



Expediente N°: E/05402/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **COMUNIDAD DE PROPIETARIOS CENTRO COMERCIAL XXXX y, TALER REAL ESTATE SL** en virtud de denuncia presentada por D. **A.A.A.** y la **SUBDELEGACION DEL GOBIERNO EN GRANADA-SECRETARIA GENERAL-SERVICIO DE ASUNTOS JURIDICOS** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de entrada 28 de julio de 2016 se recibe un escrito de la **SUBDELEGACION DEL GOBIERNO EN GRANADA** para conocimiento de esta Agencia y efectos oportunos, al que se acompaña de un documento de la Dirección General de Urbanismo del Ayuntamiento de Granada comunicando a la Subdelegación del Gobierno el requerimiento efectuado a **TALER REAL ESTATE SL** para que aporte las autorizaciones preceptivas para la colocación de cámaras de seguridad en zonas de uso público.

El documento anexo de la Dirección General de Urbanismo del Ayuntamiento de Granada se indica entre otros aspectos que la Policía Local de Granada ha podido comprobar mediante inspección la existencia de dispositivos de videovigilancia enfocando a zonas de uso público en el parque público SG-EL-11, explotado por **TALER REAL ESTATE SL** mediante concesión, no constando autorización para la instalación de las mismas.

Con fecha de entrada 3 de agosto de 2016 se recibe un escrito de D. **A.A.A.**, denunciando a la entidad **TALER REAL ESTATE SL** por la instalación, sin autorización del Ayuntamiento de Granada, de un sistema de videovigilancia por todo el recinto del parque público XXXX (SG-EL-11), concesionado a dicha entidad. _

El denunciante, que es arrendatario de un local situado en dicho parque, manifiesta ser vigilado mediante el sistema.

Y, entre otra, anexa la siguiente documentación:

Reportaje fotográfico de las cámaras instaladas.

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:

Solicitada información y documentación a la entidad denunciada, de la respuesta recibida se desprende lo siguiente:

Respecto de la identidad del responsable del sistema los representantes de **TALER REAL ESTATE SL** indican que traspasan el requerimiento de información a **COMUNIDAD DE PROPIETARIOS CENTRO COMERCIAL XXXX PLAZA** ya que indican es el responsable del sistema.

La referida COMUNIDAD DE PROPIETARIOS ha manifestado que :

1. La finalidad de la instalación fue la seguridad.
2. **El sistema de videovigilancia se encuentra inoperativo** y la mayoría de las cámaras desinstaladas. En ningún caso se captan ni graban imágenes, llevando el sistema apagado un tiempo antes de la desinstalación de las cámaras.

Las cámaras tenían inhabilitada la función de zoom y la posibilidad de movimiento.

Aportan plano de los lugares donde se ubicaban las cámaras y fotografías de los postes donde se encontraban instaladas, apreciándose en algunos casos un soporte y unos cables adosados al poste, sin cámara. Las cámaras recogían diferentes zonas del parque, tratándose de un parque de atracciones. Los representantes de la entidad indican que no se trata de vía pública.

Se aprecian dos cámaras sin desinstalar, numeradas como 6 y 7, indicando los representantes de la entidad que la cámara pendiente de retirada se encuentra apagada, cumpliendo funciones disuasorias.

3. La instalación la realizó una empresa de seguridad **EXTINMAN SL, DGP ******.
4. Las cámaras no están conectadas a ninguna Central de Alarmas.
5. Respecto de la información facilitada sobre la existencia de cámaras, la entidad aporta fotografías de dos carteles donde se informa de la existencia de cámaras de videovigilancia así como del responsable ante el que ejercitar los derechos, **COMUNIDAD DE PROPIETARIOS CENTRO COMERCIAL XXXX PLAZA**.

Aportan también modelo de formulario informativo sobre el sistema de videovigilancia.

Según las fotografías aportadas, los carteles se encuentran adosados a la valla, en los accesos al parque.

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

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.”

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 caso que nos ocupa, se denuncia la instalación por parte de la denunciada, de cámaras de videovigilancia, sin autorización del Ayuntamiento de Granada, por todo el recinto del parque público **XXXX**.

Ante dicha denuncia, se solicitada información a la denunciada, por parte de los Servicios de Inspección de esta Agencia, para el esclarecimiento de los hechos denunciados, manifestando **TALER REAL ESTATE SL** que traspasan el requerimiento de información a **COMUNIDAD DE PROPIETARIOS CENTRO COMERCIAL XXXX PLAZA** ya que indican es el responsable del sistema de videovigilancia del Parque.

La referida Comunidad ha manifestado que la finalidad de la instalación fue por seguridad, si bien el sistema de videovigilancia se encuentra inoperativo y la mayoría de las cámaras desinstaladas. Manifiesta que en ningún caso se captan ni graban imágenes, llevando el sistema apagado un tiempo antes de la desinstalación de las

cámaras. Las cámaras tenían inhabilitada la función de zoom y la posibilidad de movimiento. En prueba de lo manifestado, aportan plano de los lugares donde se ubicaban las cámaras y fotografías de los postes donde se encontraban instaladas, apreciándose en algunos casos un soporte y unos cables adosados al poste, sin cámara. Asimismo, se aprecian dos cámaras sin desinstalar, numeradas como 6 y 7, indicando los representantes de la entidad que la cámara pendiente de retirada se encuentra apagada, cumpliendo funciones disuasorias.

Por lo tanto, a la vista de lo expuesto, las cámaras objeto de denuncia han sido desinstaladas e inoperativas, por lo que no se ha acreditado la captación o grabación de imágenes vulnerando la normativa de protección de datos.

A este respecto, no puede obviarse 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, la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público recoge en su artículo 28.1: *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa”*

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.”*

El Tribunal Constitucional, en su Sentencia 24/1997, tiene establecido que *“los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:*

a) La prueba indiciaria ha de partir de hechos plenamente probados.

b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)."

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 esta imputación o de la intervención en los mismos del presunto infractor.

En el presente caso, al haberse desinstalado el sistema y encontrarse inoperativo, en la actualidad, no se ha acreditado la captación o grabación de imágenes de personas físicas identificadas o identificables, contraviniendo la normativa de protección de datos, por lo que procede el archivo del presente expediente de actuaciones previas.

En todo caso, lo antedicho no impide que si constase acreditado en el futuro el tratamiento de los datos a través de la grabación de las imágenes o su visualización en tiempo real, vulnerando la normativa de protección de datos, esta Agencia pueda adoptar las medidas y llevar a cabo las actuaciones que procedan en virtud de las competencias que a la misma otorga la LOPD, a fin de garantizar el derecho fundamental a la protección de datos de carácter personal.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **COMUNIDAD DE PROPIETARIOS CENTRO COMERCIAL XXXX, TALER REAL ESTATE SL**, a D. A.A.A. y a la **SUBDELEGACION DEL GOBIERNO EN GRANADA-SECRETARIA GENERAL- SERVICIO DE ASUNTOS JURIDICOS**.

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.

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