) Cuando el sistema de IA implique tratamiento de datos personales, la declaración de conformidad con la normativa de protección de datos (RGPD, etc.); (vi) Las referencias a las normas armonizadas aplicadas o a la especificación común pertinente; (vii) El nombre y el número de identificación del organismo notificado que haya expedido el certificado, si lo hubiere, y la descripción del procedimiento de evaluación de la conformidad seguido; y (viii) El lugar y fecha de expedición, nombre, cargo y firma de la persona que expide la declaración en representación del proveedor.

2.7. Otras consideraciones

"Los importadores proporcionarán a las **autoridades competentes pertinentes**, previa solicitud motivada, toda la información y la documentación, incluidas las referidas en el apartado 5, que sean necesarias para demostrar la conformidad de un sistema de IA de alto riesgo con los requisitos establecidos en la sección 2 en una lengua que estas puedan entender fácilmente. A tal efecto, velarán asimismo por que la documentación técnica pueda ponerse a disposición de esas autoridades". (art. 23.6 RIA)

"Los importadores cooperarán con las **autoridades competentes pertinentes** en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo introducido en el mercado por los importadores, en particular para reducir y mitigar los riesgos que este presente". (art. 23.7 RIA)

"Previa solicitud motivada de una **autoridad competente pertinente**, los distribuidores de un sistema de IA de alto riesgo proporcionarán a esa autoridad toda la información y la documentación relativas a sus actuaciones con arreglo a los apartados 1 a 4 que sean necesarias para demostrar que dicho sistema cumple los requisitos establecidos en la sección 2". (art. 24.5 RIA)

"Los distribuidores cooperarán con las **autoridades competentes pertinentes** en cualquier medida que estas adopten en relación con un sistema de IA de alto riesgo comercializado por los distribuidores, en particular para reducir o mitigar los riesgos que este presente." (art. 24.6 RIA)

"Los responsables del despliegue cooperarán con las **autoridades competentes pertinentes** en cualquier medida que estas adopten en relación con el sistema de IA de alto riesgo con el objetivo de aplicar el presente Reglamento". (art. 26 12 RIA)

Conviene entender el concepto autoridades competentes pertinentes (*relevant competent authorities*, en su versión en inglés). Este concepto puede generar confusión (o incluso inseguridad jurídica), debido al calificativo competente utilizado para referirse a distintas autoridades. El RIA menciona: 'autoridades competentes', de manera aislada; y, posteriormente, de forma concreta en relación con otros calificativos como nacional, judiciales, pertinentes, públicas, etc. (por ejemplo, 'autoridades nacionales competentes'; autoridades judiciales competentes'; 'autoridades de vigilancia del mercado competentes'; 'autoridades competentes pertinentes'; 'autoridades competentes responsables de otras disposiciones del Derecho de la Unión y nacional'; 'autoridades públicas competentes'; 'autoridades nacionales competentes pertinentes').

En primer lugar, conviene matizar que es posible que, cuando el RIA mencione a la autoridad competente pertinente, no se refiera a la autoridad nacional competente definida en el artículo 3.48 del RIA como: "una autoridad notificante o una autoridad de vigilancia del mercado; en lo que respecta a sistemas de IA puestos en servicio o utilizados por instituciones, órganos y organismos de la Unión, las referencias hechas en el presente Reglamento a autoridades nacionales competentes o a autoridades de vigilancia del mercado se interpretarán como referencias al Supervisor Europeo de Protección de Datos".

	Inglés	Español
Considerando 139 RIA	To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the AI regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. AI regulatory sandboxes established under this Regulation should be without prejudice to other law allowing for the establishment of other sandboxes aiming to ensure compliance with law other than this Regulation. Where appropriate, **relevant competent authorities** in charge of those other regulatory sandboxes should consider the benefits of using those sandboxes also for the purpose of ensuring compliance of AI systems with this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world conditions may also be operated and supervised in the framework of the AI regulatory sandbox.	Para garantizar una aplicación uniforme en toda la Unión y conseguir economías de escala, resulta oportuno establecer normas comunes para la creación de espacios controlados de pruebas para la IA, así como un marco para la cooperación entre las autoridades pertinentes implicadas en la supervisión de dichos espacios. Los espacios controlados de pruebas para la IA establecidos en virtud del presente Reglamento deben entenderse sin perjuicio de otros actos legislativos que permitan el establecimiento de otros espacios controlados de pruebas encaminados a garantizar el cumplimiento de actos legislativos distintos del presente Reglamento. Cuando proceda, las **autoridades competentes pertinentes** encargadas de esos otros espacios controlados de pruebas deben ponderar las ventajas de utilizarlos también con el fin de garantizar el cumplimiento del presente Reglamento por parte de los sistemas de IA. Previo acuerdo entre las autoridades nacionales competentes y los participantes en el espacio controlado de pruebas para la IA, las pruebas en condiciones reales también podrán gestionarse y supervisarse en el marco del espacio controlado de pruebas para la IA.
Art. 57.10 RIA	***National competent authorities*** shall ensure that, to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data, the national data protection authorities and those **other national or competent authorities** are associated with	Las **autoridades nacionales competentes** velarán por que, en la medida en que los sistemas innovadores de IA impliquen el tratamiento de datos personales o estén comprendidos dentro del ámbito de supervisión de otras autoridades nacionales o autoridades competentes que proporcionen o respalden el acceso a los datos, las autoridades nacionales de protección de datos y las **demás autoridades**

	the operation of the AI regulatory sandbox and involved in the supervision of those aspects to the extent of their respective tasks and powers.	**nacionales o competentes** estén ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de dichos aspectos en la medida en que lo permitan sus respectivas funciones y competencias.

A partir de la comparación entre los diferentes preceptos del RIA, se puede observar que el concepto de *autoridad nacional competente* está definido específicamente en el artículo 3.48 del RIA, mientras que el término de *autoridad competente pertinente* aparece en otros apartados del RIA, como el considerando 139, sin una definición clara y cerrada. Esta distinción es fundamental para comprender su ámbito de aplicación y sus posibles implicaciones jurídicas.

El artículo 3.48 delimita el concepto de autoridad nacional competente como una autoridad notificadora o autoridad de vigilancia del mercado; en cambio, en el caso de los sistemas de IA utilizados por instituciones, órganos y organismos de la Unión, se refiere al Supervisor Europeo de Protección de Datos. Esto sugiere que este tipo de autoridad tiene un ámbito claramente delimitado y vinculado, principalmente, a la supervisión del mercado y a la notificación de sistemas de IA.

Por otra parte, el considerando 139 introduce el concepto de autoridad competente pertinente e indica que este tipo de autoridad está implicada en la supervisión de los espacios controlados de pruebas para IA. Este considerando hace también referencia a la cooperación entre diferentes autoridades en la supervisión de estos espacios, incluidas las que puedan tener competencias en otras normativas más allá del RIA. Esto podría indicar que las autoridades competentes pertinentes tienen un alcance más amplio y pueden incluir a organismos con funciones de supervisión en otros ámbitos normativos, como la protección de datos, la seguridad o los derechos fundamentales; o, simplemente, en referencia a otras normativas armonizadas que regulan otros productos relacionados con la vigilancia de mercado.

Por ejemplo, en referencia al artículo 26, los responsables del despliegue tienen la obligación de cooperar con las autoridades competentes pertinentes, en cualquier medida relacionada con el uso de los sistemas de IA de alto riesgo, con el objetivo de garantizar la aplicación del RIA. El artículo 26 no menciona explícitamente a las autoridades de protección de datos como 'competentes pertinentes' al efecto; sin embargo, a partir de lo expuesto previamente en el apartado 2.4 de este trabajo y respecto del contenido general de la norma, una hipótesis/conclusión preliminar a la que se puede llegar es que estas autoridades también podrían formar parte, especialmente en relación con el uso de sistemas de identificación biométrica remota en diferido, dado su papel clave en la supervisión de este tipo de tratamientos (como se ha analizado en los apartados previos).

Esta obligación de cooperación no figuraba en la propuesta original de la Comisión, sino que aparece por primera vez en la versión del Consejo y posteriormente, con algunas modificaciones, en las enmiendas introducidas por el Parlamento. Sin embargo, el artículo 26.12 no detalla en qué debe consistir exactamente esta cooperación. Se pueden considerar diversas posibilidades, como la obligación de facilitar a las autoridades competentes pertinentes el acceso a los registros generados automáticamente por los sistemas de IA de alto riesgo (de acuerdo con lo que prevé, por ejemplo, el artículo 21.2 del RIA, que utiliza el concepto de autoridad competente en lugar de autoridad nacional competente), o bien de suministrar cualquier otra información bajo su control.

Si las autoridades de protección de datos se consideran como autoridades competentes pertinentes, como se apuntaba previamente, esta nueva obligación se alinea con las estipulaciones del RGPD, donde ya se exige que los responsables y encargados del tratamiento cooperen con las autoridades de control. Así, se consolida un marco de supervisión y colaboración esencial para abordar los retos y riesgos asociados a los sistemas de IA de alto riesgo. Tal y como se dispone en el artículo 31 del RGPD, el responsable y el encargado del tratamiento, y en su caso sus representantes, deben cooperar en el desempeño de las funciones de la autoridad de control que lo solicite, y esta es una cuestión valorable en un procedimiento sancionador (art. 83.2.*f*. RGPD y 99 RIA).

3. El nuevo rol de las autoridades de protección de datos como autoridades de derechos fundamentales

Daniel Duro Millan

Cuando hablamos de protección de datos, no solo hablamos de riesgos y beneficios, sino también de derechos fundamentales, siendo el derecho a la protección de datos uno de los más afectados por la inteligencia artificial. Prueba de ello es la designación del Supervisor Europeo de Protección de Datos como supervisor del RIA, así como las diversas guías, recomendaciones y planes de acción publicados en los últimos años por diversas autoridades de protección de datos (APD), tales como la APDCAT, la AEPD, la CNIL o el ICO, entre otros, en los que ya se alertaba sobre los riesgos que podía llegar a conllevar la IA.[20]

Consecuentemente, a la hora de publicar el listado de autoridades encargadas de proteger los derechos fundamentales (APDF), en virtud de la obligación impuesta en el artículo 77.2 del RIA, el Estado español ha designado, entre un largo listado, a tres APD:[21] la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos y el Consejo de Transparencia y de Protección de Datos de Andalucía. No obstante, sorprende la ausencia de la Autoridad Vasca de Protección de Datos en este listado, especialmente teniendo en cuenta que se han incluido las otras dos autoridades autonómicas existentes.[22]

La designación de las APDF efectuada en muchos Estados miembros, incluido el Estado español, no ha cubierto de forma exhaustiva y concreta todos los derechos fundamentales mencionados en el RIA. Es decir, no se prevé la designación de organismos *ad hoc* para la protección de ciertos derechos fundamentales. Un ejemplo destacado es el derecho a la no discriminación que, aunque el artículo 77.1 del RIA lo cita explícitamente y que cuenta con organismos para protegerlo,[23] en la lista de nombramientos no aparece ningún organismo que lo supervise. Esto contrasta con otros derechos fundamentales, como el de la

---

[20] Autoridad Catalana de Protección de Datos (APDCAT). *Inteligencia artificial. Decisiones Automatizadas en Cataluña.* 2020. [en línea] Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/intelligencia_artificial/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf

Agencia Española de Protección de Datos (AEPD). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción,* 2020. [en línea] Disponible en: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf

Commission Nationale de l'Informatique et des Libertés (CNIL). *Artificial intelligence: the action plan of the CNIL,* 2023. [en línea] Disponible en: https://www.cnil.fr/en/artificial-intelligence-action-plan-cnil

Information Comissioner's Office (ICO). *Guidance on AI and Data Protection,* Actualitzado en mayo de 2023. [en línea] Disponible en: ico.org.uk/media2/ga4lfb5d/guidance-on-ai-and-data-protection-all-2-0-38.pdf

[21] Secretaría de Estado de Digitalización e Inteligencia Artificial. *Authorities protecting fundamental rights | Spain.* 2024. [en línea] Disponible en: https://digital.gob.es/dam/es/portalmtdfp/DigitalizacionIA/AuthoritiesFundamentalRights-Spain.pdf

[22] La Autoridad Vasca de Protección de Datos no se encuentra nombrada como APDF en la fecha de publicación de este trabajo.

[23] Como en Cataluña, la Oficina d'Igualtat de Tracte i No-discriminació.

protección de datos personales que, como se ha apuntado, tiene asignadas tres de las cuatro autoridades existentes en el Estado español.

En este contexto, en el que varias APD han sido designadas como APDF, es fundamental entender qué implica esta designación. No se trata exclusivamente de un cambio nominal, sino de la adquisición de nuevas competencias, poderes y responsabilidades.

Desde el momento de designación como APDF, el trabajo proactivo debe permitir que, llegado el 2 de agosto de 2026, en que el RIA será aplicable,[24] las autoridades de protección de datos como la APDCAT hayan podido adaptar internamente sus estructuras, formar a su personal y establecer los protocolos internos necesarios para ejercer óptimamente, desde un inicio, las competencias derivadas de los artículos 73.7, 77, 79.2 y 82.1 del RIA.

Un ejemplo de este trabajo proactivo es el modelo pionero en Europa que recientemente ha publicado la APDCAT, para la evaluación de impacto sobre los derechos fundamentales en el uso de inteligencia artificial (EIDF).[25] Citando el mismo documento, se trata de un modelo que aspira a convertirse en una herramienta eficaz para desarrollar soluciones de IA fiables y centradas en el ser humano, diseñada para concretar las nuevas obligaciones establecidas por el RIA. Esta iniciativa difiere de otras metodologías aprobadas últimamente, como es el caso de HUDERIA,[26] publicada a finales de 2024 por el Consejo de Europa, ya que la propuesta catalana concreta la implementación de las variables, la gestión de los parámetros y explora la aplicación práctica del modelo mediante cuatro casos de uso reales.

Así pues, en los siguientes apartados se analizan las principales competencias que el RIA otorga a las APD nombradas como APDF, prestando especial atención a la convergencia de estas competencias con las que tienen atribuidas en virtud del RGPD.

3.1. Acceso a documentación creada o conservada de conformidad con el RIA, necesaria para cumplir su mandato (art. 77.1 RIA)

"Las autoridades u organismos públicos nacionales encargados de supervisar o hacer respetar las obligaciones contempladas en el Derecho de la Unión en materia de protección de los derechos fundamentales, incluido el derecho a la no discriminación, con respecto al uso de sistemas de IA de alto riesgo mencionados en el anexo III tendrán 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

[24] Sin embargo, el artículo 6.1 y las obligaciones correspondientes del RIA son aplicables a partir del 2 de agosto de 2027 (art. 113.*c* RIA).

[25] APDCAT. *Modelo para la EIDF: guía y casos de uso. Metodología aplicada de la evaluación de impacto sobre los derechos fundamentales en el diseño y desarrollo de la IA.* 2025. [en línea] Disponible en: https://apdcat.gencat.cat/ca/documentacio/intelligencia_artificial/

[26] Consejo de Europa, *Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (HUDERIA METHODOLOGY)* 2024. [en línea] Disponible en: https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f

documentación sea necesario para el cumplimiento efectivo de sus mandatos, dentro de los límites de su jurisdicción (...)".

Aplicable a partir del 2 de agosto de 2026.

El artículo 77.1 del RIA establece la facultad a las APDF de: (i) solicitar el acceso a cualquier documentación creada o conservada de acuerdo con el RIA; (ii) relativa a los sistemas de IA enumerados en el anexo III; y (iii) cuando este acceso sea necesario para cumplir el mandato de la autoridad, dentro de su jurisdicción. Por tanto, para que una APDF pueda solicitar documentación es necesario cumplir tres requisitos.

En primer lugar, la documentación que se podrá solicitar será la "creada o conservada con arreglo al presente Reglamento". Esto implica que las APDF pueden solicitar toda la documentación que el RIA prevé que los operadores deben crear o conservar, para permitir un adecuado seguimiento de los SIA de alto riesgo enumerados en el anexo III. Algunos ejemplos son los artículos 11, 12 y 13 del RIA.

En segundo lugar, la documentación que se solicita debe ser relativa a sistemas de IA de alto riesgo recogidos en el anexo III. Cabe destacar que, según el artículo 6 del RIA, los sistemas incluidos en el anexo III no son los únicos que el RIA reconoce como alto riesgo. Por tanto, las APDF solo pueden solicitar documentación relativa a un número concreto de sistemas de IA de alto riesgo. Sin embargo, debe tenerse en cuenta que cuando una APD sea a la vez APDF, al haber sido nombrada como tal en virtud del artículo 77.2 del RIA, puede acceder a cualquier documentación necesaria para asegurar que se cumple el RGPD, de acuerdo con el considerando 157 del RIA y el artículo 58.1 del RGPD. Así, las APD pueden acceder a cualquier documentación para ejercer sus funciones de acuerdo con el RGPD cuando un SIA, aunque no esté incluido en el anexo III, conlleve el tratamiento de datos personales. Por tanto, la circunscripción de acceso a la documentación enmarcada en el anexo III afectará a las APDF que no tengan una vía alternativa de acceso a documentación, más allá de la habilitación del artículo 77.1 del RIA.

En cualquier caso, en lo que se refiere a los SIA sobre los que las APDF pueden solicitar documentación en virtud del artículo 77.1 del RIA, el artículo 6 establece las normas generales para clasificar los sistemas de IA como sistemas de alto riesgo; por su parte, el anexo III enumera ámbitos y casos de usos específicos de sistemas de IA que deben ser considerados de alto riesgo, con diferentes excepciones asociadas. Esta clasificación ha sido objeto de numerosos debates y negociaciones durante la tramitación del proyecto normativo, hasta su versión final (Muñoz Vela 2024).

Los sistemas de IA de alto riesgo recogidos en el anexo III incluyen aplicaciones en ámbitos especialmente sensibles, como la biometría (identificación, categorización o reconocimiento de emociones), infraestructuras críticas, educación, empleo, acceso a servicios esenciales, cumplimiento normativo, migración y control fronterizo y administración de justicia y procesos democráticos.

La confección de la lista de sistemas de IA de alto riesgo incluidos en el anexo III, más allá de la clasificación general que hace el artículo 6 del RIA para determinar cuándo un SIA

debe ser considerado de alto riesgo, responde a un trabajo de la Comisión basado en la determinación de qué SIA generaban un alto riesgo para la salud, la seguridad o los derechos fundamentales de las personas (Muñoz Vela 2024). Así se recoge en el considerando 46 del articulado final del RIA y se justifica en el considerando 157, al establecer la necesidad de un procedimiento de salvaguarda específico para garantizar una ejecución adecuada y oportuna frente a SIA que presenten un riesgo para la salud, seguridad o derechos fundamentales.

Por la afectación que puede implicar a las competencias de las APDF, cabe señalar que, de acuerdo con los artículos 7 y 97 del RIA, la Comisión tiene la facultad de adoptar actos delegados para modificar o añadir casos de uso de SIA en el anexo III. A este respecto, la lista de SIA sobre los que las APDF pueden solicitar documentación, así como sobre los que pueden solicitar motivadamente la organización de pruebas, como se verá en el apartado 3.3 de este trabajo, podría variar en el futuro.

Esta decisión de dejar abierta la posibilidad de modificar o desarrollar contenido del articulado del RIA no es exclusiva para el anexo III, sino que, de acuerdo con el artículo 96 del RIA, se prevé que la Comisión elabore directrices sobre la aplicación práctica del RIA, como ha hecho recientemente con las directrices relativas a SIA prohibidos.[27] Esta fórmula debe permitir que, en un ámbito tan cambiante como la IA, en la medida de lo posible se pueda regular a la velocidad a la que evoluciona la tecnología.

El ejemplo más paradigmático, mencionado en la introducción de este informe, es la incorporación del concepto de modelos y sistemas de IA de uso general a raíz de la aparición de ChatGPT, que supusieron la adaptación del proyecto de articulado del RIA para incluir la regulación específica de estos SIA dentro del reglamento.

El último requisito a cumplir para que las APDF puedan ejercer la facultad reconocida en el artículo 77.1 del RIA es la fundamentación de la solicitud de acceso a documentación en el "cumplimiento efectivo de sus mandatos". Esto implica que cada organismo designado como APDF por un Estado miembro de la UE puede solicitar documentación relativa a SIA que suponga un riesgo para el derecho o los derechos fundamentales que protegen en relación con el anexo III. En este caso, es evidente que las APD, como la APDCAT, se enmarcan en la protección del derecho fundamental a la protección de datos personales, y del conjunto de derechos y libertades que puedan verse afectados por los tratamientos de datos.

En relación con el papel de las APD en el marco del RIA, como se ha advertido en el apartado 2.7 de este trabajo, el Reglamento prevé en el artículo 74.8 que las APD se conviertan en AVM en relación con los SIA recogidos en el anexo III. En este sentido, en la "Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial", el Comité Europeo de Protección de Datos se ha

[27] European Comission. *Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).* 2025. [en línea] Disponible en: https://digital-strategy.ec.europa.eu/en/library/la-comisión-publica-directrices-prohibited-artificial-intelligence-ai-practices-defined-ai-act

pronunciado positivamente respecto a esta posibilidad, poniendo de relieve el papel de las autoridades de protección de datos en la supervisión de estos sistemas. Esta cuestión resulta especialmente relevante —como se observará en los siguientes apartados de este trabajo—, puesto que las funciones y poderes asignados a las APDF, principalmente orientados al análisis documental en el marco de la potestad de investigación y evaluación, están estrechamente vinculados a las facultades ejecutivas otorgadas a las AVM.

En este contexto, aunque ya se conocen los organismos que el Estado español ha designado como APDF, todavía falta el pronunciamiento oficial sobre cuál o cuáles lo serán como AVM.[28] Esta designación, a diferencia de las APDF, no es preceptiva hasta el 2 de agosto de 2025. Por consiguiente, es necesario tener presente la posibilidad de que las APD puedan asumir simultáneamente los roles de APDF y AVM.

Volviendo al artículo 77.1 del RIA, como deber de los operadores se especifica que la documentación a la que pueden solicitar acceso las APDF debe transmitirse en un lenguaje y formato accesibles para los sujetos requeridos. Esta exigencia responde a uno de los principales retos de fiscalización de la IA: poder comprender los procesos que generan los resultados, así como los datos utilizados, como elemento esencial de transparencia. En este mismo sentido ya se pronunciaba un informe de la Agencia Europea de Derechos Fundamentales (FRA) del año 2021, que analizaba los principales eventos en el ámbito de los derechos fundamentales dentro de la UE y destacaba tanto los progresos realizados como las dificultades que todavía persistían.[29] Concretamente, el dictamen 6.4 del informe de la FRA trata de la posible introducción de herramientas de IA dentro de la UE, para mejorar las decisiones en asuntos de fronteras, asilo e inmigración, y señala que la falta de transparencia en relación con los datos utilizados podría dificultar que las personas afectadas pudieran refutar los resultados obtenidos por estas herramientas.

Por último, al analizar el artículo 77.1 del RIA desde la óptica de la protección de datos personales, se evidencia la semejanza con el artículo 58.1.*a* del RGPD, cuando prevé para las autoridades de protección de datos el poder "de ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones". Sin embargo, se observan tres diferencias entre ambos artículos.

- En primer lugar, el artículo 58.1.*a* del RGPD especifica claramente los sujetos a los que puede dirigirse la autoridad de protección de datos para solicitar información; en cambio, el RIA solo contempla la posibilidad de solicitar documentación, sin indicar si los destinatarios podrían ser todos los sujetos que el artículo 3.8 del RIA cataloga como operadores. Sin embargo, la lógica hace pensar que las APDF podrán solicitar

[28] En marzo de 2025 se ha presentado el Anteproyecto de ley para el buen uso y la gobernanza de la inteligencia artificial, que debe concretar esta cuestión; sin embargo, hasta que se publique el texto final no se conocerá con certeza el listado de autoridades designadas.

[29] Agencia de la Unión Europea por los Derechos Fundamentales (FRA). Informe sobre los derechos fundamentales, 2021. [en línea] Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-fundamental-rights-report-2021-opinions_es.pdf

documentación a cualquier operador del RIA que posea la documentación necesaria para el efectivo cumplimiento de su mandato, dentro de los límites de su jurisdicción.

- En segundo lugar, y como se analizará en el siguiente apartado, mientras que las autoridades de control de protección de datos no deben comunicar sus peticiones de información a ningún otro organismo, las APDF están obligadas a notificar sus solicitudes de acceso a documentación a las AVM.

- Por último, las APD pueden solicitar cualquier información requerida para cumplir sus funciones. Por el contrario, la documentación que pueden solicitar las APDF debe circunscribirse a SIA de alto riesgo enumerados en el anexo III.

Estas tres diferencias no se aprecian si, en lugar de comparar el artículo 58.1.*a* del RGPD con el artículo 77.1 del RIA, se sustituye este último por el artículo 14.4.*a* del RVM, que recoge el poder de las AVM de exigir documentación a los operadores. Así, las AVM pueden exigir cualquier documentación, sin tener que notificarlo a ninguna otra autoridad y sin limitar los productos respecto de los que pueden ejercer este poder.

Esta comparativa evidencia la diferencia entre los poderes de investigación con los que cuentan las APD en virtud del RIA y el RGPD, en el marco de sus respectivas competencias y roles, en comparación con los de las AVM. Esta diferencia se acentúa si se comparan los poderes ejecutivos con los de las APDF y AVM, como se expone en los siguientes apartados de este trabajo.

En este contexto, y como se reitera a lo largo del documento, es importante tener en cuenta que los poderes que el RIA otorga a las APDF son independientes de los que ya disponen las APD en virtud del RGPD. Esto comporta que las competencias adquiridas como APDF no puedan limitar las que ya se ejercen de acuerdo con el RGPD, tal y como establece el artículo 2.7 del RIA.

3.2. Informar a la autoridad de vigilancia del mercado de solicitudes de documentación creada o conservada de conformidad con el RIA, necesaria para cumplir su mandato (art. 77.1 RIA)

"(...) 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".

Aplicable a partir del 2 de agosto de 2026.

En cumplimiento del artículo 77.1 *in fine*, en ejercicio de la facultad de acceso a documentación que se desarrolla en el apartado 3.1 de este trabajo, las APDF deben informar a las AVM del Estado miembro correspondiente de las solicitudes de acceso a documentación que se hayan efectuado a los operadores.

Del articulado del precepto se desprende que el deber de informar no supone que sea necesaria la validación de la AVM para acceder a la documentación solicitada. Además, no se especifica el uso o servicio que esta notificación puede suponer para la AVM. Un

escenario razonable sería enmarcarlo dentro de la previsión del artículo 11.3 del RVM, que estipula que, a la hora de realizar comprobaciones de productos, las AVM deben aplicar un enfoque basado en el riesgo en el que, entre otros factores, hay que tener en cuenta la información proveniente de otras autoridades. En este contexto, se trataría de un mecanismo que ayudaría a las AVM a determinar qué SIA podrían suponer un riesgo para los DF y merecen ser evaluados. Esta previsión también podría conectarse con el artículo 79.2 del RIA, que estipula que, cuando las AVM tengan motivos suficientes para considerar que un SIA presenta un riesgo, de acuerdo con la definición del artículo 3.19 del RVM, es necesario evaluarlo.

Adicionalmente, la redacción final del RIA deja sin concretar otros aspectos de este deber, como la ausencia de un plazo específico para efectuar la notificación a la AVM, o la AVM a notificar, en caso de que haya más de una autoridad que podría ser considerada competente. A este respecto, el RIA no determina si siempre debe notificarse a una AVM del mismo estado, o bien, cuando el operador tenga el establecimiento principal en otro Estado miembro, a la AVM de ese estado.

En contraste, el considerando 36 del RGPD delimita el concepto de establecimiento principal del responsable y encargado de tratamiento, que después se usa en el artículo 56 para determinar la competencia de la autoridad de control principal. Además, el dictamen 4/2024 del CEPD[30] delimita exhaustivamente el concepto de establecimiento principal de un responsable del tratamiento, de acuerdo con el RGPD.

Adicionalmente, conviene mencionar que en el capítulo VII del RGPD se recoge el mecanismo de coherencia para la cooperación entre autoridades de protección de datos. Queda pendiente, por tanto, desarrollar el RIA en este ámbito, para que proporcione la misma seguridad jurídica que ofrece el RGPD.

3.3. Solicitud de pruebas de los sistemas de IA de alto riesgo y colaboración en la organización de las pruebas (art. 77.3 RIA)

"Cuando la documentación mencionada en el apartado 1 no baste para determinar si se ha producido un incumplimiento de las obligaciones previstas en el Derecho de la Unión en materia de protección de los derechos fundamentales, la autoridad u organismo público a que se refiere el apartado 1 podrá presentar una solicitud motivada a la autoridad de vigilancia del mercado para organizar pruebas del sistema de IA de alto riesgo a través de medios técnicos. La autoridad de vigilancia del mercado organizará las pruebas con la

[30] EDPB. *Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR*. 13 de febrero de 2024. [en línea] Disponible en: https://www.edpb.europa.eu/system/files/2024-02/edpb_opinion_202404_mainestablishment_en.pdf#:~:text=The%20French%20Supervisory%20Authority%20requested%20the%20European%20Data,mechanism%2C%20in%20particular%20regarding%20the%20notion%20of%20controll

estrecha colaboración de la autoridad u organismo público solicitante en un plazo razonable tras la presentación de la solicitud".

Aplicable a partir del 2 de agosto de 2026.

El considerando 139 del RIA desarrolla el concepto de espacio controlado de pruebas de sistemas de IA. Este recoge el deber de cooperación entre las autoridades nacionales competentes que establezcan espacios controlados de pruebas de IA, con otras autoridades, como las APDF ("cooperar con otras autoridades pertinentes, incluidas las que supervisen la protección de los derechos fundamentales").

En este contexto, y teniendo en cuenta que en el RIA no se recoge ninguna otra situación en la que las APDF pueden participar en el espacio controlado de pruebas, el análisis de este artículo parte de la premisa de que, cuando el artículo 77.3 del RIA establece que las APDF pueden presentar una solicitud motivada a la AVM para organizar pruebas de SIA de alto riesgo a través de medios técnicos, se puede entender que se refiere a la organización de pruebas en un espacio controlado de pruebas. Sin embargo, no puede descartarse que el legislador del RIA, al referirse a "organizar pruebas del sistema de IA de alto riesgo a través de medios técnicos", no esté haciendo referencia a los espacios controlados de pruebas de IA.

Hecha esta consideración previa, el artículo 77.3 del RIA expone que si, con la documentación solicitada en virtud del artículo 77.1 del RIA, una APDF no puede determinar si se ha producido un posible incumplimiento del Derecho de la Unión en materia de protección de los derechos fundamentales, se prevé un segundo mecanismo de verificación de adecuación: la solicitud motivada a la AVM para organizar pruebas del sistema de IA objeto de investigación. A pesar de no encontrarse explícitamente estipulado, se deduce que la AVM tendrá la potestad de aceptar o denegar la organización de las pruebas. En este sentido, carece de concreción en relación con los motivos o requisitos que debe cumplir la solicitud, para poder ser aceptada o denegada.

Una cuestión que el precepto no concreta es el alcance del concepto *estrecha colaboración* con que las AVM y las APDF deben organizar las pruebas. Así, si bien queda claro que la APDF es quien solicita la organización de pruebas de sistemas en la AVM, no se especifica cómo debe materializarse la colaboración a la hora de organizarlas. En cualquier caso, queda claro que el objetivo es completar la investigación iniciada por la APDF en virtud del artículo 77.1 del RIA, cuando con la documentación solicitada no haya podido determinarse si se ha producido un incumplimiento de las obligaciones de la UE en materia de protección de los DF. Asimismo, puede que el acceso a la documentación regulado en el artículo 77.1, y la posterior organización de pruebas, sea relativa a un SIA que, aparte de ser de alto riesgo del anexo III, suponga un riesgo de acuerdo con el artículo 79.1 del RIA. En este supuesto, la organización de las pruebas podría vincularse con la evaluación de SIA regulada en el artículo 79.2.

Adicionalmente, el artículo añade que la organización de pruebas debe producirse en un plazo razonable desde que se presentó la solicitud. Se infiere que el legislador no concreta el plazo, ya que se busca dotar de flexibilidad a las autoridades teniendo en cuenta variables

como la magnitud y complejidad de la prueba que deba organizarse, así como los recursos que se tengan que invertir. Sin embargo, al menos queda pendiente establecer un plazo máximo para asegurar la viabilidad de las investigaciones de las APD, en el marco de sus competencias atribuidas por el RGPD.

En este punto, cabe mencionar el artículo 57.10 del RIA, desarrollado en el apartado 2.6 de este trabajo, relativo al rol de las APD en los espacios de pruebas. De acuerdo con este artículo, las APD deben estar ligadas al funcionamiento de los espacios controlados de pruebas para los SIA que traten datos personales, así como involucradas en su supervisión.

Esto implica que el RIA prevé que las APD, por el simple hecho de serlo, tienen potestad para actuar en la supervisión de los espacios controlados de prueba de sistemas de IA, aunque el articulado del RIA tampoco concreta esta actuación. Así pues, el valor añadido que se otorga con el nombramiento como APDF es la facultad de presentar solicitudes motivadas a las AVM, para organizar pruebas en los casos en que la APDF lo considere necesario, de acuerdo con lo que prevé el artículo 77.3.

Este último matiz es relevante, puesto que esta extensión no es aplicable a los SIA sobre los que se puede solicitar la organización de pruebas, aunque en el apartado 3.1 de este trabajo se explica que, por las competencias que les otorga el RGPD, las APDF que sean a la vez APD pueden acceder a cualquier documentación, y no solo a la relativa a SIA incluidos en el anexo III. Esto es así porque el artículo 77.3 dispone que las APDF pueden solicitar la organización de pruebas respecto de los SIA a los que pueden solicitar documentación en virtud del artículo 77.1 del RIA. Es decir, respecto a los SIA de alto riesgo enumerados en el anexo III y no de cualquier SIA que trate datos personales.

Por último, aunque no se analizará, conviene mencionar que el tercer apartado del artículo 57 del RIA otorga al Supervisor Europeo de Protección de Datos, que es a la vez Supervisor del RIA, la potestad de establecer un espacio controlado de pruebas para las instituciones, órganos y organismos de la UE; también, que puede desempeñar las mismas funciones que las autoridades nacionales competentes en esta materia.

3.4. Ser informadas de la recepción de notificaciones a la AVM sobre incidentes graves a lo que se refiere el artículo 3.49.*c* del RIA (art. 73.7 RIA)

"Tras la recepción de una notificación relativa a un incidente grave a que se refiere el artículo 3, punto 49, letra c), la autoridad de vigilancia del mercado pertinente informará a las autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1. La Comisión elaborará orientaciones específicas para facilitar el cumplimiento de las obligaciones establecidas en el apartado 1 del presente artículo. Dichas orientaciones se publicarán a más tardar el 2 de agosto de 2025 y se evaluarán periódicamente".

Aplicable a partir del 2 de agosto de 2026.

El artículo 3.49.*c* del RIA define el incidente grave como aquel incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga como

consecuencia el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales. Si se produce un incidente grave de estas características, el artículo 73.7 del RIA establece que la AVM debe notificarlo a la APDF correspondiente.

Aunque el artículo 73.7 del RIA no especifica qué uso deben hacer las APDF de las notificaciones de incidentes graves, puede interpretarse que esta notificación está vinculada a las potestades que tienen reconocidas en el artículo 77.1 del RIA para cumplir su mandato y vinculadas a su jurisdicción. Este enlace permitiría a las APDF que son APD ejercer sus funciones para investigar y garantizar la protección de los derechos fundamentales afectados por el incidente (concretamente, el derecho a la protección de datos), así como abrir una investigación contra el operador (cuando también actúe como responsable o encargado del tratamiento), en caso de falta de notificación de violación de seguridad, si está obligado a hacerlo por el RGPD.

Desde la perspectiva de protección de datos, las notificaciones de incidentes graves previstas en el RIA siguen una estructura similar a las notificaciones de violación de seguridad (NVS) reguladas en los artículos 33 y siguientes del RGPD. Así, en ambos casos se trata de una notificación de un responsable del tratamiento u operador a la autoridad de control o vigilancia pertinente, para comunicar circunstancias que provocan el incumplimiento del RGPD o del RIA.

En este contexto, puede darse el caso de que un proveedor de SIA, que también sea responsable del tratamiento según el RGPD, sufra un incidente de seguridad que derive de un defecto del SIA; incidente que, a su vez, conlleve un riesgo para el derecho fundamental a la protección de datos personales. En este caso, la APD podría recibir la notificación por duplicado:

- En primer lugar, del proveedor, en virtud del artículo 33 del RGPD.
- En segundo lugar, de la AVM, de acuerdo con el artículo 73.7 del RIA, una vez que el proveedor del sistema de IA le hubiera notificado, de acuerdo con la obligación que le impone el artículo 73.1 del RIA.

Al respecto, hay académicos que consideran que los organismos que entren en el ámbito de aplicación de más de una norma de la UE pueden sufrir una sobrecarga de notificaciones. Para evitarlo, se han planteado posibles alternativas.

Una posibilidad es la exigencia a las APDF, que en calidad de APD reciben NVS de acuerdo con el RGPD, de notificar la violación de seguridad a las AVM, cuando sea consecuencia de un SIA de alto riesgo (Karathanasis 2024). Así pues, aplicando esta propuesta, cuando las APDF sean a la vez APD bajo el RGPD, las AVM no les notificarían los incidentes previstos en el artículo 3.49.*c* del RIA, como prevé el artículo 73.7 del RIA, sino que las propias APD remitirían a las AVM cualquier NVS relativa a sistemas de IA que pueda suponer un incidente grave. Este sistema de notificación se justifica en razón de la mayor probabilidad de que sean las APD las primeras en enterarse de las violaciones de seguridad, desde el punto de vista de la normativa de protección de datos, y de incidentes graves, en el sentido

del artículo 3.49.*c*, para el derecho fundamental a la protección de datos, desde el punto de vista del RIA.

Si bien, la justificación de esta propuesta no se encuentra desarrollada, podría deberse a los plazos que tanto el RGPD como el RIA prevén para las notificaciones respectivas. Así, mientras que el RGPD prevé que el responsable del tratamiento notifique al NVS en un plazo máximo de 72 horas, desde que tiene constancia de ello (art. 33.1), el RIA prevé un plazo no superior a 15 días para que los proveedores hagan la notificación a las AVM (art. 73.2), y no prevé el plazo en el que, después, la AVM debe notificarlo a la APDF (art. 73.7). Por tanto, en caso de que un operador, a la vez responsable del tratamiento, tuviera conocimiento de una vulneración del derecho fundamental a la protección de datos y lo notificara por las dos vías mencionadas, parece razonable pensar que la APD lo conociera antes. Sin embargo, el hecho de que el RIA y el RGPD supervisen materias tan distintas puede conllevar que, cuando un SIA sufra un incidente grave, que implique la vulneración de la normativa de protección de datos, los proveedores notifiquen a las AVM el incidente grave, pero no el NVS a las APD. En este sentido, junto con la disparidad en el plazo de notificación, hay que tener en cuenta que, si bien ambas notificaciones siguen un esquema similar, consistente en notificar a la autoridad pertinente una situación que vulnera su respectivo reglamento, existen otras diferencias primordiales en su naturaleza y finalidad.

La notificación de incidente grave se efectúa cuando un proveedor que introduce un SIA en el mercado de la Unión constate un incidente grave, de acuerdo con la definición que hace el artículo 3.49 del RIA. Así, este artículo contempla cuatro consecuencias del mal funcionamiento de un SIA que derivan en incidente grave: a) la muerte o perjuicio grave para la salud de una persona; b) la alteración grave e irreversible de la gestión o funcionamiento de infraestructuras críticas; c) el incumplimiento de las obligaciones en virtud del derecho de la Unión destinadas a proteger a los DF; y d) daños graves a la propiedad o el medioambiente. Cuando se produce una de estas situaciones, el proveedor lo notifica a la AVM en el plazo máximo de 15 días en general. Además, si el incidente deriva del caso *c*, adicionalmente la AVM debe notificarlo a la APDF en un plazo no establecido en el RIA.

De acuerdo con el artículo 73.8 del RIA, una de las principales consecuencias derivadas de la notificación del incidente grave es que, en un plazo no superior a 7 días desde la recepción de la notificación, las AVM deben adoptar las medidas recogidas en el artículo 19 del RVM. Estas son la facultad de recuperar o retirar el producto, entre otros que eviten la comercialización de productos que supongan un riesgo grave. Por su parte, el NVS se efectúa cuando un responsable del tratamiento constata una violación de seguridad en un tratamiento de datos personales, de acuerdo con la definición del artículo 4.12 del RGPD. Esta notificación cumple distintas funciones para las APD a las que se notifica. Por ejemplo, permite analizar el impacto en los derechos y libertades de los ciudadanos afectados, investigar si el organismo que ha sufrido la violación de seguridad cumple con la normativa y dispone de las medidas adecuadas para intentar evitarlo, así como solicitar o imponer medidas correctoras para mitigar el evento y otras posibles consecuencias.

Por tanto, en el contexto en el que una violación de seguridad en materia de protección de datos provenga de un SIA, es posible que el proveedor notifique el incidente a la AVM que supervisa el producto que el proveedor pretende comercializar (un SIA); pero puede que no

sea consecuente con su rol de responsable del tratamiento y no notifique la violación de seguridad, por ejemplo porque no ha adoptado un sistema de gobernanza integral del cumplimiento normativo. Por tanto, en los supuestos en que una violación de seguridad provenga de un SIA, es posible que la notificación prevista en el artículo 73.7 del RIA sea el único mecanismo de que dispongan las APD para tener conocimiento de ello.

En otro sentido, el plazo de 7 días recogido en el artículo 73.8 del RIA dificulta que, al encontrarnos con un incidente grave derivado del supuesto del artículo 3.49.*c* del RIA, las APDF dispongan de tiempo suficiente para evaluar el perjuicio del incidente para los DF y cooperar con las AVM para determinar las medidas más adecuadas a adoptar. Cabe decir que los apartados 3 y 4 del artículo 73 del RIA establecen dos supuestos en los que los plazos de notificación son más cortos, pero no conllevan ningún cambio significativo a la problemática planteada. En cualquier caso, no se ha previsto que la notificación del artículo 73.7 suponga la evaluación conjunta de la AVM y la ADPF del incidente, para determinar las medidas más adecuadas a tomar en virtud del artículo 73.8 del RIA. Sin embargo, parece razonable que, si el incidente grave lo es porque provoca que se incumplan las obligaciones en virtud de la UE destinadas a proteger a los DF, las autoridades encargadas de proteger estos derechos participen en la delimitación del alcance y las medidas más adecuadas para mitigar los efectos del incidente.[31]

Por último, considerando los plazos de notificación previstos en el RIA, si las APD se enteran de una violación de seguridad de protección de datos exclusivamente mediante una notificación de incidente grave, parece prudente pensar que, en la mayoría de las situaciones, esto conllevará una vulneración del plazo previsto en el artículo 33 del RGPD.

En resumen, si bien parece bastante posible que la notificación recogida en el artículo 73.7 del RIA produzca situaciones de duplicidad de notificaciones, también es un escenario a considerar que, sin la notificación de las AVM a las APDF, estas últimas no se enteren de muchas situaciones con potencial perjuicio para el derecho fundamental a la protección de datos, especialmente en los primeros años de aplicación del RIA.

3.5. Procedimiento aplicable a los sistemas de inteligencia artificial que "presentan un riesgo"

"Los sistemas de IA que presentan un riesgo se entenderán como «productos que presentan un riesgo», tal como se definen en el artículo 3, punto 19, del Reglamento (UE) 2019/1020, en la medida en que presenten riesgos que afecten a la salud, la seguridad o los derechos fundamentales de las personas". (art. 79.1 RIA)

"Cuando la autoridad de vigilancia del mercado de un Estado miembro tenga motivos suficientes para considerar que un sistema de IA presenta un riesgo mencionado en el apartado 1 del presente artículo, efectuará una evaluación del sistema de IA de que se trate

[31] En otros puntos del articulado del RIA, como el artículo 79.2, sí se regula la cooperación entre AVM y APDF cuando un SIA puede suponer un riesgo para los DF.

para verificar su cumplimiento de todos los requisitos y obligaciones establecidos en el presente Reglamento. Debe prestarse una especial atención a los sistemas de IA que presenten un riesgo para los colectivos vulnerables. Cuando se detecten riesgos para los derechos fundamentales, la autoridad de vigilancia del mercado informará también a las autoridades u organismos públicos nacionales pertinentes a que se refiere el artículo 77, apartado 1, y cooperará plenamente con ellos. Los operadores pertinentes cooperarán en lo necesario con la autoridad de vigilancia del mercado y con las demás autoridades u organismos públicos nacionales a que se refiere el artículo 77, apartado 1.

Cuando, en el transcurso de tal evaluación, la autoridad de vigilancia del mercado o, cuando proceda, la autoridad de vigilancia del mercado en cooperación con la autoridad nacional pública a que se refiere el artículo 77, apartado 1, constate que el sistema de IA no cumple los requisitos y obligaciones establecidos en el presente Reglamento, exigirá sin demora indebida al operador pertinente que adopte todas las medidas correctoras oportunas para adaptar el sistema de IA a los citados requisitos y obligaciones, retirarlo del mercado o recuperarlo, dentro de un plazo que dicha autoridad podrá determinar y, en cualquier caso, en un plazo de quince días hábiles a más tardar o en el plazo que prevean los actos legislativos de armonización de la Unión pertinentes según corresponda". (art. 79.2 RIA)

(...)

"Si, tras efectuar una evaluación con arreglo a lo dispuesto en el artículo 79 y consultar a la autoridad pública nacional a que se refiere el artículo 77, apartado 1, la autoridad de vigilancia del mercado de un Estado miembro concluye que un sistema de IA de alto riesgo, a pesar de cumplir con el presente Reglamento, presenta sin embargo un riesgo para la salud o la seguridad de las personas, para los derechos fundamentales o para otros aspectos de protección del interés público, pedirá al operador interesado que adopte todas las medidas adecuadas para garantizar que el sistema de IA de que se trate ya no presente ese riesgo cuando se introduzca en el mercado o se ponga en servicio sin demora indebida, dentro de un plazo que dicha autoridad podrá determinar". (art. 82.1 RIA)

Aplicable a partir del 2 de agosto de 2026.

La tercera sección del capítulo IX del RIA se dedica a la garantía del cumplimiento del Reglamento (artículos 74-84). En el marco de esta sección, se regulan varios procedimientos interrelacionados[32], entre ellos, el procedimiento aplicable a los SIA que presentan un riesgo. En este, intervienen las APDF tal y como se explicará seguidamente.

Ante todo, hay que tener en cuenta que cuando el procedimiento habla de sistema de IA que presenta un riesgo, este debe entenderse como "producto que presenta un riesgo", de

[32] Estos procedimientos no se aplican a los SIA asociados a productos regulados por los actos legislativos de armonización de la Unión enumerados en el anexo 1, sección A, cuando estos actos legislativos ya prevean procedimientos que garanticen un nivel equivalente de protección con un mismo objetivo (art. 74.4 RIA).

acuerdo con la definición del artículo 3.19 del RVM[33], en la medida en que presenten un riesgo para la salud, seguridad o los derechos fundamentales (art. 79.1 RIA). En este sentido, el artículo 3.19 del RVM establece que se entienden por productos que presentan un riesgo aquellos que afectan negativamente […] en un grado que va más allá de lo que se considera razonable y aceptable en relación con su finalidad prevista o en las condiciones de uso normales o razonablemente previsibles del producto en cuestión, incluida la duración de su utilización y, en su caso, los requisitos de su puesta en servicio, instalación y mantenimiento. Por tanto, cuando en este apartado se hable de "presenta un riesgo", se hará teniendo en cuenta esta definición específicamente.

El procedimiento que se inicia en el artículo 79 indica que cuando una AVM "tenga motivos suficientes"[34] para considerar que un SIA presenta un riesgo, la AVM evaluará el SIA para verificar si cumple los requisitos y obligaciones que le impone el RIA (en función de su categoría).[35] Asimismo, cuando el riesgo que se detecte lo sea por los derechos fundamentales, la AVM informará a la APDF pertinente y cooperará plenamente con ella en la evaluación del SIA correspondiente (art. 79.2 RIA)[36]. Esta evaluación puede tener dos posibles resultados: (i) bien, que se constate que el SIA evaluado no cumple con los requisitos u obligaciones del RIA; (ii) bien que se constate que sí los cumple.

Cuando de la evaluación del SIA se detecte que este no cumple con los requisitos u obligaciones del RIA, la AVM exigirá al operador pertinente que, en un plazo a determinar por la AVM[37]:

- adopte las medidas correctoras oportunas para adaptar el SIA a dichos requisitos y obligaciones;

---

[33] Artículo 3.19 del RVM: "Producto que puede afectar negativamente a la salud y la seguridad de las personas en general, a la salud y la seguridad en el trabajo, a la protección de los consumidores, al medio ambiente, a la seguridad pública o a otros intereses públicos protegidos por la legislación de armonización de la Unión aplicable, en un grado que vaya más allá de lo que se considere razonable y aceptable en relación con su finalidad prevista o en las condiciones de uso normales o razonablemente previsibles del producto en cuestión, incluida la duración de su utilización y, en su caso, los requisitos de su puesta en servicio, instalación y mantenimiento".

[34] Pueden derivarse de: la conservación de registros de eventos (art. 12.2.*a* RIA); información del responsable del despliegue (art. 26.5 RIA); evaluaciones de conformidad (art. 43 RIA); recepción de notificaciones de incidentes graves (art. 73.1 RIA); notificación de solicitud de acceso a información por parte de una APDF (art. 77.1 RIA); y reclamaciones presentadas ante una AVM (art. 85 RIA), entre otros.

[35] Este procedimiento se iniciará cuando el SIA presente un riesgo, independientemente de si se trata de un SIA prohibido, de alto riesgo o de riesgo limitado. Su categorización, eso sí, se tendrá en cuenta a la hora de evaluar sus respectivos requisitos y obligaciones.

[36] Conviene destacar que los operadores también tendrán que cooperar con las APDF en esta evaluación (art. 79.2 in fine).

[37] Inferior a 15 días hábiles o en el plazo que prevean los actos legislativos de armonización de la UE cuando proceda. (art. 79.2)

- lo retire del mercado[38]; o bien,
- lo recupere[39]..

Según el apartado 4 del artículo 79, el operador se asegurará de cumplir y aplicar las medidas en toda la UE.

En caso de que el operador no adopte las medidas adecuadas para cumplir con los requisitos u obligaciones del RIA, se seguirá el procedimiento establecido en los apartados 5 y 9 del artículo 79 y el artículo 81, tal y como se explica en el Anexo 2 de este trabajo, y la AVM adoptará las medidas provisionales necesarias para evitar que el SIA pueda suponer un perjuicio en el mercado de la UE. Esto abre la puerta a que diferentes AVM a la que inició el procedimiento también adopten medidas cuando el SIA afecte a su territorio y, por tanto, se prevé un procedimiento de salvaguarda de la Unión[40] para que la comisión evalúe si las medidas adoptadas son justificadas o no. En caso de considerarse justificadas, todos los EE. MM. tendrán que asegurarse de adoptar estas medidas e informar a la Comisión una vez que lo hagan. Por el contrario, en caso de no ser consideradas justificadas, el EM correspondiente tendrá que retirar la medida e informar también a la Comisión.

Por otra parte, cuando de la evaluación del SIA que presenta un riesgo se concluye que este cumple los requisitos y obligaciones del RIA, se abren dos nuevas posibilidades. En primer lugar, que se considere que, determinada la conformidad del SIA en el RIA, este no presenta un riesgo adicional que debe ser mitigado; en este caso, finaliza el procedimiento. En segundo lugar, que la AVM, tras consultar a la APDF, concluya que, aunque un SIA de alto riesgo cumpla con el RIA, este presenta igualmente un riesgo adicional[41] para la salud, seguridad, derechos fundamentales o para otros aspectos de protección del interés público. En este segundo supuesto, la AVM pedirá al operador pertinente que adopte las medidas necesarias para que este riesgo no se encuentre presente cuando este SIA se introduzca en el mercado de la UE o se ponga en servicio sin demora indebida (art. 82.1 RIA).

Desglosado este procedimiento, surgen ciertas dudas interpretativas sobre su alcance que cabe mencionar.

En primer lugar, en cuanto a la participación de las APDF en el procedimiento de adopción de medidas una vez que han cooperado con las AVM en la evaluación de los SIA que presentan un riesgo. Si bien el artículo 79.2 del RIA no explicita que la cooperación se extienda a la exigencia de adopción de medidas correctoras a los operadores, sería razonable su participación en relación con aquellos SIA que incumplen el RIA por presentar un riesgo para

[38] De acuerdo con la definición del artículo 3.22 del RVM.

[39] De acuerdo con la definición del artículo 3.23 del RVM.

[40] Regulado en el artículo 81 de la RIA.

[41] En este contexto se utiliza el término "riesgo adicional" para diferenciarlo del riesgo recogido en el artículo 79.1 del RIA

los derechos fundamentales. En este punto, además, cabe señalar que, cuando un sistema de IA presente un riesgo para el derecho fundamental a la protección de datos o para cualquier derecho o libertad que se vea afectado por el tratamiento de datos, las APD, en virtud de sus competencias, pueden tomar medidas cautelares de acuerdo con el artículo 66 del RGPD. Así, más allá de las medidas que las AVM puedan exigir tomar a los operadores, las APD ya tienen poderes ejecutivos para proteger el derecho fundamental a la protección de datos personales,[42] sin necesidad de recurrir a las potestades que el RIA le pueda otorgar en condición de APDF; o de tener que depender de una medida ejecutiva de la AVM. Esta potestad otorgada a las APD tiene cierto parecido con la prevista en el artículo 79.7 del RIA para las AVM.

En segundo lugar, en lo que se refiere al artículo 82.1 del RIA, parece que el legislador ha querido establecer un mecanismo de salvaguarda para las situaciones en las que, aunque se cumplan las obligaciones que establece el RIA (para que un SIA de alto riesgo pueda ser conforme al reglamento[43]), se detecte un riesgo para la salud, la seguridad, los derechos fundamentales u otros aspectos de protección del interés público, que deba ser mitigado. En este contexto, de acuerdo con el artículo 82.3 del RIA, cuando los Estados miembros se encuentren en una situación de estas características también deben informar a la Comisión y aportar una serie de detalles relativos al SIA en cuestión. Pues bien, esta obligación de informarla puede vincularse a la atribución que tiene otorgada la Comisión para adoptar actos delegados, en virtud del artículo 97 del RIA, para modificar el anexo III, la lista de SIA prohibidos y, también, ajustar las obligaciones y requisitos que debe cumplir un SIA para que su riesgo se circunscriba en los umbrales de tolerancia del derecho de la UE. Así, esta notificación puede convertirse en una herramienta para que, con la aprobación del Parlamento Europeo, la Comisión pueda adaptar el RIA a estas situaciones, a medida que las AVM las vayan identificando.

También en relación con el artículo 82.1 del RIA, procede valorar si la consulta a la APDF otorga una competencia adicional que no se enmarque dentro del deber de informar y cooperar plenamente con la APDF que tiene la AVM cuando el riesgo de que presente un SIA lo sea por los derechos fundamentales. En este sentido, de la lectura literal del artículo 82.1 del RIA se infiere que la consulta a la APDF es un requisito para que la AVM pueda pedir al operador interesado que adopte las medidas adecuadas cuando de la evaluación del SIA se constate: i) que es un SIA de alto riesgo; ii) que es conforme a los requisitos y

[42] Tomad como ejemplo la medida cautelar adoptada por la AEPD hacia Tools for Humanity Corporation, por la que exigía que cesara en la recogida y tratamiento de los datos personales que se estaba efectuando en España, en virtud de su proyecto World Coin. AEPD, *La Agencia ordena una medida cautelar que impide a Worldcoin seguir tratando datos personales en España.* 2024 [en línea] Disponible en: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-ordena-medida-cautelar-que-impide-a-worldcoin-seguir-tratando-datos-personales-en-espana

[43] Por ejemplo, la implantación, documentación y mantenimiento de un sistema de gestión del riesgo (art. 9 RIA) y la realización de una evaluación de impacto en los derechos fundamentales (art. 27 RIA), entre otros.

obligaciones del RIA; y iii) que presenta un riesgo para la salud, seguridad, derechos fundamentales u otros aspectos de protección del interés público. Así, sin efectuar esta consulta, la AVM podría pedir al operador la adopción de medidas correctoras para los SIA que no sean conformes al RIA, pero no podría hacerlo para los SIA que encajen en el contexto del artículo 82.

En tercer lugar, en cuanto a la interrelación entre los diferentes procedimientos de la sección 3 del capítulo IX del RIA que se han enunciado en este apartado, el "Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)" evidencia que el legislador del RIA concibió estos procedimientos separados en el articulado como un procedimiento único. Así, el punto 54 del Anexo[44] dispone, en el caso concreto de las prácticas prohibidas, que el procedimiento que se inicia en el artículo 79 del RIA se enlaza con el de salvaguarda de la Unión regulado en el artículo 81.

Por último, el artículo 80 del RIA, también incluido en la tercera sección del capítulo IX, regula el procedimiento aplicable a los sistemas de IA clasificados por el proveedor como no de alto riesgo en aplicación del Anexo III. En este caso, se regula un procedimiento para aquellos supuestos en los que la AVM "tenga motivos suficientes" para considerar que un SIA no clasificado como de alto riesgo por el proveedor, de acuerdo con el artículo 6.3 del RIA, sí lo es. En caso de que se detecte esta situación, la AVM pedirá al proveedor que adopte las medidas necesarias para que el SIA se adapte a los requisitos y obligaciones previstos en el RIA para los SIA de alto riesgo. En este punto, surge la duda de si este procedimiento podría afectar negativamente a las competencias de las APDF. En concreto, en caso de que una AVM "tenga motivos suficientes" para sospechar que un proveedor ha clasificado un SIA como no de alto riesgo y al mismo tiempo este presente un riesgo para los derechos fundamentales, si se priorizara el procedimiento regulado en el artículo 80, en atención a su especialidad, esto supondría la exclusión de la participación de las APDF, que no está prevista en este último procedimiento.

En cualquier caso, más allá de las dudas interpretativas que se han mencionado, cuando un SIA presente un riesgo por los derechos fundamentales, la AVM informará a la APDF pertinente y cooperará plenamente con ella en la evaluación del SIA correspondiente.

---

[44] "The procedure in the AI Act to deal with AI systems presenting a risk at national level is particularly relevant in the context of enforcing the prohibitions. Where there are cross-border implications beyond the territory of the market surveillance authority, the authority of the Member State concerned must inform the Commission and the market surveillance authorities of other Member States. All market surveillance authorities should follow a Union safeguard procedure with a decision taken by the Commission determining whether the AI system constitutes a prohibited practice. That procedure aims to ensure that the prohibitions are applied uniformly across all Member States, so as to provide legal certainty to both providers and deployers of AI systems. To ensure the uniform application of the AI Act, national market surveillance authorities should also strive for a harmonized application of the prohibitions for comparable cases that do not cross the Member State's territory by drawing inspiration from these Guidelines and cooperating within the AI Board."

4. Conclusiones

Tatiana Bianca Vulpe y Daniel Duro Millan

Este trabajo se ha elaborado con la intención de recoger y clarificar los principales retos que las autoridades de protección de datos (como la APDCAT) tendrán que afrontar debido al inicio de aplicabilidad del RIA: por su consideración como APD, el nombramiento como APDF y la próxima y probable designación como AVM para algunos sistemas de IA.[45] A continuación, se presentan las principales conclusiones.

Primera. Falta de concreción de cuestiones referentes a las funciones de las distintas autoridades

El RIA busca mejorar el funcionamiento del mercado interior, pero deja muchas cuestiones abiertas respecto a los poderes y funciones de las diferentes autoridades previstas en el articulado, que parece que no se aclararán hasta que cada Estado miembro lo regule internamente, con el peligro de llegar a conclusiones muy diversas. Además, aunque más adelante la Comisión apruebe directrices o recomendaciones para llenar huecos, estos no son textos vinculantes; por tanto, puede suceder que cada Estado miembro legisle antes o que esta legislación presente contradicciones. Nos encontramos, por tanto, en un escenario bastante incierto e inconcreto, que dificulta la seguridad jurídica en el ámbito europeo.

Algunas de las cuestiones que piden mayor concreción son la interrelación entre agentes/organismos (notificaciones, informes, solicitudes...), así como los términos *cooperación* y *colaboración*; también, los conceptos jurídicos indeterminados del artículo 57.10 del RIA, que establece que las autoridades nacionales de protección de datos deben estar ligadas al funcionamiento del espacio controlado de pruebas para la IA e involucradas en la supervisión de estos aspectos. Genera bastantes dudas sobre cómo se concretarán estos conceptos en acciones/actuaciones específicas, pero consideramos que el papel debe ser activo dado que los sistemas de IA funcionan gracias a datos que, en muchos casos, son personales.

En contraposición, aunque provoquen incertidumbre o inseguridad jurídica, las cuestiones que el RIA no concreta reflejan también la naturaleza dinámica y en constante evolución del campo regulado. No debe olvidarse que nos encontramos en las primeras etapas de la aplicación del reglamento, que incorpora diferentes plazos de aplicabilidad. El RIA funciona actualmente como un anuncio de lo que está por venir, otorgando tiempo para prepararse adecuadamente para las futuras adaptaciones y dando flexibilidad a la Comisión para

[45] Teniendo en cuenta el contenido del artículo 74.8 del RIA, así como el Anteproyecto de ley para el buen uso y gobernanza de la inteligencia artificial, presentado en marzo de 2025.

concretar cuestiones a medida que se dan a conocer nuevos avances tecnológicos. Habrá que ver si esta flexibilidad es positiva o negativa.

Segunda. El RIA tiene muy presente el papel de las autoridades de protección de datos en relación con los sistemas de identificación biométrica remota

El RIA establece disposiciones específicas que involucran a las autoridades de protección de datos en relación con los sistemas de identificación biométrica remota, tanto en tiempo real como en diferido. Si bien no necesariamente otorga nuevos poderes explícitos a estas autoridades, más allá de los ya establecidos en el RGPD, sí les confiere un papel significativo en la supervisión de la aplicación del RIA en este ámbito (recibir notificaciones, acceder a documentación de expedientes policiales bajo solicitud y elaborar y recibir informes).

