

Expediente N°: E/04909/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el **AYUNTAMIENTO DE SAN JAVIER (MURCIA)** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fechas 1 de julio y 9 de septiembre de 2015, tienen entrada en esta Agencia escritos de **D. A.A.A.**, en el que denuncia que, ha tenido conocimiento de que el Jefe de Negociado de Recursos Humanos y Director del Departamento de Seguridad del Ayuntamiento de San Javier, sin autorización, visualizó las imágenes recogidas por las cámaras de videovigilancia del citado Ayuntamiento, correspondientes a la tarde del 29 de mayo de 2015, cuando el denunciante, como Concejal en funciones de dicho Ayuntamiento, se encontraba en el interior de las Dependencias recogiendo el Despacho que debía dejar.

Asimismo, manifiesta que ha tenido conocimiento de que el citado funcionario ha cedido las imágenes a terceros.

Con fecha 5 de junio de 2015, la prensa regional, hizo eco de una información con relación al desalojo del despacho.

Manifiesta el denunciante que con fecha 11 de junio de 2015, el funcionario confesó al Alcalde **B.B.B.**, que había procedido a la conservación de las imágenes, sin autorización.

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 10 de noviembre de 2015, tiene entrada en esta Agencia un escrito remitido por el Ayuntamiento de San Javier, con relación a los hechos denunciados, en el que se pone de manifiesto:
 - 1.1. Que la persona encargada del sistema de videovigilancia del Ayuntamiento como Director de Seguridad era **D. C.C.C.**
 - 1.2. Que las causas que motivaron la instalación de las cámaras, fueron la protección de las personas y propiedades municipales.
 - 1.3. Se acompañan los carteles de información existentes en el recinto.
 - 1.4. Se acompaña detalle de las cámaras, no obstante solo cuenta con zoom la cámara instalada en la zona del Registro General.
 - 1.5. Que las personas que tienen acceso al sistema de video vigilancia, como encargados del tratamiento, son los empleados autorizados de la

mercantil Sureste Seguridad, S.L.

- 1.6. El tiempo de conservación de las imágenes es entre 20 y 30 días.
- 1.7. Que las únicas imágenes que han podido ser grabadas son las correspondientes a diferentes espacios comunes donde se encuentran ubicadas las cámaras.
- 1.8. Las imágenes objeto de esta denuncia, fueron extraídas, al determinar que se debe poner en conocimiento de la autoridad competente, los hechos y las imágenes de presuntas infracciones, ya que es una de las finalidades de la ley de seguridad privada.

Con fecha 5 de junio de 2015, salió publicada en la sección de opinión del diario regional LA VERDAD, una nota del por entonces aún, primer Teniente de Alcalde, **A.A.A.**. Según este diario, en la tarde del 29 de mayo, el citado Concejel acudió al Consistorio acompañado de una trabajadora municipal, y tras varias horas pudo vérselo salir, según manifestaciones de miembros del personal del Ayuntamiento presentes en la Casa Consistorial en ese momento, portando un carrito con varias cajas de documentos.

- 1.9. Que dichas imágenes, fueron entregadas a la Guardia Civil para su puesta a disposición de la autoridad judicial competente, en virtud del artículo 42.4 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, en virtud del cual, se debe aportar, a “propia iniciativa”, a las Fuerzas y Cuerpos de Seguridad competentes, las imágenes como evidencia de prueba para la investigación policial o judicial, para el esclarecimiento de los hechos.

Que se adjunta Diligencia de comparecencia del Director de Seguridad ante la Guardia Civil, para la entrega de las grabaciones.

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

En primer lugar, procede situar en el contexto normativo la materia de videovigilancia. 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) 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, que 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.”

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 se denuncia por parte de D. **A.A.A.**, que **D. C.C.C.**, Jefe de Negociado de Recursos Humanos y Director del Departamento de Seguridad del Ayuntamiento de San Javier, sin autorización, visualizó las imágenes recogidas por las cámaras de videovigilancia del citado Ayuntamiento, correspondientes a la tarde del 29 de mayo de 2015, cuando el denunciante, como Concejal en funciones de dicho Ayuntamiento, se encontraba en el interior de las Dependencias recogiendo el Despacho que debía dejar, cediendo las imágenes a terceros.

En primer lugar, hay que señalar que en un procedimiento sancionador o de declaración de infracción de las Administraciones Públicas, el procedimiento se inicia de oficio por la AEPD, que es quien determina la responsabilidad de los hechos constatados, independientemente de la intencionalidad del denunciante al presentar su escrito de denuncia. Asimismo, en un procedimiento declaración de infracción se imputa a la entidad que ha infringido la norma, como responsable del fichero, y no a la persona física, puesto que la infracción se habría producido en el ejercicio de su cargo y no a título individual ya que no sería responsable de ningún fichero.

Una vez aclarada dicha cuestión cabe decir que, solicitada información al Ayuntamiento de San Javier para el esclarecimiento de los hechos denunciados, éste manifiesta que las imágenes objeto de esta denuncia, fueron extraídas del sistema de videovigilancia instalado en el Ayuntamiento, cuya finalidad es la protección de las personas y las propiedades municipales, entre ellas los diversos expedientes y resto de documentación del Ayuntamiento. Las imágenes que captan el citado sistema corresponden a diferentes espacios comunes donde se hallan ubicadas y señalizadas las cámaras.

Según manifiesta el Ayuntamiento y aporta copia del recorte al respecto, con fecha 5 de junio de 2015, salió publicada en la sección de opinión del diario regional LA VERDAD, una nota según la cual, en la tarde del 29 de mayo, el entonces aún primer Teniente de Alcalde, **A.A.A.**, acudió al Consistorio acompañado de una trabajadora municipal, y tras varias horas pudo vérselo salir, según manifestaciones de miembros del personal del Ayuntamiento presentes en la Casa Consistorial en ese momento, portando un carrito con varias cajas de documentos.

Ante dicha información se procedió a extraer las imágenes del sistema de videovigilancia, al determinar que se debe poner en conocimiento de la autoridad competente los hechos y las imágenes de presuntas infracciones, ya que es una de las finalidades de la ley de seguridad privada.

El día 5 de junio del 2015, **D. C.C.C.**, en su condición de Director de Seguridad Privada, puesto para el que fue nombrado por Decreto número 1/2013, de 3 de enero de 2013, al mando del Departamento de Seguridad Privada, realiza denuncia ante la Guardia Civil- Puesto de San Javier y entrega a dicho cuerpo las grabaciones que contendrían las imágenes que pudieran guardar relación con los hechos denunciados. Las imágenes fueron extraídas por la empresa de seguridad encargada de las cámaras de grabación y directamente las depositó en las dependencias oficiales. Dichas imágenes, fueron entregadas a la Guardia Civil para su puesta a disposición de la autoridad judicial competente, en virtud del artículo 42.4 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, en virtud del cual, se debe aportar, a “propia iniciativa”, a las Fuerzas y Cuerpos de Seguridad competentes, las imágenes como evidencia de prueba para la investigación policial o judicial, para el esclarecimiento de los hechos.

A este respecto, el artículo 6.1 de la LOPD dispone lo siguiente:

“1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”. (El subrayado es de esta Agencia)

Por su parte, el apartado 2 del mencionado artículo contiene una serie de excepciones a la regla general contenida en el 6.1, estableciendo que *“2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por*

el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.”

La Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, establece, entre otros requisitos, la necesidad de legitimación para que el tratamiento de los datos de carácter personal sea lícito, y así lo dispone el artículo 2 de la citada Instrucción, anteriormente transcrito.

El tratamiento de imágenes por razones de seguridad se encuentra amparado, en el artículo 5.1 e) de la Ley 23/1992, de 30 de julio, de Seguridad Privada, que establece “1. Con sujeción a lo dispuesto en la presente Ley y en las normas reglamentarias que la desarrollen, las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades: a) Vigilancia y protección de bienes, establecimientos, espectáculos, certámenes o convenciones, b) Protección de personas determinadas, previa la autorización correspondiente, c) Depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores y demás objetos que, por su valor económico y expectativas que generen, o por su peligrosidad, puedan requerir protección especial, sin perjuicio de las actividades propias de las entidades financieras, d) Transporte y distribución de los objetos a que se refiere el apartado anterior a través de los distintos medios, realizándolos, en su caso, mediante vehículos cuyas características serán determinadas por el Ministerio del Interior, de forma que no puedan confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad, e) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, de conformidad con lo dispuesto en la Disposición adicional sexta, f) Explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas y su comunicación a las Fuerzas y Cuerpos de Seguridad, así como prestación de servicios de respuesta cuya realización no sea de la competencia de dichas Fuerzas y Cuerpos, g) Planificación y asesoramiento de las actividades de seguridad contempladas en esta Ley”.

