

Expediente Nº: E/06773/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el **AYUNTAMIENTO DE LLANES** en virtud de denuncia presentada por **UNION DE SINDICATOS INDEPENDIENTES DEL PRINCIPADO DE ASTURIAS-USIPA** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 12 de agosto de 2014 tiene entrada en esta Agencia escrito del representante legal de la **UNION DE SINDICATOS INDEPENDIENTES DEL PRINCIPADO DE ASTURIAS-USIPA** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es el **AYUNTAMIENTO DE LLANES** (en adelante el denunciado) instaladas en **"AYUNTAMIENTO DE LLANES" ubicado en (C/.....1) (ASTURIAS)**.

El denunciante manifiesta que el Ayuntamiento tiene varios ficheros inscritos en esta Agencia, entre ellos uno denominado "Control de Acceso de Empleados Públicos" y que dicho fichero se debe nutrir de dos cámaras señalizadas que hay en la puerta de entrada al Ayuntamiento y otro en la entrada a la Policía Local.

Asimismo manifiesta que en las últimas fechas han aparecidos hasta cinco microcámaras escondidas y no señalizadas que pueden llevar a conclusiones de fines distintos a los inscritos en el fichero nombrado.

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 fecha 18 de noviembre de 2014 se solicita información al denunciado teniendo entrada en esta Agencia con fecha 2 de enero y 2 de junio de 2015 escritos en los que manifiesta:

1. El responsable del sistema de videovigilancia es el Ayuntamiento de Llanes.
2. La instalación fue realizada por la empresa Soto Sistemas, empresa que ahora pertenece a la mercantil ADICO (Asturiana de Desarrollos Informáticos y Comunicaciones S.L.). La relación con la citada empresa es por adjudicación de contrato menor de suministro (se adjunta copia, anexo 1).

3. El sistema de videovigilancia fue instalado para garantizar la seguridad de edificios públicos (vigilancia, control de acceso y seguridad de edificios).
4. En el exterior existen cámaras de videovigilancia de tráfico que no requieren autorización gubernativa.
5. Aporta fotos de tres carteles exteriores y dos interiores:
 - a. uno situado en la puerta exterior de entrada a las dependencias de la Policía Local, donde se indica como dirección a la que dirigirse la de la empresa ADICO.
 - b. otro situado en la fachada principal del edificio Consistorial, con la indicación Seguridad Soto y su teléfono de contacto.
 - c. cartel con la indicación del Ayuntamiento como responsable, sin especificar su ubicación.
6. Aporta fotos de dos carteles interiores:
 - a. uno con la indicación Seguridad Soto y su teléfono de contacto.
 - b. otro cartel con la indicación del Ayuntamiento como responsable, sin especificar su ubicación.
7. Se adjunta formulario de cláusula informativa, que no está cumplimentado (nombre de fichero, responsable, destinatario, etc.).
8. El número total de cámaras instaladas es de 7, no tienen zoom ni posibilidad de movimiento. Aporta planos de estas cámaras interiores:
 - a. cámaras 1 y 2 que se encuentran en el piso bajo cubierta.
 - b. cámaras 3 y 4 que se encuentran en la segunda planta en urbanismo
 - c. cámaras 5, 6 y 7 que se encuentran en la planta baja.
9. Aporta fotos de las cámaras e imagen captada.
 - a. Las cámaras 1 y 2 no se aprecian en las fotografías, captan zona de oficinas.
 - b. Las cámaras 3 captan zona de oficina del edificio. La cámara 4 ofrece una imagen en negro, al estar averiada, según declara el denunciado.
 - c. La cámara 5 capta zona de entrada al edificio, la cámara 6 no funciona y la 7 está estropeada, según manifiesta el denunciado. La imagen de la cámara 7 aportada no permite apreciar su ubicación.
10. No aporta fotografías de los monitores donde se visualizan las imágenes captadas por las cámaras que permitan acreditar la ubicación de los mismos.
11. El acceso a las cámaras es a través de un entorno web al que se accede mediante usuario y contraseña. Las personas con acceso a las imágenes de las cámaras son: el Inspector Jefe de la Policía Local y el responsable informático.

12. Las cámaras 1, 2, 3 y 4 graban en un grabador de disco duro que almacena las imágenes durante 30 días. A esas copias se accede también a través de un entorno web. Las personas que tienen acceso a las grabaciones son las antes mencionadas.