Aunque el RIA opera sin perjuicio del RGPD (con excepciones tal y como se establece en el artículo 2.7 del RIA), el marco establecido parece reforzar la capacidad de las autoridades de protección de datos para supervisar el tratamiento de datos personales en este contexto y aplicar, en su caso, sanciones por incumplimiento del RGPD. Es decir, el articulado conlleva que las autoridades de protección de datos puedan estar enteradas de los usos que se hagan de los sistemas de identificación biométrica remota, sin prever una actuación más allá de su conocimiento (posiblemente, porque el legislador europeo considera que no es necesario, teniendo en cuenta las competencias que ya tienen gracias al RGPD). Por tanto, el RIA consolida el papel supervisor de las autoridades de protección de datos en el ámbito específico de la identificación biométrica remota y las dota de mecanismos para ampliar el alcance de conocimiento.

Tercera. Las APDF tienen un impacto significativo en la categorización de los SIA

El RIA hace referencias constantes a la protección de los derechos fundamentales ("garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta").[46] En este sentido, incorpora las APDF al proceso de supervisión del RIA, por ejemplo, mediante:

(i) La solicitud de acceso a documentación de los SIA enumerados en el anexo III y la posterior solicitud motivada en las AVM, para organizar pruebas sobre estos SIA, si la solicitud de documentación no es suficiente para determinar si incumple el RIA.

(ii) La recepción de información proveniente de las AVM, cuando se produzca un incidente grave por incumplimiento de las obligaciones de la UE en materia de DF.

(iii) La recepción de información proveniente de las AVM relativa a cualquier SIA que pueda suponer un riesgo para los DF, para evaluarlos conjuntamente y, posteriormente, categorizarlos en alguna de las cuatro categorías previstas en el RIA (según el riesgo)

[46] Considerandos 1 y 176 y el artículo 1 del RIA.

para que, finalmente, las AVM exijan a los operadores que adopten las medidas adecuadas para asegurar la conformidad con el RIA.

Estas competencias son más amplias en los casos en los que adicionalmente las APDF tienen atribuidos poderes en virtud de otra norma de la UE. En el caso de las APD designadas APDF, el RIA es explícito a la hora de afirmar que no afecta al RGPD. Por tanto, los poderes que el RGPD otorga a las APD para garantizar los derechos y libertades fundamentales de las personas, en cuanto al tratamiento de sus datos personales, se mantienen intactos. En este contexto, si bien el RIA circunscribe la documentación a la que pueden tener acceso las APDF a los SIA de alto riesgo del anexo III (art. 77 RIA), esta limitación no afecta a las APD, que pueden acceder a ellas por las competencias otorgadas por el RGPD. Adicionalmente, cuando se notifique o informe a la APDF un incidente grave relativo al derecho fundamental a la protección de datos, o bien que un SIA pueda suponer un riesgo para este derecho, las APD pueden adoptar medidas cautelares correctoras en virtud del RPGD, aunque como APDF no tengan otorgada esta potestad.

Por tanto, en relación con estas competencias, el RGPD otorga más facultades a las APD para proteger el derecho fundamental a la protección de datos que el propio RIA. Sin embargo, existen otras competencias que el RIA otorga a las APDF que sí suponen acrecentar las herramientas con las que las APD pueden proteger los datos personales:

- En primer lugar, si bien las APD pueden 'participar' en los espacios controlados de pruebas por el simple hecho de serlo (art. 57.10 RIA), las APDF pueden solicitar motivadamente a las AVM que organicen pruebas de SIA de alto riesgo del anexo III, cuando con la solicitud de documentación las APDF no puedan determinar si el SIA analizado incumple el RIA (art. 77.3 RIA).

- En segundo lugar, las AVM deben notificar a las APDF los incidentes graves en SIA que puedan suponer riesgos para los DF (art. 73.7 RIA). Como se desarrolla en el apartado 3.4, se valora la posibilidad de que, por la diferente naturaleza de notificación que supone una NVS y la notificación de un incidente grave, en algunas circunstancias, en la práctica, esta última pueda convertirse en el único mecanismo al alcance de las APD para enterarse de una violación de seguridad de datos personales en el contexto de los SIA.

- En tercer lugar, las AVM deben informar a las APDF de cualquier SIA que presente un riesgo para los DF, para que en cooperación lo evalúen y, en consecuencia, se categorice el SIA según su riesgo (prohibido, de alto riesgo, con obligaciones de transparencia/riesgo limitado, o bien de riesgo mínimo o nulo). Esto resulta especialmente relevante, puesto que el RIA impone obligaciones de acuerdo con la categorización de los SIA.

Cuarta. La adaptación de las autoridades de protección de datos requiere una preparación rigurosa y recursos adecuados para afrontar los nuevos retos con eficacia

Está claro que las autoridades de protección de datos necesitarán una preparación previa exhaustiva para responder satisfactoriamente a todas las nuevas responsabilidades. Para

abordar estos retos de forma efectiva, es esencial que dispongan de los recursos humanos y financieros adecuados. El aumento de las responsabilidades derivadas del RIA, el nombramiento como APDF y la probable designación como AVM requieren una dotación de personal cualificado y especializado en tecnologías emergentes y en la regulación de la inteligencia artificial.

Es importante subrayar que, aunque este trabajo no ha analizado el incremento de las denuncias que han recibido las autoridades de protección de datos en aplicación del RGPD y el LOPDGDD, este fenómeno es un indicador adicional de la creciente demanda y conciencia ciudadana respecto al derecho a la protección de datos personales. Por tanto, es esencial que las autoridades de protección de datos no solo estén preparadas para responder adecuadamente a las reclamaciones actuales, sino que también puedan anticipar y gestionar proactivamente las nuevas que se puedan presentar, como sucede en el ámbito de la IA.

5. Bibliografía

ABBOU, Daniel; et al. Open letter to the representatives of the European Commission, the European Council and the European Parliament. Artificial Intelligence: Europe's chance to rejoin the technological avant-garde. 2023. Disponible en: https://uploads-ssl.webflow.com/6034e2e35a869ae02e67f55f/649eadd757bee709f4fe1f49_Brandbrief%20en-US%20(2).pdf

ACCIÓ Generalitat de Catalunya. La intel·ligència artificial a Catalunya. Informes tecnològics. [en línea]. Abril de 2024. [consulta: 17 de octubre de 2024]. https://www.accio.gencat.cat/web/.content/bancconeixement/documents/informes-tecnologics/ACCIO-ia-catalunya-informe-complet-2024.pdf#:~:text=Catalunya%20va%20assolir%20les%202.102%20startups%20startups%20el

Agencia Española de Protección de Datos (AEPD). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción,* 2020. Disponible en: https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf

Agencia Española de Protección de Datos. *Construir correctamente el futuro. La inteligencia artificial y los derechos fundamentales. Resumen* [en línea]. Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_es.pdf

Agencia Española de Protección de Datos. *Requisitos para Auditorías de Tratamientos que incluyan IA.* 2021.

Agencia Española de Protección de Datos. *Tratamientos que incluyen Inteligencia Artificial (IA). Mapa de referencia*. 2022.

Agencia Española de Protección de Datos. *La Agencia ordena una medida cautelar que impide a Worldcoin seguir tratando datos personales en España.* 2024. Disponible en: https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-ordena-medida-cautelar-que-impide-a-worldcoin-seguir-tratando-datos-personales-en-espana

Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act).

ARELLANO TOLEDO, Wilma. Artículo 57. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 594-603. ISBN 978-84-18662-88-1.

ARELLANO TOLEDO, Wilma. Artículo 58. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 603-608. ISBN 978-84-18662-88-1.

Autoridad Catalana de Protección de Datos (APDCAT). *Inteligencia Artificial: Decisiones Automatizadas en Cataluña.* 2020. Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/intelligencia_artificial/documents/INFORME-INTELLIGENCIA-ARTIFICIAL-FINAL-WEB-OK.pdf

Autoridad Catalana de Protección de Datos (APDCAT). Modelo para la EIDF: guía y casos de uso. Metodología aplicada de la evaluación de impacto sobre los derechos fundamentales en el diseño y desarrollo de la IA. 2025. Disponible en: https://apdcat.gencat.cat/ca/documentacio/intelligencia_artificial/

Autoridad Catalana de Protección de Datos (APDCAT). La privacidad desde el diseño y la privacidad por defecto. Guía para desarrolladores. Junio 2024. Disponible en: https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guiaDesenvolupadors/GUIA-PDDD.pdf

BARRIO ANDRÉS, Moisés. Artículo 1. En: Barrio Andrés, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 135-147. ISBN 978-84-18662-88-1.

BARRIO ANDRÉS, Moisés. Capítulo I. Objeto, ámbito de aplicación y sentido del Reglamento Europeo de Inteligencia Artificial. En: Jiménez Serranía, Vanessa, et al. El *Reglamento Europeo de Inteligencia Artificial.* Valencia: Tirant lo Blanch, 2024. ISBN13 9788410713048.

BELANO GARÍN, Beatriz. Artículo 82. En: Barrio Andrés, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 750-752. ISBN 978-84-18662-88-1.

Consejo de Europa. *Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (huderia methodology)* 2024 [consulta: 12 de diciembre de 2024] Disponible en: https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f

EAPC. Jornada sobre inteligencia artificial y la protección de datos personales (22/11/2024). [Vídeo en línea]. 2024 [consulta: 03 de diciembre de 2024]. Disponible en: https://www.youtube.com/watch?v=wd6KauY0g8s&t=312s

CEPD. Declaración 3/2024 sobre el papel de las autoridades de protección de datos en el marco de la Ley de Inteligencia Artificial. [en línea]. Julio 2024. [consulta: 27 de febrero de 2024]. Disponible en: https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-32024-data-protection-authorities-role-artificial_es

EDBP. *Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR.* 2024 [consulta: 27 de febrero de 2024]. Disponible en: https://www.edpb.europa.eu/system/files/2024-02/edpb_opinion_202404_mainestablishment_en.pdf#:~:text=The%20French%20Supervisory%20Authority%20requested%20the%20European%20Data,mechanism%2C%20in%20particular%20regarding%20the%20notion%20of%20controll

Agencia de los Derechos Fundamentales de la Unión Europea (FRA). *Informe sobre los derechos fundamentales*. 2021. [en línea] Disponible en: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-fundamental-rights-report-2021-opinions_es.pdf

FERNÁNDEZ HERNÁNDEZ, Carlos. Artículo 5. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 180-205. ISBN 978-84-18662-88-1.

GAMERO CASADO, Eduardo. Artículo 99. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 837-844. ISBN 978-84-18662-88-1.

HERNÁNDEZ LÓPEZ, José Miguel. *Reglamento de Inteligencia Artificial: Incluye introducción, notas, cronología, webgrafía, bibliografía e índice analítico* [en línea]. Barcelona, España: J. M. Bosch Editor, 2024. ISBN 9788410044063.

KARATHANASIS, Theodoros. *AI incident notification in the EU AI Act: How does it work and is it Effective?* [en línea] Disponible en: https://ai-regulation.com/ai-act-incident-notification/

KEBER, Tobias, et al. Discussion paper: Legal basis for data protection in the use of artificial intelligence. Stuttgart: The State Commissioner for Data Protection and Freedom of Information Baden-Württemberg, 2024.

MIGUEZ MACHO, Luis y TORRES CARLOS, Marcos. Capítulo II. Sistemas de IA prohibidos y sistemas de IA de alto riesgo. En: JIMÉNEZ SERRANÍA, Vanessa, et al. El Reglamento Europeo de Inteligencia Artificial. Valencia: Tirant lo Blanch, 2024. ISBN13 9788410713048.

MUÑOZ GARCÍA, Carmen. Artículo 53. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 548-552. ISBN 978-84-18662-88-1.

MUÑOZ GARCÍA, Carmen. Capítulo III. Modelos de IA de uso general y sistemas de IA de riesgo limitado y mínimo. En: JIMÉNEZ SERRANÍA, Vanessa, et al. *El Reglamento Europeo de Inteligencia Artificial.* Valencia: Tirant lo Blanch, 2024. ISBN13 9788410713048.

MUÑOZ VELA, José Manuel. Anexo III. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 906-933. ISBN 978-84-18662-88-1.

PADÍN VIDAL, Alejandro. Artículo 83. En BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 753-756. ISBN 978-84-18662-88-1.

PERRIGO, Billy. Exclusivo: OpenAI Lobbied the E.U. to Water Down AI Regulation. En: *Time Magazine.* [en línea]. 20 de junio de 2023 [Consulta: 17 de diciembre de 2024]. Disponible en: https://time.com/6288245/openai-eu-lobbying-ai-act/

PRESNO LINERA, Miguel Ángel; MEUWESE, Anne. La regulación de la inteligencia artificial en Europa. Teoría y Realidad Constitucional. 2024, n.º 54, s. 131-161. ISSN 1139-5583.

QUADRA-SALCEDO, Tomás. Estudio Preliminar: el Reglamento Europeo de Inteligencia Artificial y su regulación en condiciones de permanente adaptación a los riesgos y a la evolución de los modelos y sistemas de IA de uso general. En: BARRIO ANDRÉS, Moisés. *Comentarios al Reglamento Europeo de Inteligencia Artificial.* Madrid: La Ley, 2024. Pág. 23-47. ISBN 978-84-18662-88-1.

URIOS APARISI, Xavier. Què passa amb les dades biomètriques? Són dades especialment protegides sempre? [en línea]. EAPC - Gestió de la informació: transparència i protecció de dades. 2024 [consulta: 09 de diciembre de 2024]. Disponible en: https://formacioooberta.eapc.gencat.cat/espaistematics/gestio-dades/que-passa-amb-les-dades-biometriques-son-dades-especialment-protegides-sempre.html

Anexo I - Identificación biométrica remota en tiempo real y en diferido

Tatiana Bianca Vulpe

Este anexo tiene como objetivo clarificar y diferenciar los sistemas de identificación biométrica remota en tiempo real y diferido. Para ello, se ofrece un resumen de diversas consideraciones extraídas del Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) (en adelante, directrices).

El artículo 5.1.*h* del RIA prohíbe el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público, con fines de garantía del cumplimiento del Derecho,[47] excepto y en la medida en que este uso sea estrictamente necesario para alcanzar uno o varios de los siguientes objetivos:

- La búsqueda selectiva de víctimas concretas de secuestro, tráfico de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas.[48]
- La prevención de una amenaza específica, importante[49] e inminente[50] para la vida o la seguridad física de las personas físicas,[51] o de una amenaza real y actual o real y previsible de un atentado terrorista.[52]
- La localización o identificación de una persona sospechosa de haber cometido un delito, con el fin de llevar a cabo una investigación o un procedimiento penal o de

[47] Sin perjuicio del artículo 9 del Reglamento (UE) 2016/679 para el tratamiento de datos biométricos con fines distintos a los fines policiales y judiciales.

[48] Tal y como estipula la Comisión Europa en sus directrices, en algunos Estados miembros la búsqueda de una persona desaparecida puede llevarse a cabo en el marco de un procedimiento administrativo y no con fines de garantía del cumplimiento del Derecho. Por ejemplo, cuando una persona vulnerable desaparece, pero no hay sospecha de ningún delito ni estamos ante otra finalidad relacionada con la garantía del cumplimiento del Derecho, el uso de sistemas de identificación biométrica en tiempo real para encontrar a esta persona no se integraría como práctica prohibida, y se regiría por las normas correspondientes establecidas por el RGPD.

[49] Una amenaza importante para la seguridad física estaría relacionada con lesiones corporales graves.

[50] Una amenaza inminente en la vida o en la seguridad física es una amenaza que puede ocurrir en cualquier momento y requiere tomar medidas inmediatas.

[51] Un ejemplo de amenaza sería la interrupción grave y la destrucción de infraestructuras críticas (por ejemplo, una central eléctrica, un suministro de agua o un hospital).

[52] El nivel de amenaza terrorista se define a escala nacional y varía de un Estado miembro a otro. Sin embargo, el concepto de amenaza real y actual o real y previsible, tal y como se utiliza en el artículo 5.1.*h.ii*, es una noción autónoma del derecho de la Unión. Por lo tanto, en principio debería evaluarse independientemente de las definiciones nacionales. La amenaza no se refiere al terrorismo en general, sino específicamente a la amenaza de un ataque terrorista.

> ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II,[53] que en el Estado miembro correspondiente se castigue con una pena o una medida de seguridad privativa de libertad con una duración máxima de cuatro años.[54]

Por tanto, además de considerar las tres excepciones, es necesario cumplir diversas condiciones acumulativas para que se aplique la prohibición del artículo 5.1.*h* del RIA: (i) el sistema de IA debe ser un sistema de identificación biométrica; (ii) remota; (iii) en relación con el uso de este sistema; (iv) en tiempo real; (v) en espacios de acceso público; y (vi) con fines de garantía del cumplimiento del Derecho.

Sistema de identificación biométrica

El concepto de datos biométricos debe interpretarse en relación con el artículo 4.14 del RGPD y el artículo 3.13 de la Directiva (UE) 2018/1725. En este sentido, los datos biométricos son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (art. 4.14 RGPD).

Los datos biométricos pueden permitir la autenticación, identificación, categorización y reconocimiento de las emociones de las personas físicas; lo referido a la identificación está prohibido.

La identificación biométrica se define como "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico[55] para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos" (art. 3.35 RIA). Por su parte, un sistema de identificación biométrica remota se define funcionalmente como un sistema de IA "destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de

---

[53] Terrorismo, tráfico de seres humanos, explotación sexual de menores y pornografía infantil, tráfico ilícito de estupefacientes o sustancias psicotrópicas, tráfico ilícito de armas, municiones o explosivos, asesinato, lesiones corporales graves, tráfico ilícito de órganos o tejidos humanos, tráfico ilícito de materiales nucleares o radiactivos, secuestro, restricción ilegal o toma de rehenes, delitos de la jurisdicción de la Corte Penal Internacional, incautación ilegal de aeronaves o buques, violación, delitos ambientales, robo organizado o a mano armada, sabotaje y participación en una organización criminal implicada en uno o más de los delitos mencionados anteriormente.

[54] La policía no puede desplegar tecnologías de reconocimiento facial en tiempo real de forma amplia y no específica, es decir, con la esperanza de encontrar a delincuentes buscados y sacarlos de las calles. En contraposición, si la policía recibe una descripción física con una fotografía de un individuo buscado, sujeto a una orden de detención europea por tráfico de drogas, y existen motivos para creer que estará en un lugar concreto, como un festival, el despliegue de tecnologías de reconocimiento facial en tiempo real para identificar al individuo puede estar cubierto por el artículo 5.1.*h.iii* del RIA.

[55] Como por ejemplo la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, la forma de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla (considerando 15 RIA).

referencia" (art. 3.17 RIA), con independencia de la tecnología, procesos o tipos de datos biométricos concretos que se utilicen.

Por tanto, deben considerarse diferentes y quedan excluidos los sistemas de IA destinados a la verificación biométrica o la autenticación, que tienen como único propósito confirmar que una persona física concreta es la persona que dice ser; también, los destinados a confirmar la identidad de una persona física con el fin exclusivo de que por ejemplo tenga acceso a un servicio, desbloquee un dispositivo o tenga acceso de seguridad a un local. Esta exclusión se justifica por el hecho de que probablemente estos sistemas tienen menos repercusión en los derechos fundamentales de las personas físicas (considerando 17).

Remota

El concepto de *remota* también debe clarificarse y ponerse en relación o contradicción con el concepto de *participación activa*. Según el artículo 3.41 del RIA, el concepto de remota implica la capacidad de los sistemas biométricos para identificar a personas sin su participación activa, normalmente a distancia, comparando los datos biométricos de una persona con los datos biométricos contenidos en una base de datos de referencia. Para la participación activa, no es suficiente que las personas estén informadas de la presencia de cámaras, sino que deben ponerse activa y conscientemente ante una cámara instalada, de forma que fomente la participación activa. Para ejemplificar el concepto, podríamos utilizar los siguientes supuestos prácticos extraídos de las directrices:

- Los sistemas de identificación biométrica remota en tiempo real que se utilizan en cámaras instaladas en las paredes o en el techo de las estaciones de metro, con fines de vigilancia. Este sistema cumple la condición de *remota*.

- Los sistemas que se utilizan para dar acceso a la estación de metro, como los billetes biométricos de metro, en los que las personas participan activamente y se acercan conscientemente al sensor biométrico para acceder a ellos. Estos sistemas no cumplen esta condición.

- En el caso de las cámaras corporales capaces de identificación biométrica remota en tiempo real utilizadas por agentes individuales de las fuerzas del orden, la filmación no dirigida, por ejemplo, durante una manifestación con cientos de participantes. En este caso, se considera que cumple la condición de *remota*.

Utilización/uso (*the use*); cada uso (*each use*)

En primer lugar, conviene matizar que en la versión castellana del RIA, para referirse al *use* de la versión inglesa original, se utiliza indistintamente *uso* y *utilización*.

También es relevante remarcar que, en el caso de los sistemas de identificación biométrica remota en tiempo real, la prohibición se limita exclusivamente a su utilización, a diferencia de los demás supuestos de prácticas prohibidas del artículo 5 del RIA donde, en general, se prohíbe su introducción, puesta en servicio y uso.

El concepto de *uso* no tiene una definición concreta en el artículo 3 del RIA ni está explícitamente definido en todo el texto normativo, a diferencia de la introducción en el

mercado (art. 3.9 RIA), la comercialización (art. 3.10 RIA) y la puesta en servicio (art. 3.11 RIA). Sin embargo, debe entenderse de forma amplia para cubrir el uso o la implementación del sistema en cualquier momento de su ciclo de vida, después de haber sido comercializado o puesto en servicio, tal y como se explica en las directrices de la Comisión. Por tanto, la restricción del artículo 5.1.*h* del RIA no se aplica a la introducción en el mercado ni a la puesta en servicio, que siguen siendo actividades permitidas bajo el régimen de los sistemas de IA de alto riesgo regulado en el artículo 6.2 y el anexo III, letra *a*, del RIA. Esto significa que estos sistemas pueden desarrollarse, venderse y desplegarse, pero su uso efectivo está sujeto a una regulación mucho más estricta.

Por otra parte, conviene matizar que, de acuerdo con el artículo 5.3 del RIA, *cada uso* (*each use*, en la versión inglesa) de un sistema de identificación biométrica remota en tiempo real requiere una autorización previa. Esto podría implicar que la simple instalación del sistema no necesita ninguna aprobación específica según el RIA, pero cada vez que se quiera utilizar en un caso concreto es necesario obtener una autorización individual de una autoridad judicial o administrativa independiente, además del resto de consideraciones necesarias, como elaborar una evaluación del impacto en los derechos fundamentales (FRIA).[56] Este matiz es esencial para garantizar que la tecnología no se utilice de forma indiscriminada y que cada aplicación concreta esté justificada y supervisada, de modo que se protejan los derechos fundamentales.

Algunos ejemplos que permiten comprender la distinción, según las directrices, son:

- Instalación del sistema: la policía instala cámaras biométricas de videovigilancia en la estación principal de tren de una ciudad. Según el RIA no se requiere ninguna autorización previa para la instalación, pero el sistema debe cumplir los requisitos de los sistemas de alto riesgo.[57] Antes del primer uso, debe realizarse una evaluación del impacto en los derechos fundamentales.

- Uso específico del sistema: la policía tiene indicios concretos de que un terrorista llegará en tren a la ciudad y decide utilizar el sistema de identificación biométrica remota en tiempo real, para identificarlo en tiempo real. Este uso requiere la autorización previa de una autoridad judicial o administrativa independiente.

Así, el RIA establece una distinción clave entre la presencia del sistema y su uso concreto, garantizando que cada aplicación individual de estas tecnologías en contextos sensibles se someta a un control riguroso para proteger los derechos fundamentales y evitar abusos.

---

[56] Cabe recordar que para llevar a cabo una EIPDF tenemos en la mano la metodología presentada por la APDCAT para la evaluación de impacto en los derechos fundamentales en materia de inteligencia artificial (EIDF), aplicada a casos concretos en Europa, disponible en: https://www.dpdenxarxa.cat/pluginfile.php/2468/mod_folder/content/0/FRIA_ca.pdf_.pdf

[57] Sin perjuicio de que el Estado miembro establezca algo distinto.

En tiempo real

Cuando el RIA menciona *en tiempo real*, significa que la recogida de los datos biométricos, la comparación y la identificación se producen "de manera instantánea, casi instantánea o, en cualquier caso, sin una importante demora" (considerando 17 RIA). En este sentido, no debe existir la posibilidad de que, generando demoras mínimas, se puedan eludir las normas previstas en el RIA en relación con el uso en tiempo real de los sistemas de IA. En términos generales, un retraso es significativo al menos cuando es probable que la persona haya abandonado el lugar en el que se tomaron los datos biométricos. Cuando el retraso es significativo entendemos que la identificación se realiza en diferido. Unos ejemplos extraídos de las directrices para comprender la diferencia serían los siguientes:

- Identificación biométrica remota en tiempo real: un sistema de IA examina al momento a todos los asistentes a un concierto.

