apdcat
Autoritat Catalana de Protecció de Dades

RGPD vs. RIA

Análisis de una intersección parcial

Autoría: Pablo Gavara Feijóo y María Piedrafita Abión, estudiantes en prácticas en la APDCAT en julio de 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

1. Introducción

Este trabajo se ha elaborado por dos estudiantes en prácticas del grado en Derecho de la Universidad Pompeu Fabra durante su estancia en la Autoridad Catalana de Protección de Datos en julio de 2024: Pablo Gavara Feijóo y María Piedrafita Abión.

Por parte del equipo de la APDCAT, Joana Marí Cardona, delegada de Protección de Datos y responsable de Proyectos Estratégicos y, Guillem López Sanz, responsable de Relaciones Institucionales y Organización, han llevado a cabo la coordinación de este trabajo.

La APDCAT considera de interés difundir este informe para dar conocer esta primera aproximación al nuevo Reglamento de Inteligencia Artificial y a su intersección, en algunos puntos, con el Reglamento General de Protección de Datos.

2. El Reglamento de Inteligencia Artificial

El pasado 12 de julio de 2024 se publicó el Reglamento 2024/1689, en materia de Inteligencia Artificial (en adelante, RIA). Es una norma que pretende establecer un marco legislativo que preserve los valores esenciales de la Unión Europea (en adelante, UE), sin restringir la competitividad europea. Es el resultado de un largo proceso legislativo de consenso que busca conciliar la libertad empresarial y el progreso tecnológico con el respeto a los derechos fundamentales y la seguridad de los sistemas de IA.

El Reglamento es una norma que, a diferencia del Reglamento 2016/679 (Reglamento General de protección de Datos; en adelante, RGPD), no pretende establecer derechos de los ciudadanos ni está dirigida a los usuarios finales de los sistemas de IA[1]. El RIA regula las condiciones de entrada de los sistemas de IA en el mercado económicode la UE. Por ello, los proveedores, distribuidores y responsables del despliegue de terceros países deberán cumplir unas obligaciones para poder introducirse en la UE. Este enfoque integral y preventivo del RIA aspira a producir el conocido como «efecto Bruselas» ya logrado en materia de protección de datos, instaurando estándares mundiales. Por lo tanto, a pesar de ser normativa de ámbito UE produce, inevitablemente, efectos extramuros de este territorio. Hasta ahora la mayoría de países de fuera de la UE, o bien han apostado por seguir el modelo de las regulaciones sectoriales o autorregulaciones del sector privado, o bien han tomado una postura que podríamos catalogar de *laissez-faire*.

El RIA tiene, según su artículo 1.1, el objetivo siguiente:

> «Mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el estado de derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en adelante, «sistemas de IA») en la Unión, así como apoyar la innovación».

[1] Véase el Anexo «Puntos de conexión entre RGPD y RIA».

Pretensión de producir un nuevo efecto Bruselas. Ejemplo.

El considerando 21 RIA dice: «Con el objetivo de garantizar la igualdad de condiciones y la protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas en el presente Reglamento deben aplicarse a los proveedores de sistemas de IA sin discriminación, **con independencia de si están establecidos en la Unión o en un tercer país**, y a los responsables del despliegue de sistemas de IA establecidos en la Unión».

En observancia de estos considerandos y del resto del articulado, creemos que los proveedores no sólo deberán cumplir con el RIA sino que también se verán afectados, consecuentemente, por otros normativas europeas a las que hay que respetar según el propio RIA. Entre estas cabe destacar la de protección de datos, es decir, el RGPD, el cual establece en su artículo 3 que el presente reglamento se aplicará, también, en caso de tratamiento de datos personales por parte de un responsable o encargado esté o no establecido en la Unión, siempre y cuando las actividades del tratamiento estén relacionadas con:

- la oferta de bienes y servicios de los interesados que residan en la Unión, independientemente de si a estos se les requiere su pago;

- el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. Principales definiciones[2]

- **Alfabetización en materia de IA (artículo 3, apartado 56 RIA)**: las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y otras personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar.

- **Evaluación de impacto relativa a los derechos fundamentales (considerando 96 RIA)**: tiene como objetivo que el responsable del despliegue de sistemas de IA determine los riesgos específicos para los derechos de las personas o colectivos de personas que probablemente se vean afectados y defina las medidas que deben adoptarse en caso de que se materialicen estos riesgos.

- **Datos biométricos (artículo 3, apartado 34 RIA)**: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos.

- **Identificación biométrica (artículo 3, apartado 35 RIA)**: el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual psicológico para determinar la identidad de una persona física comparando sus datos

[2] Véase «Glosario de definiciones».

biométricos con los datos biométricos de personas almacenados en una base de datos.

- **Modelo de IA de uso general (artículo 3, apartado 63 RIA)**: un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas diferentes, independientemente de la manera en que el modelo se introduzca en el mercado, y que pueda integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado.

- **Proveedor (artículo 3, apartado 3 RIA)**: persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el que se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente.

- **Responsable del despliegue (artículo 3, apartado 4 RIA)**: persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, excepto cuando su uso se enmarque en una actividad personal de carácter no profesional.

- **Riesgo (artículo 3, apartado 2 RIA)**: la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de este perjuicio.

- **Sistema de IA (artículo 3, apartado 1 RIA)**: sistema basado en una máquina que está diseñado para funcionar con diferentes niveles de autonomía y que puede mostrar capacidad de adaptación después del despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la forma de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

- **Sistema de IA de alto riesgo (artículo 6, apartado 1 RIA)**: un sistema de IA se considerará de alto riesgo cuando el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión o que el producto del que el sistema de IA sea componente de seguridad, o el propio sistema de IA como producto, tenga que someterse a una evaluación de conformidad de terceros para su introducción en el mercado o puesta en servicio de acuerdo con los actos legislativos de armonización de la UE.

- **Sistema de identificación biométrica remota (artículo 3, apartado 41 RIA)**: 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 referencia.

- **Sistema de identificación biométrica remota en tiempo real (artículo 3, apartado 42 RIA)**: un sistema de identificación biométrica remota, en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora

significativa; engloba no sólo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas.

- **Sistema de alto riesgo de identificación biométrica remota en diferido (artículo 3, apartado 43 RIA)**: cualquier sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real.

- **Supervisión humana (artículo 14, punto 1 RIA)**: los sistemas de IA de alto riesgo se diseñarán y desarrollarán de manera que puedan ser vigilados de manera efectiva por personas físicas durante el periodo en que estén en uso, el cual incluye dotarlos de herramientas de interfaz humano-máquina adecuadas.

4. Obligaciones del responsable del despliegue

Las obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo están fijadas en el artículo 26 RIA. Cabe destacar, a efectos del ámbito de la protección de datos, lo siguiente:

- Deben asegurar que los datos de entrada, sean pertinentes y bastante representativos en vista de la finalidad prevista. (ap. 4)

- Conservarán los archivos de registro que los sistemas generen automáticamente, durante un periodo mínimo de seis meses, excepto que otra normativa (especialmente, de protección de datos) disponga algo diferente. (ap. 6)

- Deben utilizar la información facilitada conforme al artículo 13 del RIA para hacer la EIPD por el proveedor para cumplir la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos (ap. 9)

  El artículo 13 establece las obligaciones de «Transparencia y comunicación de información a los responsables del despliegue», que no deben confundirse con las del artículo 50 «Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA». Las primeras son de los proveedores hacia los responsables del despliegue; en cambio, las segundas son de los proveedores y responsables del despliegue hacia personas físicas usuarias que se expongan a un sistema de IA o interaccionen con él.

- IA en el puesto de trabajo: se deberá informar a la representación legal de los trabajadores y a los trabajadores afectados sobre su exposición a la utilización del sistema de IA de alto riesgo. En este sentido, sería recomendable la regulación expresa de este aspecto en la norma que deba complementar el RIA en el derecho interno, de manera similar a los artículos 87-90 LOPD. (ap. 7)

- En el ámbito policial y penal: en caso de que se deniegue la autorización de uso de un sistema de alto riesgo de identificación biométrica remota en diferido, este se dejará de utilizar con efecto inmediato y se eliminarán los datos personales asociados. (ap. 10.II)

- Sin perjuicio de las obligaciones de transparencia del artículo 50, en los casos de los sistemas del anexo III, que tomen decisiones o ayuden a tomar decisiones

relacionadas con personas físicas, se informará a las personas físicas que están expuestas a la utilización del sistema. (ap. 11)

Este último punto hay que relacionarlo con diferentes preceptos del RGPD. En primer lugar, las obligaciones de transparencia del artículo 50, que son las que, en esencia, el proveedor o responsable del despliegue debe satisfacer ante las personas físicas (usuarios) de los sistemas de IA con los que interaccionen o a los que se expongan, se podrían satisfacer en el mismo momento en que hay que dar transparencia a la información que indican los artículos 13 y 14 del RGPD, en cumplimiento del principio general de transparencia del artículo 12 del RGPD (Transparencia de la información, la comunicación y las modalidades de ejercicio de los derechos del interesado). Vid. infra, el apartado «Transparencia y comunicación de la información».

Asimismo, el hecho de que estemos haciendo referencia a sistemas que tomen decisiones o ayuden a tomar decisiones relacionadas con personas físicas hace necesario conectarlo con el artículo 22 del RGPD, relativo a la toma de decisiones individuales automatizadas, incluida la elaboración de perfiles. El apartado 1 de este artículo establece que todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de forma similar. Por lo tanto, un sistema de IA de alto riesgo del anexo III no podría tomar decisiones que produzcan efectos jurídicos hacia personas físicas, si no es bajo el amparo de alguna de las causas o supuestos previstos en los apartados 2, 3 y 4 de este artículo. En el apartado 2 se prevén tres causas de inaplicación del apartado precedente: a) es necesario para la celebración o ejecución de un contrato entre el interesado y el RT; b) está autorizado por el Derecho de la Unión o los EEMM y que se establezcan medidas adecuadas para proteger los derechos, libertades e intereses legítimos de los interesados; o, c) consentimiento explícito del interesado.

Este último punto también hay que ponerlo en relación con el artículo 86 del RIA (derecho a explicación de decisiones tomadas individualmente). El artículo establece que toda persona que se vea afectada por una decisión que el responsable del despliegue haya tomado sobre la base de un sistema de IA de alto riesgo y produzca efectos jurídicos o le afecte considerablemente en los ámbitos de la salud, seguridad o DDFF, puede pedir explicaciones «claras y significativas» sobre el papel de la IA en la decisión. Se trata de uno de los pocos derechos que podríamos considerar que el RIA establece en favor de los usuarios o personas afectadas por el uso de un sistema de IA. El término persona deberíamos interpretarlo en el sentido de persona física, o al menos así se puede deducir de la referencia a la seguridad, salud y derechos fundamentales.

Hay que subrayar que el responsable del despliegue también es el responsable de realizar la evaluación de impacto de derechos fundamentales (en adelante, EIDDFF) del artículo 27 del RIA.

La sección C del anexo VIII del RIA fija la información que deben presentar los responsables del despliegue para la inscripción en el registro de sistemas de alto riesgo. Cabe destacar la necesidad de incluir un resumen de las conclusiones del EIDDFF del 27 del RIA y un resumen del EIPD, cuando proceda.

Excurso: la nueva obligación de aportar un resumen del EIPD en el ámbito de los sistemas de IA de alto riesgo

Si nos limitamos al ámbito del RGPD, no es obligatorio publicar la evaluación de impacto en materia de protección de datos del artículo 35 RGPD. Hay que apuntar, no obstante, que, si bien no representa un requisito jurídico del RGPD, según las directrices del Grupo de Trabajo del artículo 29 (ahora, Comité Europeo de Protección de Datos) sobre la evaluación de impacto relativa a la protección de datos[3], la publicación del EIPD podría ayudar a fomentar la confianza en el tratamiento de los datos y demostrar responsabilidad proactiva y transparencia. En este sentido, se apuntaba que no es necesario que se publique la evaluación entera, sino que ya sería positivo publicar algunas partes o un resumen de la misma.

El artículo 49 del RIA establece la obligación por los proveedores y responsables del despliegue (según el tipo de sistema y riesgo) de registrar los sistemas de IA en la base de datos de la UE del artículo 71 del RIA. El artículo 71 del RIA (Base de datos de la UE para los sistemas de IA de alto riesgo enumerados en el ANEXO III), en el apartado 4 establece que, con la excepción de lo previsto en el apartado 4 del artículo 49[4], la información presentada en la base de datos será accesible y estará a disposición del público de manera sencilla. El contenido que debe presentarse para la inscripción está especificado en el anexo VIII citado con anterioridad. Y por lo que aquí interesa cabe destacar la obligación de aportar un resumen de la evaluación de impacto en materia de protección de datos, que hasta ahora no era en ningún caso una obligación jurídica com tal sinó una recomendación de *soft law*.

En relación con los responsables del despliegue, cuestión que ahora nos corresponde, debemos atender a lo previsto en el artículo 49.3 y 4. El apartado 3 prescribe que antes de poner en servicio o utilizar un sistema de IA de alto riesgo del listado del anexo III, con excepción de los del apartado 2 (infraestructuras críticas), los responsables del despliegue de los sistemas de IA de alto riesgo que sean autoridades públicas, instituciones, órganos u organismos de la Unión, o personas que actúen en su nombre, se registrarán, seleccionarán el sistema y registrarán su uso en la base de datos del artículo 71. El apartado 4 que, como ya hemos avanzado, se refiere a los puntos 1, 6 y 7 del anexo III, excluye, en el caso de la sección C del anexo VIII, la obligación de presentar los puntos 4 y 5. Por lo tanto, en estos casos, no se debe aportar para la inscripción ni el EIDDFF ni el EIPD.

Por tanto, recapitulando y aclarando el alcance de esta nueva obligación en materia de protección de datos: los responsables del despliegue que sean autoridades públicas, instituciones, órganos u organismos de la Unión deberán aportar para la inscripción un resumen del EIPD, que se hará público y accesible para todos, antes de utilizar un sistema de IA de alto riesgo del anexo III (excluyendo los sistemas de los puntos 1, 2, 6 y 7).

---

[3] Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «conlleva probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, WP 248 rev. 1.

[4] Se refiere a los sistemas de IA de alto riesgo de los puntos 1, 6 y 7 del anexo III, en los ámbitos de la garantía del cumplimiento del derecho, la migración, el asilo y la gestión del control fronterizo.

Tiene sentido apuntar que tras analizar todos los supuestos de sistemas de IA de alto riesgo del anexo III se puede llegar a la conclusión de que todos, de forma directa o potencial, en mayor o menor medida, pueden tratar datos personales. El anexo III está dividido en 8 ámbitos que, a la vez, se concretan en 25 tipos de sistemas de IA diferentes. Los 8 ámbitos son los siguientes:

(1) biometría;

(2) infraestructuras críticas;

(3) educación y formación profesional;

(4) empleo, gestión de los trabajadores y acceso al autoempleo;

(5) acceso a servicios privados esenciales y servicios y prestaciones públicos esenciales, y disfrute de estos;

(6) garantía del cumplimiento del derecho;

(7) migración, asilo y gestión del control fronterizo;

(8) Administración de Justicia y procesos democráticos.

En la misma línea, el Comité Europeo de Protección de Datos ha emitido una declaración en la que recomienda que los Estados miembros atribuyan a las autoridades de Control de Protección de Datos las competencias relativas a la supervisión de los sistemas de IA de alto riesgo enumerados en el anexo III comentado anteriormente, especialmente cuando estos sistemas de IA de alto riesgo pertenezcan a sectores donde puedan verse afectados los derechos y libertades de las personas en el ámbito del tratamiento de sus datos personales. Esto, evidentemente, exceptuando los casos en que el RIA atribuya la competencia a otra autoridad con relación a un sector concreto.

Esto contrasta con el artículo 74.8 RIA, que establece la obligación a los Estados miembros de designar como autoridades de vigilancia de mercado a las autoridades de control encargadas de la protección de datos o cualquier otra autoridad designada, cuando se trate de sistemas de IA de alto riesgo de los puntos 1, 6, 7 u 8 del anexo III.

5. Transparencia y comunicación de la información

El considerando 58 del RGPD establece los fundamentos del principio de transparencia. Este exige que toda la información que se dirija, bien al interesado o al público en general, debe ser precisa, concisa, fácilmente accesible y comprensible; y que se utilice un lenguaje claro y sencillo y, en su caso, que se visualice.

Por eso, tal y como fija el artículo 12 RGPD, el responsable del tratamiento tiene la obligación de adoptar las medidas oportunas para facilitar al interesado la información que indican los artículos 13 y 14 RGPD.

La información deberá facilitarse por escrito o por otros medios. En caso de que se proporcione al público mediante una página web se podrá facilitar electrónicamente.

En este sentido, el artículo 13 establece que la información que el responsable del tratamiento facilitará al interesado será la siguiente:

- la identidad y los datos de contacto del responsable y, en su caso, de su representante;
- los datos de contacto del delegado de protección de datos, en su caso;
- las finalidades del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- los intereses legítimos del responsable o de un tercero, en caso de que se dé el supuesto del artículo 6, apartado 1, letra f);
- los destinatarios o categorías de destinatarios de los datos personales, en su caso.
- en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión;
- el plazo durante el cual se conservarán los datos personales;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento; así como el derecho a la portabilidad de los datos;
- si se trata de un supuesto del artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento;
- el derecho a presentar una reclamación ante la autoridad de control;
- si la comunicación es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales;
- la existencia de decisiones automatizadas a la que se refiere el artículo 22 RGPD;

En caso de que el responsable del tratamiento utilice los datos personales para una finalidad diferente para la que se recogieron, informará, previamente al interesado, sobre esta nueva finalidad.

Adicionalmente, el artículo 14 RGPD establece la información a facilitar por el responsable del tratamiento cuando los datos personales no se hayan obtenido directamente del interesado. En este caso, a la información que figura en el artículo 13, hay que añadir la siguiente:

- las categorías de datos personales que se tratan;

- la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

Asimismo, el apartado 4 del artículo 14 prevé que, en caso de que el responsable del tratamiento utilice los datos personales para una finalidad diferente para la que se recogió, informará, previamente al interesado, sobre esta nueva finalidad.

Si vamos al RIA, encontramos que su artículo 13 establece que los sistemas de alto riesgo deben diseñarse y desarrollarse de forma que se garantice un nivel de transparencia suficiente para que los responsables del despliegue interpreten y utilicen correctamente sus resultados de salida e, igualmente, puedan cumplir las obligaciones previstas en la sección 3 (artículos 16 a 27). También se establece que los sistemas de IA de alto riesgo deberán ir acompañados de instrucciones de uso, que deberán incluir información concisa, completa, correcta y clara, que sea pertinente, accesible y comprensible por los responsables del despliegue (ap. 2).

El apartado 3 fija el contenido mínimo de las instrucciones de uso. Cabe destacar de este contenido lo siguiente: el nivel de precisión, solidez y ciberseguridad; los eventuales riesgos que puedan aparecer y afectar a la salud y a la seguridad o a los derechos fundamentales (en conexión con el EIDDFF del artículo 27); las especificaciones relativas a los datos de entrada o cualquier información relevante sobre el conjunto de datos de entrenamiento, validación y prueba empleados, teniendo en cuenta la finalidad del sistema; cualquier información que permita interpretar los resultados de salida a los responsables del despliegue, así como utilizarla correctamente; y, una descripción de los mecanismos incluidos en el sistema que permita a los responsables obtener, almacenar e interpretar correctamente los archivos de registro (artículo 12 RIA). Toda esta información servirá también a los efectos de cumplir con las obligaciones de transparencia e información del RGPD cuando los sistemas de IA traten datos personales.

Esto, sin embargo, no debe confundirse con lo que dispone el artículo 50 RIA, que versa sobre las obligaciones de transparencia de los proveedores o responsables del despliegue hacia las personas físicas.

Concretamente, este artículo prevé que los proveedores deberán garantizar que los sistemas de IA que se destinen a interactuar con personas físicas deben diseñarse y desarrollar de manera que las personas físicas que intervienen estén informadas de que están interactuando con un sistema de inteligencia artificial. Esto no se aplicará cuando resulte evidente desde el punto de vista de una persona física razonablemente informada, atenta y perspicaz; ni cuando los sistemas de IA se destinen a detectar, prevenir, investigar o enjuiciar delitos (ap. 1). Las personas físicas deberán ser informadas de manera clara y distinguible, y no más tarde de la primera interacción o exposición al sistema de IA (ap. 5).

El artículo 11 RIA regula la documentación técnica de un sistema de alto riesgo y su contenido mínimo está especificado en el anexo IV. Por lo que aquí interesa, cabe destacar las letras g) y h) del apartado 1 del anexo mencionado, que establecen que se deben incluir una descripción básica de la interfaz de usuario facilitada al responsable del despliegue y las instrucciones de uso.

6. Protección de datos desde el diseño y por defecto. Responsabilidades.

La protección de datos desde el diseño y por defecto debe recaer en el ámbito del RIA en los proveedores de sistemas de IA, ya que los responsables del despliegue no tendrán, en muchas situaciones, capacidad de incidir en la forma como se tratan los datos por parte de aquel sistema. Así lo dejan ver diferentes considerandos del RIA, entre los que cabe destacar el 69 y el principio del 93. El considerando 69 indica que debe garantizarse el derecho a la intimidad y la protección de datos personales durante todo el ciclo de vida del sistema y se refiere, en concreto, a los principios de minimización y de protección de datos desde el diseño y por defecto. Cita, también, la anonimización, el cifrado y el uso de tecnologías que eviten la transmisión de datos entre las partes, como ejemplos de medidas a adoptar por los proveedores en cumplimiento de estos principios.

Por otro lado, el considerando 93 establece que los riesgos relacionados con los sistemas de IA pueden derivarse de su diseño tanto como de su uso. En cualquier caso, tanto en el momento de determinar los medios del tratamiento de datos personales como en el momento del mismo tratamiento, deberán adoptarse medidas técnicas y organizativas apropiadas, como la seudonimización. Igualmente, debería garantizarse que sólo son tratados, por defecto, los datos personales que sean necesarios para cada una de las finalidades específicas del tratamiento y que no serán accesibles, sin intervención de la persona responsable, a un número indeterminado de personas.[5] Sería interesante que los sistemas de IA no almacenaran aquella información que no tiene interés para la finalidad prevista. Por lo tanto, que el SIA pudiera identificarla para suprimirla inmediatamente, en observancia del principio de limitación del fin y del de minimización de datos.

En este sentido, conviene llevar a colación el considerando 78 del RGPD, expresión del acentuado carácter tuitivo y preventivo que presenta la normativa de protección de datos, que dispone lo siguiente:

> «La protección de los derechos y libertades de las personas físicas respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. Con objeto de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Estas medidas podrían consistir, entre otros, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y, al responsable del tratamiento, crear y mejorar elementos de seguridad. **Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, debe alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones**, y que se aseguren, con la debida atención al estado de la técnica, que **los responsables y los encargados del tratamiento están en condiciones de cumplir con sus obligaciones en materia de protección de datos**. Los principios de la protección

[5] Debería verse el impacto de este último punto en el ámbito de las inteligencias artificiales generativas.

de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.»

La intervención del proveedor debe permitir cumplir al resto de actores los principios del artículo 25 RGPD. Después se deberán, por tanto, elegir de forma acertada (por parte de los responsables del despliegue) los productos, servicios y aplicaciones (en este caso, sistema de IA) que, conforme el estado de la técnica, cumplan con la normativa de protección de datos de forma también proactiva. En definitiva, que deben elegir sistemas de IA *privacy friendly*.

Por lo tanto, llevando esta observación al ámbito de la inteligencia artificial, podemos concluir que, sí, los proveedores también deben tener en cuenta («... debe alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos ...») el derecho a la protección de datos cuando diseñen y programen los sistemas de IA. Así, los proveedores deben diseñar sistemas de IA que sean aptos para que los responsables del despliegue puedan utilizarlos sin infringir la normativa de protección de datos por razones que no les son imputables.

Aunque el artículo 16 («Obligaciones de los proveedores de los sistemas de IA de alto riesgo») no fije ninguna obligación directa en materia de protección de datos, sí que podemos atribuirlas en virtud de:

- (1) la remisión que hace el artículo en la **sección 2** del mismo capítulo, de la que han de velar el cumplimiento; en ella se encuentra, entre otros, el artículo 10 «Datos y gobernanza de datos»;

- (2) el **considerando 10** del RIA cuando dice que «El presente Reglamento no pretende afectar a la aplicación del Derecho de la Unión vigente en materia de protección de datos personales ...» y el **artículo 2.7** RIA («... El presente Reglamento no afectará a los reglamentos (UE) 2016/679 o (UE) 2018/1725 ni a las directivas 2002/58/CE o (UE) 2016/680, sin perjuicio del artículo 10, apartado 5, y el artículo 59 del presente Reglamento.») en relación con el **considerando 78** del RGPD mencionado.

Podemos concluir que, si bien el tratamiento de datos derivado del uso de sistemas de IA es responsabilidad del responsable del despliegue, en cuanto al principio de protección desde el diseño y por defecto también recaería en un grado importante sobre el proveedor. Además, se debería tener en cuenta el principio de responsabilidad proactiva en cuanto a la valoración de si la protección de datos ha sido un aspecto tenido en cuenta a la hora de elegir el sistema de IA.

7. Supervisión humana y alfabetización

El RIA no crea ni prevé ninguna figura específica para realizar las tareas de supervisión o vigilancia de los sistemas de IA. Sin embargo, el considerando 73 y el artículo 26.2 (obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo) establecen que los responsables del despliegue encargarán la supervisión humana de los

sistemas a personas físicas que tengan la competencia, la formación y la autoridad necesarias.

Por lo tanto, habrá que formar a los trabajadores de la entidad. En este punto, son importantes los considerandos 20 y 91 y el artículo 4 RIA, en materia de alfabetización.

El considerando 20 nos indica que la alfabetización en materia de IA debe proporcionar a todos los agentes pertinentes de la cadena de valor de la IA los conocimientos necesarios para garantizar el cumplimiento adecuado y la correcta ejecución del RIA. Y, por su parte, el considerando 91 establece que los responsables del despliegue deben garantizar que las personas encargadas de poner en práctica las instrucciones de uso y la supervisión humana establecidas en la RIA tienen las competencias necesarias, en particular un nivel adecuado de alfabetización, formación y autoridad en materia de IA para ejercer adecuadamente estas tareas.

El principal artículo dentro del texto del RIA en materia de alfabetización es el 4, «Alfabetización en materia de IA». Este prevé lo siguiente:

> «Los proveedores y responsables del despliegue de sistemas de IA adoptarán medidas para garantizar que, en la mayor medida posible, su personal y otras personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA, teniendo en cuenta sus conocimientos técnicos, su experiencia, su educación y su formación, así como el contexto previsto de uso de los sistemas de IA y las personas o los colectivos de personas en las que se utilizarán estos sistemas».

Igualmente, el considerando 83 recuerda que para garantizar la seguridad jurídica y facilitar el cumplimiento del Reglamento es necesario esclarecer la función y las obligaciones específicas de los operadores de toda la cadena de valor.

Sería interesante también analizar qué papel debe tomar el delegado de Protección de Datos en relación con la normativa de inteligencia artificial. En todo caso, respecto a los sistemas de IA que traten datos personales mantendría todas sus funciones.

8. Cadena de valor de la IA y proceso de mejora continua

Es relevante lo que fija el artículo 25 RIA (véase también el considerando 84), que hace que, en ciertas situaciones, otras figuras como el responsable del despliegue, asuman obligaciones propias del proveedor en los sistemas de alto riesgo. Este supuesto se da cuando, por ejemplo, un responsable del despliegue pone su nombre o marca en un sistema de alto riesgo, modifica sustancialmente este sistema o modifica la finalidad prevista de un sistema de IA (incluidos los de uso general), de tal forma que se convierte en un sistema de IA de alto riesgo.

El artículo 26.5 RIA establece que los responsables del despliegue tienen el deber de vigilar el correcto funcionamiento de los sistemas sobre la base de las instrucciones de uso y, cuando proceda, el de informar al proveedor o distribuidor y a la autoridad nacional competente (vigilancia poscomercialización). El deber de información «sin demora indebida» se aplica si se aprecia que el uso de sistema podría generar un riesgo en el sentido del

artículo 79.1, cuando se detecte un incidente grave. Se entienden como riesgos que puedan generar un incidente grave aquellos que afecten a la salud, la seguridad o los derechos fundamentales. Por lo tanto, la protección de datos, como derecho fundamental, quedaría incluida dentro del ámbito de vigilancia de los responsables del despliegue que pueden dar lugar a riesgos que hagan activar el procedimiento del artículo 79 que puede hacer que se suspenda el uso del sistema en cuestión.

Estos procedimientos harán que la relación entre el proveedor y el responsable del despliegue sea estrecha, de tal forma que, al encontrar un error este sea enmendado de la forma más rápida posible por la persona correspondiente dentro de la cadena de valor.

9. Medidas de promoción por los responsables del despliegue

El artículo 62 prevé una serie de medidas a tomar por los Estados miembros (en particular en las pymes y empresas emergentes, y en algún caso en las autoridades públicas locales). En concreto, se establecen las siguientes:

- Acceso prioritario a los espacios controlados de pruebas para la IA.
- Actividades de sensibilización y formación específicas sobre el RIA.
- Canales de comunicación, con la intención de proporcionar asesoramiento y responder a dudas planteadas en relación con el RIA.
- Fomento de la participación en el proceso de desarrollo de la normalización.

También se establecen obligaciones para la Oficina de la IA (Comisión Europea), como las siguientes:

- Facilitar modelos normalizados.
- Desarrollar una plataforma única de información.
- Organizar campañas de comunicación para sensibilizar con respecto a las obligaciones derivadas del RIA.
- Evaluar y fomentar la convergencia de las mejores prácticas en los procedimientos de contratación pública en relación con los sistemas de IA.

10. Bibliografía

Barrio Andrés, M. (dir.) (2024). *El Reglamento Europeo de Inteligencia Artificial*. Tirant lo Blanch.

Terrón Santos, D., & Domínguez Álvarez, J. L., (2019). *Nueva regulación de la protección de datos: y su perspectiva digital* (Tercera edición). Editorial Comares.

Glosario de definiciones

Alfabetización en materia de IA (artículo 3, apartado 56 RIA): las capacidades, los conocimientos y la comprensión que permiten a los proveedores, responsables del despliegue y otras personas afectadas, teniendo en cuenta sus respectivos derechos y obligaciones en el contexto del presente Reglamento, llevar a cabo un despliegue informado de los sistemas de IA y tomar conciencia de las oportunidades y los riesgos que plantea la IA, así como de los perjuicios que puede causar.

Archivos de registro (artículo 12, punto 1 RIA): registro automático de eventos a lo largo de todo el ciclo de vida del sistema.

Autoridad de control (artículo 4, apartado 21 RGPD): la autoridad pública independiente establecida por un Estado miembro de acuerdo con el artículo 51.

Autoridad de vigilancia del mercado (artículo 3, apartado 26 RIA): la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020.

Autoridad nacional competente (artículo 3, apartado 48 RIA): una autoridad notificante o una autoridad de vigilancia del mercado; en cuanto 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.

Autoridad notificante (artículo 3, apartado 19 RIA): la autoridad nacional responsable de establecer y llevar a cabo los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su supervisión.

Evaluación de conformidad (artículo 3, apartado 20 RIA): el proceso por el que se demuestra si se han cumplido los requisitos establecidos en el capítulo III, sección 2, en relación con un sistema de IA de alto riesgo.

Evaluación de impacto relativa a los derechos fundamentales (considerando 96 RIA): tiene como objetivo determinar los riesgos específicos para los derechos de las personas o colectivos de personas que probablemente se vean afectados y define las medidas que deben adoptarse en caso de que se materialicen estos riesgos.

