



Expediente N°: E/06115/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **PLINIO TURISTICA S.L** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 16 de septiembre de 2014 tiene entrada en esta Agencia escrito remitido por D. **A.A.A.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de un sistema de videovigilancia instalado en el inmueble comunitario del **HOTEL PANAMÁ** sito en (C/.....1) (**MALLORCA**), cuyo titular es la entidad **PLINIO TURÍSTICA S.L** (en adelante el denunciado).

En su escrito, el denunciante manifiesta la existencia de un sistema de videovigilancia en las instalaciones comunitarias del Hotel Panamá, sin estar autorizado. El sistema no está debidamente señalizado. El acceso a las imágenes está autorizado a cualquier trabajador del citado establecimiento.

Adjunta a la denuncia reportaje fotográfico.

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 3 de noviembre de 2014 se solicita información al titular del sistema, resultando la misma devuelta por el servicio de Correos con la indicación "AUSENTE REPARTO".
2. Con fecha 3 de diciembre de 2014 se reitera la solicitud de información al responsable del sistema, teniendo entrada en esta Agencia escrito de fecha 8 de enero de 2015 en el que la representante de la entidad denunciada manifiesta:

*La entidad **PLINIO TURÍSTICA S.L** explota turísticamente la mayor parte de apartamentos que componen el edificio, sito en (C/.....1), bajo la denominación **HOTEL PANAMÁ** que forma parte de la empresa hotelera "Ola Hoteles".*

El edificio en el cual se ubica el citado hotel, se comparte con otros apartamentos que son privados.

*Desde principios del año 2014 las instalaciones del Hotel vienen sufriendo continuos sabotajes y daños intencionados, motivo por el cual la entidad **PLINIO TURÍSTICA S.L**, como titular del establecimiento, solicitó a la empresa de seguridad TASP la instalación, en el apartamento **B27** del Hotel Panamá, de una carcasa de microcámara que nunca estuvo en funcionamiento pero*

que motivó el fin de los sabotajes.

Al efecto se acompaña: (1) copia de denuncias interpuestas a raíz de los hechos expuestos (**Doc.2**), (2) copia del acta policial levantada con fecha 24 de noviembre de 2014 en los apartamentos Panamá, por *“realizar una actividad insalubre”* en las habitaciones **B23** y **B24** (**Doc.3**) y (3) certificado de la empresa de seguridad TSAP, mediante el cual informan: *“que el día 6 de octubre de 2014 se instaló en el apartamento B27 del Hotel Panamá, concretamente entre unas toallas, la carcasa de una microcámara oculta que jamás estuvo conectada ni registró imagen alguna. Se trató de una gestión para la empresa “Ola Hoteles”, ya que la compañía TASP tenía un vigilante de seguridad prestando sus servicios en el complejo, que sufría constantes sabotajes en la planta y concretamente en la zona de pasillo. Tras instalar dicho dispositivo y filtrarlo al personal del establecimiento, finalizaron los sabotajes”* (**Doc.4**).

3. Previa diligencia telefónica de inspección, con fecha 27 de enero de 2015, se solicita al responsable del sistema información complementaria, teniendo entrada en esta Agencia varios escritos de fechas 13, 16 y 23 de febrero de 2015, en los cuales comunica:

Las cámaras de seguridad a las que se refiere el requerimiento, no están funcionando desde hace varios años.

Con objeto de acreditar los hechos expuestos, presenta certificado emitido con fecha 10 de febrero de 2015 por la empresa de seguridad TSP, en el cual pone de manifiesto: *“Desplazado un técnico de la empresa al Hotel Panamá, puede verificar que existe instalado un sistema de CCTV. El sistema está compuesto por dos cámaras localizadas en detectores de incendios obsoletas y una cámara exterior averiada. No se dispone de monitor de visualización ni de equipo de videograbación. Se acompaña reportaje fotográfico acreditativo”* (**Doc.5**).

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

En primer lugar 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 presente expediente, se denuncia por D. **A.A.A.** la existencia de un sistema de videovigilancia instalado en el inmueble comunitario del **HOTEL PANAMÁ** sito en (C/.....1) (**MALLORCA**), cuyo titular es la entidad **PLINIO TURÍSTICA S.L.**, sin estar autorizado. Asimismo, el sistema no está debidamente señalizado.

A este respecto, solicitada información al denunciado por parte de los Servicios de Inspección de esta Agencia, manifiesta que la entidad **PLINIO TURÍSTICA S.L** explota turísticamente la mayor parte de apartamentos que componen el edificio, sito en (C/.....1), bajo la denominación HOTEL PANAMÁ que forma parte de la empresa hotelera “Ola Hoteles”. El edificio en el cual se ubica el citado hotel, se comparte con otros apartamentos que son privados, entre los que se encuentra el apartamento del denunciante.

Las cámaras objeto de denuncia, están ubicadas en el hall de recepción del hotel y en la parte trasera del hotel. Manifiesta el denunciado que estas cámaras, no están funcionando desde hace varios años. Con objeto de acreditar los hechos expuestos, presenta certificado emitido con fecha 10 de febrero de 2015 por la empresa de seguridad TSP, en el cual pone de manifiesto: *“Desplazado un técnico de la empresa al Hotel Panamá, puede verificar que existe instalado un sistema de CCTV. El sistema está compuesto por dos cámaras localizadas en detectores de incendios obsoletas y una cámara exterior averiada. No se dispone de monitor de visualización ni de equipo de videograbación. Se acompaña reportaje fotográfico acreditativo.*

Por lo tanto, las cámaras objeto de denuncia ubicadas en el hall y en la parte trasera del hotel se encuentran inoperativas y por lo tanto no captan ni graban imagen alguna.

Debe recordarse que la sanción debe basarse en hechos probados y en tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”*. De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común en lo sucesivo LRJPAC), establece que *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aún a título de simple inobservancia.”*

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

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)."

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 encontrarse las cámaras actualmente inoperativas no se ha podido acreditar la captación o grabación de imágenes por parte del denunciado vulnerando la normativa de protección de datos, por lo que atendiendo al principio de presunción de inocencia se procede al archivo del presente expediente de actuaciones previas.

No obstante y aun cuando se proceda al archivo del presente expediente por los motivos expuestos, debe tenerse en cuenta que las cámaras se encuentran instaladas en una zona que se presume que es zona de paso del denunciante para acceder a sus apartamentos, sin que conste y se desconoce al efecto si hay constituida algún tipo de comunidad de propietarios al respecto que haya aprobado la instalación de las cámaras. Por lo tanto, la ubicación de dichas cámaras enfocadas a espacios sustraídos del ámbito privado, genera una expectativa de captación de imágenes de las personas que circulan por la zona comunitaria que supone una afectación de sus derechos. Por ello, de acuerdo con lo previsto en los apartados a) y f) del artículo 37 de la LOPD, se le requiere formalmente para que retire las cámaras o sustituya por otros dispositivos que se adecuen a la normativa de protección de datos. A este respecto, en las Comunidades de Propietarios, la Junta de propietarios es el órgano de gobierno de la Comunidad que puede autorizar la instalación de las videocámaras. El acuerdo para la instalación de las cámaras deberá reflejarse en el acta de la Junta en los términos que determina la Ley 49/1960, de 21 de julio, de Propiedad Horizontal, resultando de aplicación lo dispuesto en el artículo 17.3 de dicha Ley. Asimismo, con carácter general se dará cumplimiento a lo previsto en la Instrucción 1/2006 en lo que respecta al deber de información e inscripción de fichero cuando se proceda a la grabación de imágenes.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **PLINIO TURISTICA S.L** 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 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