De otra parte, dicho tipo de tratamiento de datos resulta conforme con el artículo 10. 2 a) del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que señala que “No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando (...) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

- ***El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.”***

De la documentación obrante en el expediente, se extrae que, en el presente supuesto, el tratamiento de datos por medio de cámaras y/o videocámaras con fines de seguridad queda incardinado en la esfera del interés legítimo de la entidad denunciada, por cuanto la misma tiene un evidente interés en la instalación y mantenimiento de cámaras de seguridad; y la finalidad de seguridad es también legítima, sin que se

oponga a norma u obligación de ningún tipo.

Así, según se señala por la entidad denunciada, tras la noticia publicada en el periódico, se procedió a extraer las imágenes del sistema de videovigilancia por si en ellas hubiera algún tipo de hecho objeto de infracción. Dichas imágenes fueron depositadas, por el Director de Seguridad Privada del Ayuntamiento, en las dependencias de la Guardia Civil con la correspondiente denuncia.

El interés legítimo es un presupuesto legitimador del tratamiento de datos personales. Así, el artículo 7 de la Directiva 95/46/CE, de 24 de octubre determina: *“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: (...) f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva.: en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales”*.

En este sentido, la Sentencia del Tribunal de Justicia de las Comunidades Europeas de 24 de noviembre de 2011, que resuelve una cuestión prejudicial planteada por el Tribunal Supremo, ha clarificado que el artículo 7.f) de la Directiva 95/46/CE tiene efecto directo.

En consonancia con lo anterior, el Tribunal Supremo en Sentencia de 8 de febrero de 2012 anuló el artículo 10.2.b) del RD 1720/2007, de 21 de diciembre por considerar que el Reglamento vulneraba la regulación contenida en la Directiva. Así, la Audiencia Nacional realiza una ponderación caso por caso entre el interés legítimo del responsable del tratamiento y los derechos y libertades fundamentales de los afectados, como en Sentencias de la Sección Primera de la Sala de lo Contencioso Administrativo de 5 de marzo y 31 de mayo de 2012.

En el supuesto objeto del presente expediente, los derechos y libertades fundamentales de los afectados —esto es, las personas cuyas imágenes son captadas, grabadas y visionadas por las cámaras de seguridad de la entidad denunciada— no se ven lesionados hasta el punto de prevalecer sobre el interés legítimo de dicha empresa relacionado con la seguridad.

En definitiva, el interés legítimo supone la legitimación de la entidad denunciada, y de quien ésta ha designado para el tratamiento de imágenes, siempre que se cumplan las garantías establecidas en la Instrucción 1/2006 antes mencionada, destacando en particular el deber de información y los derechos de las personas a que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

IV

Por otro lado, se plantearía en el presente caso, la aportación de las grabaciones realizadas por las cámaras del Ayuntamiento, en el seno de un procedimiento judicial, como prueba de las supuestas infracciones que se pudieran haber cometido. En este punto hemos de estudiar las implicaciones que lo denunciado presenta al respecto del

derecho a la protección de datos en relación con el derecho a la tutela judicial efectiva de los protagonistas, por lo que partiremos de un análisis general relativo a la conexión de dichos derechos. Así, al respecto del derecho a la tutela judicial efectiva, nuestra norma suprema en el artículo 24 de la Constitución Española, en sus apartados 1 y 2, dispone lo siguiente:

“1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso, pueda producirse indefensión.

2. Asimismo, todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa.”

Así, constitucionalmente se consagra el derecho de los ciudadanos, ya sean personas físicas o jurídicas, a la tutela judicial efectiva y al derecho a utilizar los medios de prueba que consideren adecuados para el sostenimiento de su pretensión. Sin embargo, de dicha previsión, surge una colisión entre el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva de los jueces y tribunales referida, contenido en el artículo 24 de la Constitución, anteriormente transcrito, dadas a los bienes jurídicos afectados en su aplicación.

Por ello, ante tales situaciones, el Legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio Legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En efecto, la exigibilidad del consentimiento del titular de los datos que pudieran ser objeto de un tratamiento en un procedimiento judicial, para dicho tratamiento de sus datos supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que una persona pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos o la dependencia en su aplicación a quien manejara la titularidad del dato, implicaría, lógicamente, una merma en la posibilidad de aportación por el interesado de *“los medios de prueba pertinentes para su defensa”*, vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) *“el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho”*.

Por otro lado, junto a lo dispuesto en el artículo 6.2 de la LOPD, el artículo 11 de la LOPD, recoge otras excepciones, a la exigencia del consentimiento:

“1.- Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con

las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2.-El consentimiento exigido en el apartado anterior no será preciso:

a.-Cuando la cesión esté autorizada en una ley.(...)

d.-Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.(...)" (el subrayado es de la Agencia Española de Protección de Datos).

En este sentido, entraría en liza lo dispuesto en el artículo 299 de la Ley 1/2000, de 7 de enero de Enjuiciamiento Civil, que admite la aportación como medio de prueba, de medios de reproducción de imágenes que sean relevantes para el proceso. Así establece, el precitado artículo:

"1. Los medios de prueba de que se podrá hacer uso en juicio son:

- 1. Interrogatorio de las partes.*
- 2. Documentos públicos.*
- 3. Documentos privados.*
- 4. Dictamen de peritos.*
- 5. Reconocimiento judicial.*
- 6. Interrogatorio de testigos.*

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso..

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias".

Por lo tanto, en cuanto a lo aportado en el juicio, dicho cuerpo legal admite la aportación como medio de prueba de los medios de reproducción de la palabra, el sonido y la imagen, lo cual implica la posibilidad de tratamiento de datos dentro de dichas propuestas de prueba, debiendo ser el correspondiente órgano jurisdiccional quien se manifieste sobre la legitimidad de lo presentado, no constando en el presente caso, pronunciamiento en contra en este sentido.

Además, hemos de tener en cuenta que, la Audiencia Nacional en sentencia de 22 de octubre de 2010 (rec. 409/2009) nos dice, en cuanto a la obtención de medios probatorios y su validez en el procedimiento, pese a no ser solicitadas ni obtenidas por vía judicial, lo siguiente:

“De un lado ha de tenerse en cuenta que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD).

Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, parecer ser, y así se desprende del acta de juicio, ocurrió en el presente supuesto.

Por otra parte, y si bien es cierto que los procedimientos judiciales tampoco son ajenos a la normativa de protección de datos, tal y como indicamos en la SAN 9-10-2009 (Rec. 37/2009) dado que el derecho de protección de datos, en cuanto derecho fundamental y autónomo previsto en el artículo 18.4 CE , vincula a todos los poderes públicos (Art. 53 CE) y entre ellos al Poder Judicial, tal y como igualmente indica la STS 18-9-2006 Rec. 274/2002 . Sin embargo dicha LOPD debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos.

Además de que el sometimiento de los ficheros judiciales a la LOPD ha de entenderse (según la misma SAN 9-10-2009 Rec. 37/2009) sin menoscabo de la función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE , hasta el punto de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales." (el subrayado es de la Agencia Española de Protección de Datos).

En el caso que nos ocupa, el denunciado estaba legitimado para presentar, ante el Juzgado la citada prueba videográfica, al existir una habilitación legal para ello, a tenor del artículo 11.2.d).

A este respecto, se debe traer a colocación la Sentencia del TS67/2014 de 28 enero, que recoge “la STS 485/2013, de 5 de junio, considera que el material fotográfico y videográfico obtenido en el ámbito público y sin intromisión indebida en la intimidad personal o familiar tiene un valor probatorio innegable. La doctrina jurisprudencial de esta Sala en sentencias de 6 de mayo de 1993, 7 de febrero, 6 de abril, 31 de mayo de 1994, 18 de diciembre de 1995, 27 de febrero de 1996, 5 de mayo de 1997, 968/1998 de 17 de julio, 188/1999, de 15 de febrero, 1207/1999, de 23 de julio, 387/2001, de 13 de marzo, 27 de septiembre de 2002, 180/2012 de 14 de marzo, entre otras muchas)ha considerado legítima y no vulneradora de derechos fundamentales los espacios o vías públicas, estimando que la captación de imágenes de actividades que pueden ser constitutivas de acciones delictivas se encuentra autorizada por la ley en el curso de una investigación criminal, siempre que se limiten la grabación de lo que ocurre

en espacios públicos fuera del recinto inviolable del domicilio o de lugares específicos donde tiene lugar el ejercicio de la intimidad. (...).

Asimismo, la STS núm. 883/1994, de 11 de mayo en su Fundamento Jurídico 3 afirma que: *“... la grabación de las palabras de los acusados realizada por el denunciante con el propósito de su posterior revelación no vulnera ningún derecho al secreto, ni a la discreción, ni a la intimidad del recurrente. La Constitución y el derecho ordinario, por otra parte, no podrían establecer un derecho a que la exteriorización de propósitos delictivos sea mantenida en secreto por el destinatario de la misma. En principio, tal derecho resulta rotundamente negado por la obligación de denunciar que impone a todos los ciudadanos el art. 259 LECrim...Por lo demás, no se alcanza a comprender el interés constitucional que podría existir en proteger el secreto de los propósitos delictivos” (...). Dicha resolución se apoya asimismo, para fundamentar dicho criterio en que, “De la misma forma que hubiera podido revelar el contenido de correspondencia a él dirigida o presentar su propio diario personal para acreditar sus dichos, el testigo denunciante ha podido poner a disposición del Tribunal de la causa una grabación privada. No existe ninguna disposición que exija un control judicial para tales obtenciones privadas de pruebas. Tampoco existe ninguna disposición que impida valorar como pruebas tales grabaciones.”*

Por tanto, y en base a la doctrina y jurisprudencia instaurada dentro del ámbito de protección de datos vista, la aportación de los datos recabados, dentro de un procedimiento judicial no supone una vulneración de la LOPD, por lo que para este caso no cabría calificar como ilegítima la actuación del mismo.

V

Por último, procede analizar si el tratamiento de las imágenes realizado cumplía o no con los restantes requisitos exigibles en materia de protección de datos de carácter personal, recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, como son, entre otros, **el deber de informar a los interesados**, tanto a través de la colocación de carteles informativos y la notificación de la existencia de los ficheros a la Agencia Española de Protección de Datos.

A este respecto, el artículo 5.1 de la LOPD, obliga a que se cumpla con el **deber de informar** a los afectados, dispone que:

“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”.

En cuanto al modo en que debe facilitarse la información recogida en el artículo 5 de la LOPD, el artículo 3 de la Instrucción 1/2006, 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, según consta en el expediente, las áreas videovigiladas se encuentra debidamente señalizadas tanto en el exterior como en el interior de las dependencias municipales. Dichos carteles son acordes al previsto en el artículo 3 a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD.

En consecuencia, el sistema de captación de imágenes por medio de cámaras o videocámaras al que se refieren las presentes actuaciones cumple con el deber de información recogido en el artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Por otro lado, respecto al cumplimiento de la 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 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 recoge 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.”

El artículo 20.1 de la LOPD, establece que la creación, modificación o supresión de ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente. Por su parte el artículo 53.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, determina que cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

En el caso que nos ocupa, el fichero de videovigilancia ha sido creado por medio de Decreto nº 1555/07, publicado en el Boletín Oficial de Comunidades 00204 de fecha 9 de abril de 2007 y consta debidamente inscrito el fichero denominado VIDEOVIGILANCIA, cuyo responsable es la entidad denunciada, en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos, con fecha

03/06/2008 y modificado el 24/03/2015.

Asimismo las imágenes se conservan entre 20 y 30 días como máximo, de conformidad con el artículo 6 de la Instrucción 1/2006, que recoge: *“Los datos serán cancelados en el plazo máximo de un mes desde su captación”*.

A este respecto cabe decir que las imágenes captadas fueron de fecha 29 de mayo de 2015 y extraídas y presentadas ante la correspondiente denuncia ante la Guardia Civil el 5 de junio de 2015, por lo tanto, fueron presentadas los días inmediatamente posteriores a la fecha en la que se produjeron los hechos.

A la vista de todo lo expuesto, se procede al archivo del presente expediente de actuaciones previas, al no apreciarse vulneración a la normativa de protección de datos.

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 **AYUNTAMIENTO DE SAN JAVIER (MURCIA)** y a D. **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 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.



Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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