

Expediente Nº: E/02122/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 11 de febrero de 2015, tuvo entrada en esta Agencia escrito de D. **A.A.A.** en nombre y representación del Comité de empresa **ZETA ESPACIAL**, asistido por su letrada, comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de un sistema de videovigilancia cuyo titular es la entidad **ZETA ESPACIAL S.A.** (en adelante el denunciado).

El denunciante manifiesta que la citada entidad ha instado un sistema de cámaras de videovigilancia sin el informe previo a los representantes de los trabajadores como dónde van a estar ubicadas, características de las mismas, el motivo de su instalación, ...

Adjunta escrito remitido a la entidad de fecha 14 de noviembre de 2014, solicitando información a la misma relativas a cuántas cámaras han sido instaladas, su ubicación, finalidad y la advertencia a toda la plantilla; Acta de reunión entre la Dirección de la empresa y el Comité de empresa de fecha 30 de diciembre de 2014; escrito de la entidad al Comité de empresa de fecha 30 de diciembre de 2014 y contestación a ésta última del Comité de empresa de fecha 8 de enero de 2015 y dirigida a la entidad.

SEGUNDO: Tras la recepción de la denuncia, la Subdirección General de Inspección de Datos procedió a la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 8 de abril de 2015, se solicita información a la entidad **ZETA ESPACIAL, S.A.**, teniendo entrada en esta Agencia con fecha 30 de abril de 2015, escrito en el que manifiesta:

- El responsable del sistema es **ZETA ESPACIAL S.A.**
- La empresa instaladora del sistema de videovigilancia es **VALLES SEGURETAT S.A.**
- El sistema de videovigilancia no está en funcionamiento sino en periodo de instalación y pruebas, por lo que del mismo no se genera en estos momentos fichero de datos, aunque se ha declarado el correspondiente fichero preventivamente.
- El sistema cuya instalación se está realizando en estos momentos tiene como finalidad, al amparo de lo establecido en el artículo 20.3 del ET, la vigilancia y control para el cumplimiento por el trabajador de sus obligaciones

y deberes laborales, así como una mejora y control de los procesos productivos.

En cuanto a la primera finalidad viene motivada por los requerimientos establecidos en el Sistema de Gestión de Calidad de la sociedad cuya actividad y plan de trabajo requieren de la videovigilancia como herramienta de ayuda en la gestión de los procesos productivos, así como por la necesidad de cumplir con los más exigentes estándares internacionales de producción y control sanitario y alimentario, exigidos por los clientes de la sociedad.

En cuanto a la segunda finalidad indicada, la existencia de turnos de trabajo, el tamaño de las instalaciones, la complejidad del proceso productivo y la organización del personal de fábrica hacen necesario el establecimiento de un sistema que permita garantizar la seguridad alimentaria y el cumplimiento de las normas vigentes.

- No existen cámaras instaladas en el exterior ni se capta imagen de la vía pública.
- Aun cuando el sistema no está aún operativo al encontrarse en fase de instalación y prueba se instalaron carteles indicativos, que se ajustan al modelo propuesto por la Agencia, situados en los accesos a las instalaciones y visibles antes de acceder a las mismas.
- No se posee todavía el modelo de formulario informativo, ni existe captación al no haberse decidido las características definitivas del sistema.
- En reunión con el Comité de empresa de fecha 30 de diciembre de 2014 se informó de la próxima instalación del sistema de videovigilancia, así como de su finalidad, Se adjunta carta al respecto.

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 el contexto normativo en materia de videovigilancia. Así el artículo 1 de la LOPD dispone: *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma señala: *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o*

identificables”.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.*

El artículo 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”.*

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”.* Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”.* Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”.*

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.

El tratamiento objeto de esta Instrucción comprende la grabación, captación,

transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.”

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

“1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.”

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

III

En el caso que nos ocupa, D. **A.A.A.**, en nombre y representación del Comité de empresa **ZETA ESPACIAL S.A.** manifiesta que la entidad **ZETA ESPACIAL S.A** ha instalado en la misma un sistema de videovigilancia sin el informe previo a los representantes de los trabajadores como dónde van a estar ubicadas, características de las mismas, el motivo de su instalación,...

Así, solicitada información a la entidad denunciada, por parte de los Servicios de Inspección de esta Agencia, para el esclarecimiento de los hechos denunciados, se recibe escrito de contestación A la misma en la que manifiesta que el sistema de videovigilancia no está en funcionamiento sino en periodo de instalación y pruebas, sin que se aporte por el denunciante pruebas que desvirtúen dicha afirmación.

Así las cosas, hemos de tener en cuenta que, en base a sus especiales consecuencias, el derecho administrativo sancionador es especialmente garantista con los administrados, por lo que le son de aplicación, sin excepciones, pero con matices, los principios del procedimiento penal, destacando entre ellos el principio de presunción de inocencia, el cual ha de ser respetado 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.

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 aun a título de simple inobservancia.”

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.”

Asimismo, se debe tener en cuenta, en relación con el principio de presunción de inocencia lo que establece el art. 137 de LRJPAC:

“1. Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario.”

Por lo tanto, si el sistema a fecha 24 de abril de 2015 no se encontraba aun

operativo, no captaba ni grababa datos personales. Al no existir todavía tratamiento de datos, no es preceptivo cumplir entre otros el deber de información, inscripción de ficheros y cuantas exigencias requiere la normativa de protección de datos.

No obstante, a pesar de que a la fecha de contestación a la solicitud de información de esta Agencia, 24 de abril de 2015, el sistema no se encontrara operativo, la entidad denunciada debe tener en cuenta, entre otros requisitos, todos los que seguidamente se exponen antes de poner en funcionamiento el citado sistema de videovigilancia.

En primer lugar, se plantearía 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.

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.

El apartado 2 del artículo 6 de la LOPD exime del necesario consentimiento cuando los datos se refieran *“a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento...”*

En el ámbito laboral, el Ordenamiento 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 haya legitimada para tratar las imágenes de los 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.).

De todo ello se desprende que el empresario, en este caso la entidad denunciada, se haya legitimada para tratar las imágenes de los 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.).

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.

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, se aplicaría toda la normativa y jurisprudencia recogida *“ut supra”*, es decir 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.

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.

A este respecto la entidad denunciada manifiesta que el sistema cuya instalación se está realizando en estos momentos tiene como finalidad, al amparo de lo establecido en el artículo 20.3 del ET, la vigilancia y control para el cumplimiento por el trabajador de sus obligaciones y deberes laborales, así como una mejora y control de los procesos productivos.

Así, 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.»

Ahora bien, este deber de información que recoge el artículo 5 de la LOPD, es necesario ampliarlo cuando el sistema de videovigilancia es utilizado para el control laboral de los empleados, como es el caso que nos ocupa. A este respecto la entidad denunciada debe tener en cuenta la reciente sentencia del Tribunal Supremo 2618/2014, de 13 de mayo de 2014 (Rec. 1685/13). En esta sentencia se recogía una vulneración empresarial de los derechos fundamentales del artículo 18.4 CE, en la instalación de videocámaras de vigilancia para un fin-desconocido para la trabajadora afectada- y distinto del expresamente señalado por la empresa. Se trataba de la captación de imágenes de la cajera despedida, e intento de utilización de las mismas como prueba del despido.

A este respecto, recoge la citada Sentencia del Tribunal Supremo 2618/2014 en su Fundamento de Derecho SEXTO: *“.-1.- En el supuesto ahora enjuiciado, como se ha adelantado, resulta que en el local del supermercado, donde coinciden el " lugar de trabajo ", que es donde pueden movilizarse por los trabajadores las garantías fundamentales, con los espacios físicos utilizados por los clientes que, en el presente caso, estaban sujetos a control mediante sistemas tecnológicos a través de varias cámaras instaladas con carácter permanente y esencialmente para controlar las puertas de acceso y los lineales, aunque una de ellas estaba ubicada en la zona de cajas; que ésta fue la cámara que se utilizó expresamente por la empleadora para controlar el puesto de trabajo de la cajera despedida, sin que se acredite que la información de un cliente fuera la que produjo la sospecha sobre la conducta de la trabajadora y la subsiguiente actuación empresarial, utilizando las cámaras de seguridad con tal fin de control de la actividad laboral para luego con base exclusiva en imágenes captadas por dicha cámara intentar acreditar los hechos imputados en la carta de despido (evitar en la caja el escaneo de diversos productos en beneficio de su pareja) (HP 4º y 5º); constando, además, en los hechos probados "que el sistema de vigilancia está dirigido a evitar robos por parte de clientes " (HP 3º), que " no consta haber sido comunicada la existencia del sistema de vigilancia a la representación unitaria " (HP 3º), que el representante de los trabajadores en el año 2008 " momento en el que se produjo la instalación de cámaras en el local, interpeló al responsable del local en orden a si se trataba de un sistema de vigilancia laboral. El responsable en aquella época le repuso seguidamente que no, que únicamente se trataba de un sistema destinado a evitar robos por terceros y que algunas de las cámaras no serían operativas. No se precisó cuales funcionarían y cuáles no " (HP 11º) y que el responsable nacional de seguridad al servicio de la demandada " advirtió que el sistema de cámaras existente en las*

instalaciones de aquélla no está preparado para la vigilancia del personal, sino únicamente para disuadir a terceros de robos " (HP 11º).

2.- Como se deduce de lo anteriormente expuesto, y se refleja razonadamente en la sentencia recurrida, por la empresa no se dio información previa a la trabajadora de la posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras instaladas permanentemente, ni, lo que resultaría más trascendente, tampoco se informó, con carácter previo ni posterior a la instalación, a la representación de los trabajadores de 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, ni explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo; por el contrario, al requerir tales representantes de los trabajadores a la empresa, una vez instaladas, se les indicó que su finalidad era evitar robos por terceros y no se trataba de un sistema para el control de la actividad laboral, que unas funcionarían y otras no y sin precisar tampoco el almacenamiento o destino de tales grabaciones, y que, a pesar de ello, " lo cierto es que en este concreto caso se usó con la indicada y distinta finalidad de controlar la actividad de la demandante y luego para sancionar a la misma con el despido " y sin que se acredite que la información de un cliente fue la que produjo la sospecha sobre la conducta de la trabajadora y la subsiguiente actuación empresarial.

3.- Destacando, por otra parte, la sentencia de suplicación, lo que compartimos, que la ilegalidad de la conducta empresarial no desaparece por el hecho de que la existencia de las cámaras fuera apreciable a simple vista, puesto que conforme a la citada STC 29/2013 " No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores 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".

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 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.”

Asimismo, de conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

Los datos serán cancelados (mediante bloqueo) en el plazo máximo de un mes desde su captación.

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida,

tratamiento o acceso no autorizado. Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas. El responsable deberá informar del deber de secreto a las personas con acceso a los datos.

Siempre se tendrán en cuenta los derechos específicos de los trabajadores respetando los derechos a la intimidad y el derecho fundamental a la protección de datos en relación con espacios vetados a la utilización de este tipo de medios como vestuarios, baños, taquilla o zonas de descanso; se respetará la vida privada en el entorno laboral no registrando en particular conversaciones privadas.

A la vista de lo expuesto, se procede al archivo del presente expediente de actuaciones.

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 **ZETA ESPACIAL S.A.** 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