- Identificación biométrica remota en diferido: un sistema filma a todos los asistentes que entran en un concierto. Se produce un incidente y, después del concierto, se emplea el sistema para identificar al delincuente.

La distinción no siempre será del todo clara y será necesario un análisis caso por caso. Por ejemplo, cuando una autoridad policial fotografía a una persona con un dispositivo móvil y la envía a una base de datos para una búsqueda inmediata, dependiendo de las circunstancias esto puede caer bajo la prohibición del artículo 5.1.*h* del RIA, según se determine si el retraso es significativo o no.

En definitiva, los sistemas de identificación biométrica en tiempo real permiten analizar y comparar de inmediato datos captados por cámaras u otros dispositivos similares. Por ejemplo, cuando una cámara situada en un aeropuerto escanea los rostros de las personas que pasan por ella e, instantáneamente, los compara con una base de datos de personas buscadas por la policía, estamos ante un sistema en tiempo real. Si existe una coincidencia, el sistema genera una alerta inmediata para que los agentes puedan actuar al instante. En este caso, el procesamiento de la información es simultáneo a la captación, posibilitando una respuesta inmediata.

Por el contrario, los sistemas en diferido funcionan con una importante demora entre la captación y el procesamiento de los datos biométricos. Esto ocurre, por ejemplo, cuando la policía investiga un delito y analiza grabaciones de vídeo de una cámara de seguridad, para identificar a un sospechoso. Las imágenes ya han sido captadas previamente y la comparación se realiza posteriormente, mediante un sistema de IA. En este caso, no existe un procesamiento inmediato, sino que se trabaja con material ya grabado, como imágenes de archivo captadas por cámaras de videovigilancia o dispositivos privados.

Así, la diferencia fundamental entre estos dos tipos de sistemas reside en el momento en que se produce el análisis y la comparación. Mientras que en los sistemas en tiempo real la identificación se hace en directo o casi en directo, en los sistemas en diferido este análisis es posterior, utilizando información ya existente.

Espacios de acceso público

Tal y como se constata en las directrices, en cuanto al concepto de espacio público, es importante tener presente que algunos espacios pueden tener una doble función. Por ejemplo, un aeropuerto se considera generalmente un espacio de acceso público en lo que se refiere a sus zonas comunes, pero el área dedicada al control fronterizo (donde están los funcionarios de aduanas y se hacen los pasaportes o los controles de identidad) queda excluida del ámbito de la prohibición. Como se aclara en el considerando 19 del RIA, la evaluación de si un espacio es accesible al público debe realizarse con un análisis caso por caso.

Finalidades de garantía del cumplimiento del Derecho

También hay que considerar que el artículo 3.46 del RIA describe la garantía del cumplimiento del Derecho como "las actividades realizadas por las autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas".[58] Por tanto, cuando se habla de garantía del cumplimiento del Derecho, debe entenderse realizada por las autoridades garantes de cumplimiento directamente, o en su nombre.

Según el artículo 3.45 del RIA, las autoridades garantes del cumplimiento del Derecho son "toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, o cualquier otro organismo o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas".[59]

Por tanto, conviene hacer énfasis y entender qué implica la actuación *en nombre de las autoridades garantes*. Algunos ejemplos de delegaciones, extraídos de las directrices, serían los siguientes:

- Empresas de transporte público requeridas por las autoridades policiales para garantizar la seguridad en las redes de transporte público, bajo sus instrucciones y supervisión.

[58] Algunas actividades de las autoridades policiales están excluidas del ámbito de aplicación, como cuando realizan tareas administrativas (como recursos humanos); estas actividades se llevan a cabo fuera del marco de aplicación del Reglamento. Están bajo el RGPD. Véase el considerando 19 del RGPD.

[59] En el Estado español, es importante poner en relación estas definiciones con la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ya que en muchos casos una autoridad competente según la Ley 7/2021 también será una autoridad garante del cumplimiento del Derecho según el RIA.

- Federaciones deportivas requeridas por las autoridades policiales para actuar bajo sus instrucciones y supervisión, para proporcionar seguridad en eventos deportivos.

- Entidades financieras que son requeridas por las autoridades policiales para realizar ciertas acciones para prevenir la ejecución de determinados delitos en casos específicos, bajo las instrucciones y supervisión de las autoridades policiales.

Estas actividades entran dentro de la definición *con finalidades de garantía del cumplimiento del Derecho*, ya que estas entidades actúan *en nombre de las autoridades policiales*. En contraposición, si actuaran en nombre propio a la hora de detectar y combatir delitos (como el fraude o el blanqueo de capitales), no se consideraría que entran en la prohibición establecida en el artículo 5.1.*h* del RIA.

Por último, otro aspecto a tener en cuenta es la exclusión del ámbito de aplicación del RIA para determinadas materias, como la seguridad nacional, la defensa y las finalidades militares, de acuerdo con lo que establece el artículo 2 del RIA. Esta exclusión no es absoluta, ya que si un sistema de IA inicialmente destinado a finalidades militares, de defensa o de seguridad nacional se utiliza posterior o simultáneamente (temporal o permanentemente) con otras finalidades (como por ejemplo civiles o humanitarios), pasa a estar dentro del ámbito de aplicación del RIA y, por tanto, sujeto a sus requisitos normativos. Por ejemplo, si una agencia de seguridad nacional utiliza un sistema de identificación biométrica remota en tiempo real, con finalidades de seguridad nacional, ese uso quedaría excluido del RIA. Ahora bien, si el mismo sistema se destinara a localizar a personas desaparecidas, entonces sí estaríamos ante un supuesto regulado por el Reglamento.

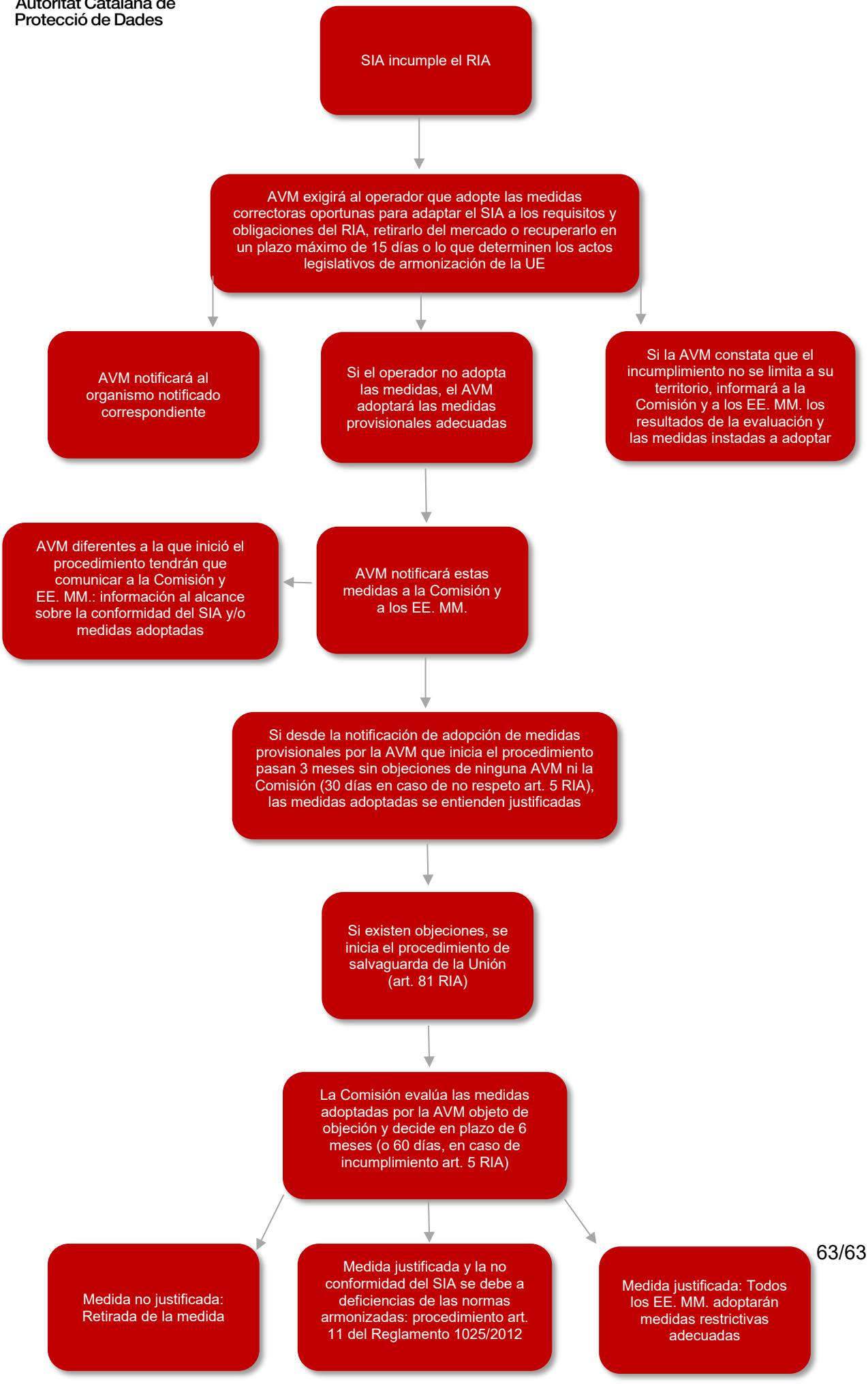
Esta diferenciación es especialmente relevante en relación con las finalidades de garantía del cumplimiento del Derecho, tal y como define el artículo 3.46 del RIA. Este criterio es esencial para determinar cuándo un uso concreto de un sistema de IA está excluido, sometido a la prohibición del artículo 5.1.*h* del RIA o cuando se considera uso permitido, pero clasificado como sistema de alto riesgo. Para entender esta diferencia, se pueden tener presentes los siguientes ejemplos extraídos de las directrices:

- Una organización privada dedicada a la búsqueda de niños desaparecidos decide utilizar un sistema de identificación biométrica remota en tiempo real. No tiene mandato alguno para ejercer la autoridad y los poderes públicos, ni para prevenir delitos o tareas de prevención de amenazas a la seguridad pública. Este uso no entra dentro de la prohibición establecida en el artículo 5.1.*h* del RIA. Sin embargo, este sistema se calificará de alto riesgo (punto 1.*a* del anexo III) y puede hacerse una EIPD (art. 35 RGPD) y, en su caso, una consulta previa a la autoridad de protección de datos, de acuerdo con el artículo 36 del RGPD.

- En cambio, si las autoridades policiales solicitaran a la misma organización que actuara en su nombre para la búsqueda de niños desaparecidos, en un contexto policial y bajo la supervisión y las instrucciones de las autoridades policiales competentes, sería necesaria una autorización previa de acuerdo con el artículo 5.3 del RIA.

Anexo II - Procedimiento aplicable a los sistemas de IA que presentan un riesgo

Daniel Duro Millan


SIA incumple el RIA
AVM exigirá al operador que adopte las medidas correctoras oportunas para adaptar el SIA a los requisitos y obligaciones del RIA, retirarlo del mercado o recuperarlo en un plazo máximo de 15 días o lo que determinen los actos legislativos de armonización de la UE
AVM notificará al organismo notificado correspondiente
Si el operador no adopta las medidas, el AVM adoptará las medidas provisionales adecuadas
Si la AVM constata que el incumplimiento no se limita a su territorio, informará a la Comisión y a los EE. MM. los resultados de la evaluación y las medidas instadas a adoptar
AVM diferentes a la que inició el procedimiento tendrán que comunicar a la Comisión y EE. MM.: información al alcance sobre la conformidad del SIA y/o medidas adoptadas
AVM notificará estas medidas a la Comisión y a los EE. MM.
Si desde la notificación de adopción de medidas provisionales por la AVM que inicia el procedimiento pasan 3 meses sin objeciones de ninguna AVM ni la Comisión (30 días en caso de no respeto art. 5 RIA), las medidas adoptadas se entienden justificadas
Si existen objeciones, se inicia el procedimiento de salvaguarda de la Unión (art. 81 RIA)
La Comisión evalúa las medidas adoptadas por la AVM objeto de objeción y decide en plazo de 6 meses (o 60 días, en caso de incumplimiento art. 5 RIA)
Medida no justificada: Retirada de la medida
Medida justificada y la no conformidad del SIA se debe a deficiencias de las normas armonizadas: procedimiento art. 11 del Reglamento 1025/2012
Medida justificada: Todos los EE. MM. adoptarán medidas restrictivas adecuadas