LA GUIA

PRÁCTICA DE INTELIGENCIA ARTIFICIAL

Nº 6

ENERO 2026

IA y protección de datos

ARANZADI LA LEY | KARNOV GROUP

En esta sexta entrega de la Guía Práctica de la Inteligencia Artificial, que Aranzadi LA LEY te facilita de forma gratuita, Moisés Barrio Andrés, letrado del Consejo de Estado, profesor de Derecho digital y experto internacional en regulación digital, analiza la interacción entre el nuevo Reglamento Europeo de Inteligencia Artificial y el Reglamento General de Protección de Datos, explicando cómo ambos marcos deben aplicarse conjuntamente, qué obligaciones imponen en el tratamiento de datos personales y qué retos plantea el uso de la IA en términos de bases jurídicas, derechos de los interesados, gobernanza de datos y gestión de riesgos.

IA y protección de datos

Moisés Barrio Andrés
Letrado del Consejo de Estado, profesor de Derecho digital y experto internacional en regulación digital

El asistente legal basado en Inteligencia Artificial más seguro, preciso y fiable ya está aquí.

Obtén **respuestas fiables** basadas en la normativa siempre vigente, en la **jurisprudencia**, doctrina administrativa y artículos doctrinales.

Obtén una visión completa de la **evolución interpretativa y tendencias en materia administrativa** basada en más de **330.000 documentos y 150 órganos resolutorios**.

Evolución continua
K+ mejora constantemente para adaptarse a las nuevas tendencias del sector legal.

Resume documentación oficial, así como contenido práctico y de autor.

Traduce documentos, resúmenes y las respuestas del asistente legal a **9 idiomas**.

Analiza automáticamente tus documentos y escritos.

Orienta tu caso utilizando argumentos y contrargumentos, localiza y consulta fundamentaciones jurídicas, interpreta preceptos legales y analiza tendencias jurisprudenciales con informes estructurados.

Conversa con los **documentos** de la base de datos y también con los tuyos y extrae la información más relevante en segundos.

Descubre las soluciones en las que hemos incorporado las capacidades de Inteligencia Artificial generativa gracias a **K+**.

ARANZADI Ley

ARANZADI Supra

ARANZADI Infinita

Legalteca

ARANZADI Fusión

ARANZADI One

CISS Fiscal

CISS Laboral

CISS Contable Mercantil

www.aranzadilaley.es/inteligencia-artificial

ARANZADI LA LEY | KARNOV GROUP

Introducción

01

1. INTRODUCCIÓN

El Reglamento europeo de inteligencia artificial (RIA)[1], se promulgó en respuesta a diversas **preocupaciones y riesgos singulares** que plantean las tecnologías de inteligencia artificial (IA). En el ámbito específico de la protección de datos, cabe citar el caso SyRI en los Países Bajos, donde los tribunales sentenciaron que un algoritmo de puntuación de riesgos introducido por el Gobierno holandés no respetaba el derecho a la vida privada.

Ahora bien, el RIA es una normativa muy diferente del Reglamento General de Protección de datos (RGPD), ya que se basa en las normas que regulan la seguridad de los productos y no en la legislación sobre protección de datos[2].

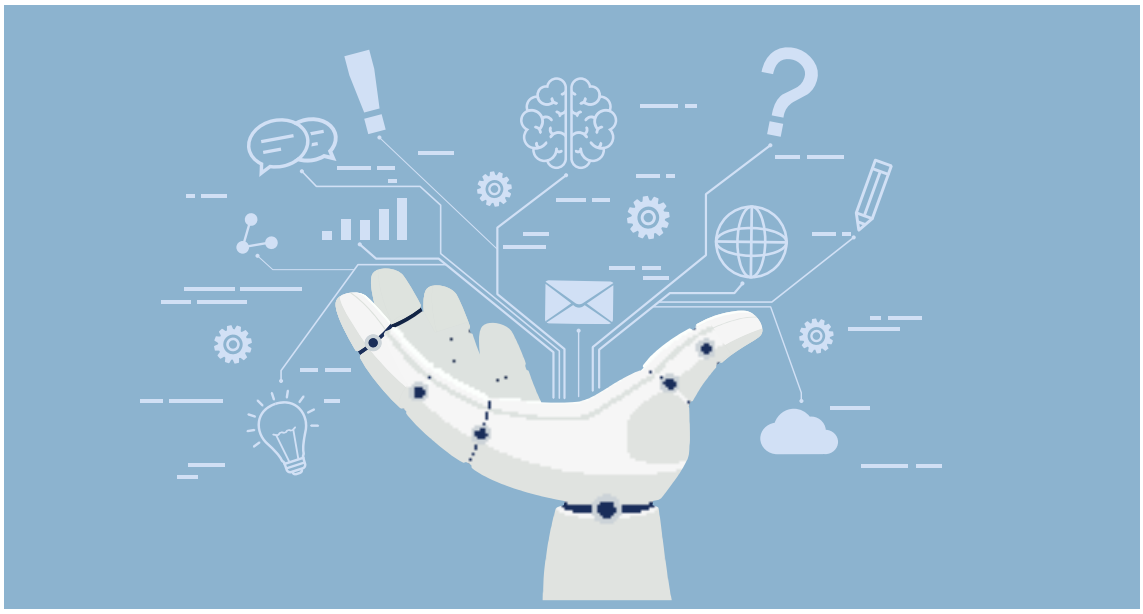
Una **diferencia significativa entre el RGPD y el RIA** proviene de su objeto, es decir, de lo que regulan esas normas jurídicas. El RGPD se centra en el tratamiento de datos personales; dicho de otro modo, en lo que se hace con los datos. El RIA se centra, en cambio, en las tecnologías utilizadas para llevar a cabo ese tratamiento. Regula los sistemas de IA, que define como un tipo de sistema informático capaz de realizar tareas tales como generar contenidos, recomendaciones o incluso tomar decisiones (artículo 3.1 RIA). El Reglamento de inteligencia artificial también incluye algunas reglas dirigidas a los modelos de IA, que son los componentes que permiten a los sistemas de IA ejecutar esas tareas. Dado que regulan vertientes diferentes, estas normas jurídicas siguen enfoques distintos.

Sin embargo, no se deben sobreestimar las diferencias entre el RGPD y el RIA. Ambos instrumentos crean **obligaciones para minimizar los riesgos** generados por los objetos que regulan:

- El artículo 25 del RGPD obliga a los responsables del tratamiento de datos a adoptar medidas y salvaguardias para hacer frente a los riesgos para los principios de protección de datos, mientras que el artículo 32 del RGPD establece la obligación de abordar los riesgos para la ciberseguridad.
- En el RIA, los proveedores de sistemas de IA de alto riesgo están obligados a adoptar medidas de gestión de riesgos (artículo 9 RIA), mientras que los responsables del despliegue de esos sistemas deben adoptar sus propios enfoques para hacer frente a los riesgos que aparecen en una herramienta específica (art. 26 RIA), como las evaluaciones de impacto que se requieren en algunos casos.

1 Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

2 Barrio Andrés, Moisés: "Prólogo", en Barrio Andrés, Moisés (dir.): ***Comentarios al Reglamento Europeo de Inteligencia Artificial***. Editorial La Ley, Madrid, 2024.



Sin embargo, el RIA no aplica un conjunto uniforme de normas a todos los sistemas y modelos de IA. En su lugar, separa ***ex lege*** esos sistemas y modelos en diferentes clases, cada una de las cuales está sujeta a su propio marco jurídico. Si bien los proveedores y los responsables del despliegue de sistemas de IA siguen estando obligados a identificar y abordar los riesgos que esos sistemas crean en la práctica, dicha evaluación se lleva a cabo dentro de las categorías definidas por el RIA: sistemas prohibidos (artículo 5 RIA) y sistemas de alto riesgo (artículo 6 RIA), y en menor medida sistemas de riesgo limitado (artículo 50 RIA).

Por último, el RIA no establece un marco general para los sistemas de IA que no sean de alto riesgo. Por eso, en su mayor parte, considera que los riesgos de **los sistemas que no entran en las dos primeras categorías mencionadas anteriormente están adecuadamente cubiertos por las normas en vigor**, como el RGPD y la normativa específica del sector a nivel de la UE y nacional.

Ámbito de aplicación

02

2. ÁMBITO DE APLICACIÓN

El entrenamiento, el despliegue y el uso de los sistemas de IA no sería posible sin un tratamiento de datos, y singularmente con datos «personales». Así, los puntos de contacto con el RGPD son evidentes. La relación concurrente entre el RIA y el RGPD se regula en el artículo 2.7 del RIA. Según el mismo, el RGPD y el RIA deben **aplicarse en paralelo**. En efecto, el cumplimiento del RIA no exime de cumplir los preceptos que correspondan respecto a la normativa vigente en materia de protección de datos de carácter personal.

De este modo, el RIA no constituye una ***lex specialis*** del RGPD. Por lo tanto, los proveedores y los responsables del despliegue de sistemas de IA deben también abordar la cuestión de cómo pueden garantizar el uso de los sistemas de IA en sus entidades de conformidad con la regulación vigente de protección de datos.

a) Categorías de datos en el tratamiento de sistemas de IA

Los datos personales pueden desempeñar tres funciones en lo que respecta a los sistemas de IA:

A) Los datos personales pueden ser una **entrada** para el funcionamiento de un sistema de IA. Por ejemplo, un sistema de recomendación puede tomar información sobre los intereses personales de un usuario en una plataforma de redes sociales para averiguar qué contenido le gustaría ver a ese usuario.

B) Los datos personales también pueden ser el **resultado** del funcionamiento de un sistema de IA. Por ejemplo, un sistema de IA creado para generar puntuaciones de riesgo de comisión de un delito (como el fraude financiero) recibe información sobre una persona y luego le asigna una puntuación de riesgo que representa la probabilidad de que cometa ese delito.

C) Los datos personales pueden ser un **elemento constitutivo** de un sistema o modelo de IA. Por ejemplo, un modelo de aprendizaje automático destinado a los tipos de tareas mencionados anteriormente con seguridad se entrenará con datos personales sobre personas que sean relevantes para el problema, como los usuarios de la plataforma y las investigaciones previas de fraude financiero, respectivamente.

Como sugieren los ejemplos, estas funciones suelen estar interconectadas. Es probable que un sistema de IA destinado a procesar datos personales genere resultados que puedan asociarse a personas, y que los datos personales se utilicen en su proceso de construcción para garantizar la calidad de sus resultados.

El RIA, siguiendo las prácticas técnicas del sector, distingue entre tres tipos de conjuntos de datos que son relevantes en la construcción de un sistema de IA:

– **Datos de entrenamiento**: según el artículo 3.29) del RIA, son aquellos que se utilizan para entrenar el sistema de IA ajustando los parámetros de entrenamiento del sistema de IA sobre la base de estos datos. En el caso de un sistema de aprendizaje supervisado, se tratará normalmente de un conjunto de ejemplos que

emparejan algunos datos de entrada con el resultado esperado (por ejemplo, fotos de gatos con la etiqueta «gato»). En los sistemas de aprendizaje no supervisado, no se proporcionan resultados esperados, sino únicamente los datos de entrada. Y en los sistemas de aprendizaje reforzado, no se facilitan respuestas esperadas, pero se debe suministrar al sistema información sobre la rentabilidad de las diferentes opciones.

- **Datos de validación**: de conformidad con el artículo 3.30) del RIA, son aquellos usados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje para, entre otras cosas, evitar el subajuste o el sobreajuste. Los datos de validación se utilizan para ajustar el modelo entrenado, lo que permite a los creadores del modelo elegir entre diferentes procesos y estrategias de aprendizaje. Por ejemplo, propicia a los creadores evitar el fenómeno de sobreajuste, en el que un modelo aprende reglas que describen bien el conjunto de entrenamiento, pero que no se generalizan correctamente.
- **Datos de prueba**: según el artículo 3.32) del RIA, se utilizan para proporcionar una evaluación independiente del sistema de IA, "con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio". Es decir, ofrecen una base para evaluar el sistema después de cualquier proceso de validación técnica.

Asimismo, y para el funcionamiento de un sistema de IA, el RIA también introduce la categoría de **datos de entrada**: según el artículo 3.33), se trata de datos que se proporcionan a un sistema de IA o que este adquiere directamente y sobre cuya base el sistema produce una salida. Estos datos pueden estar contenidos en la solicitud del usuario, el ***prompt***, o proceder de una cuenta de usuario a la que el sistema de IA tiene acceso.

b) Aplicabilidad del RGPD

De conformidad con el artículo 2.1 del RGPD, este se aplica al tratamiento de datos personales, total o parcialmente automatizado, y al tratamiento de datos personales no automatizado que se almacenen o se tengan la intención de almacenar en un fichero.

Por lo tanto, en el ámbito de sistemas de IA, la **referencia personal** de los datos tratados suele ser decisiva para la aplicabilidad del RGPD. Según el artículo 4.1 del RGPD, al que también se refiere el artículo 3.50) del RIA, se entiende por datos personales toda información sobre una persona física identificada o identificable. No se aplican normas especiales a la validación, las pruebas y los datos de entrada en lo que respecta a la determinación de la referencia personal.

Modalidades de uso de los datos

03

3. MODALIDADES DE USO DE LOS DATOS

Podemos distinguir cuatro formas o modalidades de uso de los datos personales en un sistema de IA.

a) Recopilación directa de datos

Una entidad puede **comenzar a tratar** algunos tipos de datos que son relevantes para el sistema de IA que desea desarrollar. Esos datos pueden adoptar diversas formas, tales como:

1. **Medición de las interacciones de los usuarios**: por ejemplo, un juguete inteligente podría recopilar datos sobre la frecuencia con la que los niños interactúan con sus juguetes, o sobre sus patrones de habla, para el diseño de nuevas funcionalidades para sus productos.
2. **Análisis de datos internos**: por ejemplo, una universidad puede utilizar sus datos brutos sobre los estudiantes para generar métricas, que posteriormente podrían introducirse en un sistema de IA.
3. **Crear nuevos datos a partir de la combinación de fuentes existentes**: por ejemplo, un hospital podría integrar los datos de los pacientes de diferentes áreas de sus operaciones para obtener una visión holística de la salud de los pacientes.

Al recopilar esos datos, la entidad se convierte en responsable del tratamiento de los datos para las operaciones relacionadas con la recopilación de estos datos y su utilización hacia un sistema de IA.

b) Reutilización de datos personales

Algunas entidades **acumulan datos personales como parte de su funcionamiento**. Por ejemplo, un hospital no puede llevar a cabo sus funciones básicas sin información detallada sobre sus pacientes. Esos datos son un activo crucial para el desarrollo de tecnologías de IA, pero su uso está sujeto a restricciones legales que se analizan más adelante en esta guía.

