

Expediente N°: E/03000/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el **CONCELLO DE PONTE CALDELAS** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fechas 25 de marzo y 27 de mayo de 2015 tienen entrada en esta Agencia escritos remitido por D. **A.A.A.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia localizadas en el **C.C.C.** sito en la localidad de **CONCELLO DE PONTE CALDELAS**, cuyo titular es **CONCELLO DE PONTE CALDELAS**(en adelante el denunciado).

En los citados escritos, el denunciante manifiesta *“la instalación de un sistema de cámaras en los viales del Polígono de A Reigosa sin que cuenten con la correspondiente autorización administrativa para la vigilancia de la vía pública. El propio Concello de Ponte Caldelas, en calidad de responsable del sistema, afirma que las cámaras se encuentran apagadas pero por la propia ubicación de las mismas se crea una expectativa a las personas que circulan por la vía pública”*

Adjunta a su denuncia fotocopia del escrito (expediente **E.E.E.**) remitido al Valedor do Pobo por el Concello de Ponte Caldelas, con fecha 13 de junio de 2014, en el cual le comunican: *“La instalación de un sistema de videovigilancia a finales del año pasado en el Parque Empresarial Da Reigosa, con objeto de mejorar la seguridad del citado polígono industrial y ante la demanda expresada por las empresas instaladas en la zona, para prevenir la existencia de robos muy frecuentes en todos los polígonos industriales. El Concello para ello tramitó las correspondientes autorizaciones a la Comisión de Garantía de Videovigilancia de Galicia...y teniendo en cuenta que la Comisión informó desfavorablemente ... no puso en funcionamiento el sistema y no lo hará en tanto la Comisión no autorice su instalación y funcionamiento...”*.

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 11 de septiembre de 2015 se solicita información al titular del sistema, teniendo entrada en esta Agencia escrito con fecha 2 de octubre de 2015, en el que manifiesta:

Ser el responsable del sistema de videovigilancia instalado, en las vías públicas del Polígono Industrial “A Reigosa”, al amparo de la Ley Orgánica 4/1997 de 4 de agosto por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicas, así como su

Reglamento de desarrollo aprobado por el Real Decreto 596/1999 de 16 de abril.

La empresa GALEGA E TÉCNICAS E INVESTIMENTOS realizó la instalación del sistema.

Se acompaña copia del contrato “Suministro e Instalación de Sistemas de Seguridad y Vigilancia para el Parque Empresarial de Areigosa” suscrito entre las partes con fecha 13 de noviembre de 2013 (**Doc.1**).

Dada la instalación de diversas empresas en el Parque Empresarial A Reigosa, el Concello detectó una nueva necesidad de seguridad y vigilancia en los espacios públicos así como la prevención de hurtos o robos que se pudiesen producir en la urbanización y el entorno del citado parque, motivo por el cual determinó instalar el sistema de videovigilancia.

Existían carteles de videovigilancia instalados en las vías públicas del parque advirtiendo de la existencia del sistema, pero desde el momento que se tuvo conocimiento que el mismo no contaba con la autorización gubernativa los carteles fueron retirados por la Policía Local y actualmente permanecen en la sede del Ayuntamiento.

Respecto a los formularios informativos a disposición de los ciudadanos, se comunica que el Consistorio no dispone de los mismos ya que el sistema actualmente no se encuentra en funcionamiento.

El sistema de videovigilancia cuenta con 14 cámaras distribuidas en los viales públicos del Parque Empresarial, cuyo campo de vigilancia se limita al espacio público del Polígono Industrial destinado al tránsito.

Actualmente el sistema no se encuentra operativo ni se prevé su entrada en funcionamiento.

Al respecto se acompaña copia del Informe nº **F.F.F.** de fecha 26 de febrero de 2014 emitido por la Jefatura de Policía Local del Concello Ponte Caldelas para la Comisión de Garantías de Videovigilancia de Galicia, que incluye entre otros documentos el plano de situación del sistema y el reportaje fotográfico del ámbito de grabación de las videocámaras (**I.I.I.**).

El Concello carece de la autorización administrativa emitida por la autoridad gubernativa correspondiente que acredite el sistema de videovigilancia instalado.

En su caso, el acceso al sistema de videovigilancia estaría autorizado a la propia empresa instaladora y a la Policía Local

El sistema contaba en su día con un monitor de visualización y un equipo de grabación localizado en una caja de registro, además de otro equipo de visualización/grabación ubicado en las dependencias de la Policía Local, el cual actualmente permanece instalado pero que debido a las incidencias técnicas que presentaba y

posteriormente a la falta de autorización administrativa del sistema fue desactivado por parte de la Jefatura de Policía Local.

Se desconocen los detalles del sistema de grabación.

*Existe fichero denominado “**H.H.H.**” inscrito con el código **G.G.G.** en el Registro General de Protección de Datos con la finalidad de “videovigilancia en el Polígono Industrial para la prevención del delito y la garantía de la seguridad en las vías públicas”, cuyo responsable figura el **B.B.B.***

Se acompaña documentación acreditativa de la creación y registro del fichero (Doc.3).

El sistema de videovigilancia no se encuentre conectado a central de alarmas.

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 Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal aprobada por Real Decreto 1720/2007, de 21 de diciembre, 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 **A.A.A.** denuncia la existencia de cámaras de videovigilancia localizadas en los viales del Polígono de A Reigosa, cuyo titular es el **CONCELLO DE PONTE CALDELAS** sin que cuenten con la correspondiente autorización administrativa para la vigilancia de la vía pública y que el propio Concello, afirma que las cámaras se encuentran apagadas pero por la ubicación de las mismas se crea una expectativa a las personas que circulan por la vía pública.

Ante dicha denuncia, por parte de la Inspección de Datos de esta Agencia se solicita información al responsable del sistema, a efectos de esclarecer determinadas cuestiones del sistema de videovigilancia denunciado, recibiendo contestación al mismo en el que manifiesta, entre otras cosas, que el sistema de videovigilancia instalado, en las vías públicas del Polígono Industrial “A Reigosa”, fue realizado al amparo de la Ley Orgánica 4/1997 de 4 de agosto por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos, así como su Reglamento de desarrollo aprobado por el Real Decreto 596/1999 de 16 de abril. El sistema de videovigilancia cuenta con 14 cámaras distribuidas en los viales públicos del Parque Empresarial, cuyo campo de vigilancia se limita al espacio público del Polígono Industrial destinado al tránsito, si bien el sistema no se encuentra operativo ni se prevé su entrada en funcionamiento dado que, con fecha 26 de febrero de 2014, se remitió el Informe nº **F.F.F.** por la Jefatura de Policía Local del Concello Ponte Caldelas para la Comisión de Garantías de Videovigilancia de Galicia, que incluye entre otros documentos el plano de situación del sistema y el reportaje fotográfico del ámbito de grabación de las videocámaras, sin que conste la autorización administrativa emitida al respecto, por la autoridad gubernativa correspondiente que acredite el sistema de videovigilancia instalado.

Por lo tanto, el sistema de videovigilancia no se encuentra operativo, por los motivos expuestos, por lo que no captaría imágenes de personas físicas identificadas o

identificables.

Sobre esta cuestión debe señalarse que el Tribunal Constitucional ha declarado de forma reiterada 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 la imputación o de la intervención en los mismos del presunto infractor.

En el presente caso, al tratarse de cámaras inoperativas, no captarían imágenes de personas físicas identificadas o identificables, por lo que, al no quedar acreditada la existencia de un tratamiento de datos personales, la cuestión se encuentra al margen de la normativa de protección de datos. Por consiguiente es de aplicación el principio de presunción de inocencia, pues de la mera existencia de una cámara de videovigilancia no se desprende automáticamente que la misma funcione y que por tanto capte imágenes de personas y, en consecuencia, que exista un tratamiento de datos personales, no constando en el expediente indicio alguno de que dicho tratamiento se esté llevando a cabo.

Alcanzada la conclusión anterior, es conocido que en otros supuestos similares esta Agencia ha venido considerado que la instalación de dispositivos que generaban la apariencia de que habían sido instaladas cámaras de videovigilancia que, en su caso, podrían ser susceptibles de ser puestas en funcionamiento, con el consiguiente tratamiento de datos personales, podía generar una situación de alarma entre las personas, que entendían que eran vigiladas a través de dichos dispositivos, al producirse una apariencia de tratamiento. Teniendo esto en cuenta, y aun cuando por esta Agencia se acordaba el archivo del expediente en cuestión, se requería igualmente la retirada del dispositivo.

Sin embargo, esta Agencia consideró necesario revisar el mencionado criterio, en los términos que se plasman, entre otras, en la resolución del PS/00542/2015 de fecha 11 de noviembre de 2015. De este modo, la inexistencia de prueba alguna acerca de un posible de datos de carácter personal implica que la presente resolución de archivo no incorpore ningún tipo de requerimiento en el sentido que se ha mencionado, al prevalecer el principio de presunción de inocencia.

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.

Asimismo se informa que el artículo 35 de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal, recoge: *“La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones”*. Por su parte, el artículo 37 de la LOPD delimita dichas funciones, destacando la primera de ellas que es *“Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación...”*. Y es que según el artículo 1 de la LOPD, dicha norma 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”*. Por tanto, el ámbito propio de actuación de esta Agencia se refiere, con carácter general, a los datos de carácter personal definidos en el artículo 3. a) LOPD.

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 **CONCELLO DE PONTE CALDELAS** 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