



Expediente Nº: E/04359/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante **COMUNIDAD PROPIETARIOS (C/...2)** en virtud de denuncia presentada por D. **A.A.A. (EASY FACTORY SERVICES S.L.)** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 6 de julio de 2017, tiene entrada en la Agencia Española de Protección de Datos (AEPD) escrito de D. **A.A.A.**, en representación de la compañía EASY FACTORY SERVICES S.L., (en adelante denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad **COMUNIDAD DE PROPIETARIOS** (en adelante denunciado) instaladas en **(C/...2)**, enfocando a las personas que entran y salen del edificio, el cartel informativo se encuentra en blanco y no consta fichero inscrito en el Registro General de Protección de Datos.

Añade, que la cámara se encuentra instalada en la entrada al edificio grabando el portal y el acceso de la vía pública. Que han suscrito un contrato de arrendamiento de un piso sito en **Sevilla en (C/...1)**.

Se adjunta reportaje fotográfico, "2" fotografías, en una de ellas figura una estancia que podría ser un portal de un edificio, en la que se observa una cámara instalada en la parte superior de una pared, posiblemente enfocando a la puerta de acceso a la finca, y en la otra fotografía un cartel ZONA VIDEOVIGILADA pero no consta información del responsable ante el que ejercitar los derechos.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

El Secretario-administrador de la Comunidad de Propietarios ha informado a la Inspección de Datos, con fecha de 4 de diciembre de 2017, en relación con la cámara instalada en el portal de la finca ubicada en **(C/...2)** lo siguiente:

La cámara de video-grabación ubicada en el portal es simulada y así consta en la factura emitida por el instalador Miguelservicios10, de fecha 26 de junio de 2017, por el concepto "*Suministro y colocación de dispositivo de control de acceso simulado, trabajos realizados: suministro e instalación de dispositivo de control de acceso simulado en la zona de entrada al edificio con alimentación eléctrica, sustituyendo las pilas que suministra el fabricante y proporcionándole corriente directa para el dispositivo led*". Se adjunta copia de la factura y fotografía de la ubicación de la cámara, que coincide con la aportada por el denunciante.

Respecto de la causa por la cual fue instalada la cámara manifiestan que en un piso de la finca han instalado un negocio y que han procedido a denunciar ante la Policía y el Delegado de Seguridad y Movilidad del Ayuntamiento de Sevilla, se adjunta copia de esta última, en la que se especifica que el negocio ha sido instalado en el **piso 4ºA**.

Que en la Asamblea General Extraordinaria de la Comunidad de Propietarios, de fecha 22 de junio de 2017, se acuerda instalar una cámara en el portal y que copia de dicha Acta se remitió a los inquilinos del piso del negocio para que fueran conocedores de la instalación de la misma. Se adjunta copia de dicha Acta.

Por otra parte, en el Acta de la Asamblea General Ordinaria, de fecha 13 de noviembre de 2017, se acuerda (punto sexto) lo siguiente: *“En el mes de junio de 2017 se instaló una cámara simulada de video-grabación en la planta baja con efectos disuasorios. A la vista de lo indicado con el archivo de la denuncia, se acuerda instalar cámaras de video-grabación reales en las plantas del Edificio para garantizar la seguridad de los vecinos. Se acuerda solicitar presupuestos antes de proceder a la instalación”*. Se adjunta copia de la citada Acta.

Añaden, que no se ha producido infracción a la normativa de protección de datos ya que no se ha producido captación ni tratamiento de imágenes.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

“Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.”

III

Con carácter previo, procede situar la materia de videovigilancia en su contexto normativo.

Así, el artículo 1 de la LOPD dispone: *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma señala: *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida,*

grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.

El artículo 5.1. f) del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal aprobada por Real Decreto 1720/2007, de 21 de diciembre, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”.*

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”.* Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquella.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”.* Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”.*

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.”

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

“1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.”

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

IV

En el presente expediente D. **A.A.A.**, en representación de la compañía **EASY FACTORY SERVICES S.L.**, denuncia la instalación de una cámara de videovigilancia en la **COMUNIDAD DE PROPIETARIOS (C/...2)**, enfocando a las personas que entran y salen del edificio, el cartel informativo se encuentra en blanco y no consta fichero inscrito en el Registro General de Protección de Datos.

