

Expediente Nº: E/04656/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **COMUNIDAD DE PROPIETARIOS XXXXXXXXX** en virtud de denuncia presentada por D^a. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 8 de abril de 2013 tiene entrada en esta Agencia escrito de D^a. **A.A.A.** (en adelante la denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la **COMUNIDAD DE PROPIETARIOS XXXXXXXXX** (en adelante el denunciado) instaladas en **(C/.....1) - LAS PALMAS DE GRAN CANARIA**.

La denunciante manifiesta que ha tenido conocimiento a través del Acta de la Junta General Ordinaria, celebrada el día uno de abril de 2013 en la comunidad de vecinos donde residen sus padres, de que en la misma aparecen sus datos personales, y de la existencia de una grabación de su persona realizada por medio de videovigilancia, de fecha 25 de diciembre de 2012 la cual, según consta en dicho documento, sigue en poder de la junta directiva.

Con fecha 18 de febrero de 2013, mediante carta certificada dirigida a la presidenta conforme a la L.O. 15/1999, solicitó el acceso a sus imágenes.

Manifiesta que con fecha 29 de marzo de 2013, se entrega en mano a sus padres, escrito de acompañamiento de pendrive con la grabación de las imágenes, a fin de que pueda visualizarlas, todo ello 95 días después de su captación y sobrepasando con creces el plazo establecido en el art.6 de la Instrucción 1/2006. Visionadas las mismas se observan al menos dos personas que no tienen nada que ver con el hecho en sí, por lo que podrían quedar afectados sus legítimos derechos (*art. 5 -2 de la Instrucción 1/2006*).

Manifiesta que a la entrada del edificio existe cartel amarillo de "ZONA VIDEOVIGILADA", pero no aparecen por ningún lado, ni el modelo de "CLAUSULA INFORMATIVA" - *contemplado en la Instrucción 1/2006* - ni los obligados impresos de información previstos en el art. 5 -1 de la citada L.O. 15/1999, por lo que ante la inexistencia de tal información, surge duda razonable en cuanto a si dicho fichero con datos de carácter personal y de titularidad privada, se halla legalmente inscrito en esa AEPD.

La denunciante aporta copia del Acta de la Junta General Ordinaria de Propietarios de la Comunidad de Propietarios de la calle **(C/.....1) - LAS PALMAS DE GRAN CANARIA**, en la que consta:

"se informa que está grabada una incidencia muy grave, por haberse caído la propietaria D^a. B.B.B. en el zaguán, con motivo de sacar, el día 25-12-2012, sobre las 3 de la tarde, C.C.C., hija de Don D.D.D. y D^a E.E.E., el perro propiedad de sus padres y

dejar que orinara a la salida del ascensor y no limpiarlo enseguida, que fue lo que produjo la caída; luego no sacarlo a la calle, sino que lo entró en el jardín, para que terminara de hacer sus necesidades. A continuación, hubo un amplio cambio de impresiones, y con este motivo, quedaron aprobados los siguientes cuatro puntos, que son de obligado cumplimiento para todos:

*1) Comunicar ahora el incidente por carta a D. **D.D.D.** y D^a **E.E.E.**, que devolverán una copia firmada para la Comunidad; siguiendo igual procedimiento para todos.*

2) Decirles que dicho incidente ahora se puede justificar con la grabación que está en poder de la Directiva y que si esta actitud continúa, se tomaran las medidas pertinentes al respecto.

3) Que esta costumbre de no limpiar lo que ensucian los perros, es también de otros, que lo dejan y no lo limpian, sin tener en cuenta el peligro que supone para los que entran o salen. Que cuando esto suceda, hay que limpiarlo enseguida, no dejarle para después, o para que otro lo limpie, porque en ese intervalo no se sabe lo que puede ocurrir, como pasó en este caso.

4) Que ahora con las cámaras, se sabrá quién lo hace y con todos se procederá igual. Teniendo en cuenta que si alguien se cae y se hace daño, el responsable es siempre el causante que provoque el accidente, porque se podrá justificar con la grabación.

La denunciante aporta copia del escrito remitido a la presidenta de la Comunidad en el que solicita el acceso a las grabaciones de su persona, comunicando como domicilio a efectos de notificación **C/ (C/.....1) LAS PALMAS DE GRAN CANARIA.**

La denunciante aporta copia del escrito de acuse de recibo de un pen drive entregado por la presidenta de la Comunidad a sus padres en la dirección indicada por la misma a efectos de notificaciones, en el que consta “Según nos solicitó por carta su hija **C.C.C.**, les entrego el pendrive para que visualicen el incidente acaecido y que se acordó en junta comunicarles”.

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:

1. Con fecha 27 de septiembre y 11 de diciembre de 2013 y 25 de febrero de 2014 se solicita información a la presidenta de la comunidad, siendo devuelto por el servicio de correos anotando como motivo de la devolución “**AUSENTE REPARTO**”

2. El día 17 de marzo de 2014 se realizó una visita de inspección en la Comunidad, poniéndose de manifiesto los siguientes hechos:

1. La Comunidad dispone de un sistema de videovigilancia compuesto por 3 cámaras de video, un monitor y un grabador.
2. La instalación de dicho sistema ha sido aprobado en Junta General por motivos de seguridad, como consecuencia de los daños que se venían produciendo en las zonas comunes de la misma.

3. Tanto el monitor como el videograbador se encuentran ubicados en un cuarto de la comunidad de propietarios junto al cuarto de contadores. Dicho cuarto se encuentra cerrado con llave y tan solo tiene acceso las personas autorizadas.
4. Las imágenes capturadas por las cámaras se graban en soporte que las conserva durante 30 días, ya que se va reescribiendo pasado dicho tiempo.
5. Al sistema de videovigilancia tan solo acceden dos vecinos que han sido autorizados por la Comunidad, ya que para acceder al sistema se necesita una contraseña que solo conocen estas personas.
6. Existen dos carteles informativos situados uno junto a la puerta de entrada y el otro en el tablón de anuncios ubicado en el hall. En dichos carteles se informa de la existencia de una zona videovigilada y del responsable ante el que ejercer los derechos de protección de datos de carácter personal.
7. La presidente manifiesta que aproximadamente en marzo de 2013 la presidenta de la Comunidad sufrió una caída al resbalarse con la orina que había en el vestíbulo, comprobándose a través de las imágenes del sistema de videovigilancia que la orina la había ocasionado el perro de uno de los propietarios que salía del edificio junto a la hija del propietario. Estas imágenes fueron extraídas del sistema para conservarlas con objeto de poder probar los hechos y como medio de prueba ante posibles reclamaciones. Estos hechos fueron puestos en conocimiento de los propietarios en una reunión de la Junta. Posteriormente, la referida persona que sacaba el perro solicitó el acceso a las imágenes, procediéndose por parte de la Comunidad a atender dicha solicitud haciendo entrega de un dispositivo de memoria USB que contenías las imágenes en el domicilio de sus padres, que fue el domicilio aportado en el escrito de solicitud. Por otro lado, manifiestan que la Comunidad no disponía de otro domicilio de la solicitante para hacer entrega de lo solicitado.

2.4 No consta en el Registro General de Protección de Datos ningún fichero inscrito cuyo responsable sea la Comunidad.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

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 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, 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 aquélla.

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." (el subrayado es de la Agencia Española de Protección de Datos).

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.

III

En el presente expediente, la denuncia se refiere a la instalación de un sistema de videovigilancia en el interior de una Comunidad de Propietarios, por lo que procede establecer los requisitos necesarios para su instalación verificando si se ha procedido al cumplimiento de los mismos.

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.

En el caso que nos ocupa, la instalación de las cámaras en la Comunidad obedeció a motivos de seguridad como consecuencia de los daños que se venían produciendo en las zonas comunes de la misma.

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 aquella.

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.”

En el caso que nos ocupa, en inspección realizada por inspectores de esta Agencia en fecha 17 de marzo de 2014 se comprueba la existencia de dos carteles informativos situados uno junto a la puerta de entrada y el otro en el tablón de anuncios ubicado en el hall. En dichos carteles se informa de la existencia de una zona videovigilada y del responsable ante el que ejercer los derechos recogidos en la Ley de Protección de Datos. Por lo tanto, el cartel cumple los requisitos exigidos en la normativa de protección de datos, al contrario de lo manifestado por la denunciante, identificando claramente al responsable del fichero: **LA COMUNIDAD DE PROPIETARIOS XXXXXXXXX**.

Por otro lado respecto a los impresos informativos a disposición de los interesados, también denunciado por la denunciante, si bien en este caso, la Comunidad tiene instalados los carteles informativos de conformidad con el artículo 5.1 de la LOPD y conforme a lo estipulado en el Anexo de la Instrucción 1/2006, también deberá disponer de los citados formularios a disposición de los interesados. Estos formularios puedan estar preimpresos y preparados por el responsable del tratamiento, o tener la posibilidad de imprimirlos en el momento de su demanda, bien por tener preparado un documento Word o por tener conexión a Internet que permita acceder a la página web de la Agencia Española de Protección de Datos y poder descargarse el modelo de formulario referido.

Por lo tanto, ha de entenderse que la existencia de una conexión con Internet, fija o móvil, permitirá siempre el acceso a dicho modelo y el mismo podría ser facilitado por el titular del fichero a los afectados.

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 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.”

En el caso que nos ocupa, las imágenes se conservan por un periodo de 30 días, sin que conste inscrito el correspondiente fichero de videovigilancia en el Registro

General de la Agencia Española de Protección de Datos, por lo que se procede a pasar nota al Registro General de esta Agencia para que proceda a requerir la inscripción del fichero a la Comunidad denunciada.

Por otro lado, 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”.

En el caso que nos ocupa, la instalación del sistema de videovigilancia se acordó mediante su aprobación por unanimidad de los presentes y representados en la Junta General Ordinaria de fecha 29 de enero de 2010, aportando la Comunidad copia de la misma.

Por lo tanto el sistema de videovigilancia denunciado, con la salvedad establecida, cumple los requisitos establecidos.

IV

Por último, respecto a las manifestaciones de la denunciante relativas a que se hizo entrega a sus padres, titulares de un piso perteneciente a la Comunidad, del pendrive solicitado por la misma, 95 días después de su captación cabe decir, en primer lugar, respecto al ejercicio de los derechos de acceso, rectificación, cancelación y oposición que el artículo 25. 1 c) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, recoge que el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero que contendrá entre otros datos la dirección a efectos de notificaciones, fecha y firma del solicitante. Así en el caso que nos ocupa, la denunciante estableció precisamente el domicilio de sus padres a efectos de notificaciones, según escrito realizado por la misma en fecha 18 de febrero de 2013 y notificado el 26 de febrero de 2013, siéndole entregado precisamente en la citada dirección.

Asimismo, el artículo 29.1 del citado Reglamento establece que el responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. En el caso que nos ocupa, la recepción de la solicitud del derecho de acceso se produjo el 26 de febrero de 2013, siendo entregado el pendrive con las imágenes en fecha 29 de marzo de 2013, por lo que se cumplió el

plazo legalmente establecido.

Por último, respecto a que se superó el plazo establecido respecto a la conservación de las imágenes debe decirse que la Agencia se ha pronunciado en diversas ocasiones sobre esta cuestión, señalando que respecto al plazo, sobre el que han de conservarse las imágenes, la elección de dicho plazo, no es arbitraria y sino que encuentra su fundamento tanto en la Instrucción 1/1996, sobre ficheros automatizados establecidos con la finalidad de acceder de controlar el acceso a los edificios, que en su norma quinta prescribe que *“Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados”*.

Ahora bien, la cuestión se plantea ante la existencia de alguna incidencia respecto de la grabación, como es el caso que se plantea. Así, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal viene a señalar que la cancelación dará lugar al bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que *“la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”*.

Este precepto, a su vez, se complementa con la previsión contenida en el transcrito artículo 16.5 de la Ley Orgánica 15/1999. En relación con esta cuestión, ya se indicaba en informes de esta Agencia de fecha 30 de julio de 2004 y 1 de agosto de 2005 lo siguiente:

“(…) la Ley Orgánica 15/1999 viene regular el bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que “la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”.

Este precepto, a su vez, se complementa con la previsión contenida en el artículo 16.5 que indica que “los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado”.

Del análisis conjunto de las normas citadas se desprende que existirán supuestos en los que si bien deberá procederse a la cancelación de los datos, al haber dejado de ser necesarios para la finalidad que justificó su tratamiento, como sucederá cuando se haya producido la completa consumación del contrato que vincula al responsable del tratamiento con sus clientes, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, salvo en determinadas circunstancias, descritas por el artículo 16.3 de la Ley Orgánica, no implicará automáticamente ese borrado.

Así, el artículo 16.3 viene a reconocer, en consonancia con lo previsto en el artículo 16.5 de la Ley, que existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el responsable del fichero y que determina,

en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de toda índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley, impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.

En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, y al margen de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto “en las disposiciones aplicables” o a la “atención de las posibles responsabilidades nacidas del tratamiento”, tal y como prevé la meritada Ley.

En este sentido, para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributaria y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).

En todo caso, debe recordarse que el mantenimiento del dato bloqueado, supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que “cumplido el citado plazo deberá procederse a la supresión”).

En consecuencia, a nuestro juicio, la cancelación no supone automáticamente en todo caso un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento.

En lo atinente a la determinación de los períodos en que el dato habrá de permanecer bloqueado, en relación con lo dispuesto en el artículo 16.3, resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, como ya se ha indicado con anterioridad, los plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con su cliente, así como los derivados de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave. (...)”

Por lo tanto, en el supuesto que nos ocupa, la captación de las imágenes objeto de denuncia, fueron conservadas al existir un incidente en las mismas como era el accidente de una persona de la comunidad, constituyendo un medio de prueba ante una eventual reclamación o procedimiento judicial, estando amparadas la conservación de

las imágenes, en el artículo 16.3 de la LOPD, que señala que *“la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”*.

A la vista de lo expuesto se procede al archivo del presente expediente de actuaciones previas.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **COMUNIDAD DE PROPIETARIOS XXXXXXXXXX** y a D^a. **A.A.A.**.

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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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.

José Luis Rodríguez Álvarez

Director de la Agencia Española de Protección de Datos