



Expediente Nº: E/07088/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **OLINVEST 2005 S.L.U. (HOTEL XXXX)** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 24 de abril de 2013 tiene entrada en esta Agencia escrito de D. **A.A.A.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de una cámara de videovigilancia cuyo titular es el **HOTEL XXXX** (en adelante el denunciado) instaladas en **(C/.....1) (ILLES BALEARS)**.

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:

Con objeto de aclarar los términos de la citada denuncia presentada por D. **A.A.A.**, se procedió a la apertura de las actuaciones de inspección de referencia **E/4403/2013**, en el marco de las cuales se requirió al Ayuntamiento de Soller información en relación con la cámara denunciada, entre otras. Del escrito de respuesta del Ayuntamiento de Soller, se pone de manifiesto que la cámara situada en la **(C/.....1)** de dicho municipio pertenece al **HOTEL XXXX**.

Con fecha 12 de diciembre de 2013 se solicita información al responsable del **HOTEL XXXX**, teniendo entrada en esta Agencia con fecha 10 de enero de 2014 escrito de dicho responsable en el que se pone de manifiesto lo siguiente:

La sociedad titular del Hotel es **OLINVEST, S.L.U.**, y también responsable de la cámara de video objeto de denuncia.

El representante de la sociedad manifiesta que la cámara no funciona, lo cual se puede comprobar a través de la página web del hotel www....hotel....

Se ha verificado por la inspección de datos que la página web <http://www....hotel...> dispone de un enlace denominado "webcam", al cual no es posible acceder, ya que al pinchar en el enlace se obtiene un mensaje de error indicando que no se ha podido establecer la conexión.

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 los 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 caso que nos ocupa, se denuncia la existencia de una cámara de videovigilancia instalada en la **(C/.....1) (MALLORCA)**, sin que se encuentre señalizada.

Con objeto de aclarar los términos de la citada denuncia presentada por D. **A.A.A.**, se procedió a la apertura de las actuaciones de inspección de referencia **E/4403/2013**, en el marco de las cuales se requirió al Ayuntamiento de Soller información en relación con la cámara denunciada, entre otras. Del escrito de respuesta del Ayuntamiento de Soller, se pone de manifiesto que la cámara situada en la **(C/.....1)** de dicho municipio pertenece al **HOTEL XXXX**.

Solicitada información por parte de los Servicios de Inspección de esta Agencia al responsable del **HOTEL XXXX**, tiene entrada en esta Agencia escrito de respuesta en el que el representante del citado hotel manifiesta que la cámara no funciona, pudiéndose verificar a través de la página web del hotel www....hotel.....

Se ha verificado por la inspección de datos que la página web <http://www....hotel...> dispone de un enlace denominado “webcam”, al cual no es posible acceder, ya que al pinchar en el enlace se obtiene un mensaje de error indicando que no se ha podido establecer la conexión.

Se trataba de una cámara webcam con una finalidad de información turística del entorno y tiempo meteorológico. A este respecto deben realizarse una serie de precisiones respecto a este tipo de cámaras.

Así, la captación de imágenes de paisajes o panorámicas en la medida en que no permitan identificar a las personas cuya imagen pueda ser captada quedaría fuera del ámbito de aplicación de la normativa de protección de datos y no existiría transgresión de ninguno de los principios recogidos en esta materia por lo que, sin perjuicio de otra normativa que pudiera ser de aplicación en cada caso concreto, no habría ninguna limitación y dicha difusión podría realizarse en abierto, es decir, sin necesidad de activar ningún tipo de control de acceso a las imágenes captadas por la cámara.

Ahora bien, la captación de imágenes de la vía pública de personas identificadas o identificables y fuera de un ámbito estrictamente privado o doméstico se encuentra reservada, con carácter exclusivo, a las Fuerzas y Cuerpos de Seguridad del Estado con fines de videovigilancia, en consonancia con lo establecido en la Ley Orgánica 4/1997. Resulta por lo tanto contrario a la normativa de protección de datos, salvo la excepción citada, la captación y difusión de imágenes de la vía pública en las que pueda identificarse a las personas. La captación y difusión de imágenes de este tipo a través de Internet excedería con mucho el ámbito privado o doméstico por lo que se produciría una vulneración del principio de legitimación.

Así, y dado que no se ha podido acceder a las imágenes que en caso de funcionar captaría la citada webcam, no se ha acreditado la captación de imágenes, al margen de la normativa de protección de datos.

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

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

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

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

En el presente caso, al no haberse acreditado la captación de imágenes al margen de la normativa de protección de datos y en base al principio de presunción de inocencia se procede al archivo del presente expediente de actuaciones previas.

No obstante, la ubicación de dicha cámara, enfocada a espacios sustraídos del ámbito privado, genera una expectativa de captación de imágenes de las personas que circulan por la vía pública que supone una afectación de sus derechos, y que entra en colisión con la reserva legal atribuida en exclusiva en tales supuestos a las Fuerzas y Cuerpos de Seguridad. 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 o redirija la cámara para que enfoquen al interior de su propiedad.

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 **OLINVEST 2005 S.L.U. (HOTEL XXXX)** 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