No se indica nada sobre la grabación de las imágenes captadas por la cámara 5 de entrada al edificio.

Mediante una diligencia se ha comprobado la inscripción de dos ficheros en el Registro General de Protección de Datos de esta Agencia cuyo responsable es el Ayuntamiento:

Fichero de "Videovigilancia de Edificios Públicos" con nº ***CÓD.1.

Fichero de "Control de Acceso de Empleados Públicos" con nº ***CÓD.2.

13. El sistema de videovigilancia no está conectado a una central de alarmas.
14. Sobre el procedimiento empleado para informar a los trabajadores de la finalidad por la cual se han instalado las cámaras de videovigilancia y la documentación acreditativa del cumplimiento del citado procedimiento:

"El servicio de Vicesecretaría controla las entradas y salidas de la Casa Consistorial".

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

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.

III

En el presente expediente el representante legal de la **UNION DE SINDICATOS INDEPENDIENTES DEL PRINCIPADO DE ASTURIAS-USIPA** denuncia el incumplimiento del deber de información por parte del Ayuntamiento de Llanes donde se encuentra instalado un sistema de videovigilancia y su posible utilización para fines distintos a los recogidos en el fichero inscrito a tal efecto.

En primer lugar procede plantear si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo, al amparo del artículo 6.1 de la LOPD, para continuar, con la verificación de si el sistema

de videovigilancia instalado en dependencias municipales del Ayuntamiento de Llanes, objeto de denuncia, cumple con el deber de información e inscripción de ficheros en materia de videovigilancia.

A este respecto es necesario realizar varias aclaraciones respecto al consentimiento en el ámbito laboral. Así, el consentimiento, elemento base en el tratamiento de los datos, entraña cierta complejidad, especialmente cuando nos referimos al ámbito laboral, dado que resulta de difícil cumplimiento que en ese ámbito concurren los requisitos legalmente previstos para considerar que se ha obtenido libremente el consentimiento. El artículo 3 h) de la LOPD lo define como *“Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen”*.

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

La concurrencia de estos requisitos resulta de difícil cumplimiento en el ámbito laboral. En consecuencia, vista la dificultad que entraña obtener el consentimiento, la Agencia Española de Protección de Datos, ha entendido que lo procedente es acudir a las normas que legitimen el tratamiento de los datos. Por tanto, en el ámbito laboral, el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del

empresario y es en éste articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del Estatuto de los Trabajadores (ET) dispone que *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso”*.

De todo ello se desprende que el empresario, en este caso la entidad denunciada, se halla legitimada para tratar las imágenes de sus trabajadores en el ámbito laboral, al amparo del artículo 20.3 del ET. Ahora bien, esta legitimación no es absoluta y exige por parte del empresario la obligación de informar de dicho tratamiento a los trabajadores(cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD.).

Sin embargo, en el caso que nos ocupa, el Ayuntamiento denunciado ha manifestado que la finalidad del sistema de videovigilancia instalado es la seguridad de edificios públicos (vigilancia, control de acceso y seguridad de edificios), sin que conste ni se aporten pruebas al respecto por parte del denunciante que acrediten que el sistema de videovigilancia es utilizado para fines distintos que no sean los de seguridad de las instalaciones y del personal de la misma, por lo tanto no existiría una finalidad de control de los trabajadores.

Es necesario en este punto diferenciar si la instalación de la cámara en el centro de trabajo es como medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales o si es una medida de seguridad para proteger la instalación y sus empleados (como es el caso que nos ocupa).

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral, como establece la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero de 2013, debe ir precedido de *“una información previa y expresa, precisa, clara e inequívoca a los trabadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”*.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, es necesario el cumplimiento de la LOPD, el Reglamento de Desarrollo de la LOPD y la Instrucción 1/2006. Por lo tanto, debería

cumplirse, entre otros, el deber de información recogido en el artículo 5 de la LOPD, disponiendo de distintivos informativos de zona de videovigilancia acordes a la Instrucción 1/2006 e impresos informativos.

Por lo tanto, el tratamiento de las imágenes por parte del responsable, obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD el cual reza lo siguiente:

“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 hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que 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, el Ayuntamiento de Llanes ha aportados diversas fotografías de la existencia de diversos carteles informativos de la existencia de las cámaras ubicados en el exterior e interior de las dependencias municipales: en los carteles exteriores se identifica a la empresa que procedió a la instalación del sistema de videovigilancia y en el cartel interior, es acorde al previsto en el artículo 3 a) de la Instrucción 1/2006, donde se establece como responsable al Ayuntamiento de Llanes. Ahora bien, dado que los carteles exteriores son distintos se recomienda que el Ayuntamiento proceda a instalar en el exterior carteles como el instalado en el interior del edificio donde se identifica al responsable del fichero: Ayuntamiento de Llanes. No obstante, no procede la apertura de procedimiento de infracción alguno al deducirse tal circunstancia de su ubicación, en consonancia con lo recogido en la guía de videovigilancia de esta Agencia en su página 47: *“En determinados entornos, como la entrada de una tienda o pequeño negocio, en los que el responsable es el propietario del establecimiento la simple ubicación del cartel permite establecer la identidad del responsable...”*.

Asimismo se ha aportado modelo de formulario informativo, de conformidad con el artículo 3.b) de la citada Instrucción, si bien en caso de solicitarse por algún interesado deberá entregarse debidamente cumplimentado.

Por lo tanto la citada entidad cumple el deber de información recogido en el artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD, dado que la finalidad del sistema de videovigilancia no es el control de los trabajadores sino la vigilancia y seguridad de las instalaciones y del personal, informando tanto a los ciudadanos que acceden a las dependencias como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado, sin que conste su utilización a efectos de control laboral ni se informe, en consecuencia, del uso de sus imágenes a tal fin.

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 del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

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 hace constar 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.

Pues bien, a los efectos que aquí interesan que son los relativos al sistema de cámaras de videovigilancia, consta la Resolución publicada en el Boletín Oficial del Principado de Asturias nº141 en fecha 19 de junio de 2013, por la que se aprueba la creación, regulación e inscripción del fichero denominado “Videovigilancia de edificios públicos del Ayuntamiento de Llanes”. Dicho fichero consta debidamente inscrito en el Registro General de la Agencia Española de Protección de Datos con el nombre “Videovigilancia de edificios públicos del Ayuntamiento de Llanes”, en fecha 13/08/2013 y cuya finalidad es garantizar la seguridad de edificios públicos (vigilancia, control de acceso y seguridad de edificios públicos) y que sería el fichero inscrito como consecuencia de la instalación del sistema de videovigilancia que posee el citado Ayuntamiento.

Asimismo el acceso a las cámaras de videovigilancia es a través de un entorno web al que se accede mediante usuario y contraseña. Las personas con acceso a las imágenes de las cámaras son: el Inspector Jefe de la Policía Local y el responsable informático.

Por otro lado, independiente del sistema de videovigilancia, existe inscrito en el Registro de esta Agencia el fichero denominado “Control de Accesos de empleados públicos”, en fecha 10/03/2010, que es al que hace alusión el denunciante, siendo el servicio de Vicesecretaría quien controla las entradas y salidas de la Casa Consistorial.

Asimismo el sistema de grabación almacena las imágenes durante 30 días, de conformidad al artículo 6 de la citada Instrucción 1/2006, que recoge: *“Los datos serán cancelados en el plazo máximo de un mes desde su captación”*.

IV

Por último, respecto a las manifestaciones realizadas por el denunciante relativas a la aparición de microcámaras escondidas que pueden llevar a conclusiones de fines distintos a las inscritas en el fichero, como ya ha sido desarrollado “ut supra”, no consta ni se aportan pruebas que acrediten que el sistema de videovigilancia es utilizado para fines distintos que no sean los de seguridad de las instalaciones y del personal de la misma.

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."*

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.

Por otro lado, de la ubicación de las cámaras que componen el sistema de videovigilancia, no se aprecia una vulneración del principio de proporcionalidad y calidad de los datos consagrado en el artículo 4.1 de la LOPD cuando señala: *"los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"*.

Por tanto, siguiendo el criterio de la citada Instrucción 1/2006, no puede considerarse, en el presente caso, que la instalación de las videocámaras en los términos expuestos vulnere los principios de calidad, proporcionalidad y finalidad del tratamiento.

Por lo tanto, a la vista de todo lo expuesto, se procede al archivo del presente expediente de actuaciones previas.

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 **AYUNTAMIENTO DE LLANES** y a **UNION DE SINDICATOS INDEPENDIENTES DEL PRINCIPADO DE ASTURIAS-USIPA**.

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.

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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos