

La AEPD fija las garantías para incorporar inteligencia artificial a sistemas de videovigilancia

La Agencia Española de Protección de Datos (AEPD) ha emitido dos advertencias preventivas dirigidas a ayuntamientos que proyectan implantar sistemas de videovigilancia con funcionalidades de inteligencia artificial (IA) para el análisis automatizado de imágenes. A través de estas actuaciones, la Agencia recuerda que la normativa de protección de datos no prohíbe el uso de tecnologías de IA, pero exige que su implantación se lleve a cabo con garantías adecuadas y de conformidad con los principios de protección de datos desde el diseño y por defecto.

Puntos clave a destacar

- La AEPD recuerda que el uso de IA en sistemas de videovigilancia, requiere la implementación de garantías adecuadas.
- Destaca la protección de datos desde el diseño y por defecto, que debe integrarse desde las fases iniciales del proyecto, incluyendo la selección, configuración e implantación de las tecnologías utilizadas.
- Cada funcionalidad basada en IA debe someterse a un análisis específico de necesidad, idoneidad y proporcionalidad.
- Advierte de la necesidad de realizar una Evaluación de Impacto relativa a la Protección de Datos (EIPD) antes de su puesta en marcha, en la medida en que el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas.
- Las funcionalidades que impliquen el tratamiento de datos biométricos destinados a identificar de manera unívoca a una persona estarán sujetas a un régimen reforzado de garantías.



1. Antecedentes

El 6 de octubre de 2026, la AEPD informó de la emisión de dos advertencias dirigidas a ayuntamientos cuyos proyectos de videovigilancia contemplaban funcionalidades de IA para el análisis automatizado de imágenes.

Ambas actuaciones se enmarcan en la facultad prevista en el artículo 58 del RGPD, que permite a las autoridades de control advertir cuando determinadas operaciones de tratamiento previstas puedan infringir la normativa de protección de datos. La AEPD recuerda que la finalidad de esta medida no es sancionar una conducta ni declarar la existencia de una infracción, sino advertir de que determinados tratamientos podrían resultar contrarios a dicha normativa.

Las advertencias de la AEPD tienen su origen en dos proyectos municipales de videovigilancia que contemplaban la incorporación de funcionalidades de inteligencia artificial para el análisis automatizado de imágenes. Entre las capacidades previstas figuraban, la detección y clasificación de personas y vehículos, la generación de metadatos, las búsquedas de personas a partir de determinados atributos físicos o imágenes de referencia y, en uno de los proyectos, funcionalidades de reconocimiento facial.

2. Análisis de la AEPD

Más allá de las circunstancias concretas de los expedientes analizados, la AEPD consideró necesario recordar las principales obligaciones y garantías que deben observarse cuando se incorporan herramientas de inteligencia artificial a sistemas de videovigilancia, especialmente cuando puedan afectar de forma significativa a los derechos y libertades de las personas o implicar tratamientos de datos biométricos.

a. Protección de datos desde el diseño y por defecto

La Agencia recuerda la importancia de integrar los principios de protección de datos desde el diseño y por defecto en aquellos proyectos que incorporen IA a sistemas de videovigilancia.

De conformidad con el artículo 25 del RGPD y el artículo 28 de la Ley Orgánica 7/2021, estas garantías deben tenerse en cuenta tanto en la determinación de los medios del tratamiento como durante toda su ejecución.

Según la AEPD, este enfoque permite identificar y mitigar los riesgos asociados al tratamiento antes de la puesta en funcionamiento de la tecnología y exige la adopción de medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de la normativa.

Como manifestación de estos principios, la AEPD recuerda que la mera disponibilidad técnica de una funcionalidad no constituye una justificación suficiente para su utilización. Funcionalidades como el reconocimiento facial, la búsqueda por atributos o la localización de personas deben analizarse y justificarse individualmente en atención a la finalidad perseguida, acreditando su necesidad, idoneidad y proporcionalidad.

b. Especial atención al tratamiento de datos biométricos

La AEPD presta una especial atención a aquellas funcionalidades que puedan implicar el tratamiento de datos biométricos destinados a identificar de manera unívoca a una persona.

La Agencia advierte de que en estos supuestos resultará aplicable el régimen reforzado previsto en los artículos 4.14 y 9 del RGPD y en el artículo 13 de la Ley Orgánica 7/2021, debiendo concurrir además una base habilitante adecuada y garantías específicas para los derechos y libertades de las personas afectadas.

Las consideraciones de la Agencia se alinean con el Reglamento de IA, que somete los sistemas de identificación biométrica remota a un régimen particularmente estricto. En especial, el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la ley está, con carácter general, prohibido, salvo en los supuestos excepcionales expresamente previstos por la norma y sujetos a condiciones específicas. Por su parte, los sistemas de identificación biométrica remota que no queden comprendidos en dicha prohibición pueden estar clasificados como sistemas de alto riesgo, resultándoles aplicables las correspondientes obligaciones reforzadas en materia de gestión de riesgos, gobernanza y calidad de datos, supervisión humana, documentación y evaluación de conformidad.

c. Evaluación previa de los riesgos para los derechos y libertades de los interesados

La AEPD recuerda que los responsables del tratamiento deben evaluar, con carácter previo a la puesta en marcha del sistema, los riesgos que el tratamiento pueda comportar para los derechos y libertades de las personas afectadas, incluidos usuarios, trabajadores y terceros.

En este sentido, la Agencia destaca que la incorporación de funcionalidades avanzadas de inteligencia artificial aplicadas a la videovigilancia, especialmente aquellas que permiten clasificar personas, generar metadatos, realizar búsquedas por atributos físicos, utilizar imágenes de referencia o incorporar capacidades de identificación, exige una valoración específica de su impacto sobre los derechos fundamentales de los afectados.

Asimismo, recuerda que, cuando el tratamiento sea susceptible de entrañar un alto riesgo en los términos previstos en el artículo 35 del RGPD y en el artículo 35 de la Ley Orgánica 7/2021, deberá realizarse, con carácter previo al inicio del tratamiento, la correspondiente evaluación de impacto relativa a la protección de datos.

Por otro lado, la Agencia señala que, en el caso de videocámaras fijas instaladas en lugares públicos, debe efectuarse además un análisis de necesidad y proporcionalidad que tenga en cuenta tanto la finalidad perseguida como el potencial impacto para la ciudadanía. Esta valoración no debe limitarse a la instalación de las cámaras, sino que debe extenderse a cada una de las funcionalidades de inteligencia artificial incorporadas al sistema.

Aunque las advertencias no califican expresamente los proyectos analizados como tratamientos de alto riesgo, las funcionalidades examinadas evidencian la necesidad de realizar una valoración rigurosa de los riesgos asociados al tratamiento y, en su caso, de llevar a cabo una evaluación de impacto con carácter previo a su despliegue.

3. Conclusiones

Las advertencias emitidas por la AEPD evidencian que la utilización de sistemas de videovigilancia dotados de funcionalidades de IA no resulta incompatible con la normativa de protección de datos.

Sin embargo, su implantación exige una evaluación previa y rigurosa de los riesgos asociados, así como la adopción de garantías adecuadas atendiendo a las características y finalidades concretas de cada tratamiento.



La AEPD presta especial atención a aquellas funcionalidades que puedan implicar el tratamiento de datos biométricos destinados a identificar de manera unívoca a una persona, supuesto en el que resultará de aplicación un régimen reforzado de garantías. Del mismo modo, destaca la necesidad de realizar evaluaciones de impacto cuando el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de las personas afectadas.

En definitiva, estas advertencias refuerzan la importancia de adoptar un enfoque de responsabilidad proactiva en el desarrollo e implementación de soluciones de IA aplicadas a la videovigilancia, permitiendo compatibilizar el aprovechamiento de las capacidades que ofrecen estas tecnologías con la adecuada protección de los derechos fundamentales de las personas.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60