Algunos problemas relacionados con la calidad de los datos pueden reducir la utilidad de los datos disponibles anteriormente:

1. **Relevancia**: es necesario evaluar si las dimensiones captadas en los datos existentes son relevantes para el problema que el sistema o modelo de IA pretende resolver. Por ejemplo, una universidad podría utilizar datos sobre los cursos que sigue cada estudiante para programar la compra de libros para la biblioteca, pero estos datos no resultarían especialmente útiles para crear un *chatbot*.
2. **Supuestos implícitos en los datos**: a pesar de lo que pueda sugerir el término «datos brutos», incluso los conjuntos de datos más completos contienen

algunas asunciones: por ejemplo, qué datos son lo suficientemente relevantes como para ser almacenados, cómo se debe medir esta variable, cómo tratar los valores que faltan, etc. Si no se comprueban, esos supuestos pueden crear problemas. Por ejemplo, si un hospital quiere crear una herramienta para ayudar en el diagnóstico de infartos, esa herramienta debe tener en cuenta las diferencias en los síntomas entre hombres y mujeres. De lo contrario, podría centrarse en las métricas que suelen reflejar los síntomas masculinos y no servir a más de la mitad de la población.

3. **Errores, datos obsoletos y datos incompletos**: hay que evaluar la calidad y pertinencia que presenta el conjunto de datos existente y de cómo se gestionan. Por ejemplo, ¿cómo trata un fabricante del IoT la información duplicada que recibe de los sensores? ¿Qué mecanismos de corrección de errores adopta en los datos transmitidos?

c) Adquisición de datos de terceros intermediarios

En el mercado, existe un tipo de actores, los denominados «intermediarios de datos» (o *data broker*s), cuyo modelo de negocio está basado en la **comercialización de datos sobre personas físicas y jurídicas**. Si una entidad decide adquirir datos de ellos, debe actuar con cautela. Además, las mismas cuestiones de calidad de los datos descritas anteriormente siguen siendo relevantes en este caso.

Del mismo modo, hay que tener en cuenta si el intermediario ha obtenido legalmente el control de esos datos y si existen bases legales para la transferencia. De hecho, algunos modelos de intermediación ya han sido cuestionados desde el punto de vista jurídico, lo que ha dado lugar a algunas sanciones y a litigios en curso.

Por lo tanto, una entidad debe actuar con la debida diligencia al adquirir datos de terceros y considerar cómo se verá afectado su sistema o modelo de IA si se determina que ese modelo de adquisición de los datos no cumple con el RGPD "no cumple con el RGPD". Y resulta fundamental regular contractualmente el pleno cumplimiento del RGPD por parte del tercero para tener todas las garantías en el retorno de la inversión del sistema de IA y su aplicación para el caso de uso.

d) Creación de datos sintéticos

En ocasiones, una entidad no puede basarse en datos totalmente anonimizados. Si una aplicación implica la elaboración de perfiles de personas físicas, por ejemplo, no puede entrenarse ni utilizarse sin algún tipo de referencia a dichas personas. Para ilustrarlo, un sistema de IA para diagnósticos médicos acabará utilizándose en un paciente de carne y hueso, generando un dato personal sobre esa persona (su estado de salud). Dado que el uso de datos personales a gran escala para tales aplicaciones puede ser arriesgado, algunas voces han propuesto el **uso de datos sintéticos como alternativa**.

Dado que los datos sintéticos no se refieren a una persona real (identificada o identificable), quedarían fuera de la definición de datos personales del RGPD. Por lo tanto, en la medida en que los datos sintéticos ofrezcan una reproducción fiel de la población a la que se aplica el sistema de IA, permitirían el uso de la IA sin crear riesgos para la protección de datos.

La exención de aplicación del RGPD solo se aplica si los datos son **realmente** sintéticos. Si es posible encontrar información sobre personas físicas a partir del conjunto de datos sintéticos, ésta sigue estando cubierta por la normativa de protección de datos. Esto es así incluso si los valores atribuidos a esa persona no se corresponden con la realidad. Por ejemplo, consideremos una situación en la que una base de datos sintética guarda los nombres reales de las personas para la puntuación crediticia, pero les asigna valores aleatorios para cada métrica. Esa base de datos no permitirá a un observador descubrir información correcta sobre las personas concretas. Sin embargo, asocia esa información a sus identidades, y la definición de datos personales del RGPD no incluye ninguna excepción para la información incorrecta.

Incluso si los datos en sí mismos no tienen ninguna asociación con una persona física identificada o identificable, la normativa de protección de datos también podría aplicarse a su generación. Este es el caso si los datos sintéticos se generan a partir de un conjunto de datos que contiene información sobre personas físicas reales.

Aunque la base de datos resultante puede no contener datos personales, su creación requiere el tratamiento de datos personales. Por ejemplo, un hospital podría utilizar algunos de sus registros médicos para crear un conjunto de datos sintéticos. En ese caso, el hospital sigue estando obligado a cumplir el RGPD al crear el conjunto de datos, aunque el uso de ese conjunto de datos pueda no estar cubierto por él.

Independientemente de su clasificación jurídica, los datos sintéticos siguen estando sujetos a las **cuestiones de calidad de los datos** planteadas anteriormente. Este tipo de datos no es la panacea para la construcción de la IA. No obstante, pueden ser útiles si se utilizan con prudencia.

Responsabilidades en virtud de la legislación sobre protección de datos

04

4. RESPONSABILIDADES EN VIRTUD DE LA LEGISLACIÓN SOBRE PROTECCIÓN DE DATOS

Según el artículo 4.7 del RGPD, la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o conjuntamente con otros, determine los fines y medios del tratamiento de datos personales es responsable en virtud de la legislación en materia de protección de datos.

No existen requisitos especiales para los datos de validación y prueba a este respecto. El tratamiento de los datos de **entrenamiento** en la fase de desarrollo del sistema de IA puede asignarse a un responsable del tratamiento utilizando las reglas ordinarias.

Ahora bien, la delimitación de responsabilidades durante el **funcionamiento** de un sistema de IA es más difícil. Solo en raras ocasiones una entidad tendrá la capacidad de desarrollar y desplegar un sistema de IA enteramente por sí misma. En la mayoría de los casos, se basará en sistemas disponibles en el mercado y los integrará en sus procesos internos (por ejemplo, GPT de OpenAI, Gemini de Google o Llama de Meta). En este escenario, su responsabilidad en materia de tratamiento de datos sobre los datos de entrenamiento y los datos de entrada depende fundamentalmente de la forma de implementación.

La forma más común de implementación en la actualidad es que el sistema se ejecute a través de los **servidores del proveedor** (en su nube, «*on cloud*»). En este entorno, el proveedor es el único que decide los fines y los medios del tratamiento de los datos de entrenamiento y, por lo tanto, es el responsable. Lo mismo se aplica al tratamiento de los datos de entrada, a menos que la entidad que lleva a cabo la implementación especifique a qué datos de usuario puede acceder el sistema y con qué fines. En particular en lo que respecta a los datos de entrada, también es concebible la responsabilidad conjunta con esta forma de implementación. Según el artículo 26.1 del RGPD, este es el escenario si dos o más responsables del tratamiento deciden conjuntamente los fines y los medios del tratamiento.