Evaluación de impacto relativa a la protección de datos (considerando 90 RGPD): el responsable, antes del tratamiento, debe hacer una con el fin de valorar su gravedad y la probabilidad del alto riesgo, teniendo en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento y los orígenes del riesgo.

Comercialización (artículo 3, apartado 10 RIA): el suministro de un sistema de IA o de un modelo de IA de uso general para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, previo pago o gratuitamente.

Componente de seguridad (artículo 3, apartado 14 RIA): un componente de un producto o un sistema de IA que cumpla una función de seguridad para tal producto o sistema de IA, o cuyo fallo o defecto de funcionamiento ponga en peligro la salud y la seguridad de las personas o bienes.

Consentimiento del interesado (artículo 4, apartado 11 RGPD): toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le concierne.

Datos biométricos (artículo 3, apartado 34 RIA): datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos.

Datos de entrada (artículo 3, apartado 33 RIA): datos proporcionados a un sistema de IA u obtenidos por este destinados a producir un resultado de salida.

Datos de entrenamiento (artículo 3, apartado 29 RIA): los datos utilizados para entrenar un sistema de IA mediante el ajuste de sus parámetros entrenables.

Datos personales (artículo 4, apartado 1 RGPD): toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de esta persona.

Destinatario (artículo 4, apartado 9 RGPD): la persona física o jurídica, autoridad pública, servicio u otro organismo a quien se comunican datos personales, se trate o no de un tercero. Sin embargo, no se considerarán destinatarios a las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o los Estados miembros; el tratamiento de estos datos por estas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.

Distribuidor (artículo 3, apartado 7 RIA): una persona física o jurídica que forme parte de la cadena de suministro, diferente a la del proveedor o del importador, que comercialice un sistema de IA en el mercado de la Unión.

Elaboración de perfiles (artículo 4, punto 4 RGPD): toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o preceder aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de esta persona física.

Empresa (artículo 4, apartado 18 RGPD): persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desarrollen regularmente una actividad económica.

Espacios controlados de pruebas para la IA (artículo 3, apartado 55 RIA): marco controlado establecido por una autoridad competente que ofrece a los proveedores y proveedores potenciales de sistemas de IA la posibilidad de desarrollar, entrenar, validar y probar, en condiciones reales cuando proceda, un sistema de IA innovador, con arreglo a un plan del espacio controlado de pruebas y durante un tiempo limitado, bajo supervisión reguladora.

FINALIDAD prevista (artículo 3, apartado 12 RIA): el uso por el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica.

Garantía del cumplimiento del Derecho (artículo 3, apartado 46 RIA): 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 ante amenazas para la seguridad pública y la prevención de estas amenazas.

Identificación biométrica (artículo 3, apartado 35 RIA): el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos.

Incidente grave (artículo 3, apartado 49 RIA): un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las consecuencias siguientes:

a) la muerte de una persona o un perjuicio grave para la salud;

b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas;

c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales;

d) daños graves a la propiedad o al medio ambiente.

Infraestructura crítica (artículo 3, apartado 62 RIA): una infraestructura crítica tal como se define en el artículo 2, punto 4, de la Directiva (UE) 2022/2557.

Instrucciones de uso (artículo 3, apartado 15 RIA): la información facilitada por el proveedor para informar al responsable del despliegue, en particular, de la finalidad prevista y de la utilización correcta de un sistema de IA.

Introducción en el mercado (artículo 3, apartado 9 RIA): la primera comercialización en el mercado de la Unión de un sistema de IA o de un modelo de IA de uso general.

Limitación del tratamiento (artículo 4, apartado 3 RGPD): la marcación de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

Modelo de IA de uso general (artículo 3, apartado 63 RIA): un modelo de IA, también uno entrenado con un gran volumen de datos utilizando autosupervisión a gran escala, que presenta un grado considerable de generalidad y es capaz de realizar de manera competente una gran variedad de tareas diferentes, independientemente de la manera en que el modelo se introduzca en el mercado, y que pueda integrarse en diversos sistemas o aplicaciones posteriores, excepto los modelos de IA que se utilizan para actividades de investigación, desarrollo o creación de prototipos antes de su introducción en el mercado.

Oficina de IA (artículo 3, apartado 47 RIA): la función de la Comisión consistente en contribuir a la implantación, el seguimiento y la supervisión de los sistemas de IA y modelos de IA de uso general, y en la gobernanza de la IA prevista por la Decisión de la Comisión de 24 de enero de 2024, las referencias hechas en el presente Reglamento en la Oficina de IA se entenderán hechas a la Comisión.

Operador (artículo 3, apartado 8 RIA): un proveedor, fabricante del producto, responsable del despliegue, representante autorizado, importador o distribuidor.

Organización internacional (artículo 4, apartado 26 RGPD): una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

Puesta en servicio (artículo 3, apartado 11 RIA): suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista.

Proveedor (artículo 3, apartado 3 RIA): persona física o jurídica, autoridad pública, órgano u organismo que desarrolle un sistema de IA o un modelo de IA de uso general o para el cual se desarrolle un sistema de IA o un modelo de IA de uso general y lo introduzca en el mercado o ponga en servicio el sistema de IA con su propio nombre o marca, previo pago o gratuitamente.

Seudonimización (artículo 4, apartado 5 RGPD): el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que esta información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Representante (artículo 4, apartado 17 RGPD): persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento de acuerdo con el artículo 27, represente al responsable o al encargado en lo referente a sus respectivas obligaciones en virtud del presente Reglamento.

Responsable del despliegue (artículo 3, apartado 4 RIA): persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, excepto cuando su uso se enmarque en una actividad personal de carácter no profesional.

Responsable del tratamiento (artículo 4, apartado 7 RGPD): la persona física o jurídica, autoridad pública, servicio u organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Riesgo (artículo 3, apartado 2 RIA): la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de este perjuicio.

Sistema de IA (artículo 3, apartado 1 RIA): sistema basado en una máquina que está diseñado para funcionar con diferentes niveles de autonomía y que puede mostrar capacidad de adaptación después del despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la forma de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

Sistema de IA de alto riesgo (artículo 6, apartado 1 RIA): un sistema de IA se considerará de alto riesgo cuando el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto que entre en el ámbito de aplicación de los actos legislativos de armonización de la Unión o que el producto del que el sistema de IA sea componente de seguridad, o el propio sistema de IA como producto, tenga que someterse a una evaluación de conformidad de terceros para su introducción en el mercado o puesta en servicio de acuerdo con los actos legislativos de armonización de la UE.

Sistema de identificación biométrica remota (artículo 3, apartado 41 RIA): 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 referencia.

Sistema de identificación biométrica remota en tiempo real (artículo 3, apartado 42 RIA): un sistema de identificación biométrica remota, en el que la recogida de los datos biométricos, la comparación y la identificación se producen sin una demora significativa; engloba no sólo la identificación instantánea, sino también, a fin de evitar la elusión, demoras mínimas limitadas.

Sistema de alto riesgo de identificación biométrica remota en diferido (artículo 3, apartado 43 RIA): cualquier sistema de identificación biométrica remota que no sea un sistema de identificación biométrica remota en tiempo real.

Sistema de vigilancia poscomercialización (artículo 3, apartado 25 RIA): todas las actividades realizadas por los proveedores de sistemas de IA destinadas a recoger y examinar la experiencia obtenida con el uso de sistemas de IA que introduzcan en el mercado o pongan en servicio, con objeto de detectar la posible necesidad de aplicar inmediatamente cualquier tipo de medida correctiva o preventiva que sea necesaria.

Supervisión humana (artículo 14, punto 1 RIA): los sistemas de IA de alto riesgo se diseñarán y desarrollarán de manera que puedan ser vigilados de manera efectiva por personas físicas durante el periodo en que estén en uso, el cual incluye dotarlos de herramientas de interfaz humano-máquina adecuadas.

Tercero (artículo 4, apartado 10 RGPD): persona física o jurídica, autoridad pública, servicio u organismo diferente del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Tratamiento (artículo 4, apartado 2 RGPD): cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por

procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación para transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Anexo: Puntos de conexión entre el RGPD y el RIA[6]

- Artículo 1. Objeto

- Artículo 2. Ámbito de aplicación material vs. artículo 2. Ámbito de aplicación.

- El RIA, a diferencia del RGPD, no establece los principios de la normativa que desarrolla. Asimismo, tampoco establece derechos, ni se dirige a los consumidores finales, sino que se centra básicamente en el establecimiento de obligaciones para los proveedores, responsables del despliegue de los sistemas, etc.

- Definiciones: art. 4 vs. art. 3. El número de definiciones difiere en gran medida, ya que en el RGPD hay 26 y en el RIA hay más del doble, 68. Esto se debe esencialmente a que el RIA es una norma mucho más técnica que el RGPD.

[6] A lo largo de este anexo se han utilizado las versiones oficiales de los reglamentos en castellano.

RGPD	RIA
Artículo 1. Objeto 1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. 2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. 3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.	**Artículo 1. Objeto** 1. El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, «sistemas de IA») en la Unión así como prestar apoyo a la innovación. 2. El presente Reglamento establece: a) normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión; b) prohibiciones de determinadas prácticas de IA; c) requisitos específicos para los sistemas de IA de alto riesgo y obligaciones para los operadores de dichos sistemas; d) normas armonizadas de transparencia aplicables a determinados sistemas de IA; e) normas armonizadas para la introducción en el mercado de modelos de IA de uso general; f) normas sobre el seguimiento del mercado, la vigilancia del mercado, la gobernanza y la garantía del cumplimiento; g) medidas en apoyo de la innovación, prestando especial atención a las pymes, incluidas las empresas emergentes.
Artículo 2. Ámbito de aplicación material 1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. 2. El presente Reglamento no se aplica al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;	**Artículo 2. Ámbito de aplicación** 1. El presente Reglamento se aplicará a: a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA o que introduzcan en el mercado modelos de IA de uso general en la Unión, con independencia de si dichos proveedores están establecidos o ubicados en la Unión o en un tercer país; b) los responsables del despliegue de sistemas de IA que estén establecidos o ubicados en la Unión; c) los proveedores y responsables del despliegue de sistemas de IA que estén establecidos o ubicados en un tercer país, cuando los resultados de salida generados por el sistema de IA se utilicen en la Unión; d) los importadores y distribuidores de sistemas

RGPD	RIA
c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención. 3.El Reglamento (CE) n.o 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.o 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98. 4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.	de IA; e) los fabricantes de productos que introduzcan en el mercado o pongan en servicio un sistema de IA junto con su producto y con su propio nombre o marca; f) los representantes autorizados de los proveedores que no estén establecidos en la Unión; g) las personas afectadas que estén ubicadas en la Unión. 2. A los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 1, y relativos a productos regulados por los actos legislativos de armonización de la Unión enumerados en la sección B del anexo I, únicamente se les aplicará el artículo 6, apartado 1, y los artículos 102 a 109 y el artículo 112. El artículo 57 se aplicará únicamente en la medida en que los requisitos para los sistemas de IA de alto riesgo en virtud del presente Reglamento se hayan integrado en dichos actos legislativos de armonización de la Unión. 3. El presente Reglamento no se aplicará a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afectará a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado el desempeño de tareas en relación con dichas competencias. El presente Reglamento no se aplicará a los sistemas de IA que, y en la medida en que, se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades. El presente Reglamento no se aplicará a los sistemas de IA que no se introduzcan en el mercado o no se pongan en servicio en la Unión en los casos en que sus resultados de salida se utilicen en la Unión exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades. 4. El presente Reglamento no se aplicará a las autoridades públicas de terceros países ni a las

RGPD	RIA
	organizaciones internacionales que entren dentro del ámbito de aplicación de este Reglamento conforme al apartado 1 cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de acuerdos o de la cooperación internacionales con fines de garantía del cumplimiento del Derecho y cooperación judicial con la Unión o con uno o varios Estados miembros, siempre que tal tercer país u organización internacional ofrezca garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas. 5. El presente Reglamento no afectará a la aplicación de las disposiciones relativas a la responsabilidad de los prestadores de servicios intermediarios que figuran en el capítulo II del Reglamento (UE) 2022/2065. 6. El presente Reglamento no se aplicará a los sistemas o modelos de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad. 7. El Derecho de la Unión en materia de protección de los datos personales, la intimidad y la confidencialidad de las comunicaciones se aplicará a los datos personales tratados en relación con los derechos y obligaciones establecidos en el presente Reglamento. El presente Reglamento no afectará a los Reglamentos (UE) 2016/679 o (UE) 2018/1725 ni a las Directivas 2002/58/CE o (UE) 2016/680, sin perjuicio del artículo 10, apartado 5, y el artículo 59 del presente Reglamento. 8. El presente Reglamento no se aplicará a ninguna actividad de investigación, prueba o desarrollo relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio. Estas actividades se llevarán a cabo de conformidad con el Derecho de la Unión aplicable. Las pruebas en condiciones reales no estarán cubiertas por esa exclusión. 9. El presente Reglamento se entenderá sin perjuicio de las normas establecidas por otros actos jurídicos de la Unión relativos a la protección de los consumidores y a la seguridad de los productos.

RGPD	RIA
	10. El presente Reglamento no se aplicará a las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional. 11. El presente Reglamento no impedirá que la Unión o los Estados miembros mantengan o introduzcan disposiciones legales, reglamentarias o administrativas que sean más favorables a los trabajadores en lo que atañe a la protección de sus derechos respecto al uso de sistemas de IA por parte de los empleadores ni que fomenten o permitan la aplicación de convenios colectivos que sean más favorables a los trabajadores. 12. El presente Reglamento no se aplicará a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto, a menos que se introduzcan en el mercado o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 o del artículo 50.

Definiciones del artículo 4 del RGPD[7]	Definiciones del artículo 3 del RIA
1. Datos personales	1. Sistema de IA
2. Tratamiento	2. Riesgo
3. Limitación del tratamiento	3. Proveedor
4. Elaboración de perfiles	4. Responsable del despliegue
5. Seudonimización	5. Representante autorizado
6. Archivo	6. Importador
7. Responsable del tratamiento o responsable	7. Distribuidor
8. Encargado del tratamiento o encargado	8. Operador
9. Destinatario	9. Introducción en el mercado
10. Tercero	10. Comercialización
11. Consentimiento del interesado	11. Puesta en servicio
12. Violación de la seguridad de los datos personales	12. Finalidad prevista
13. Datos genéticos	13. Uso indebido razonablemente previsible
14. Datos biométricos	14. Componente de seguridad
15. Datos relativos a la salud	15. Instrucciones de uso
16. Establecimiento principal	16. Recuperación de un sistema de IA
17. Representante	17. Retirada de un sistema de IA
18. Empresa	18. Funcionamiento de un sistema de IA
19. Grupo empresarial	19. Autoridad notificante
20. Normas corporativas vinculantes	20. Evaluación de la conformidad
21. Autoridad de control	21. Organismo de evaluación de la conformidad
22. Autoridad de control interesada	22. Organismo notificado
23. Tratamiento transfronterizo	23. Modificación sustancial
24. Objeción pertinente y motivada	24. Marcaje CE
25. Servicio de la sociedad de la información	25. Sistema de vigilancia poscomercialización
26. Organización internacional	26. Autoridad de vigilancia del mercado
	27. Norma armonizada
	28. Especificación común
	29. Datos de entrenamiento
	30. Datos de validación
	31. Conjunto de datos de validación
	32. Datos de prueba
	33. Datos de entrada
	34. Datos biométricos
	35. Identificación biométrica
	36. Verificación biométrica
	37. Categoría especial de datos personales
	38. Datos operativos sensibles
	39. Sistema de reconocimiento de emociones
	40. Sistema de categorización biométrica
	41. Sistema de identificación biométrica remota
	42. Sistema de identificación biométrica remota en tiempo real
	43. Sistema de identificación biométrica remota en diferido
	44. Espacio de acceso público
	45. Autoridad garante del cumplimiento del

[7] Código de colores: remisión del RIA al RGPD (verde); paralelismos (naranja); y diferencias (rojo).

Definiciones del artículo 4 del RGPD[7]	Definiciones del artículo 3 del RIA
	Derecho 46. Garantía del cumplimiento del Derecho 47. Oficina de IA 48. Autoridad nacional competente 49. Incidente grave 50. Datos personales 51. Datos no personales 52. Elaboración de perfiles 53. Plan de la prueba en condiciones reales 54. Plano del espacio controlado de pruebas 55. Espacio controlado de pruebas para la IA 56. Alfabetización en materia de IA 57. Pruebas en condiciones reales 58. Sujeto 59. Consentimiento informado 60. Ultrasuplantación 61. Infracción generalizada 62. Infraestructura crítica 63. Modelo de IA de uso general 64. Capacidades de gran impacto 65. Riesgo sistémico 66. Sistema de IA de uso general 67. Operación de coma flotante 68. Proveedor posterior

- La definición 37 (Categorías especiales de datos personales) del RIA remite al artículo 9, apartado 1, del RGPD (Tratamiento de categorías especiales de datos personales).

- Las definiciones 50 y 51 (Datos personales y datos no personales) del RIA remiten a la definición 1 (Datos personales) del RGPD.

- La definición 52 (Elaboración de perfiles) del RIA remite a la definición 4 (Elaboración de perfiles) del RGDP.

- La definición 34 (Datos biométricos) del RIA se podría haber remitido a la definición 14 (Datos biométricos) del RGPD:

Definición 14 del RGPD	Definición 34 del RIA
«datos biométricos»: 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.	«datos biométricos»: los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos.

- Podemos establecer un paralelismo entre las definiciones siguientes:

RGPD	RIA
Definició 7: «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.	Definició 4: «responsable del despliegue»: una persona física o jurídica, o autoridad pública, órgano u organismo que utilice un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional.
Definició 11: «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.	Definició 59: «consentimiento informado»: la expresión libre, específica, inequívoca y voluntaria por parte de un sujeto de su voluntad de participar en una determinada prueba en condiciones reales tras haber sido informado de todos los aspectos de la prueba que sean pertinentes para su decisión de participar.
Definició 12: «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.	Definició 49: «incidente grave»: un incidente o defecto de funcionamiento de un sistema de IA que, directa o indirectamente, tenga alguna de las siguientes consecuencias: a) el fallecimiento de una persona o un perjuicio grave para su salud; b) una alteración grave e irreversible de la gestión o el funcionamiento de infraestructuras críticas; c) el incumplimiento de obligaciones en virtud del Derecho de la Unión destinadas a proteger los derechos fundamentales; d) daños graves a la propiedad o al medio ambiente.
Definició 17: «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.	Definició 5: «representante autorizado»: una persona física o jurídica ubicada o establecida en la Unión que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA o de un modelo de IA de uso general para cumplir las obligaciones y llevar a cabo los procedimientos establecidos en el presente Reglamento en representación de dicho proveedor.

RGPD	RIA
Definició 21: «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51.	Definició 26: «autoridad de vigilancia del mercado»: la autoridad nacional que lleva a cabo las actividades y adopta las medidas previstas en el Reglamento (UE) 2019/1020.
	Definició 48: «autoridad nacional competente»: 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.

- Cierta similitud entre lo que pretende realizar la sección 1 del capítulo IV del RGPD (establecer obligaciones por el responsable del tratamiento y el encargado del tratamiento -art. 24 a 31-) y ciertos apartados del RIA, como bien, la sección 3 del capítulo III (Obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y de otras partes -art. 16 a 27-), capítulo IV (Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA -art. 50-), secciones 2 y 3 del capítulo V (Obligaciones de los proveedores de modelos de IA de uso general -art. 53 y 54-; Obligaciones de los proveedores de modelos de IA de uso general con riesgo sistémico -art. 55-).

- El capítulo VII del RIA (Gobernanza -art. 64 a 70-) se puede asimilar a diferentes apartados del RGPD:

    - El equivalente de la sección 1 del capítulo VII RIA (Gobernanza a escala de la Unión -art. 64 a 69-) sería la sección 3 del capítulo VII RGPD (Comité europeo de protección de datos -art. 68 a 76-).

    - El equivalente de la sección 2 del capítulo VII RIA (Autoridades nacionales competentes -art. 70-) sería el capítulo VI RGPD (Autoridades de control independientes -art. 51 a 59-). También se podría considerar equivalente a la sección 4 del capítulo III (Autoridades notificantes y organismos notificados -art. 28 a 39-).

- El equivalente del artículo 35 del RGPD (Evaluación de impacto relativa a la protección de datos) sería el artículo 27 del RIA (Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo).

Article 35 RGPD	Article 27 RIA
Artículo 35. Evaluación de impacto relativa a la protección de datos 1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares. 2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos. 3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de: a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público. 4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68. 5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de	**Artículo 27. Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo** 1. Antes de desplegar uno de los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2, con excepción de los sistemas de IA de alto riesgo destinados a ser utilizados en el ámbito enumerado en el anexo III, punto 2, los responsables del despliegue que sean organismos de Derecho público, o entidades privadas que prestan servicios públicos, y los responsable del despliegue de sistemas de IA de alto riesgo a que se refiere el anexo III, punto 5, letras b) y c), llevarán a cabo una evaluación del impacto que la utilización de dichos sistemas puede tener en los derechos fundamentales. A tal fin, los responsables del despliegue llevarán a cabo una evaluación que consistirá en: a) una descripción de los procesos del responsable del despliegue en los que se utilizará el sistema de IA de alto riesgo en consonancia con su finalidad prevista; b) una descripción del período de tiempo durante el cual se prevé utilizar cada sistema de IA de alto riesgo y la frecuencia con la que está previsto utilizarlo; c) las categorías de personas físicas y colectivos que puedan verse afectados por su utilización en el contexto específico; d) los riesgos de perjuicio específicos que puedan afectar a las categorías de personas físicas y colectivos determinadas con arreglo a la letra c) del presente apartado, teniendo en cuenta la información facilitada por el proveedor con arreglo al artículo 13; e) una descripción de la aplicación de medidas de supervisión humana, de acuerdo con las instrucciones de uso; f) las medidas que deben adoptarse en caso de que dichos riesgos se materialicen, incluidos los acuerdos de gobernanza interna y los mecanismos de reclamación. 2. La obligación descrita con arreglo al apartado 1 se aplicará al primer uso del sistema de IA de alto riesgo. En casos similares, el responsable del despliegue podrá basarse en evaluaciones de impacto relativas a los derechos fundamentales realizadas previamente o a evaluaciones de impacto existentes realizadas por los proveedores. Si, durante el uso del sistema de IA de alto riesgo, el responsable del despliegue

Article 35 RGPD	Article 27 RIA
impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité. 6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión. 7. La evaluación deberá incluir como mínimo: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. 8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos. 9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la	considera que alguno de los elementos enumerados en el apartado 1 ha cambiado o ha dejado de estar actualizado, adoptará las medidas necesarias para actualizar la información. 3. Una vez realizada la evaluación a que se refiere el apartado 1 del presente artículo, el responsable del despliegue notificará sus resultados a la autoridad de vigilancia del mercado, presentando el modelo cumplimentado a que se refiere el apartado 5 del presente artículo. En el caso contemplado en el artículo 46, apartado 1, los responsables del despliegue podrán quedar exentos de esta obligación de notificación. 4. Si ya se cumple cualquiera de las obligaciones establecidas en el presente artículo mediante la evaluación de impacto relativa a la protección de datos realizada con arreglo al artículo 35 del Reglamento (UE) 2016/679 o del artículo 27 de la Directiva (UE) 2016/680, la evaluación de impacto relativa a los derechos fundamentales a que se refiere el apartado 1 del presente artículo complementará dicha evaluación de impacto relativa a la protección de datos. 5. La Oficina de IA elaborará un modelo de cuestionario, también mediante una herramienta automatizada, a fin de facilitar que los responsables del despliegue cumplan sus obligaciones en virtud del presente artículo de manera simplificada.

Article 35 RGPD	Article 27 RIA
seguridad de las operaciones de tratamiento. 10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento. 11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.	

- El artículo 31 RGPD establece, en el marco de las obligaciones generales que se imponen al responsable del tratamiento y al encargado del tratamiento, la cooperación con la autoridad de control. Igualmente, el RIA hace lo mismo en el artículo 21 (cooperación con las autoridades competentes), en el marco de las obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y otras partes.

- La sección 5 del capítulo IV RGPD regula los códigos de conducta y certificación (art. 40 a 43), la sección 4 del capítulo V RIA regula los códigos de buenas prácticas (art. 56) y el capítulo X RIA regula los códigos de conducta y directrices (art. 95 y 96). También se podría relacionar con la sección 5 del capítulo III (Normas, evaluación de la conformidad, certificados, registro -art. 40 a 49-).

- Podemos realizar una conexión entre el artículo 59 del RIA, que se refiere al tratamiento ulterior de datos personales para el desarrollo de determinados sistemas de IA a favor del interés público en el espacio controlado de pruebas para la IA, y circunstancia prevista en la letra g) del apartado 2 del artículo 9 del RGPD («[e] el tratamiento es necesario por razones de un interés público esencial ...»), que es una excepción a la prohibición del apartado 1 del artículo 9 del RGPD, que se refiere al tratamiento de categorías especiales de datos personales.

- La sección 2 del capítulo IV RGPD (Seguridad de los datos personales -art. 32 a 34-), que regula en el artículo 33 la notificación de una violación de la seguridad de los datos personales a la autoridad de control, es asimilable, mutatis mutandis, a la

sección 2 del capítulo IX RIA (Intercambio de información sobre incidentes graves -art. 73-), que regula en su único artículo la notificación de incidentes graves.

- El equivalente del capítulo X del RGPD (Actos delegados y actos de ejecución -art. 92 y 93-) sería el capítulo XI del RIA (Delegación de poderes y procedimiento de comité -art. 97 y 98-).

- Obviamente, en ambos reglamentos, el último capítulo (XI del RGPD -art. 94 a 99- y XIII del RIA -art. 102 a 113-) se refiere a las disposiciones finales.

¿En qué puntos el RIA cita explícitamente al RGPD?

Se cita un total de 29 veces: 13 en los considerandos, 14 en el articulado y 2 en los anexos.

Ubicación en el RIA	Referencia al RGPD	Contexto/contenido
Considerando 10, 1.er párrafo	Reglamento en general.	Con respecto al derecho fundamental a la protección de datos personales.
Considerando 14	Artículo 4, punto 14.	Concepto de «datos biométricos».
Considerando 39 (dos veces)	Artículo 9, apartado 1 (dos veces).	Tratamiento de datos biométricos.
Considerando 53, 2.º párrafo	Artículo 4, punto 4.	Si el sistema de IA conlleva la elaboración de perfiles en el sentido del RGPD presentan un riesgo significativo de menoscabar la salud, la seguridad o los DDFF.
Considerando 54	Artículo 9, apartado 1.	Clasificación como sistemas de alto riesgo los destinados a ser utilizados para la categorización biométrica conforme a atributos o características sensibles ex 9.1 RGPD.
Considerando 67, 1.er párrafo	Reglamento en general.	Gestión y gobernanza de los datos. Transparencia sobre el fin original de la recopilación de los datos.
Considerando 70 (dos veces)	Reglamento en general. Artículo 9, apartado 2, letra g).	Tratamiento de categorías especiales de datos personales, como cuestión de interés público, para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo y evitar eventuales discriminaciones.
Considerando 95	Reglamento en general.	Garantías de los derechos de identificación biométrica remota en diferido.

Ubicación en el RIA	Referencia al RGPD	Contexto/contenido
Considerando 140 (tres veces)	Artículo 6, apartado 4, y artículo 9, apartado 2, letra g). Obligaciones de los responsables del tratamiento y los derechos de los interesados, en general. Artículo 22, apartado 2, letra b).	Base jurídica para que los proveedores y los proveedores potenciales en el espacio controlado de pruebas para la IA utilicen datos personales recabados para otros fines para desarrollar determinados sistemas de IA a favor del interés público en el espacio controlado de pruebas para la IA. Siguen siendo aplicables. El RIA no debe ofrecer una base jurídica en este sentido.
Artículo 2, apartado 7	Reglamento en general.	Ámbito de aplicación del RIA. El RIA no afectará al RGPD.
Artículo 3, puntos 37, 50, 51 y 52 (cuatro veces)	Artículo 9, apartado 1. Artículo 4, punto 1 (dos veces). Artículo 4, punto 4.	Definiciones de los conceptos de «categorías especiales de datos personales», «datos personales», «datos no personales» y «elaboración de perfiles». Se remite al RGDP.
Artículo 5, apartado 1, letra h), *in fine*	Artículo 9.	Prácticas de IA prohibidas. La prohibición de la letra h) se entiende sin perjuicio de lo dispuesto en el artículo 9 del RGPD en cuanto al tratamiento de datos biométricos con fines diferentes de la garantía del cumplimiento del Derecho.
Artículo 10, apartado 5, al inicio y la letra f) (dos veces)	Reglamento en general (dos veces).	Datos y gobernanza de datos. Tratamiento de categorías especiales de datos personales por parte de los proveedores, para garantizar la detección y corrección de los sesgos asociados a los sistemas de IA de alto riesgo.
Artículo 26, apartados 9 y 10.IV (dos veces)	Artículo 35. Artículo 9.	Obligaciones de los responsables del despliegue de sistemas de IA de alto riesgo. Los responsables utilizarán la información facilitada conforme el artículo 13 del RIA cuando realicen la evaluación de impacto del artículo 35 del RGPD.
Artículo 27, apartado 4	Artículo 35.	Evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo. Si con la evaluación de impacto del RGPD ya se cumple alguna de las obligaciones establecidas en el artículo 27 del RIA, la evaluación de

Ubicación en el RIA	Referencia al RGPD	Contexto/contenido
		impacto de DDFF complementará la de datos del RGDP.
Artículo 50, apartado 3	Reglamento en general.	Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA. Respecto de la normativa de tratamiento de datos por los responsables del despliegue de un sistema de reconocimiento de emociones o de un sistema de categorización biométrica, además de informar sobre el funcionamiento del sistema a las personas físicas expuestas a él.
Artículo 59, apartado 1, letra c)	Artículo 35.	Tratamiento ulterior de datos personales para el desarrollo de determinados sistemas de IA a favor del interés público en el espacio controlado de pruebas para la IA. En el espacio controlado de pruebas, se podrán tratar datos personales recabados lícitamente para otros fines para desarrollar, entrenar y probar determinados sistemas de IA cuando se cumplan, entre otras condiciones, que existan mecanismos de supervisión eficaces para detectar si pueden producirse, durante la experimentación en el espacio controlado de pruebas, riesgos elevados para los derechos y libertades de los interesados.
Artículo 74, apartado 8	Las autoridades de control encargadas de la protección de datos de acuerdo con el Reglamento.	Vigilancia del mercado y control de los sistemas de IA en el mercado de la Unión. En el caso de los sistemas de IA de alto riesgo del anexo III del RIA, punto 1, en la medida en que los sistemas se utilicen a 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 RIA bien a las autoridades de control encargadas de la protección de datos competentes de acuerdo con el RGPD o la Directiva

Ubicación en el RIA	Referencia al RGPD	Contexto/contenido
		(UE) 2016/680, bien a cualquier otra autoridad designada respetando las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680.
Anexo V, apartado 5	Reglamento en general.	Declaración UE de conformidad. Deberá contener, entre otras cosas, una declaración que el sistema de IA, cuando implique el tratamiento de datos personales, se ajusta al RGDP, entre otras normas.
Anexo VIII, sección C, apartado 5	Artículo 35.	Información que debe presentarse para la inscripción en el registro de sistemas de IA de alto riesgo de conformidad con el artículo 49. Sección C - Información que deben presentar los responsables del despliegue de sistemas de IA de alto riesgo de conformidad con el artículo 49, apartado 3. Entre otra información, deberá contener un resumen de la evaluación de impacto relativa a la protección de datos del artículo 35 del RGPD, cuando proceda según el artículo 26, apartado 8, del RIA.