

Newsletter Derecho Digital, IT y protección de datos

Novedades en protección de datos e inteligencia artificial: *web scraping*, anonimización, videovigilancia y decisiones automatizadas



En los últimos meses, las autoridades europeas y nacionales en materia de inteligencia artificial y protección de datos han publicado nuevos criterios sobre algunos de los principales retos asociados al uso de la inteligencia artificial. Entre ellos destacan la obtención masiva de datos publicados en Internet para entrenar modelos generativos, los requisitos para considerar que una información está verdaderamente anonimizada, el uso de IA en sistemas de videovigilancia y la utilización de algoritmos en el ámbito laboral. Asimismo, repasamos algunas de las actuaciones e iniciativas más recientes de las autoridades de protección de datos.

Índice de contenidos

Nuevos criterios del CEPD en materia de anonimización.....	3
Novedades en materia de web scraping	4
Criterios y actuaciones recientes de la AEPD.....	6
Novedades normativas sobre el uso de algoritmos.....	8
Novedades normativas de la APDCAT	9

Nuevos criterios del CEPD en materia de anonimización

Las **Directrices 02/2026 del Comité Europeo de Protección de Datos**, adoptadas el 7 de julio de 2026 para consulta pública hasta el 30 de octubre, actualizan los criterios para determinar cuándo los datos personales pueden considerarse anonimizados.

Los datos anónimos quedan fuera del ámbito de aplicación del RGPD. Sin embargo, si existe una posibilidad razonable de identificar a las personas, la información continúa siendo un dato personal y debe tratarse conforme al RGPD. Por tanto, no basta con eliminar el nombre, el DNI u otros identificadores directos para afirmar que los datos han sido anonimizados.

Cómo considerar que unos datos son anonimizados

Las Directrices plantean dos preguntas principales para examinar si unos datos pueden considerarse anónimos:

1. ¿Esta información se refiere a una persona física?
2. ¿Esa persona está identificada o puede llegar a ser identificada?

Si la respuesta a alguna de estas preguntas es **NO**, la información puede considerarse anónima. No obstante, el análisis debe tener en cuenta si existen medios razonables que permitan identificar a la persona.

La anonimización dependerá de quién tenga acceso a los datos

Una novedad importante de estas Directrices es que la anonimización debe analizarse desde la perspectiva de las entidades que puedan acceder a la información. Por ello, unos mismos datos pueden ser anónimos para una organización, pero continuar siendo datos personales para otra que disponga de información adicional o de otros medios para identificar a las personas. Por lo tanto, antes de considerar que la anonimización es efectiva, debe comprobarse:

- quién tendrá acceso a los datos;
- qué información adicional tiene o puede conseguir;
- qué relación existe entre las entidades participantes;
- qué recursos técnicos y económicos tiene a su alcance;
- y si podría recurrir a terceros para identificar a las personas.

Cuando una entidad trata los datos siguiendo las instrucciones de otra organización, como ocurre con un encargado del tratamiento, el análisis deberá efectuarse desde la perspectiva del responsable. El responsable no puede evitar la aplicación del RGPD encargando el tratamiento a una empresa que, por sí sola, no pueda identificar a las personas.

Medios que se podrían usar para identificar una persona

Los medios de identificación pueden ir desde una búsqueda sencilla en Internet hasta la combinación de distintas bases de datos o el uso de herramientas de inteligencia artificial. No es necesario que el riesgo de identificación sea totalmente inexistente para considerar anónimos los datos, pero sí debe ser insignificante en la práctica. Las restricciones contractuales pueden contribuir a limitar el riesgo de reidentificación, pero no se consideran suficientes por sí mismas para garantizar la anonimización. Deben acompañarse de medidas técnicas y organizativas que impidan o dificulten realmente la identificación.

A partir de dichas Directrices, es esencial que las entidades revisen sus procedimientos de anonimización de datos para las distintas finalidades que se prevean, tales como, análisis estadísticos, reutilización de datos en el ámbito de la administración, a los efectos de evidenciar que los datos generados no se engloban en el ámbito de aplicación del RGPD.

Novedades en materia de web scraping

Las [Directrices 03/2026 del CEPD](#), adoptadas el 7 de julio de 2026 para consulta pública también hasta el 30 de octubre, estudian la extracción automatizada de información disponible en Internet (web scraping) cuando se utiliza para entrenar o ajustar modelos de inteligencia artificial generativa. Se refieren principalmente a los supuestos en los que una entidad privada realiza directamente el *web scraping*, encarga su ejecución a un tercero o reutiliza un conjunto de datos previamente recopilado por otra organización.

Antes de iniciar el *web scraping*, el responsable debe definir con precisión:

- La finalidad perseguida.
- Identificar las fuentes y categorías de datos que pretende recopilar.
- Delimitar los criterios de recogida.
- Adoptar medidas para evitar datos innecesarios.
- Determinar el rol de las entidades participantes.
- Determinar la base jurídica que legitima el tratamiento.

En el ámbito privado, las Directrices señalan que la base utilizada con mayor frecuencia será el interés legítimo, aunque su aplicación no puede presumirse y deberá justificarse mediante un análisis previo y específico. Por esto, cuando el responsable pretenda fundamentar el *web scraping* en el interés legítimo del artículo 6.1.f) del RGPD, deberá comprobar, antes de iniciar el tratamiento, el cumplimiento de tres condiciones acumulativas:

1. **Existencia de un interés legítimo:** el interés debe ser lícito, real, actual y estar formulado de manera clara y precisa. No basta con decir que el interés es “mejorar la IA” y, por lo tanto, se tiene que explicar qué objetivo se pretende alcanzar y si responde a una finalidad concreta.

2. **Necesidad del tratamiento:** hay que acreditar que el tratamiento de datos personales permite alcanzar el objetivo perseguido y que no existe otra alternativa igualmente eficaz y menos intrusiva.
3. **Ponderación de los derechos e intereses en conflicto:** el responsable debe valorar si su interés prevalece sobre los derechos, libertades e intereses de las personas afectadas. Para ello deberá tener en cuenta la naturaleza de los datos, el contexto en el que fueron publicados, el volumen de información recopilada, las posibles consecuencias del tratamiento y las expectativas razonables de las personas.

El CEPD recuerda que el hecho de que la información sea públicamente accesible no excluye la aplicación del RGPD. También deben considerarse las medidas adoptadas por el sitio web para impedir el *scraping*, como los archivos robots.txt o ai.txt, los sistemas CAPTCHA o la necesidad de iniciar sesión. Asimismo, deberán valorarse las características de las personas afectadas, especialmente cuando se trate de menores o de colectivos vulnerables.

Cuando la ponderación inicial no sea favorable, el responsable podrá valorar la introducción de medidas adicionales para reducir el impacto sobre las personas. Entre ellas pueden incluirse la exclusión de determinadas categorías de datos, la limitación temporal de la recopilación, la implantación de mecanismos de oposición previa, la eliminación o anonimización de los datos y la adopción de garantías frente a la memorización o reproducción de información personal por el modelo. Si, pese a estas medidas, los derechos de las personas continúan prevaleciendo, el tratamiento no podrá basarse en el interés legítimo.

Transparencia frente a las personas afectadas

El CEPD reconoce que, debido a la escala del *web scraping*, proporcionar información individual puede resultar imposible o exigir un esfuerzo desproporcionado. En estos casos podría resultar aplicable la excepción del **artículo 14.5.b) del RGPD**. Sin embargo, esta excepción no puede invocarse de forma automática y deberá justificarse teniendo en cuenta factores como el número de personas afectadas, la antigüedad de la información, las dificultades reales de contacto y las garantías adoptadas. Esto implica que, pese a no ser posible informar de manera individual, el responsable tendrá que facilitar información en su web o en cualquier otro medio accesible.

Las Directrices prestan especial atención al principio de minimización. Este principio obligaría al responsable a evitar la recopilación de datos personales que no sean necesarios para la finalidad perseguida, con el objetivo de que cada dato personal resulte realmente necesario y proporcionado para la finalidad del tratamiento. Durante y después de la recopilación, también se tendrán que usar mecanismos para detectar y borrar datos personales identificables por su formato, como números de teléfono o de afiliación a la Seguridad Social y, cuando sea viable, los datos reales deberán sustituirse por datos sintéticos o someterse a procesos de anonimización o, alternativamente, seudonimización.

Categorías especiales de datos

Las Directrices reconocen que el *web scraping* puede recoger accidentalmente datos especialmente protegidos, aunque el responsable haya adoptado medidas para evitarlo. En estos casos, deberá valorarse si resulta aplicable el criterio establecido por el TJUE en el asunto GC y otros, C-136/17, que tiene en cuenta las posibilidades reales del responsable para controlar el tratamiento. La recogida deberá ser accidental, difícil de detectar previamente y haberse producido pese a las medidas

adoptadas. Este criterio no permite recopilar deliberadamente este tipo de datos sin cumplir alguna de las excepciones del artículo 9.2 del RGPD.

Como mínimo, deberán implantarse filtros antes de la recopilación, eliminarse estos datos cuando sean detectados, impedir que puedan extraerse o reproducirse desde el modelo y supervisar de forma continua las respuestas generadas por el sistema. El responsable también deberá revisar periódicamente la eficacia de estas medidas y adaptarlas a la evolución de la tecnología.

Criterios y actuaciones recientes de la AEPD

La AEPD señala las garantías necesarias para utilizar la IA en sistemas de videovigilancia

La Agencia Española de Protección de Datos (AEPD) ha dirigido dos advertencias a dos ayuntamientos que tenían previsto incorporar funciones de inteligencia artificial en sus sistemas de videovigilancia.

Estas advertencias tienen carácter preventivo, ya que los tratamientos todavía no se habían iniciado. Por tanto, la AEPD no declara que se haya cometido una infracción ni impone una sanción. Su objetivo es avisar de los posibles riesgos para que los ayuntamientos incorporen las garantías necesarias antes de poner en funcionamiento los sistemas.

Uno de los proyectos incluía funciones de detección o reconocimiento facial, si bien la documentación analizada no permitía determinar si dichas funcionalidades serían efectivamente activadas ni si implicarían la identificación biométrica de las personas. El otro preveía, entre otras posibilidades:

- detectar personas y vehículos;
- generar y guardar información sobre las imágenes;
- buscar personas según su apariencia, como la ropa, el pelo, el sexo o el grupo de edad;
- y localizar a una persona utilizando como referencia una imagen o fotografía.

La AEPD aclara que la normativa de protección de datos no prohíbe utilizar inteligencia artificial en los sistemas de videovigilancia. Sin embargo, estas tecnologías deben utilizarse con garantías adecuadas y teniendo en cuenta los riesgos que pueden generar.

Por ello, antes de activar cada funcionalidad de IA, el responsable deberá analizar:

- qué objetivo concreto persigue;
- si su utilización es realmente necesaria y proporcionada;
- qué datos genera;
- durante cuánto tiempo se conservarán;
- quién podrá acceder a ellos;

- y qué medidas tendrán que aplicarse si el sistema se actualiza o incorpora nuevas funciones.

Las funciones que no sean necesarias tendrán que permanecer desactivadas por defecto. Además, no basta con justificar de forma general la instalación de las cámaras, sino que debe analizarse por separado cada función adicional, como el reconocimiento facial, la búsqueda por apariencia o el seguimiento de una persona a través de varias grabaciones.

El responsable también deberá estudiar los riesgos que el sistema puede generar para las personas. Si el tratamiento puede suponer un alto riesgo, deberá realizar una **evaluación de impacto relativa a la protección de datos** antes de ponerlo en funcionamiento.

La AEPD presta especial atención a las funciones que puedan utilizar datos biométricos para identificar de forma única a una persona. No toda detección de rostros implica necesariamente el tratamiento de datos biométricos. Sin embargo, si el sistema crea plantillas u otras representaciones técnicas para identificar a las personas, deberán aplicarse las garantías reforzadas previstas para este tipo de datos.

Por tanto, es necesario que el responsable conozca cómo funciona la herramienta, qué información genera y para qué se utiliza.

En el caso de tratamientos realizados por la Policía Local para prevenir, detectar o investigar infracciones, también deberá justificarse cada función teniendo en cuenta si resulta necesaria, adecuada y proporcionada para la finalidad de seguridad perseguida. En definitiva, la disponibilidad técnica de una función de IA no justifica por sí sola su uso. Las garantías de protección de datos deben incorporarse desde el inicio del proyecto.

Primera brecha de datos notificada a la AEPD causada por un agente de IA

La AEPD ha recibido la primera notificación de una brecha de datos personales en la que el ataque habría sido ejecutado mediante un agente de inteligencia artificial. De acuerdo con la información comunicada por la organización afectada, el agente habría buscado vulnerabilidades, accedido correctamente al sistema y, una vez dentro, habría continuado analizando la aplicación de forma autónoma hasta conseguir modificar datos personales y acceder a facturas.

La AEPD aclara que estos hechos todavía deben analizarse y que la utilización de un determinado modelo de lenguaje no significa que el propio modelo o la infraestructura de su proveedor hayan sido comprometidos. Tampoco implica que la herramienta estuviera diseñada para realizar actividades maliciosas. Lo relevante es que un tercero habría utilizado un agente de IA para ejecutar y conectar distintas fases del ataque.

A diferencia de otras herramientas de IA que se limitan a ayudar en tareas concretas, un agente puede recibir un objetivo, planificar los pasos necesarios, utilizar herramientas y adaptar su comportamiento a los resultados obtenidos. Aunque la IA no crea necesariamente nuevas amenazas, sí puede aumentar la velocidad, el alcance y la capacidad de adaptación de ataques ya conocidos.

Aunque esta primera notificación no permite afirmar que exista una tendencia general, demuestra que los ataques mediante agentes de IA han dejado de ser un riesgo meramente teórico. Por ello, las organizaciones deberían:

- **Incluir expresamente los ataques mediante IA en los análisis de riesgos**, sin limitarse a referencias generales al phishing, el *malware* o los accesos no autorizados.
- **Revisar los tiempos de respuesta**, ya que un agente puede analizar varios sistemas, probar distintas vías de acceso y modificar rápidamente su actuación.
- **Proteger las cuentas y credenciales**, como contraseñas, claves API o tokens, y evitar que tengan permisos más amplios de lo necesario.
- **Implantar sistemas rápidos de detección y respuesta**, porque la intervención manual puede no ser suficiente para detener un ataque automatizado.

Este primer incidente se produce, además, en un contexto de fuerte **incremento de brechas de datos personales** tal y como ha puesto de manifiesto recientemente la AEPD. Durante el primer semestre de 2026 la AEPD recibió 3.027 notificaciones, un 138 % más que en el mismo periodo del año anterior y una cifra superior a la registrada durante todo 2025. Entre las causas de este aumento destacan el avance de la ciberdelincuencia, los ataques de ransomware y los incidentes que afectan simultáneamente a varios responsables a través de un mismo proveedor o encargado del tratamiento.

Novedades normativas sobre el uso de algoritmos

Nuevas obligaciones sobre el uso de algoritmos en el ámbito laboral

[El Real Decreto 723/2026, de 9 de septiembre](#), en vigor desde el 5 de octubre de 2026, establece nuevas obligaciones de información para las empresas que utilicen sistemas algorítmicos o automatizados de toma de decisiones.

La principal novedad es la obligación de transparencia por la que la empresa deberá informar por escrito a cada persona trabajadora de la existencia de estos sistemas y, cuando intervengan en decisiones sobre:

- la jornada laboral;
- la asignación de tareas;
- el salario;
- la promoción profesional;
- el lugar de trabajo;
- la movilidad interna;
- la finalización de la relación laboral.

En las nuevas relaciones laborales, esta información tendrá que entregarse antes de que empiece la prestación de servicios, y los cambios relevantes en el funcionamiento del sistema deberán comunicarse lo antes posible y, como máximo, el mismo día en que empiecen a aplicarse. En las relaciones laborales que ya estén vigentes, la persona trabajadora podrá solicitar esta información y la empresa dispondrá de **30 días hábiles** para facilitársela.

Estas nuevas obligaciones de transparencia deben entenderse juntamente con las garantías establecidas por la normativa de protección de datos para el uso de sistemas algorítmicos en decisiones laborales. En este sentido, resulta ilustrativa la advertencia [AI-00009-2026](#) emitida por la AEPD sobre una herramienta de inteligencia artificial que todavía no se había implantado en España. La herramienta estaba prevista para procesos de selección y movilidad interna. Analizaría currículums, asignaría una puntuación en función de la adecuación de cada persona al puesto y ordenaría las candidaturas. Por tanto, podría influir directamente en el acceso al empleo y en la promoción profesional.

Asimismo, la AEPD señala que no basta con que una persona confirme formalmente la decisión propuesta por el algoritmo. Quien revise el resultado debe entender las limitaciones de la herramienta, contar con información suficiente y tener capacidad real para cambiar su recomendación.

Si la persona acepta siempre la puntuación del sistema sin revisarla de forma crítica, la decisión podría considerarse automatizada en la práctica. Es decir, aunque formalmente intervenga una persona, quien estaría decidiendo realmente sería el algoritmo.

No todo uso de un sistema algorítmico supone una decisión automatizada a efectos del artículo 22 del RGPD. Este artículo se aplica cuando la decisión se adopta únicamente de forma automática y produce consecuencias importantes para la persona, como descartarla de un proceso de selección o impedir su promoción. En estos casos, la persona afectada deberá poder solicitar una revisión humana, explicar su situación e impugnar la decisión.

Novedades normativas de la APDCAT

Nueva Circular 1/2026 de la APDCAT sobre videovigilancia: nuevas obligaciones para administraciones y entidades públicas

La Circular 1/2026 de la “*Autoritat Catalana de Protecció de Dades*” APDCAT actualiza el régimen aplicable a los sistemas de videovigilancia en Cataluña, adaptándolo al RGPD y a la LOPDGDD, y se aplicará a administraciones, entidades del sector público y determinadas entidades privadas a partir del 8 de noviembre de 2026.

Entre las principales novedades, la Circular refuerza las obligaciones de análisis previo y proporcionalidad, exige incluir los tratamientos de videovigilancia en el Registro de Actividades de Tratamiento, aunque no exista grabación de imágenes, actualiza los requisitos de información mediante carteles informativos y establece medidas específicas en materia de conservación, seguridad y gestión de derechos. Asimismo, presta especial atención al uso de tecnologías de inteligencia artificial y reconocimiento facial, sometiéndolas a requisitos adicionales de cumplimiento normativo.

Para más información sobre la Circular 1/2026 puede consultar nuestra [Nota informativa](#).

Contacto



Carme Setó

Socia | Derecho Digital, IT y
protección de datos
cseto@duransindreu.com
93 602 52 22



Núria Galera

Abogada | Derecho Digital, IT y
protección de datos
ngalera@duransindreu.com
93 602 52 22



Iván Roda

Abogado | Derecho Digital, IT y
protección de datos
iroda@duransindreu.com
93 602 52 22



Bàrbara Boguñá

Abogada | Derecho Digital, IT y
protección de datos
bboguena@duransindreu.com
93 602 52 22