Muchos de los principales proveedores de servicios en la nube, como Amazon Web Services (AWS), Microsoft Azure y Google Cloud, tienen su sede fuera de Europa. Esto suscita **inquietudes sobre las transferencias transfronterizas de datos** y el cumplimiento del RGPD, como se observa en las preocupaciones generales sobre las transferencias internacionales de datos. Las entidades también tendrán que hacer frente a otras posibles fuentes de riesgo, como las vulnerabilidades potenciales de la infraestructura en la nube que podrían ser explotadas por agentes maliciosos.

Por otro lado, existen las denominadas implementaciones «*on-premise*», en las que el sistema se encuentra en los **servidores de la entidad correspondiente** y las conexiones con el proveedor están deshabilitadas. En estos casos, la entidad que realiza la implementación decide regularmente sobre los fines y medios del tratamiento y, por lo tanto, es la única responsable en el sentido del RGPD.

Bases jurídicas para el tratamiento de datos personales ordinarios

05

5. BASES JURÍDICAS PARA EL TRATAMIENTO DE DATOS PERSONALES ORDINARIOS

Los datos son esenciales para los sistemas y modelos de IA. Cuando hablamos de modelos de aprendizaje automático (el *machine learning*), las reglas que residen en el núcleo de esos modelos se derivan de los patrones estadísticos presentes en sus datos de entrenamiento, que luego se generalizan. Pero incluso los sistemas de IA impulsados por otros tipos de tecnologías de IA, como los sistemas basados en el conocimiento, seguirán necesitando datos de entrada para generar sus resultados, que a menudo equivalen a datos en sí mismos. Por lo tanto, en la medida en que esos tipos de datos se refieran a personas físicas identificadas o identificables, un sistema o modelo de IA estará impregnado de datos personales.

De este modo, si los datos personales se tratan con la ayuda de un sistema de IA, **se requiere una base jurídica de tratamiento** en virtud de la legislación en materia de protección de datos, independientemente de los requisitos del RIA, que se aplican además de las disposiciones del RGPD.

En principio, todas las bases jurídicas para el tratamiento enumeradas en el artículo 6.1 del RGPD siguen siendo teóricamente viables para los sistemas y modelos de IA. Sin embargo, muchas de ellas estipulan que el tratamiento debe ser «necesario» para el cumplimiento de alguna tarea. Dada la interpretación restrictiva de la necesidad que prevalece en la legislación sobre protección de datos, es poco probable que las letras b) a e) del artículo 6.1 del RGPD amparen el tratamiento a gran escala para el uso de la IA. En la mayoría de los casos, la consecuencia es que los responsables del tratamiento de datos tendrán que basarse en el consentimiento del interesado o en la existencia de un interés legítimo que justifique el tratamiento. Ambas opciones exigen un trabajo considerable por parte de la entidad.

a) Consentimiento (art. 6.1.a) RGPD)

De acuerdo con el artículo 6.1.a) del RGPD, el tratamiento de datos personales es lícito si el interesado ha dado su consentimiento para uno o varios fines específicos (es decir, claramente definidos). Además de una **expresión de voluntad voluntaria e inequívoca**, un requisito previo para el consentimiento es que se haya otorgado de manera suficientemente específica e informada (artículo 4.11 RGPD).

El entrenamiento de un sistema de IA a gran escala puede requerir datos de miles, o incluso millones de personas. La entidad tendría que identificarlas y ponerse en contacto con ellas para obtener su consentimiento. Por eso, en la práctica, el cumplimiento de los requisitos de protección de datos para el tratamiento de datos basado en el consentimiento por parte de los sistemas de IA puede suponer un **reto**.

A esta dificultad hay que añadir que consentimiento informado requiere el conocimiento por el interesado del proceso de tratamiento de datos, que puede ser técnicamente muy complejo. La falta de transparencia y de trazabilidad puede contrarrestarse en cierta medida proporcionando al interesado al menos información sobre los aspectos clave del tratamiento de datos, como la comunicación sobre los fines del tratamiento de datos y la identidad del responsable del tratamiento (por ejemplo, en sus avisos de protección de datos).

b) Tratamiento necesario para la ejecución de un contrato (art. 6.1.b) RGPD)

El artículo 6.1.b), inciso primero, del RGPD permite el tratamiento de datos personales en la medida en que sea necesario para la **ejecución de un contrato en el que el interesado sea parte**. Paralelamente, el inciso segundo se aplica a las medidas precontractuales.

El siguiente ejemplo puede ilustrar la aplicación del principio de necesidad. Si una persona utiliza un generador de voz con IA entrenado con su voz, parece bastante clara la justificación para el tratamiento de los datos de voz necesarios para ello sobre la base del artículo 6.1.b) del RGPD. De lo contrario, sin la voz, el objeto del contrato –a saber, la creación de la salida de voz personalizada del generador de voz de la persona solicitante– difícilmente sería alcanzable. Por otra parte, el uso de los datos de voz proporcionados para mejorar aún más un modelo básico de GPAI sería, en el mejor de los casos, útil para la ejecución del contrato y, por lo tanto, no estaría cubierto por el artículo 6.1.b) del RGPD por no ser «necesario».

c) Tratamiento necesario para el cumplimiento de una obligación legal (art. 6.1.c) RGPD)

El tratamiento de datos personales puede estar justificado, de conformidad con el artículo 6.1.c) del RGPD, para el **cumplimiento de una obligación legal** aplicable al responsable del tratamiento.

La obligación legal se refiere aquí a una obligación legal genuina, es decir, una «obligación» de tratar los datos. Por lo general, el responsable del tratamiento no tiene libertad de elección. Además, existe un requisito más estricto en lo que respecta a la base jurídica y también a la necesidad de limitar el tratamiento dentro de este marco a lo absolutamente necesario.

Por eso, la base jurídica del artículo 6.1.c) del RGPD ofrece un ámbito de aplicación muy limitado en el contexto de las aplicaciones de IA.

d) Interés público o autoridad pública (art. 6.1.e) RGPD)

La redacción general del artículo 6.1.e) del RGPD enumera dos posibilidades de tratamiento. O bien el tratamiento **debe ser de interés público**, **o bien debe realizarse en el ejercicio de poderes públicos** conferidos al responsable del tratamiento. Sin embargo, en ambos casos, debe encomendarse una tarea al responsable del tratamiento.

En este supuesto, y según el artículo 6.3 del RGPD en relación con el considerando 45 del RGPD, se requiere una **habilitación jurídica en el Derecho de la Unión o en el Derecho de los Estados miembros**.

Por eso, el artículo 6.1.e) del RGPD no crea una base jurídica para el tratamiento de datos personales, sino que solo se aplica en relación con, por ejemplo, las bases jurídicas del Derecho estatal y autonómico que se presentan específicamente aquí (por ejemplo, art. 145 de la Ley 5/2025, de 24 de julio, por la que se modifican el texto refundido de la Ley sobre

responsabilidad civil y seguro en la circulación de vehículos a motor, aprobado por el Real Decreto Legislativo 8/2004, de 29 de octubre, y la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras).

e) Intereses legítimos (art. 6.1.f) RGPD)

De conformidad con el artículo 6.1.f) del RGPD, el tratamiento de datos personales está autorizado si es **necesario para los fines de los intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, salvo que prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

El artículo 6.1.f) del RGPD está **redactado de forma abierta a la innovación** y, en general, puede considerarse una base jurídica para las operaciones de tratamiento de datos en el ámbito de la inteligencia artificial.

En el caso de operaciones de tratamiento más complejas, son muchas las circunstancias que influyen en el proceso de ponderación inherente al RGPD. Dado que los interesados no esperan que sus datos sean tratados en todas las situaciones, esto puede dar lugar a imprevisibilidad para los interesados, por un lado, y a inseguridad jurídica para el responsable del tratamiento, por otro.

De conformidad con párrafo segundo de este apartado, esta base jurídica no se aplica al tratamiento por parte de autoridades públicas en el cumplimiento de sus funciones. Por lo tanto, se **excluye** la aplicación de esta base de tratamiento a los organismos públicos, como los municipios o las comunidades autónomas.

El término «interés legítimo» se entiende en sentido amplio. Por consiguiente, el interés legítimo perseguido por el responsable del tratamiento puede consistir, en principio, en cualquier interés jurídico, económico o no pecuniario (pero legalmente admisible) del responsable del tratamiento o de un tercero.

Por último, los intereses o derechos y libertades fundamentales del interesado no deben prevalecer sobre los intereses legítimos del responsable del tratamiento o de un tercero. El **equilibrio** entre los respectivos derechos e intereses opuestos depende, en general, de las circunstancias específicas de cada caso concreto. Entre otros elementos, deben tenerse en cuenta el alcance del tratamiento en particular, su impacto en los interesados y la cuestión de si el interesado podía esperar que sus datos personales fueran tratados en la situación concreta. Si se ven afectadas categorías especiales de datos personales con arreglo al artículo 9 del RGPD, además del artículo 6.1.f) del RGPD, también debe aplicarse una excepción con arreglo al artículo 9, apartados 2 a 4, del RGPD.

El hecho de que un servicio basado en la IA se preste de forma gratuita, por ejemplo, no significa que los datos personales de los usuarios puedan ser tratados automáticamente para cualquier interés del responsable del tratamiento. La mejora del producto con los datos tratados como parte del uso de la aplicación de IA también puede ser cuestionable a pesar de la disposición de uso gratuito, especialmente si también se tratan datos personales de menores de edad.

Si un **interesado se opone** al tratamiento de sus datos personales sobre la base del artículo 61.f) del RGPD por motivos relacionados con su situación particular, el responsable del tratamiento solo podrá continuar con el tratamiento de los datos si puede demostrar «motivos legítimos imperiosos» para el tratamiento (art. 21.1. RGPD). Estos deben prevalecer sobre los intereses, derechos y libertades del interesado, o ser necesarios para la formulación de reclamaciones legales.

Los motivos derivados de la situación particular de un interesado se refieren a particularidades atípicas de naturaleza jurídica, económica, ética, social, societal y/o familiar. Este contexto cobra relevancia, por ejemplo, cuando el proveedor de una red social anuncia que tiene la intención de utilizar en el futuro los contenidos generados por los usuarios en la plataforma para el entrenamiento de la IA. Sin embargo, ya existen dudas sobre si se puede suponer un interés legítimo superior de la plataforma en el sentido del artículo 6.1.f) del RGPD.

f) Cambio de finalidad (art. 6.4 RGPD)

El RGPD regula el caso del tratamiento posterior de datos personales en caso de cambio de finalidad en el artículo 6.4 del RGPD. Esto significa el tratamiento para una **finalidad distinta de aquella para la que se han recogido** los datos personales.

La disposición es especialmente importante cuando se entrenan sistemas de IA si los datos de entrenamiento subyacentes se recogieron previamente para una finalidad diferente y ahora se van a utilizar para el entrenamiento. Surge así la pregunta crucial de si el tratamiento de datos personales es admisible en el ámbito del artículo 6.4. Según la opinión dominante, con una nueva finalidad se requiere también otra base jurídica.

Bases legales para la reutilización de datos personales

06

6. BASES LEGALES PARA LA REUTILIZACIÓN DE DATOS PERSONALES

En ocasiones, una entidad puede querer utilizar datos que ya ha recopilado para fines distintos a la construcción de un sistema de IA. Por supuesto, dicho tratamiento debe tener una base legal en el RGPD. Si dicha base no es el consentimiento del interesado, el responsable del tratamiento **debe comprobar si ese nuevo fin es compatible con el fin de la recopilación original**.

El artículo 6.4 del RGPD establece una lista abierta de criterios que deben tenerse en cuenta en este contexto, como la relación entre los fines de la recogida original y el tratamiento posterior previsto o la existencia de garantías adecuadas. Esos criterios deben evaluarse en el uso de tales datos para el entrenamiento de la IA, al igual que en cualquier otro tratamiento.

Tratamiento de categorías especiales de datos personales

07

7. TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS PERSONALES

Como es lógico, se aplican **requisitos de protección más estrictos** si categorías especiales de datos personales, de conformidad con el artículo 3.37) del RIA en relación con el artículo 9.1 del RGPD, son objeto de tratamiento en un sistema de IA.

Se trata de datos personales «que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física».

Están asociados a una sensibilidad específica en materia de derechos fundamentales y a un mayor riesgo de discriminación, lo que conlleva un **riesgo elevado para los derechos** y libertades de las personas físicas (***cfr***. art. 35.5.b) RGPD). Debido a la alta necesidad de protección que conllevan, las categorías especiales de datos personales del artículo 9 del RGPD deben interpretarse de manera amplia.

Una regla particular en este campo es el artículo 10.5 del RIA. Permite el tratamiento de categorías especiales de datos personales en el entrenamiento de sistemas de IA de alto riesgo si dicho **tratamiento es necesario para detectar y corregir sesgos**. Siempre que se invoque esta excepción, además deben cumplirse las siguientes condiciones:

a) Que el tratamiento de otros datos, como los sintéticos o los anonimizados, no permita efectuar de forma efectiva la detección y corrección de sesgos;

b) Que las categorías especiales de datos personales estén sujetas a limitaciones técnicas relativas a la reutilización de los datos personales y a medidas punteras en materia de seguridad y protección de la intimidad, incluida la seudonimización;

c) Que las categorías especiales de datos personales estén sujetas a medidas para garantizar que los datos personales tratados estén asegurados, protegidos y sujetos a garantías adecuadas, incluidos controles estrictos y documentación del acceso, a fin de evitar el uso indebido y garantizar que solo las personas autorizadas tengan acceso a dichos datos personales con obligaciones de confidencialidad adecuadas;

d) Que las categorías especiales de datos personales no se transmitan ni transfieran a terceros y que estos no puedan acceder de ningún otro modo a ellos;

e) Que las categorías especiales de datos personales se eliminen una vez que se haya corregido el sesgo o los datos personales hayan llegado al final de su período de conservación, si esta fecha es anterior; y

f) Que los registros de las actividades de tratamiento con arreglo a los Reglamentos (UE) 2016/679 y (UE) 2018/1725 y la Directiva (UE) 2016/680 incluyan las razones por las que el tratamiento de categorías especiales de datos personales era estrictamente necesario para detectar y corregir sesgos, y por las que ese objetivo no podía alcanzarse mediante el tratamiento de otros datos.

Por lo tanto, el RIA amplía las posibilidades de utilizar categorías especiales de datos personales durante el proceso de entrenamiento de los sistemas de IA de alto riesgo, pero impone restricciones considerables al hacerlo.

Prohibición de la toma de decisiones individuales automatizadas con arreglo al artículo 22 del RGPD

08

8. PROHIBICIÓN DE LA TOMA DE DECISIONES INDIVIDUALES AUTOMATIZADAS CON ARREGLO AL ARTÍCULO 22 DEL RGPD

El artículo 22.1 del RGPD establece un derecho especial de los interesados, que debe clasificarse como una **prohibición sujeta a la posibilidad de autorización** en la aplicación de la norma.

Esta regla no sustituye los requisitos para la admisibilidad del tratamiento automatizado de datos. Más bien, la disposición da lugar a requisitos adicionales de legalidad para el uso de los resultados del tratamiento automatizado de datos, que deben observarse además de los artículos 6 y 9 del RGPD. El objetivo es proteger al interesado de los riesgos particulares para sus derechos y libertades asociados al tratamiento automatizado de datos personales.

El artículo 22.1 del RGPD es aplicable bajo tres **condiciones**: en primer lugar, se requiere un tratamiento automatizado de datos. En segundo lugar, se precisa una decisión basada únicamente en dicho tratamiento automatizado. Por último, la decisión en cuestión debe tener efectos jurídicos o afectar al interesado de manera significativa de forma similar.

Así, en cuanto al requisito del tratamiento automatizado de datos se cumplirá siempre que se utilicen sistemas de IA en el sentido del RIA.

La cuestión de si una decisión tiene **efectos jurídicos o perjuicios significativos similares** debe evaluarse caso por caso. El factor decisivo para evaluar los efectos jurídicos es si la situación jurídica de la persona afectada se ve alterada de alguna manera. Por otra parte, existe un perjuicio significativo de manera similar si la persona afectada se ve perturbada de forma permanente en su desarrollo económico o personal por la decisión.

De mayor importancia para el uso de la IA es el hecho de que la redacción del artículo 22.1 del RGPD solo se refiere a las decisiones que se basan «exclusivamente» en el tratamiento automatizado de datos. Esto significa que en principio solo se incluyen las decisiones que se toman sin intervención humana (cdo. 71 RGPD). Ahora bien, la jurisprudencia reconoce asimismo que el uso de sistemas de asistencia con IA para la toma de decisiones en casos individuales también está incluido en el precepto.

El trasfondo del debate es la sentencia ***Schufa***[3] del TJUE en un procedimiento prejudicial en el que tuvo que abordar el ámbito de aplicación del artículo 22.1 del RGPD. Concretamente, el tribunal aclaró si existe una decisión en el sentido del artículo 22.1 del RGPD cuando se calcula un valor de probabilidad de la solvencia de una persona física con la ayuda de un sistema de IA y este valor se utiliza posteriormente en el proceso de toma de decisiones de un tercero, que decide si concede un préstamo sobre esta base. El TJUE ha fallado que el término «decisión» en el sentido del artículo 22.1 del RGPD debe interpretarse de manera amplia. Por lo tanto, el cálculo del valor de probabilidad y la decisión de conceder el préstamo deben evaluarse como una única «decisión automatizada en casos individuales» si la concesión del préstamo depende significativamente del valor de probabilidad.

3 STJUE de de 7 de diciembre de 2023, asunto C-634/21, ***SCHUFA Holding AG***.

El TJUE sitúa el problema subyacente en la interpretación del término «decisión». Califica el cálculo del valor de probabilidad como basado «únicamente en el tratamiento automatizado» y, a continuación, considera que forma parte de una única decisión automatizada por parte del tercero en el sentido del artículo 22.1 del RGPD, con sujeción a la condición de pertinencia. Sin embargo, como resultado, el TJUE cambia el punto de referencia del criterio de exclusividad y, por lo tanto, suaviza considerablemente su significado. Al menos según la jurisprudencia del TJUE, ya no es importante si una persona física participó en el proceso de toma de decisiones. Más bien, basta con que un acto preparatorio se base exclusivamente en el tratamiento automatizado y que el resultado de dicho acto preparatorio influya de manera significativa en la decisión final de un tercero. Por lo tanto, la existencia de una decisión final humana puramente formal ya no es suficiente en este contexto.

La posterior STJUE ***Dun & Bradstreet Austria***[4] aporta presiones acerca de cómo debe interpretarse el concepto «información significativa sobre la lógica aplicada» –que figura también en los arts. 13 y 14 RGPD relativos a la información a facilitar a los interesados en la obtención de datos–, así como en relación con el tratamiento de las situaciones en las que el responsable del tratamiento considera que esa información puede incluir secretos comerciales, objeto de tutela por la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas, o de datos de terceros protegidos por el RGPD.

La nueva STJUE establece que la expresión «información significativa sobre la lógica aplicada», a los efectos del artículo 15.1.h) del RGPD, abarca «la explicación del procedimiento y de los principios concretamente aplicados para explotar, de forma automatizada, los datos personales del interesado con el fin de obtener un resultado determinado, como un perfil de solvencia» (apartado. 58). Como esa explicación debe facilitarse en forma concisa, transparente, inteligible y de fácil acceso, no puede satisfacerse con la mera comunicación de una fórmula matemática compleja, como un algoritmo, ni con la descripción de las etapas de la adopción de una decisión automatizada (apdo. 59).

Por el contrario, esa información debe describir el procedimiento y los principios concretamente aplicados de tal manera que el interesado pueda comprender qué datos personales se han utilizado y cómo en la adopción de la decisión automatizada (apdo. 61). Como ejemplo de información que puede resultar apropiada en relación con la elaboración de perfiles de solvencia, la sentencia menciona la relativa a la medida en una variación a nivel de los datos personales tomados en consideración habría conducido a un resultado diferente (apdo. 62).

Además, de la aplicabilidad del artículo 22.1 del RGPD no se deduce que la decisión asistida por IA esté siempre prohibida. Más bien, en este caso deben tenerse en cuenta los requisitos adicionales de los apartados 2 a 4 del precepto. Las decisiones en el sentido del artículo 22.1 del RGPD también pueden adoptarse de conformidad con el artículo 22.3 del RGPD, si son necesarias para la celebración o el cumplimiento de un contrato entre el interesado y el responsable del tratamiento (artículo 22.3.a) RGPD) o cuentan con el consentimiento explícito del propio interesado (artículo 22.3.c) RGPD). Además, la Unión y los Estados

4 STJUE de 27 de febrero de 2025, asunto C-203/22, ***Dun & Bradstreet Austria***.

miembros pueden promulgar leyes en virtud de las cuales se autorice, con carácter excepcional, una decisión que entre en el ámbito de aplicación del artículo 22.1 del RGPD (artículo 22.2.b) RGPD).

Del mismo modo, cabe señalar que la clasificación de un sistema de IA como de alto riesgo en el RIA no debe entenderse simultáneamente como una autorización del sistema en el sentido del artículo 22.2.b) del RGPD (cdo. 140 RIA).

Por lo demás, el **RIA ofrece detalles adicionales sobre estas obligaciones** en lo que respecta a los sistemas de IA de alto riesgo. En virtud del artículo 14 del RIA, los proveedores de sistemas de IA de alto riesgo están obligados a adoptar medidas técnicas que faciliten la supervisión. Deben construir el sistema de manera que permita a las personas que lo supervisan:

a) Entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados;

b) Ser conscientes de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo («sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión;

c) Interpretar correctamente los resultados de salida del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles;

d) Decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o descartar, invalidar o revertir los resultados de salida que este genere; e

e) Intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema pulsando un botón de parada o mediante un procedimiento similar que permita que el sistema se detenga de forma segura.

Aunque estas medidas no son obligatorias para ningún otro sistema de IA que no sea de alto riesgo, ni para la toma de decisiones automatizada no basada en IA, constituyen un punto de partida para comprender lo que exige el cumplimiento del artículo 22.3 del RGPD.

Obligaciones adicionales para los sistemas de IA de alto riesgo

09

9. OBLIGACIONES ADICIONALES PARA LOS SISTEMAS DE IA DE ALTO RIESGO

Los principios generales descritos anteriormente se concretan en el cuerpo del RGPD. En particular, los artículos 25 y 32 del RGPD exigen a los desarrolladores de sistemas de IA que adopten medidas técnicas y organizativas que apliquen dichos principios. Los derechos de los interesados también se rigen por dichos principios. A ello hay que sumar las obligaciones en materia de gestión de datos introducidas por el RIA.

En virtud del artículo 10 del RIA, el proveedor de un sistema de IA de alto riesgo debe adoptar una serie de **medidas de gobernanza de datos**. El artículo 10.2 del RIA define un conjunto de prácticas de gobernanza y gestión de datos que deben observarse. Todo proveedor que utilice datos para entrenar un sistema de IA de alto riesgo debe supervisar y controlar cómo se utilizan los datos, en particular:

a) Las decisiones pertinentes relativas al diseño;

b) Los procesos de recogida de datos y el origen de los datos y, en el caso de los datos personales, la finalidad original de la recogida de datos;

c) Las operaciones de tratamiento oportunas para la preparación de los datos, como la anotación, el etiquetado, la depuración, la actualización, el enriquecimiento y la agregación;

d) La formulación de supuestos, en particular en lo que respecta a la información que se supone que miden y representan los datos;

e) Una evaluación de la disponibilidad, la cantidad y la adecuación de los conjuntos de datos necesarios;

f) El examen atendiendo a posibles sesgos que puedan afectar a la salud y la seguridad de las personas, afectar negativamente a los derechos fundamentales o dar lugar a algún tipo de discriminación prohibida por el Derecho de la Unión, especialmente cuando las salidas de datos influyan en las informaciones de entrada de futuras operaciones;

g) Medidas adecuadas para detectar, prevenir y mitigar posibles sesgos detectados; y

h) La detección de lagunas o deficiencias pertinentes en los datos que impidan el cumplimiento del RIA, y la forma de subsanarlas.

Los **requisitos de calidad de los datos** figuran en el artículo 10.3 del RIA. En virtud de esta disposición, los conjuntos de datos de entrenamiento, validación y datos deben ser:

- Pertinentes
- Suficientemente representativos
- En la medida de lo posible, libres de errores y completos en vista del propósito previsto.

El carácter relativo de las dos últimas obligaciones es crucial, dado que no existen datos perfectos. No obstante, esta obligación impone a los proveedores de sistemas de IA de alto riesgo **buscar la exhaustividad y la precisión en sus conjuntos de datos**. La calidad de los datos es uno de los requisitos clave para el éxito de los sistemas de IA.

Por último, el artículo 10.4 del RIA exige a los proveedores que utilicen conjuntos de datos que consideren algunos **elementos contextuales**. En la medida en que esos elementos sean necesarios para la finalidad del sistema, los conjuntos de datos deben tener en cuenta las características o elementos que sean «particulares del entorno geográfico, contextual, conductual o funcional específico en el que está previsto que se utilice el sistema de IA de alto riesgo». Por ejemplo, una universidad debe valorar las características socioeconómicas de su alumnado, mientras que un hospital debe considerar (entre otras cosas) si algunas enfermedades que quiere diagnosticar con IA se ven afectadas por factores geográficos.

Esas medidas pretenden ser criterios de calidad para los datos utilizados en el proceso de entrenamiento de un sistema de IA. Al estar dirigidas a sistemas de IA de alto riesgo, no son obligatorias para ningún otro tipo de sistema o modelo. Aun así, representan las mejores prácticas que las organizaciones podrían considerar como punto de partida para diseñar su propia arquitectura de gobernanza de datos.

Derechos de los interesados

10

10. DERECHOS DE LOS INTERESADOS

Uno de los enfoques distintivos de la legislación de la UE en materia de protección de datos es que otorga derechos individuales. Los interesados cuyos datos son tratados adquieren determinados derechos que pueden invocar frente a los responsables de dicho tratamiento, y se han positivizado en los artículos 12 a 22 del RGPD.

Esos derechos **son aplicables al entrenamiento y la implementación de sistemas de IA** siempre que dichas prácticas utilicen datos personales, tal y como se ha comentado en los apartados anteriores. Sin embargo, las peculiares características técnicas de la IA tienen algunas implicaciones en cuanto a la forma en que esos derechos pueden ejercerse en la práctica.

A continuación, examinaremos los aspectos más problemáticos de cumplimiento en relación con los sistemas de IA.

a) Limitación y oposición al tratamiento en los sistemas de IA

El RGPD concede a los interesados dos derechos que les permiten influir en la forma en que los responsables del tratamiento tratan sus datos. En virtud del artículo 18 del RGPD, los interesados tienen derecho a **limitar** el tratamiento de sus datos personales si se da alguna de las condiciones enumeradas. El artículo 21 del RGPD permite a los interesados **oponerse** por completo al tratamiento.

Estos derechos tienen significados diferentes y cada uno de ellos tiene sus propias excepciones y condiciones de aplicación. Sin embargo, su aplicación a los sistemas y modelos de IA se enfrenta a **obstáculos** similares.

Es probable que esos obstáculos aparezcan cuando el interesado intente ejercer su derecho a limitar (u oponerse) al uso de sus datos en el entrenamiento de sistemas y modelos de IA. En primer lugar, es posible que el interesado ni siquiera sea consciente de que sus datos se están utilizando para el entrenamiento.

Además, es plausible que el interesado no tenga acceso directo a la organización que entrena el modelo o el sistema. Por ejemplo, un paciente de un hospital puede saber que el hospital utiliza para el diagnóstico un sistema de IA basado en un modelo desarrollado por un proveedor externo. Si un paciente desea oponerse al uso de sus datos para el entrenamiento del modelo, el hospital no debe utilizar esos datos para el entrenamiento (o el ajuste del modelo) y tiene que asegurarse de que el proveedor no los utilice para el entrenamiento.

Las cosas se complican para el interesado cuando el modelo de IA no se entrena con datos específicos de una entidad. En ese caso, es poco probable que la entidad que utiliza el modelo tenga control sobre el proceso de entrenamiento. Los interesados deberán ejercer su derecho a limitar (u oponerse) a la organización que entrena el modelo.

b) Derechos de rectificación y supresión

Otro conjunto de derechos de los interesados se refiere al contenido de los datos. Los interesados pueden solicitar a los responsables del tratamiento que **corrijan o rectifiquen** las inexactitudes (artículo 16 RGPD), o incluso que **supriman** los datos personales que les conciernen (artículo 17 RGPD). Pero, una vez más, su aplicación se complica cuando se trata del entrenamiento de un sistema de IA.

El **reto**, en este caso, es que muchos sistemas de IA no representan la información de la misma manera que los sistemas informáticos tradicionales. Rara vez ocurre que una información concreta se almacene en un único lugar dentro del sistema. Por el contrario, los datos sobre una persona suelen estar dispersos entre miles de millones (o más) de parámetros dentro de una red neuronal, por ejemplo. Por lo tanto, cambiar o eliminar esa información no es tan sencillo como modificar una entrada en una base de datos.

Sin embargo, los responsables del tratamiento de datos siguen estando obligados a rectificar y suprimir los datos personales siempre que sean aplicables esos derechos. Si no lo hacen, las autoridades de protección de datos pueden imponer diversas sanciones, entre ellas el «desagravio algorítmico» (***algorithmic disgorgement***), es decir, la eliminación obligatoria de los modelos que no cumplan con la ley. Esta medida aún no ha sido aplicada por las autoridades de protección de datos de la UE, y es probable que sea una medida de ***ultima ratio*** contra el incumplimiento reiterado.

Se han propuesto varias medidas como alternativas técnicas y organizativas a la eliminación completa del modelo. Algunas de ellas tienen por objeto eliminar los datos de los pesos de todo el modelo, lo que permite su eliminación una vez que el modelo ha sido entrenado. Otras intentan hacer viable la eliminación cambiando la forma en que se entrena el modelo. Por ejemplo, la técnica CPR permite que un modelo se base no solo en sus datos de entrenamiento básicos, sino también en un almacén de datos privados que puede olvidarse instantáneamente.

Estas técnicas se encuentran todavía en una fase temprana de desarrollo y, como tales, es posible que no estén lo suficientemente maduras para cumplir todos los requisitos legales establecidos en el RGPD. No obstante, un profesional de la protección de datos deberá colaborar con los desarrolladores de IA para comprender si este enfoque técnico es viable en el caso que nos ocupa.

c) Derecho a la portabilidad de los datos

El artículo 20 del RGPD otorga a los interesados el derecho a la portabilidad de los datos. Si los resultados de un sistema de IA se consideran datos personales, el interesado tiene derecho a solicitar su portabilidad. Del mismo modo, el interesado tiene derecho a pedir la portabilidad de los datos personales utilizados como entrada para un sistema de IA. En ambos casos, la conexión de los datos con el sistema de IA no introduce complicaciones adicionales en comparación con otros tipos de portabilidad.

No se puede decir lo mismo de la **portabilidad de los pesos** de un sistema de IA basado en el aprendizaje automático. Dado que la información suele estar repartida entre los pesos, puede resultar difícil asociar pesos específicos a una persona física. Incluso si dicha identificación fuera posible, los pesos dentro de una red neuronal son específicos de la arquitectura de esa red. Por lo tanto, no pueden simplemente «enchufarse» a otra red.

Sin embargo, ese trasplante de reglas podría ser factible en otros tipos de sistemas de IA. Por ejemplo, las reglas codificadas en un sistema experto podrían implementarse en otro sistema si se dispone de las mismas variables. Por lo tanto, un profesional de la protección de datos tendrá que consultar con el equipo técnico para determinar si el funcionamiento interno del modelo en cuestión incorpora datos personales en un formato que pueda ser transferido. Las futuras directrices de las autoridades de protección de datos aportarán más claridad al respecto.

Gestión de los riesgos relacionados con la protección de datos

11

11. GESTIÓN DE LOS RIESGOS RELACIONADOS CON LA PROTECCIÓN DE DATOS

En virtud de la legislación sobre protección de datos, los responsables del tratamiento de datos están obligados a **abordar los riesgos** que plantean los sistemas de IA, tanto en el momento del desarrollo inicial como en cualquier tratamiento posterior de datos personales:

- El artículo 25 del RGPD establece la obligación de abordar los **riesgos para los principios de protección de datos**. Por ejemplo, si la precisión de un sistema se degrada tras su implementación, el responsable del tratamiento debe adoptar medidas técnicas y organizativas para garantizar que esto no perjudique a los interesados. Dichas medidas pueden incluir cambios en el sistema (como mejorar su modelo), o en su contexto organizativo (como eliminar el sistema de algunas aplicaciones críticas en las que podría generar un mayor riesgo).
- El artículo 32 del RGPD establece la obligación de hacer frente a los **riesgos de seguridad**. Por ejemplo, los actores maliciosos podrían encontrar una forma de anular las salvaguardias adoptadas en un modelo y extraer los datos utilizados para su entrenamiento. Si eso ocurre, el responsable del tratamiento debe adoptar medidas para prevenir y responder a las infracciones.

Esas obligaciones se aplican durante el **desarrollo** del software. Pero también se aplican una vez que el sistema está **en servicio**, ya que los riesgos para la protección de datos y la ciberseguridad también deben afrontarse siempre que se traten datos personales.

Ambos artículos del RGPD estipulan cuatro **factores que deben tenerse en cuenta** en la evaluación de los riesgos para la protección de datos: el estado de la técnica; el coste de la implementación; la naturaleza, el alcance, el contexto y los fines del tratamiento, y la probabilidad y gravedad de los riesgos. Todos estos factores deben valorarse para cada caso de tratamiento, pero la importancia relativa de cada uno de ellos dependerá del contexto.

El RIA también puede servir de guía sobre las medidas que deben aplicarse. Sin embargo, en este caso es considerablemente más impreciso que en las medidas de evaluación de riesgos. Los **artículos 10 a 15 del RIA estipulan los requisitos técnicos** que deben cumplir todos los sistemas de IA de alto riesgo, pero solo definen los «elementos esenciales» de dichos requisitos. Se espera que los proveedores de sistemas de IA interpreten estos elementos esenciales y diseñen sus propias medidas para cumplir con ellos. Aun así, la lista de requisitos esenciales del RIA ofrece un punto de partida que los proveedores pueden ajustar a sus necesidades si no están obligados a seguirla.

Por último, las obligaciones de evaluación de riesgos del RGPD y del RIA son **obligaciones continuas**. No terminan con el desarrollo de un sistema, ni siquiera con su implementación inicial. Esto supone que los responsables del tratamiento de datos deben considerar el momento de sus intervenciones para abordar el riesgo. A veces, puede ser más fácil desarrollar una solución alternativa para un problema conocido en un sistema de IA que resolverlo por medios técnicos. Por ejemplo, si el sistema de IA de una universidad para pronosticar los resultados de los estudiantes no funciona bien con los estudiantes de orígenes no tradicionales, la universidad podría simplemente crear pronósticos manuales para esos estudiantes, especialmente si son pocos. Sin embargo, una organización debe asegurarse de que realmente está abordando estas cuestiones en todo el ciclo de funcionamiento. De lo contrario, la falta de medidas organizativas (o su insuficiencia) podría constituir en sí misma un incumplimiento de las obligaciones en materia de protección de datos y seguridad desde el diseño.

Nueva generación de
BASES DE DATOS con [IA]

La unión perfecta de experiencia y tecnología

Aranzadi LA LEY crea una nueva generación
de bases de datos jurídicas con lo mejor de ambas marcas:

EXPERIENCIA Y RIGOR JURÍDICO UNIDOS A LA MÁS AVANZADA TECNOLOGÍA CON EL IMPULSO DE LA IA.

ARANZADI Ley

ARANZADI Supra

ARANZADI Infinita

Soluciones modulares y escalables,
diseñadas para adaptarse a tus necesidades.

Descubre la evolución del conocimiento

www.aranzadilaley.es

ARANZADI LA LEY | KARNOV GROUP

www.aranzadilaley.es

Síguenos en: