



Expediente Nº: E/01572/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fechas de 29 de febrero, 8 y 9 de abril de 2016 tienen entrada en esta Agencia escritos remitidos 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 en el **CENTRO DE TRABAJO** sito en (C/...1) de **BARCELONA** cuyo titular es la mercantil **CLOQUER S.A** (en adelante el denunciado).

En escrito el denunciante manifiesta *“la instalación, con fecha 20/07/2015, de un sistema espía de videovigilancia cuya finalidad es el control laboral. Se localiza concretamente oculto en el techo de la oficina ubicada en el 1º piso de la nave, donde el denunciante viene desarrollando su actividad. Este sistema es adicional a otro ya existente, compuesto por cámaras visibles al personal. En ninguno de los casos expuestos, se ha informado a los trabajadores sobre el uso, tratamiento y finalidad de los mencionados sistemas”*.

Paralelamente, el denunciante presentó denuncia ante Inspección de Trabajo y Seguridad Social de Barcelona, ya que consideraba que los hechos expuestos afectan al ámbito laboral.

Adjunta a su escrito: **(1)** Copia de la denuncia presentada ante Dirección General de Inspección de Trabajo y Seguridad Social registrada el 31/10/2015, **(2)** copia del escrito de fecha 18/02/2016 de *“citación de comparecencia ante Inspección de Trabajo y Seguridad Social”*, en relación al expediente nº *****EXPT.1** y **(3)** reportaje fotográfico.

Cabe mencionar que con fecha 18/07/2016, tiene entrada en esta Agencia escrito remitido por el denunciante, en el cual manifiesta: *“...que tras conversaciones mantenidas con la Dirección de la empresa denunciada, ha tenido conocimiento de las circunstancias concretas que dieron lugar a la instalación del sistema denunciado. Siendo así, que debido a una denuncia de acoso formulada por una trabajadora de la empresa, la mercantil adoptó la decisión de instalar cámaras de vigilancia, que nunca llegaron a ponerse en funcionamiento ya que la propia empresa verificó la falta de veracidad de las afirmaciones vertidas por la ahora ex empleada denunciante, considerando por tanto innecesaria la adopción de dichas medidas...”*. En virtud de lo expuesto, ha solicitado a esta Agencia tenga por DESISTIDO todas las manifestaciones y requerimientos formulados en su denuncia.

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 19 de abril de 2016 se solicita información al responsable del sistema.

Del análisis de las manifestaciones y documentación aportada por el Representante legal de la entidad denunciada, con fecha de entrada en esta Agencia 18 de mayo de 2016, se desprende:

La mercantil CLOQUER S.A es la responsable del sistema de videovigilancia instalado.

La empresa INSTALACIONES ELÉCTRICAS MOGASA S.L fue la encargada de reubicar el sistema de videovigilancia, instalado en el antiguo domicilio de la mercantil y que volvió a entrar en funcionamiento el año 2011 en la nueva sede.

Se acompaña como documento Anexo I copia de la factura de instalación de fecha 02/01/2008 y como Anexo II certificado expedido por la empresa instaladora detallando el proceso de instalación.

Las cámaras se instalaron con un doble motivo:

- o Por razones de seguridad, para la prevención de robos y actos vandálicos, alguno de ellos sufridos por la mercantil con fecha 5 de febrero de 2011. Se acompaña copia de la denuncia (Anexo III).*
- o Como medida de control de la actividad laboral de los empleados, al amparo de lo previsto en el art. 20.3 del RD 2/2015 de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.*

Existen carteles informativos visibles y ubicados en todos los accesos a la zona videovigilada.

En documento Anexo IV se adjunta reportaje fotográfico.

Existen formularios informativos, bajo la custodia del Gerente de la empresa y a disposición de cualquiera que los solicite, sobre el tratamiento de datos con la finalidad de "seguridad de las instalaciones a través de un sistema de videovigilancia".

La mercantil conserva una copia de los mismos, firmada por cada uno de los empleados.

A modo de ejemplo, se acompaña modelo de cláusula informativa firmada con fecha 22/10/2015 (Anexo V).

El sistema de videovigilancia está compuesto por siete cámaras, sin posibilidad de movimiento ni zoom, ubicadas en diversas zonas interiores de la instalación.

No se encuentra en funcionamiento desde finales de noviembre de 2015, fecha en la que sufrió una avería. Las cámaras permanecen instaladas, sin funcionar.

El sistema incluía un monitor de visualización, que actualmente se encuentra desguazado y no ha sido reemplazado; por lo que se acompaña documento gráfico de las cámaras y su ubicación (Anexo VI), que intenta reproducir el campo de visión que captaban cada una de ellas.

De este modo, se distinguen las siguientes zonas de influencia:

- o Puerta entrada a la escalera principal (CAM 1).*
- o Puerta de carga/descarga en la planta inferior (CAM 2).*
- o Puerta de acceso nave (CAM 3).*
- o Puerta montacargas (CAM 4).*
- o Puerta de acceso a oficina y el área interior de dicha zona, en la que se distinguen varias mesas de trabajo (CAM 5).*
- o Puerta de acceso a la escalera principal (CAM 6).*
- o Puerta de entrada principal a la empresa, pudiendo observarse la zona de vía pública inmediata el mismo (CAM 7).*

Cuando el sistema estaba funcionando sólo el Gerente de la empresa estaba autorizado para su acceso, siendo el responsable de operar el grabador y monitor que se situaban en su lugar de trabajo.

Las imágenes quedaban grabadas durante un plazo de diez días. Su acceso estaba autorizado exclusivamente al Gerente y al Director Financiero.

*Existe fichero de videovigilancia inscrito en el Registro General de Protección de Datos, con el código ***CÓD.1.*

Se acompaña copia del Documento de Seguridad emitido por la empresa (Anexo VII)

El sistema, durante el tiempo de funcionamiento, no se encontraba conectado a central de alarmas.

Al respecto, los trabajadores fueron informados de la existencia y finalidad del sistema de videovigilancia de forma verbal y a través de las siguientes vías:

- o Mediante carteles informativos de zona videovigilada expuestos en el recinto.*
- o Por los formularios informativos sobre el tratamiento de datos personales con fines de videovigilancia, entregados al personal. La empresa conserva una copia de los mismos, firmada por cada uno de los trabajadores.*
- o Documento específico, de fecha 22 de octubre de 2015, firmado por el personal, mediante el cual se*

les informa sobre la existencia y finalidad del sistema de videovigilancia y se les comunica expresamente que “las referidas cámaras también tienen por objeto controlar su actividad laboral como trabajador de la empresa, pudiendo ser sancionado en el caso de apreciarse la comisión de una conducta disciplinaria tipificada en el convenio colectivo o en el Estatuto de los Trabajadores...”. Se adjunta copia del modelo (Anexo VIII)

Respecto a la cámara localizada en el primer piso de la nave, objeto de esta denuncia, se indica:

- o Se localiza junto a un detector de humo.*
- o Fue instalada por la empresa DEFENSCON S.L con fecha 14 de julio de 2015, con motivo de una serie de desavenencias producidas entre dos empleados de la empresa y la apertura de una investigación en relación a la denuncia por acoso y mobbing laboral formulada por parte de uno de estos trabajadores.*

Se adjunta copia de la factura de instalación (Anexo IX).

- o La cámara, tipo micro, captaba todo el ambiente de la oficina administrativa y a los trabajadores que estuvieran en ella.*

No se dispone de reportaje fotográfico sobre las imágenes captadas por la misma, ya que la única persona que tenía acceso a las grabaciones era el detective privado contratado al efecto.

- o Posteriormente fue desconectada con fecha 9 de enero de 2016.*

En documento Anexo X se acompaña copia del Informe Confidencial emitido al respecto, con fecha 30 de marzo de 2016.

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

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 Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado 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 se denuncia por parte de D. **A.A.A.** la existencia de cámaras de videovigilancia en el **CENTRO DE TRABAJO** sito en (C/...1) de **BARCELONA** cuyo titular es la mercantil **CLOQUER S.A** que pudieran vulnerar la normativa de protección de datos. El denunciante manifiesta la instalación, con fecha 20/07/2015, de un sistema espía de videovigilancia cuya finalidad es el control laboral. Este sistema es adicional a otro ya existente, compuesto por cámaras visibles al personal. Asimismo manifiesta que en ninguno de los casos expuestos, se ha informado a los trabajadores sobre el uso, tratamiento y finalidad de los mencionados sistemas.

En primer lugar, se plantea por el denunciante el posible incumplimiento del deber de información a los trabajadores de la existencia de las citadas cámaras de videovigilancia.

Ahora bien, en esta cuestión, en primer lugar se plantea 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.

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, está 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, 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”*.

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, debe tratarse por separado el sistema de videovigilancia instalado en la entidad, de la cámara oculta denunciada ubicada en el primer piso de la nave donde el denunciante desarrollaba su actividad.

En primer lugar, respecto al sistema de videovigilancia la entidad denunciada manifiesta que se instalaron con una doble finalidad: por un lado por razones de seguridad, para la prevención de robos y actos vandálicos, alguno de ellos sufridos por la mercantil con fecha 5 de febrero de 2011 y por otro lado, como medida de control de la actividad laboral de los empleados, al amparo de lo previsto en el art. 20.3 del RD 2/2015 de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

Por lo tanto, el sistema de cámaras instalado en el establecimiento cumpliría una doble función: de seguridad para proteger la instalación y sus empleados; y como medida de vigilancia y control del empresario, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales

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.”

En el caso que nos ocupa, la entidad denunciada aporta fotografías de la existencia de carteles informativos de videovigilancia visibles y ubicados en los accesos a la zona videovigilada. Dichos carteles son acordes al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo, dispone de cláusula informativa, a disposición de los interesados, de conformidad con el artículo 3.b) de la Instrucción 1/2006.

Por lo tanto, la entidad denunciada cumple el deber de información respecto a las personas que accedan a sus instalaciones.

Respecto a su vertiente de herramienta para el control laboral, la entidad denunciada manifiesta que los trabajadores fueron informados de la existencia y

finalidad del sistema de videovigilancia de forma verbal y a través de las siguientes vías: mediante carteles informativos de zona videovigilada expuestos en el recinto.;por los formularios informativos sobre el tratamiento de datos personales con fines de videovigilancia, entregados al personal. La empresa conserva una copia de los mismos, firmada por cada uno de los trabajadores y con el documento específico, de fecha 22 de octubre de 2015, firmado por el personal, mediante el cual se les informa sobre la existencia y finalidad del sistema de videovigilancia y se les comunica expresamente que *“las referidas cámaras también tienen por objeto controlar su actividad laboral como trabajador de la empresa, pudiendo ser sancionado en el caso de apreciarse la comisión de una conducta disciplinaria tipificada en el convenio colectivo o en el Estatuto de los Trabajadores...”*. Se adjunta copia del modelo.

Por lo tanto, la entidad denunciada cumple con el deber de información recogido en el artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD, informando tanto a las personas que acceden a las instalaciones de la entidad como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado.

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.”

En el caso que nos ocupa, consta la inscripción en el Registro General de la Agencia Española de Protección de Datos, por parte de la entidad denunciada, del fichero denominado “VIDEOVIGILANCIA”, cuyo responsable es CLOQUER, S.A.

El citado sistema de videovigilancia estaba compuesto por siete cámaras ubicadas en diversas zonas interiores pero según manifiesta la entidad denunciada, desde finales de noviembre de 2015 sufrieron una avería y permanecen sin funcionar.

En segundo lugar, respecto a la cámara oculta localizada en el primer piso de la nave, objeto de denuncia, manifiesta la entidad que fue instalada por la empresa DEFENSCON S.L con fecha 14 de julio de 2015, con motivo de una serie de desavenencias producidas entre dos empleados de la empresa y la apertura de una investigación en relación a la denuncia por acoso y mobbing laboral formulada por parte de uno de estos trabajadores. La cámara, tipo micro, captaba todo el ambiente de la oficina administrativa y a los trabajadores que estuvieran en ella. No se dispone de reportaje fotográfico sobre las imágenes captadas por la misma, ya que la única persona que tenía acceso a las grabaciones era el detective privado contratado al efecto. Posteriormente fue desconectada con fecha 9 de enero de 2016.

En cuanto a las sentencias dictadas respecto a cámaras no permanentes sino instaladas “ad hoc”, como es el caso que nos ocupa, para descubrir determinados sucesos acaecidos tenemos, la Sentencia 186/2000 del Tribunal Constitucional de 10 de julio en la que se desestima el recurso de amparo de un trabajador que fue captado por cámaras instaladas al efecto en el economato de su empresa como consecuencia de diversos descuadros ocurridos, e igualmente la [Sentencia 84/2015 del Tribunal Superior de Justicia de Madrid de 9 de febrero de 2015](#), que desestima el recurso de suplicación interpuesto contra la sentencia del juzgado de lo Social número 2 de Madrid que declaró procedente el despido del trabajador, considerando que se trata de una grabación episódica y de breve duración al existir sospechas fundadas de que la falta de prendas y otros objetos del establecimiento mercantil obedecía a su sustracción por algún trabajador.

Esta última sentencia ha establecido su pronunciamiento respecto a las cámaras temporales resolviendo en su texto las diferencias existentes entre las sentencias del TC y TS.

El TSJ de Madrid entiende que al tratarse de cámaras temporales, *"el presente supuesto tiene mayor conexión con el resuelto en la STC 186/00 que con los examinados en la STC 29/13 y en la STS 13-5-14 rec. 1685/2013"*, por lo que entraría en juego el artículo 18.1 CE (al tratarse de una grabación episódica) y no el 18.4 CE (al tratarse de una grabación con carácter preventiva). Recuerda el TSJM que *"En el supuesto de la STC 186/00 también se trata de la instalación ocasional y temporal de una cámara de grabación en el puesto de trabajo - las cajas registradoras - tras acreditadas sospechas razonables de incumplimientos contractuales que fueron acreditados de esta manera"*. Existen en ambos casos ilícitos laborales previos cuya averiguación era necesaria.

Al tratarse por ello de un supuesto episódico y de corta duración entiende el TSJM que *"sería absurdo exigir a la empresa una comunicación a los trabajadores de la instalación de unas cámaras de grabación advirtiéndoles "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", así como la colocación de carteles de publicidad ,pues de esta forma se arruinaría con toda seguridad la finalidad buscada"*.

Además entiende el TSJM que el derecho del trabajador a ser informado conforme al 18.4 CE tiene que ser ponderado con el derecho al empresario a la tutela judicial efectiva del 24.1 CE entendiendo que *"La actuación de la empresa en este caso en cuanto medida restrictiva de un derecho fundamental, el del art. 18.4 de la Constitución , supera el juicio de proporcionalidad, pues cumple los tres requisitos o condiciones siguientes (STC 186/00): si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y finalmente si es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto). La idoneidad no es cuestionable pues la grabación demostró en el juicio la conducta del trabajador que se le atribuía en la carta de despido e hizo posible la extinción del contrato de trabajo mediante despido disciplinario procedente por haber incurrido en un comportamiento muy grave. La necesidad es negada por el recurrente aduciendo que podría haberse utilizado un registro, pero no explica por qué un registro en la persona del trabajador es menos invasivo que una grabación de imágenes, aparte de que esta medida de control es menos idónea, ya que si resulta fallido un primer registro es claro que el trabajador culpable ya queda alertado. Y en cuanto a la proporcionalidad en sentido estricto el interés general de evitar la impunidad de conductas como la sancionada resulta superior al leve menoscabo relativo al tratamiento de datos, sobre todo teniendo en cuenta que las imágenes ni siquiera fueron tomadas por la demandada sino por una empresa del sector de vigilancia, se informó previamente al presidente del comité de empresa y no consta que hayan sido utilizadas para otra finalidad que su presentación en juicio"*.

En el presente caso, la instalación de la cámara respondió a esclarecer las desavenencias producidas entre dos empleados de la empresa y la apertura de una investigación en relación a la denuncia por acoso y mobbing laboral formulada por parte de uno de estos trabajadores. Por lo tanto la cámara oculta, objeto de denuncia, no formaba parte del sistema de videovigilancia instalado permanente y previamente a que ocurrieran los sucesos que dieron lugar a la instalación de la citada cámara, sino que la

cámara, en el presente caso, se instaló de forma puntual para descubrir lo que estaba ocurriendo al respecto y una vez resuelta la cuestión fue desconectada, por lo que se entiende en base a las sentencias descritas, legítima la actuación de la entidad denunciada.

Por lo tanto, a la vista de todo lo expuesto, en el presente caso no se aprecia vulneración por parte de la entidad denunciada, de la normativa aplicable en materia de videovigilancia, por lo que procede el archivo del presente expediente de actuaciones previas.

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 **CLOQUER, 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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

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.

Mar España Martí

Directora de la Agencia Española de Protección de Datos