Ante dicha denuncia, por parte de la Inspección de Datos de esta Agencia se solicita información a la Comunidad de Propietarios, a efectos de esclarecer determinadas cuestiones del sistema de videovigilancia denunciado, manifestando ésta que la cámara de video-grabación ubicada en el portal es simulada y así consta en la factura emitida por el instalador Miguelservicios10, de fecha 26 de junio de 2017, por el concepto *“Suministro y colocación de dispositivo de control de acceso simulado, trabajos realizados: suministro e instalación de dispositivo de control de acceso simulado en la zona de entrada al edificio con alimentación eléctrica, sustituyendo las pilas que suministra el fabricante y proporcionándole corriente directa para el dispositivo led”*. Se adjunta copia de la factura y fotografía de la ubicación de la cámara, que coincide con la aportada por el denunciante.

Por lo tanto, a la vista de la documentación aportada, se desprende que la cámara denunciada es simulada por lo que no puede captar o grabar imagen alguna.

Sobre esta cuestión debe señalarse que el Tribunal Constitucional ha declarado de forma reiterada que al Derecho Administrativo Sancionador le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad de los principios de presunción de inocencia. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del ius puniendi en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.



En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”*.

De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común en lo sucesivo LRJPAC), establece que *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aún a título de simple inobservancia.”*

Conforme señala el Tribunal Supremo (STS 26/10/98) el derecho a la presunción de inocencia *“no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”*

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que *“Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate.”*

En definitiva, aquellos principios impiden imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan la imputación o de la intervención en los mismos del presunto infractor.

En el presente caso, al tratarse de una cámara simulada, no captaría imágenes de personas físicas identificadas o identificables, por lo que, al no quedar acreditada la existencia de un tratamiento de datos personales, la cuestión se encuentra al margen de la normativa de protección de datos. Por consiguiente es de aplicación el principio de presunción de inocencia, pues de la mera existencia de una cámara de videovigilancia no se desprende automáticamente que la misma funcione y que por tanto capte imágenes de personas y, en consecuencia, que exista un tratamiento de datos personales.

Alcanzada la conclusión anterior, es conocido que en otros supuestos similares esta Agencia ha venido considerado que la instalación de dispositivos que generaban la apariencia de que habían sido instaladas cámaras de videovigilancia que, en su caso, podrían ser susceptibles de ser puestas en funcionamiento, con el consiguiente tratamiento de datos personales, podía generar una situación de alarma entre las personas, que entendían que eran vigiladas a través de dichos dispositivos, al producirse una apariencia de tratamiento. Teniendo esto en cuenta, y aun cuando por esta Agencia se acordaba el archivo del expediente en cuestión, se requería igualmente la retirada del dispositivo.

Sin embargo, esta Agencia consideró necesario revisar el mencionado criterio, en los términos que se plasman, entre otras, en la resolución del PS/00542/2015 de fecha 11 de noviembre de 2015. De este modo, la inexistencia de prueba alguna acerca de un posible de datos de carácter personal implica que la presente resolución de archivo no incorpore ningún tipo de requerimiento en el sentido que se ha mencionado, al prevalecer el principio de presunción de inocencia.

V

Por otro lado, dado que la Comunidad denunciada manifiesta que ha aprobado la instalación de un sistema de videovigilancia real, conviene realizar varias aclaraciones y establecer los requisitos necesarios, en materia de protección de datos, respecto a la instalación de cámaras de videovigilancia en Comunidades de Propietarios.

Así la instalación de cámaras de videovigilancia en el caso de una comunidad de propietarios con el fin de evitar determinadas situaciones de inseguridad para los residentes o sus visitantes, ha de ser una medida proporcional en relación con la infracción que se pretenda evitar y en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia, por lo que desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, tal y como señala la propia Instrucción, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de “una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad”.

Así, el artículo 4 de la Instrucción 1/2006 recoge los principios de calidad, proporcionalidad y finalidad del tratamiento estableciendo lo siguiente:

“1.- De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2.- Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3.- Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.”

En este sentido, si la finalidad de la instalación de cámaras de videovigilancia tiene como objetivo controlar por ejemplo, determinados actos de vandalismo, robos o acciones violentas que vienen siendo habituales en la finca, en principio, la medida podría considerarse idónea, necesaria y proporcional, siempre y cuando se limitase estrictamente a esa finalidad. No obstante lo anterior, sería necesario atender las circunstancias particulares de la Comunidad de propietarios de que se trate.

Además, es necesario indicar, que el tratamiento de las imágenes por parte del responsable del tratamiento, en este caso la Comunidad de Propietarios, le obliga a cumplir con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD, que dispone lo siguiente:

“1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento”.

La obligación que impone este artículo 5 es, por tanto, la de informar al afectado en la recogida de datos, pues sólo así queda garantizado el derecho del afectado a tener una apropiada información y a consentir o no el tratamiento, en función de aquélla.

En cuanto al modo en que hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

“Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.”

“ANEXO-

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.”

Por otro lado, respecto al deber de inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos”

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.

El responsable del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

Además, el responsable del fichero, tiene una serie de obligaciones, que se empiezan a producir incluso con anterioridad a ser responsable. Una vez que se disponga a recabar datos personales, que hay decidido la finalidad del tratamiento y que deba crear un fichero de datos, comienza su obligación de inscribirlo en el Registro General de Protección de Datos.

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se hace constar en la Instrucción 1/2006 , al señalar en su artículo 7 que *“1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.*

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.”

Asimismo, señalar que la decisión de la instalación de las cámaras en el recinto de una Comunidad de Vecinos debe ser aprobado por la Junta de Propietarios, según establece la Ley 49/1960, de 21 de julio de Propiedad Horizontal.

Así, el artículo 2 de la citada Ley 49/1960, dispone en lo que se refiere a su ámbito de aplicación:

“Esta Ley será de aplicación:

- a *A las comunidades de propietarios constituidas con arreglo a lo dispuesto en el artículo 5.*
- b *A las comunidades que reúnan los requisitos establecidos en el artículo 396 del Código Civil y no hubiesen otorgado el título constitutivo de la propiedad horizontal.*

Estas comunidades se regirán, en todo caso, por las disposiciones de esta Ley en lo relativo al régimen jurídico de la propiedad, de sus partes privativas y elementos comunes, así como en cuanto a los derechos y obligaciones recíprocas de los comuneros.

- c *A los complejos inmobiliarios privados, en los términos establecidos en esta Ley.”*

Mientras que el artículo 14 de la misma Ley 49/1960, establece que: *“Corresponde a la Junta de propietarios: (...)*

- d) *Aprobar o reformar los estatutos y determinar las normas de régimen interior.*

e) *Conocer y decidir en los demás asuntos de interés general para la comunidad, acordando las medidas necesarios o convenientes para el mejor servicio común.”*

El artículo 17 de la citada Ley, regula el quorums y régimen de la aprobación de acuerdos por la Junta de Propietarios señalando que: *“Los acuerdos de la Junta de propietarios se sujetarán a las siguientes normas:*

1 *La unanimidad sólo será exigible para la validez de los acuerdos que impliquen la aprobación o modificación de las reglas contenidas en el título constitutivo de la propiedad horizontal o en los estatutos de la comunidad.*

El establecimiento o supresión de los servicios de ascensor, portería, conserjería, vigilancia u otros servicios comunes de interés general, incluso cuando supongan la modificación del título constitutivo o de los estatutos, requerirá el voto favorable de las tres quintas partes del total de los propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación. El arrendamiento de elementos comunes que no tenga asignado un uso específico en el inmueble requerirá igualmente el voto favorable de las tres quintas partes del total de los propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación, así como el consentimiento del propietario directamente afectado, si lo hubiere.

(...)

A los efectos establecidos en los párrafos anteriores de esta norma, se computarán como votos favorables los de aquellos propietarios ausentes de la Junta, debidamente citados, quienes una vez informados del acuerdo adoptado por los presentes, conforme al procedimiento establecido en el artículo 9, no manifiesten su discrepancia por comunicación a quien ejerza las funciones de secretario de la comunidad en el plazo de 30 días naturales, por cualquier medio que permita tener constancia de la recepción.

Los acuerdos válidamente adoptados con arreglo a lo dispuesto en esta norma obligan a todos los propietarios”.

Por último, se debe señalar que el sistema de videovigilancia que se instale en la Comunidad de Propietarios, no debe captar imágenes de la vía pública.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **SECRETARIO-ADMINISTRADOR COMUNIDAD PROPIETARIOS (C/...2)**, y D. **A.A.A. (EASY FACTORY SERVICES S.L.)**.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos