

- Expediente N.º: EXP202308696

RESOLUCIÓN DE PROCEDIMIENTO DE APERCIBIMIENTO

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 20 de junio de 2023 se interpuso reclamación ante la Agencia Española de Protección de Datos por una posible infracción imputable a **A.A.A.** con NIF *****NIF.1** (en adelante, **A.A.A.**).

Los hechos que se ponen en conocimiento de esta autoridad son los siguientes:

La parte reclamante, vecina de **A.A.A.**, asegura que reside en un inmueble que consta de dos plantas, con una vivienda en cada una de ellas. El inmueble se encuentra situado en la *****DIRECCIÓN.1**. Manifiesta que **A.A.A.** ha instalado un dispositivo de grabación en la entrada de acceso al inmueble por su parte exterior y que realiza el control de las imágenes captadas mediante un teléfono móvil. Señala que el dispositivo se orienta hacia elementos comunes, como es el acceso al edificio, sin que cuente con el acuerdo entre las partes. Señala que la zona videovigilada no se encuentra debidamente señalizada mediante los preceptivos carteles informativos.

Junto a su reclamación aporta:

- Fotografía de un dispositivo con cámara, situado en el marco exterior de la puerta de acceso a un edificio, orientado hacia la mencionada puerta de acceso. El dispositivo cuenta con una etiqueta en la que se pueden leer el nombre y apellidos de **A.A.A.**
- Copia de la denuncia presentada el 26 de junio de 2023 por la parte reclamante ante (...) en la que, entre otros asuntos, se denuncia que **A.A.A.** ha instalado un dispositivo de grabación de imagen y video sin previo acuerdo entre las partes en el inmueble anteriormente mencionado.
- Extracto de las características identificativas de un modelo concreto de dispositivo de grabación de imágenes, que se reproduce a continuación:

“*MODELO.1** *Timbre Inalámbrico con Cámara, Inalámbrico Videoportero Timbre, Alerta con un Clic, Alimentado por Batería, Detección Humana, Visión Nocturna, Audio de 2 Vías, Ip66, SD/en La Nube,*

Acerca de este producto:

- **【 Líder 2K FHD y Visión Nocturna 】** *El intercomunicador de video inalámbrico ***MODELO.1 adopta un sensor actualizado para mejorar la calidad de la imagen a 2304 x 1296. Modo de día y noche de buena resolución, puede capturar más detalles. Puedes ver en vivo lo que sucede en la puerta de tu casa aún cuando no estés.*
- **【Detección Humana y Alerta con un Clic】** *Equipado con un algoritmo AI de tercera generación, ajustable y precisa detección humana. Si alguien se*

acerca al timbre, te avisará en tu móvil y poder ver quién anda merodeando.

Haga clic en "Sirena" en la aplicación y el timbre emitirá un sonido de alerta de alto decibelio para ahuyentar a los visitantes inesperados.

- **【Altavoz Inalámbrico Portátil】** El intercomunicador de video inalámbrico *****MODELO.1** viene con un altavoz inalámbrico (incluidas 3 baterías AAA). La instalación es fácil y la batería dura mucho tiempo. Escuchará el timbre donde quiera que esté, puede ponerlo donde quiera, como dormitorio, baño, cocina, patio trasero, etc. El rango de conexión es máx 150 metros. (Basado en la prueba al aire libre vacía).

- **【Comunicación Bidireccional Visible】** Gracias a la calidad de imagen 2K y la función de comunicación bidireccional, puede comunicarse claramente con los repartidores incluso cuando no está en casa. Tiene gran amplitud de visión de 166°, permitiéndole ver todo lo que sucede al otro lado de la puerta. Incluso puedes asistir a visitas cuando no estás en casa, o al menos saber quién estuvo si no quieres contestar.

- **【Más Sobre el Videoportero ***MODELO.1】** Este videoportero Wi-Fi admite conexión de múltiples altavoces, la duración de la batería dura más de 3 meses (10 despertadores por día), manual en español, impermeabilización IP66, almacenamiento en tarjeta SD (hasta 128 GB) y almacenamiento en la nube (7 días gratis), monitoreo en línea de varias personas de múltiples escenas y control de aplicaciones gratuito y fácil de usar. (Solo admite Wi-Fi de 2,4 Ghz)

Información extraída de "(...)".

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a **A.A.A.**, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

La notificación del traslado de la reclamación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), se produjo el 1 de septiembre de 2023 mediante correo postal.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 20 de septiembre de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación.

CUARTO: Con fecha 6 de febrero de 2025, la Presidencia de la Agencia Española de Protección de Datos acordó iniciar procedimiento de apercibimiento a la parte reclamada, por las presuntas infracciones de los artículos 6.1 y 13 del RGPD, tipificadas respectivamente en los artículos 83.5.a) y 83.5 b) del RGPD.

QUINTO: La notificación del citado acuerdo de iniciación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), resultó infructuosa. El primer intento de entrega se realizó el 14 de febrero de 2025, con resultado “ausente” y el segundo intento de entrega tuvo lugar el 18 de febrero de 2025, de nuevo con resultado “ausente”. En consecuencia, fue devuelto por Correos el 25 de febrero de 2025 tras no haber sido retirado de la oficina, a pesar de haber dejado aviso en el buzón.

Conforme al artículo 44 de la LPACAP, la publicación en el Boletín Oficial del Estado (BOE) del acuerdo de iniciación del presente procedimiento se produjo en fecha 3 de marzo de 2025.

SEXTO: Una vez transcurrido el plazo otorgado para la formulación de alegaciones, se ha constatado que no se ha recibido alegación alguna por la parte reclamada.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes

HECHOS PROBADOS

PRIMERO: Existe un dispositivo de videovigilancia en la fachada exterior de un edificio, en concreto, en el marco de la puerta de acceso al inmueble sito en *****DIRECCIÓN.1.**

SEGUNDO: El dispositivo de videovigilancia se encuentra ubicado en un elemento común del inmueble y capta zonas comunes sin contar con la preceptiva autorización de la comunidad de propietarios.

TERCERO: El sistema de videovigilancia carece del preceptivo cartel informativo de zona videovigilada en lugar visible.

CUARTO: El responsable del dispositivo de videovigilancia es **A.A.A.** con NIF *****NIF.1.**

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1 y 64.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGD), es competente para iniciar y resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

II Procedimiento

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *“Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos”.*

Considerando la naturaleza de los hechos que han dado lugar a las actuaciones y las circunstancias concurrentes, el presente procedimiento de apercibimiento se sigue de conformidad con lo establecido en el artículo 64.3 de la LOPDGDD.

El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones, de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

III La imagen es un dato personal

El artículo 4.1) del RGPD, define «dato personal» como: “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”.

El artículo 4.2) del RGPD, define «tratamiento» como: “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.”

El artículo 4.7) del RGPD, define al «responsable del tratamiento» o «responsable» como: “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.

La imagen física de una persona, a tenor del artículo 4.1 del RGPD, es un dato personal y su protección, por tanto, es objeto de dicho Reglamento.

Las imágenes captadas por un sistema de cámaras o videocámaras son datos de carácter personal, por lo que su tratamiento está sujeto a la normativa de protección de datos.

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que **A.A.A.** realiza, entre otros tratamientos, la recogida y conservación de datos personales al contar con un sistema de videovigilancia que realizaría captaciones de imágenes de personas físicas.

A.A.A. realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad en virtud del artículo 4.7 del RGPD.

IV

Normativa sobre protección de datos

El artículo 6.1 del RGPD establece los supuestos que permiten considerar lícito el tratamiento de datos personales.

Además, el tratamiento de datos personales está sometido a la totalidad de los principios del tratamiento contenidos en el artículo 5 del RGPD. Destacaremos el principio de minimización de datos contenido en el artículo 5.1.c) del RGPD que dispone que los datos personales serán *“adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”*.

En cuanto al tratamiento con fines de videovigilancia, el artículo 22 de la LOPDGDD establece que las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Esto significa que en un tratamiento concreto sólo pueden tratarse los datos personales oportunos, que vengan al caso y que sean los estrictamente necesarios para cumplir la finalidad para la que son tratados. El tratamiento debe ser ajustado y proporcional a la finalidad a la que se dirige. La pertinencia en el tratamiento de los datos debe producirse tanto en el momento de la recogida de los datos como en el posterior tratamiento que se realice de los mismos.

Conforme a lo antedicho, debe restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de estos.

La aplicación del principio de minimización de datos en materia de videovigilancia comporta que no puedan captarse imágenes de la vía pública, puesto que el tratamiento de imágenes en lugares públicos sólo puede ser realizado por las Fuerzas y Cuerpos de Seguridad previa autorización gubernativa.

En algunas ocasiones, para la protección de espacios privados, donde se hayan instalado cámaras en fachadas o en el interior, puede ser necesario para garantizar la finalidad de seguridad la grabación de una porción de la vía pública.

Es decir, las cámaras y videocámaras instaladas con fines de seguridad no podrán obtener imágenes de la vía pública salvo que resulte imprescindible para dicho fin, o

resulte imposible evitarlo por razón de la ubicación de aquéllas. Y, en tal caso extraordinario, las cámaras sólo podrán captar la porción mínima necesaria para preservar la seguridad de las personas y bienes, así como de sus instalaciones.

En ningún caso se admitirá el uso de prácticas de vigilancia más allá del entorno objeto de la instalación y, en particular, no pudiendo afectar a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

Las cámaras instaladas no pueden obtener imágenes de espacio privativo de tercero y/o espacio público sin causa justificada debidamente acreditada, ni pueden afectar a la intimidad de transeúntes que transiten libremente por la zona.

No está permitida, por tanto, la colocación de cámaras hacia la propiedad privada de vecinos con la finalidad de intimidarlos o afectar a su ámbito privado sin causa justificada.

Tampoco pueden captarse ni grabarse imágenes en espacios propiedad de terceros sin el consentimiento de sus titulares, o, en su caso, de las personas que en ellos se encuentren, al contravenir el artículo 5 del RGPD, anteriormente indicado.

La captación de imágenes en zonas o elementos comunes de comunidades de propietarios requiere el acuerdo de la junta de propietarios en los términos previstos en la Ley 49/1960, de 21 de julio, sobre propiedad horizontal (en adelante LPH).

Cumplido este requisito, la comunidad de propietarios como responsable del tratamiento, estará sujeta a las restantes obligaciones impuestas por la normativa de protección de datos. Las cámaras sólo podrán captar las zonas comunes de la comunidad, no siendo factible la grabación de imágenes de la vía pública, a excepción de una franja mínima de los accesos al inmueble. Tampoco se podrá realizar la captación de imágenes de terreros y viviendas colindantes o de cualquier otro espacio ajeno. En este último caso, si se usan cámaras orientables y/o con zoom, será necesaria la instalación de máscaras de privacidad para evitar esta grabación.

La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a la comunidad del cumplimiento de la legislación de protección de datos.

V

Obligaciones en materia de videovigilancia

El tratamiento de imágenes a través de un sistema de videovigilancia, para ser conforme con la normativa vigente (artículo 22 de la LOPDGDD) debe cumplir los requisitos específicos siguientes:

1.- La personas físicas o jurídicas, públicas o privadas, pueden establecer un sistema de videovigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

Se ha de valorar si la finalidad pretendida puede lograrse de otra forma menos intrusiva para los derechos y libertades de los ciudadanos. Los datos personales solo

deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios, de acuerdo con el considerando 39 del RGPD.

2.- Las imágenes obtenidas no puedan utilizarse para una finalidad ulterior incompatible con la que motivó la instalación del sistema de videovigilancia.

3.- Se deberá cumplir con el deber de informar a los afectados previsto en los artículos 12 y 13 del RGPD, y 22 de la LOPDGDD.

En tal sentido, se prevé en relación con la videovigilancia un sistema de “información por capas”.

La primera capa ha de referirse, al menos, a la existencia del tratamiento (videovigilancia), la identidad del responsable, la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD y dónde obtener más información sobre el tratamiento de los datos personales.

Esta información se contendrá en un dispositivo colocado en un lugar suficientemente visible y debe suministrarse por adelantado.

La información de la segunda capa debe estar disponible en un lugar fácilmente accesible al afectado, ya sea una hoja informativa en una recepción, cajero, etc..., colocada en un espacio público visible o en una dirección web, y ha de referirse al resto de elementos del artículo 13 del RGPD.

No es necesario especificar la ubicación precisa del equipo de videovigilancia.

Este deber de información se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible, y como mínimo, en los accesos a las zonas vigiladas ya sean interiores o exteriores. En caso de que el espacio videovigilado disponga de varios accesos deberá disponerse de dicho distintivo de zona videovigilada en cada uno de ellos

Esta información debe suministrarse por adelantado -considerando 39 del RGPD-. El objetivo es que quede claro el contexto de la vigilancia

4.- El tratamiento de las imágenes mediante la instalación de sistemas de cámaras o videocámaras deberá ser lícito y ajustarse al principio de proporcionalidad y al de minimización de datos, en los términos ya señalados.

5.- Las imágenes podrán conservarse por un plazo máximo de un mes, salvo en aquellos supuestos en que se deban conservar para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

En este segundo supuesto, deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

6.- El responsable deberá llevar un registro de actividades de los tratamientos efectuados bajo su responsabilidad en el que se incluya la información a la que hace referencia el artículo 30.1 del RGPD.

7.- El responsable deberá realizar un análisis de riesgos o, en su caso, una evaluación de impacto en la protección de datos, para detectar los derivados de la implantación del sistema de videovigilancia, valorarlos y, en su caso, adoptar las medidas de seguridad apropiadas.

8.- Cuando se produzca una brecha de seguridad que afecte a los tratamientos de cámaras con fines de seguridad, siempre que exista riesgo para los derechos y libertades de las personas físicas, deberá notificarlo a la AEPD en un plazo máximo de 72 horas.

Se entiende por brecha de seguridad la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

9.- Cuando el sistema esté conectado a una central de alarma, únicamente podrá ser instalado por una empresa de seguridad privada que reúna los requisitos contemplados en el artículo 5 de la Ley 5/2014 de Seguridad Privada, de 4 de abril.

La Agencia Española de Protección de Datos ofrece a través de su página web [<https://www.aepd.es>] acceso a:

- la legislación en materia de protección de datos personales, incluyendo el RGPD y la LOPDGDD (apartado “Informes y resoluciones” / “normativa”),
- la Guía sobre el uso de videocámaras para seguridad y otras finalidades,
- la Guía para el cumplimiento del deber de informar (ambas disponibles en el apartado “Guías y herramientas”).

VI

Obligación incumplida. Licitud del tratamiento

El artículo 6 del RGPD, que regula la licitud del tratamiento, establece lo siguiente:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
- d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
- e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no 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.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

- a) el Derecho de la Unión, o*
- b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.*

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

- a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;*
- b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;*
- c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;*
- d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;*

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización."

Además, tal y como se ha indicado, la instalación de un sistema de videovigilancia en zonas comunes o que realice captación de elementos comunes de una finca, requiere de previo acuerdo de la comunidad propietarios, tal y como se deriva de los artículos 6 y 17.3 de la LPH. La comunidad de propietarios tendrá la condición de responsable.

En el presente caso, **A.A.A.** ha instalado un dispositivo de grabación de imágenes en el marco de la puerta de acceso al edificio en el que se encuentra su vivienda. El dispositivo se encuentra ubicado en un elemento común del inmueble, como es la fachada, captando zonas comunes, como la puerta de entrada al inmueble.

El dispositivo permite la grabación de imágenes de personas físicas. No obstante, **A.A.A.** no cuenta con la preceptiva autorización de la comunidad de propietarios.

Por tanto, de conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos son constitutivos de una infracción, imputable a **A.A.A.** por vulneración del artículo 6 del RGPD transcrito anteriormente.

VII

Tipificación de la infracción del artículo 6 del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, que se sancionará, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;"

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679."

VIII

Obligación incumplida. Información que deberá facilitarse cuando los datos personales se obtengan del interesado

El artículo 13 del RGPD establece la información que deberá facilitarse cuando los datos personales se obtengan del interesado, en virtud del cual:

"1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

- a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;*
- b) los datos de contacto del delegado de protección de datos, en su caso;*
- c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;*
- d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;*
- e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;*
- f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.*

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

- a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*
- b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*
- c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;*
- d) el derecho a presentar una reclamación ante una autoridad de control;*
- e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;*
- f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información*

significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

En el presente caso, el sistema de videovigilancia consistente en un dispositivo que realiza grabación de imágenes no cuenta con el preceptivo cartel informativo de manera visible en la zona videovigilada. Esto implica el incumplimiento de lo contenido en el artículo 13 del RGPD respecto a la obligación de suministrar información a los interesados en el momento de la recogida de sus datos personales. Suministro de información que, además, en relación con la videovigilancia, el artículo 22 de la LOPDGDD prevé a través de un sistema de "información por capas".

Por tanto, de conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos son constitutivos de una infracción, imputable a **A.A.A.**, por vulneración del artículo 13 del RGPD transcrito anteriormente.

IX

Tipificación de la infracción del artículo 13 del RGPD y calificación a efectos de prescripción

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, que se sancionará, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"b) los derechos de los interesados a tenor de los artículos 12 a 22;"

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica."

X

Apercibimientos

Cuando concurre una infracción de los preceptos del RGPD, entre los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, el artículo 58.2 de dicho Reglamento contempla los siguientes:

"2 Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(...)

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

(...)

El artículo 64.3 de la LOPDGDD establece que la AEPD, previa audiencia al responsable o encargado del tratamiento podrá dirigir un apercibimiento.

En el presente caso, atendida la naturaleza de los hechos y circunstancias expuestas en los fundamentos de derecho precedentes, se estima que por cada una de las infracciones de los artículos anteriormente mencionados procede dirigir a **A.A.A.** un apercibimiento.

XI

Medidas correctivas

Confirmadas las infracciones, la resolución puede establecer las medidas correctivas que la entidad infractora deberá adoptar para poner fin al incumplimiento de la legislación de protección de datos personales, en este caso de los artículos 5.1c) y 13 del RGPD, de acuerdo con lo establecido en el citado artículo 58.2.d) del RGPD, según el cual cada autoridad de control podrá *"ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado..."*

En el presente caso, se requiere a **A.A.A.** para que, en el plazo de un mes a contar desde la fecha de ejecutividad de la resolución finalizadora de este procedimiento, adopte las medidas siguientes:

- Acredite la retirada del dispositivo de grabación de imágenes o, en su defecto, que cuenta con autorización la comunidad de propietarios.
- En caso de que obtuviera autorización de la comunidad de propietarios, acredite haber procedido a la colocación del cartel informativo en lugar suficientemente visible de la zona videovigilada, incluyendo entre la información ofrecida en el mismo: la identificación de al menos la existencia de

un tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en la normativa de protección de datos.

Se advierte que no atender la orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, a tenor de lo anteriormente expuesto, la Presidencia de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DIRIGIR UN APERCIBIMIENTO a **A.A.A.**, con NIF *****NIF.1** por:

- La infracción del artículo 6.1 del RGPD, tipificada en el artículo 83.5.a) del RGPD.
- La infracción del artículo 13 del RGPD, tipificada en el artículo 83.5.b) del RGPD.

SEGUNDO: ORDENAR a **A.A.A.**, con NIF *****NIF.1**, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 1 mes desde que la presente resolución sea firme y ejecutiva, acredite haber procedido al cumplimiento de las medidas establecidas en el fundamento de derecho XI.

TERCERO: NOTIFICAR la presente resolución a **A.A.A.**.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la

citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

1403-16012024

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