

Ref.: EXP202621928
Asunto: Advertencia

PRIMERO. - Examinada la documentación correspondiente al expediente de contratación 1616529E, «*Suministro, instalación, puesta en marcha y mantenimiento de sistema de videovigilancia para la seguridad ciudadana*», promovido por el *****AYUNTAMIENTO A.A.A.**, se han identificado por la Agencia Española de Protección de Datos (AEPD) determinadas previsiones que ponen de manifiesto la posible realización futura de tratamientos de datos personales mediante funcionalidades de análisis automatizado de imágenes.

En particular, el Pliego de Prescripciones Técnicas (PPT), fechado el 22 de junio de 2026, contempla la instalación de nuevos sistemas de videovigilancia en diferentes instalaciones municipales (edificios públicos y otras áreas municipales acotadas), su gestión y visualización centralizada desde las dependencias de la Policía Local y, en las especificaciones técnicas de los grabadores recogidas en las páginas 10 y 11 del PPT, requiere expresamente funcionalidades de «detección/reconocimiento facial».

La inclusión de dichas funcionalidades constituye un indicio de que el sistema podría realizar operaciones de análisis de imágenes de personas mediante inteligencia artificial y, eventualmente, tratamientos dirigidos a su identificación unívoca. La documentación examinada no permite determinar si estas funcionalidades serán efectivamente activadas ni si se generarán plantillas, vectores o representaciones biométricas, se efectuarán comparaciones 1:1 o 1:N o se utilizarán galerías o bases de imágenes de referencia.

Debe diferenciarse, en función de la finalidad concreta de cada operación de tratamiento, entre aquellas sometidas al Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), y aquellas que, por ser realizadas por una autoridad competente para la prevención, detección, investigación o enjuiciamiento de infracciones penales o para la protección y prevención frente a amenazas contra la seguridad pública, queden sometidas a la Ley Orgánica 7/2021, de 26 de mayo.

SEGUNDO. - El artículo 55.1 del RGPD dispone que “*cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro*”.

El art. 58.2 del RGPD establece que cada autoridad de control dispondrá de todos poderes correctivos indicados a continuación, y entre ellos el recogido en su letra a) de dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en dicho Reglamento.

De acuerdo con el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD) corresponde a la AEPD, entre otras facultades, ejercer las potestades previstas en el artículo 58 del RGPD.

De la misma forma, los artículos 48 y 50 de la Ley Orgánica 7/2021 atribuyen a la AEPD, como autoridad de protección de datos independiente, entre otras, la potestad de advertencia y control de lo exigido en esa Ley Orgánica.

TERCERO. - Por otra parte, tal y como resulta de jurisprudencia constante del Tribunal de Justicia de la Unión Europea, el objetivo del RGPD (véase, por ejemplo, apartado 53 de la Sentencia del Tribunal de Justicia (Sala Cuarta), de 7 de marzo de 2024, C-604/22, consiste en “*garantizar un nivel elevado de protección de los derechos y libertades fundamentales de las personas físicas, sobre todo de su derecho a la vida privada respecto del tratamiento de los datos personales, consagrado en el artículo 8, apartado 1, de la Carta y en el artículo 16 TFUE, apartado 1 [sentencia de 4 de mayo de 2023, Bundesrepublik Deutschland (Buzón electrónico judicial), C-60/22, EU:C:2023:373, apartado 64].*”

Por ello, las facultades y poderes correctivos de las autoridades de control habrán de interpretarse de una manera amplia. Véase por analogía, apartado 37 de la sentencia del Tribunal de Justicia, de 26 de septiembre de 2024, C-768/21.

CUARTO. - Por otro lado, no hay que olvidar que dentro de las facultades que configura el RGPD para las autoridades de control existe también una labor “cautelar” o “preventiva”. Así, por ejemplo, el apartado 188 de las Conclusiones del Abogado General Sr. Dean Spielmann, de 23 de septiembre de 2025, en el Asunto C-474/24 dice:

188. (...) el artículo 58, apartado 2, del mencionado Reglamento enumera los diferentes poderes correctivos de que dispone la autoridad de control, que cuenta, a este respecto, con un margen de apreciación en lo que atañe a la elección de los medios adecuados y necesarios. (112) Entre los poderes de la autoridad de control establecidos en el artículo 58, apartado 2, letra a), del RGPD, esta puede dirigir una «advertencia» a todo responsable del tratamiento cuando las operaciones de tratamiento «previstas» «puedan» infringir lo dispuesto en el RGPD, lo que se inscribe en un enfoque que cabe calificar de «cautelar» respecto de los derechos del interesado. (113)

QUINTO.- Por lo demás, esa facultad cautelar o preventiva que el RGPD otorga a las autoridades de control está expresada en términos amplios en el art. 58.2.a) RGPD, de manera que esta norma ha otorgado a las autoridades de control la facultad de dirigir a todo responsable o encargado del tratamiento una advertencia, no necesariamente cuando esta haya comprobado que el tratamiento es contrario al RGPD, sino cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento.

La utilización de esta expresión “puedan” se inserta dentro de dicha función cautelar o preventiva, que hay que entenderla, cuando la autoridad de control decide dirigir una advertencia, no como una realidad de que dichas operaciones efectivamente infringen el RGPD, sino de que existe la posibilidad (como contrario a certeza) de que dichas operaciones pueden infringir el Reglamento.

De forma similar, la facultad cautelar o preventiva de la AEPD está expresada en el artículo 50 de la Ley Orgánica 7/2021.

Por ello, en el ejercicio de esta función cautelar, la autoridad de control podrá, sobre la base de la información recibida, e incluso de la que no haya recibido, emitir una advertencia al responsable o encargado del tratamiento, acerca de la posibilidad de que dichos tratamientos de datos infrinjan el Reglamento, para que el responsable o encargado extraiga de dicha advertencia las enseñanzas o criterios apropiados y, conforme a su obligación de responsabilidad proactiva, pueda adaptar dichos tratamientos de datos al Reglamento.

No cabe, por último, tampoco, excluir que la información de que disponga la autoridad de control sea incompleta, por cualquier razón. Ello no hará menos efectiva su advertencia – y por tanto el objetivo de la normativa de protección de datos de proteger a los interesados-, por cuanto el objetivo de la advertencia no es sancionar una conducta del responsable o encargado, sino advertir (esto es, llamar la atención del responsable o encargado) de que unos determinados tratamientos podrían infringir la normativa de protección de datos, sin necesidad de que exista una certeza de que dichos tratamientos la incumplen.

SEXTO. – A partir de la información analizada, cabe realizar por esta Autoridad las siguientes consideraciones.

La utilización de dispositivos de videovigilancia dotados de funcionalidades de inteligencia artificial en departamentos de la Administración pública, particularmente en órganos policiales, puede ofrecer oportunidades para mejorar su eficiencia, proporcionando instrumentos de apoyo que contribuyan a garantizar la seguridad. Asimismo, adecuadamente diseñadas y utilizadas, estas herramientas pueden contribuir a mejorar la eficacia y calidad de determinados tratamientos de datos y de las inferencias obtenidas a partir de ellos.

La normativa de protección de datos no impide la utilización de estas tecnologías en dichos procesos, sino que exige que los tratamientos de datos personales que comporten se desarrollen con las garantías adecuadas a sus características y riesgos. Desde esta perspectiva, cabe integrar dichas garantías en el propio proceso de diseño, evaluación, selección, configuración e implantación de la herramienta. Este enfoque favorece que el desarrollo y adopción de soluciones innovadoras pueda realizarse de forma responsable, aprovechando sus posibles beneficios y preservando al mismo tiempo los derechos y libertades de las personas afectadas.

Esta visión se proyecta, en particular, a través de la protección de datos desde el diseño y por defecto prevista en el artículo 25 del RGPD y en el artículo 28 de la Ley Orgánica 7/2021, que exigen integrar de manera efectiva los principios y garantías de protección de datos, tanto al determinar los medios del tratamiento, particularmente en la fase de adquisición y configuración tecnológica, como durante su ejecución.

La integración de las exigencias de protección de datos desde las fases iniciales de un proyecto tecnológico permite, precisamente, identificar los riesgos asociados al tratamiento y adoptar las medidas adecuadas para gestionarlos. La gestión del riesgo constituye, por tanto, un elemento inherente al sistema de responsabilidad proactiva y debe acompañar al tratamiento durante su ciclo de vida. En aquellos supuestos en los que, atendiendo a la naturaleza, alcance, contexto o fines del tratamiento, este sea susceptible de entrañar un alto riesgo para los derechos y libertades de las personas físicas, deberá realizarse, antes del tratamiento, una evaluación de impacto relativa a

la protección de datos en los términos establecidos en el artículo 35 del RGPD y en el artículo 35 de la Ley Orgánica 7/2021.

En el escenario analizado se hace especialmente relevante garantizar el cumplimiento de la normativa de protección de datos, al referirse a un sistema de videovigilancia en un municipio cuyo censo supera los 30.000 habitantes. Así, antes de la puesta en servicio del sistema deberá analizarse y documentarse, entre otros extremos: la necesidad y proporcionalidad de cada funcionalidad de inteligencia artificial respecto de la finalidad concreta perseguida; la aplicación efectiva de los principios de minimización de datos y limitación de la finalidad; que las funcionalidades no necesarias permanezcan deshabilitadas por defecto; los datos y metadatos generados, sus plazos de conservación, los perfiles de acceso y las posibilidades de acceso remoto; y las garantías aplicables a posteriores actualizaciones, ampliaciones o cambios de configuración que puedan incorporar nuevas capacidades de análisis o identificación.

Si el reconocimiento facial fuese utilizado para la identificación unívoca de personas, deberá valorarse además el régimen previsto en los artículos 4.14 y 9 del RGPD para los datos biométricos.

De acuerdo con lo previsto en los artículos 6 y 11 de la Ley Orgánica 7/2021, la utilización de inteligencia artificial y, particularmente, de reconocimiento facial deberá justificarse específicamente, atendiendo a la finalidad policial perseguida, sin que la mera disponibilidad técnica de la funcionalidad determine por sí misma la necesidad de su utilización. En consecuencia, las funcionalidades de **reconocimiento facial** u otras formas de identificación o re-identificación de personas deberán permanecer deshabilitadas cuando no se haya justificado previamente su necesidad y proporcionalidad para una finalidad policial concreta.

Si el sistema genera o utiliza datos biométricos destinados a identificar de manera unívoca a una persona, resultará aplicable el régimen reforzado del artículo 13 de la Ley Orgánica 7/2021. El tratamiento deberá responder a criterios de estricta necesidad y quedar sometido a garantías adecuadas para los derechos y libertades de las personas afectadas. La evaluación deberá alcanzar específicamente al sistema de reconocimiento facial, las imágenes o bases de referencia empleadas, el procedimiento de comparación, los umbrales de coincidencia, los falsos positivos y negativos, la intervención humana y las consecuencias derivadas de una eventual coincidencia.

La instalación y utilización de sistemas de grabación deberá cumplir los requisitos de los artículos 15 y 16 de la Ley Orgánica 7/2021, respetando el principio de proporcionalidad y respondiendo a alguno de los fines legalmente establecidos, entre ellos la protección de edificios e instalaciones públicas, la prevención, detección o investigación de infracciones penales y la protección frente a amenazas contra la seguridad pública, particularmente si se trata de **videocámaras fijas instaladas en vías o lugares públicos**. La proporcionalidad deberá valorarse no solo respecto de la instalación de las cámaras, sino también respecto de cada funcionalidad adicional de análisis automatizado de las imágenes.

Cuando a la operación de tratamiento le resulte de aplicación el artículo 18 de la Ley Orgánica 7/2021, deberán respetarse las reglas específicas sobre utilización, puesta a disposición de la autoridad judicial y conservación de las grabaciones, que con

carácter general deberán destruirse en el plazo máximo de tres meses desde su captación, salvo los supuestos excepcionales previstos legalmente. Deberá determinarse asimismo el régimen de conservación aplicable a los datos derivados de las imágenes, incluidos metadatos, plantillas biométricas, vectores, resultados de coincidencia o cualesquiera otros datos producidos mediante inteligencia artificial.

El análisis de riesgos deberá abarcar todo el ciclo de vida del sistema, comprendiendo la definición de requisitos, contratación, selección de equipos y software, instalación y parametrización, puesta en funcionamiento, utilización operativa, mantenimiento, actualizaciones de software o modelos de inteligencia artificial, incorporación de nuevas bases de datos o funcionalidades, ampliaciones, cambios de finalidad y retirada definitiva del sistema. Cualquier modificación que suponga la activación de nuevas capacidades de identificación o reidentificación de personas deberá ser objeto de una evaluación previa específica, sin que su mera disponibilidad en el hardware o software adquirido pueda justificar automáticamente su utilización.

Conforme a las obligaciones de suministro de información que, en función de la finalidad de la operación de tratamiento de videovigilancia, imponen al responsable del tratamiento los artículos 12 a 14 del RGPD (y las especialidades para el cumplimiento de estas obligaciones que la LOPDGGD establece en sus artículos 22 y 89), así como el artículo 21 de la Ley Orgánica 7/2021, las personas afectadas deberán recibir información clara, accesible y comprensible sobre el tratamiento de sus datos personales y, en particular, sobre sus finalidades y sobre la función que el sistema desempeña en el proceso, con el alcance exigible en cada caso.

En virtud de todo lo expuesto, y en aplicación de los poderes que le han sido atribuidos por el artículo 58.2.a) del RGPD y el artículo 50 de la Ley Orgánica 7/2021, esta Agencia procede a dirigir la siguiente **ADVERTENCIA** al *****AYUNTAMIENTO A.A.A.:**

- En el proceso de evaluación e implantación de sistemas de videovigilancia con funcionalidades de inteligencia artificial, el responsable de tratamiento deberá cumplir con sus obligaciones de protección de datos desde el diseño y por defecto y adoptar, de conformidad con los artículos 24 y 25 del RGPD y los artículos 27 y 28 de la Ley Orgánica 7/2021, las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales.
- En particular, deberá evaluar los riesgos que el tratamiento pueda comportar para los derechos y libertades de las personas afectadas: usuarios, trabajadores y terceros, 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, realizar, antes del tratamiento, la correspondiente evaluación de impacto relativa a la protección de datos.
- Deberá garantizarse el cumplimiento del principio de transparencia respecto de las personas afectadas, en particular, aunque no de manera exclusiva, el suministro de información previsto en el artículo 13 RGPD y en el artículo 21 de la Ley Orgánica 7/2021.
- Aquellas operaciones que sean realizadas por la Policía Local para los fines comprendidos en la Ley Orgánica 7/2021 deberán ajustarse específicamente, en

particular, a los artículos 6, 11, 13, 15, 16 y 18, debiendo valorarse antes de su implantación efectiva la licitud, estricta necesidad, idoneidad, proporcionalidad e intervención mínima de las funcionalidades de inteligencia artificial y las garantías necesarias.

Finalmente, se procede a señalar que, en el supuesto de no adoptar las medidas que, en su caso, fueran necesarias para adecuar su actuación a lo legalmente establecido, podría incurrir en una infracción en el ámbito competencial de esta Agencia, que podría dar lugar al inicio de actuaciones previas de investigación y/o actuaciones correctivas, incluyendo las sancionadoras.

290-030320

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos