

Expediente Nº: E/02331/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha de 11 de febrero de 2014 tiene entrada en esta Agencia un escrito de **A.A.A.** en el que declara:

<<El denunciante era trabajador de la denunciada con antigüedad de 19 de abril de 1996.

El 18 de abril de 2013, la empresa instaló un sistema de videocámaras ocultas, por sospechas de robos por parte del personal, sin notificarlo a la plantilla, ni cómo y dónde ejercitar los derechos de acceso, rectificación y cancelación. Tales imágenes eran grabadas en un ordenador de la empresa al que se desconoce quién tenía acceso. Y la creación del fichero de videovigilancia no fue inscrita en el Registro General de la Agencia Estatal de Protección de Datos hasta el 16 de julio de 2013.

*El día 11 de mayo de 2013, el denunciante fue grabado con dicho sistema de videocámaras, y haciendo uso de tales imágenes y sonido, la empresa interpuso denuncia ante la Policía Nacional, dando lugar a las Diligencias previas Nº ****/2013, del Juzgado de Instrucción Nº DOS de Torrent.*

Con base en las mismas grabaciones, el día 23 de mayo de 2013, el trabajador fue despedido de su empleo.

El 6 de junio de 2013, se formuló una nueva denuncia con base en grabaciones efectuadas el día 1 de mayo de 2013, con exceso por tanto del plazo máximo de conservación de grabaciones prevenido en la Ley Orgánica de Protección de Datos y en su normativa de desarrollo.>>

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

1. De la información y documentación aportada por ALCIÓN se desprende:
 - a. Presenta la entidad acreditación de tener inscrito un fichero, con código de inscripción ***CÓD.1, denominado VIDEOVIGILANCIA, declarando como finalidad "SEGURIDAD PRIVADA. SEGURIDAD Y CONTROL DE ACCESO A EDIFICIOS. VIDEOVIGILANCIA"
 - b. Informa la entidad que la instalación ha sido realizada por dos

empresas, Ralco Networks S.L. y L'Alcudia Elect.y Sistem. Seguridad, S.L.

c. Respecto a la motivación de la instalación, informa ALCIÓN:

<<La finalidad de las cámaras de videovigilancia instaladas por la empresa Alción Plásticos S.L. atiende a motivos de seguridad y control de acceso a los edificios de la empresa.

El interés legítimo perseguido por la empresa es controlar las posibles irregularidades cometidas en la empresa, en concreto la sustracción de material plástico de la empresa.

La empresa Alción Plásticos S.L. se vio obligada a instalar cámaras de videovigilancia en la empresa a raíz de unas sospechas fundadas sobre la sustracción de material plástico de la empresa de forma continuada.

Decimos sospechas fundadas porque gracias a las cámaras de videovigilancia la empresa pudo comprobar en el año 2013 que un trabajador de la empresa, en connivencia con otras dos personas ajenas a la misma, sustraía dicho material.

*Ese trabajador fue despedido por causas disciplinarias y el despido confirmado por Sentencia del Juzgado de lo Social nº 15 de Valencia, Autos ****/2013, que adjuntamos a la presente.*

Así mismo, dicha sustracción continuada de material dio lugar a la apertura de las Diligencia Previas nº 2030/13 por el Juzgado de Instrucción nº2 de Torrente, diligencias que continúan abiertas para la investigación de un posible delito de hurto agravado y continuado.>>

d. Aporta la entidad:

- Sentencia del Juzgado de lo Social nº 15 de Valencia, Autos ****/13 sobre despido disciplinario, en la que consta en el Fundamento de Derecho Segundo:

<<... la representación del actor insistió en el juicio en la impugnación de la prueba de reproducción de los videos, por ilegalidad, que contra esta tesis, la motivación que impulsa la colocación de cámaras, su comunicación a los representantes de los trabajadores y a la AEPD, su localización, encaves donde se desarrollan tareas que en modo alguno afectan a la intimidad, cubren en el caso los requisitos de idoneidad (es medida susceptible de conseguir el objetivo propuesto), necesidad (no hay otra con igual eficacia para conseguir el propósito) y proporcionalidad (genera más beneficios o ventajas para el interés general que perjuicio sobre los bienes eventualmente en conflicto) - por todas STC 207/1996 – dado que en definitiva, comprobado por la empresa que se estaba produciendo sustracción desde su propio entramado, desde luego a todas luces con ocultación, como al fin revelan las grabaciones, es notorio que tales eran el medio indicado e idóneo y al fin necesario de comprobación al que acudir.>>

- Auto de incoación de diligencias previas del Procedimiento Abreviado **00****/2013** del Juzgado de Instrucción 2 de Torrente fechado el 17/5/2013 por un presunto delito de HURTO.
- Auto del Procedimiento Abreviado **00****/2013** del Juzgado de Instrucción 2 de Torrente fechado el 17/2/2014, en el que, en sus Razonamientos Jurídicos se expresa:

<<Las imágenes fueron captadas por cámaras que cumplían toda la normativa administrativa tal y como resulta del oficio remitida por la Agencia Española de Protección de Datos. Estaban situadas en lugares visibles y en cualquier caso el propio imputado en su declaración reconoció que sabía de la existencia de dichas cámaras. Ninguna violación respecto de la intimidad del imputado se ha producido. La jurisprudencia constitucional en el ámbito laboral STC 29/2013 determina que cuando la empresa pretenda valerse de las grabaciones captadas por las cámaras de seguridad para fines de control laboral debe informar previamente a los trabajadores de tal posibilidad, es decir, “en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósitos”....

El imputado conocía perfectamente que estaba siendo grabado, como se ha dicho. Las cámaras estaban situadas dentro del recinto de la empresa y se cumplieron los requisitos administrativos, la aportación se efectúa al objeto de esclarecer la presunta comisión de una actuación delictiva...

Se puede exigir que el trabajador sea informado de que en el supuesto de que se cometa una infracción disciplinaria pudiera ser utilizado, pero no es necesario que se le informe de manera expresa de que si comete un delito, ya sea contra la empresa o contra cualquier otra persona, puedan ser utilizado dichas imágenes, ni en consecuencia se haya producido vulneración de derecho fundamental alguno por su aportación al proceso.>>

- Y en su parte dispositiva, el titular del Juzgado manifiesta:

<<Se desestima el recurso de reforma frente a la providencia de 28 de octubre de 2013, librándose los oficios solicitados y admitiéndose como prueba las imágenes aportadas por la representación de la parte denunciante.>>

- e. Aporta la entidad copia del cartel informativo de zona videovigilada, en la que se identifica plenamente a la entidad, así como su dirección a efecto del ejercicio de derechos ARCO
- f. Aporta igualmente copia del formulario informativo de que ha de disponer, en cumplimiento del art. 3.a de la Instrucción 1/2006 de esta Agencia.
- g. Aporta fotografías de las cámaras instaladas, contando con un total de once cámaras. Vistas las imágenes y el croquis de ubicación de las cámaras aportado, se concluye que todas ellas son cámaras enfocadas al interior de los locales de la empresa, no apreciándose que estén enfocadas a zonas de descanso o aseos.
- h. Informa la entidad que el tiempo de retención de las imágenes es de 30 días. Solicitadas a la entidad expresamente copia de las imágenes más antiguas de que dispone, se comprueba que son de un mes anterior a la fecha de referencia.
- i. Según informa la entidad hay un total de cinco personas con autorización de acceso al sistema, cuatro de ellas son cargos orgánicos de la entidad, siendo el último un técnico. El sistema no está conectado a central de alarmas.
- j. Respecto a la forma de informar a los trabajadores, la entidad manifiesta que se informó al Comité de Empresa y se colocaron carteles informativos. Aporta copia de las cartas remitidas y

firmadas por el Comité de Empresa acerca de la instalación de cámaras, la primera, de fecha 27/11/2008 relativa a la instalación de dos cámaras en los accesos de la entidad, y posteriores, de fecha 30/03/2009 (al Comité y a todo el Personal) informando de la ampliación del sistema de videovigilancia y de fecha 10/04/2013 al Comité de Empresa de nueva ampliación con motivo de la sustracción de material que se está produciendo en el almacén.

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 presente expediente se denuncia por parte D. **A.A.A.**, la instalación de un sistema de cámaras en la empresa para la que prestaba sus servicios ALCIÓN, sin notificación a los trabajadores, utilizando las imágenes grabadas para interponer denuncia ante la Policía Nacional contra su persona, dando lugar a las Diligencias Previas ****/2013, del Juzgado de Instrucción nº 2 de Torrent. Asimismo denuncia que las grabaciones fueron de fecha 1 y 11 de mayo de 2013, habiendo sido inscrito el fichero de videovigilancia el 16 de julio de 2013 y excediendo el plazo de conservación de las imágenes.

En primer lugar, se plantea por el denunciante el posible incumplimiento del deber de información a los trabajadores de la existencia del sistema 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, 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 el cartel anunciador, el impreso establecido por la Instrucción 1/2006 y mediante información a los trabajadores.

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.

En el caso que nos ocupa, la entidad denunciada manifiesta que la finalidad del sistema de videovigilancia atiende a motivos de seguridad y control de acceso a los edificios de la empresa, así como controlar las posibles irregularidades cometidas en la empresa, en concreto la sustracción de material de la misma. Manifiesta que la empresa se vio obligada a instalar cámaras de videovigilancia a raíz de una sospechas fundadas sobre la sustracción de material plástico de forma continuada.

Pues bien, 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 sociedad denunciada, ha aportado fotografías de la existencia de carteles informativos de la existencia de las cámaras ubicados en diferentes ubicaciones de las instalaciones de la entidad. 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, en el que se recoge la doble finalidad de seguridad y control de la actividad interna de la empresa.

Respecto a la información del sistema de videovigilancia a los trabajadores, la entidad copia de las cartas remitidas y firmadas por el Comité de Empresa acerca de la instalación de cámaras, la primera, de fecha 27/11/2008 relativa a la instalación de dos cámaras en los accesos de la entidad, y posteriores, de fecha 30/03/2009 (al Comité y a todo el Personal) informando de la ampliación del sistema de videovigilancia y de fecha 10/04/2013 al Comité de Empresa de nueva ampliación con motivo de la sustracción de material que se está produciendo en el almacén.

Por lo tanto los trabajadores eran conocedores de la existencia del sistema de videovigilancia y la finalidad del mismo, con independencia de donde se encontraran ubicadas las cámaras, a través de los diversos comunicados e escritos anteriormente recogidos. 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 pudieran acceder al recinto como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado.

IV

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.

En el caso que nos ocupa, la sociedad denunciada, es responsable del fichero dado que decide sobre la finalidad, contenido y uso del tratamiento derivado de las imágenes, requisitos necesarios para considerarse responsable del fichero, al amparo del artículo 3 d) de la LOPD.

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 sociedad denunciada, del fichero denominado “VIDEOVIGILANCIA” en fecha 16 de julio de 2013.

Sobre la cuestión planteada por el denunciante relativa a que, las grabaciones objeto de denuncia se realizaron en fecha 1 y 11 de mayo de 2013 y que con base en las grabaciones el día 23 de mayo de 2013 el trabajador fue despedido, habiendo sido inscrito el fichero el 16 de julio de 2013 cabe decir que, si el citado hecho fuera constitutivo de infracción sería de carácter leve, según se recoge en el artículo 44.2.b) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), que señala: *,” Son infracciones leves:... b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de*

Protección de datos.”.

Asimismo el artículo 47 de la LOPD señala:

“1. Las infracciones... leves prescribirán al año...

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador...”.

Respecto del cómputo de la prescripción el artículo 132.2 de la LRJPAC *“2. El plazo de prescripción de las infracciones comenzará a contarse desde el día en que la infracción se hubiera cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviera paralizado más de un mes por causa no imputable al presunto responsable.”*

El cómputo de prescripción de la infracción comienza a contar en el día de la comisión de ésta y termina cuando se dicta el acuerdo de inicio con conocimiento del denunciado, es decir, el día que éste recibe la notificación.

La prescripción, responde al principio de seguridad jurídica, que garantiza que los administrados no queden, indefinidamente, sometidos al ejercicio por la administración de su poder sancionador, y puedan conocer con certeza, el momento en que no serán sancionados por el ilícito cometido. Así lo ha entendido la jurisprudencia al considerar que la prescripción opera con el fin de que sea pronta la reacción social al incumplimiento de la normativa protegida por la amenaza de la sanción prevista en la ley administrativa (STS de 13 de febrero de 1991).

En el presente caso, las grabaciones objeto de denuncia son de 1 y 11 de mayo de 2013 y en fecha 16 de julio de 2013 se inscribió el fichero, es decir, el plazo de prescripción comienza a contarse el día que se cometió la presunta infracción. Por lo tanto dado el tiempo transcurrido desde la supuesta actuación constitutiva de la posible infracción, relativa a la falta de inscripción de fichero a la fecha de la grabación, hasta la fecha de presentación de la denuncia, se habría producido la prescripción de la presunta infracción que, en su caso se hubiera producido, a tenor del artículo 47 de la LOPD, que establece en un año las infracciones leves.

Así la Sentencia de la Audiencia Nacional de 7 de junio de 2005 dice *“sólo podrá operar con efecto interruptor del plazo de prescripción la fecha de comunicación al interesado del acuerdo de iniciación del expediente sancionador...”*

En cuanto a los efectos de la prescripción, y ante el silencio tanto de la LOPD como de la Ley 30/1992, hay que aplicar lo previsto en el artículo 6 del RD 1398/1993 que recoge el procedimiento para el ejercicio de la potestad sancionadora y del que resulta que cuando de las actuaciones previas se concluya que ha prescrito la infracción, el órgano competente acordará la no procedencia de iniciar el procedimiento sancionador; en caso de que ya se hubiera iniciado el procedimiento, debería acordarse su archivo o si se hubiera interpuesto recurso contencioso debería estimarse la impugnación por entender que la resolución administrativa impugnada se había dictado fuera de plazo.

Por último, señalar que la prescripción al actuar por ministerio de la ley actúa “ipso iure”, es decir una vez que se ha cumplido el plazo respectivo. Por ello, si la conducta presuntamente infractora de la LOPD se produjo en mayo de 2013, la prescripción extintiva aconteció, por ministerio del artículo 47 de la LOPD, en mayo de 2014 (para la infracciones leves). Antes de ésta última fecha, debería haberse dictado el acuerdo de inicio, cuestión prácticamente inviable dada la fecha de presentación de la denuncia.

Asimismo, indicar que con poco después de las citadas grabaciones objeto de denuncia fue inscrito el fichero en fecha 16 de julio de 2013.

Por otro lado, plantea el denunciante que el 6 de junio de 2013, se formuló una nueva denuncia con base en grabaciones efectuadas el día 1 de mayo de 2013, con exceso por tanto del plazo máximo de conservación de grabaciones prevenido en la LOPD y en su normativa de desarrollo. A este respecto debe decirse que la Agencia se ha pronunciado en diversas ocasiones sobre esta cuestión, señalando que respecto al plazo, sobre el que han de conservarse las imágenes, la elección de dicho plazo, no es arbitraria y sino que encuentra su fundamento tanto en la Instrucción 1/1996, sobre ficheros automatizados establecidos con la finalidad de acceder de controlar el acceso a los edificios, que en su norma quinta prescribe que *“Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados”*.

Ahora bien, la cuestión se plantea ante la existencia de alguna incidencia respecto de la grabación, como es el caso de la resolución que ahora se recurre. Así, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal viene a señalar que la cancelación dará lugar al bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que *“la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”*.

Este precepto, a su vez, se complementa con la previsión contenida en el transcrito artículo 16.5 de la Ley Orgánica 15/1999. En relación con esta cuestión, ya se indicaba en informes de esta Agencia de fecha 30 de julio de 2004 y 1 de agosto de 2005 lo siguiente:

“(…) la Ley Orgánica 15/1999 viene regular el bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que “la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”.

Este precepto, a su vez, se complementa con la previsión contenida en el artículo 16.5 que indica que “los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado”.

Del análisis conjunto de las normas citadas se desprende que existirán supuestos en los que si bien deberá procederse a la cancelación de los datos, al haber dejado de ser necesarios para la finalidad que justificó su tratamiento, como sucederá cuando se

haya producido la completa consumación del contrato que vincula al responsable del tratamiento con sus clientes, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, salvo en determinadas circunstancias, descritas por el artículo 16.3 de la Ley Orgánica, no implicará automáticamente ese borrado.

Así, el artículo 16.3 viene a reconocer, en consonancia con lo previsto en el artículo 16.5 de la Ley, que existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el responsable del fichero y que determina, en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de toda índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley, impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.

En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, y al margen de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto “en las disposiciones aplicables” o a la “atención de las posibles responsabilidades nacidas del tratamiento”, tal y como prevé la meritada Ley.

En este sentido, para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributaria y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).

En todo caso, debe recordarse que el mantenimiento del dato bloqueado, supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que “cumplido el citado plazo deberá procederse a la supresión”).

En consecuencia, a nuestro juicio, la cancelación no supone automáticamente en todo caso un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento.

En lo atinente a la determinación de los períodos en que el dato habrá de permanecer bloqueado, en relación con lo dispuesto en el artículo 16.3, resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, como ya se ha indicado con anterioridad, los

plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con su cliente, así como los derivados de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave. (...)

Por último, en cuanto al modo de llevar a cabo el bloqueo, deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia.”

Por lo tanto, en el supuesto que nos ocupa, la captación de las imágenes objeto de denuncia, fueron aportadas como medio de prueba en un procedimiento judicial, estando amparadas la conservación de las imágenes, en el artículo 16.3 de la LOPD, que señala que “la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”.

V

Por último, hemos de estudiar las implicaciones que lo denunciado presenta al respecto del derecho a la protección de datos en relación con el derecho a la tutela judicial efectiva de los protagonistas, por lo que partiremos de un análisis general relativo a la conexión de dichos derechos. Así, al respecto del derecho a la tutela judicial efectiva, nuestra norma suprema en el artículo 24 de la Constitución Española, en sus apartados 1 y 2, dispone lo siguiente:

“1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso, pueda producirse indefensión.

2. Asimismo, todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa.”

Así, constitucionalmente se consagra el derecho de los ciudadanos, ya sean personas físicas o jurídicas, a la tutela judicial efectiva y al derecho a utilizar los medios de prueba que consideren adecuados para el sostenimiento de su pretensión. Sin embargo, de dicha previsión, surge una colisión entre el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva de los jueces y tribunales referida, contenido en el artículo 24 de la Constitución, anteriormente transcrito, dadas a los bienes jurídicos afectados en su aplicación.

Por ello, ante tales situaciones, el Legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio Legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos,

incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En efecto, la exigibilidad del consentimiento del titular de los datos que pudieran ser objeto de un tratamiento en un procedimiento judicial, para dicho tratamiento de sus datos supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que una persona pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos o la dependencia en su aplicación a quien manejara la titularidad del dato, implicaría, lógicamente, una merma en la posibilidad de aportación por el interesado de *“los medios de prueba pertinentes para su defensa”*, vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) *“el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho”*.

Por otro lado, junto a lo dispuesto en el artículo 6.2 de la LOPD, el artículo 11 de la LOPD, recoge otras excepciones, a la exigencia del consentimiento:

“1.- Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2.-El consentimiento exigido en el apartado anterior no será preciso:

a.-Cuando la cesión esté autorizada en una ley.(...)

d.-Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.(...)”(el subrayado es de la Agencia Española de Protección de Datos).

En este sentido, entraría en liza lo dispuesto en el artículo 299 de la Ley 1/2000, de 7 de enero de Enjuiciamiento Civil, que admite la aportación como medio de prueba, de medios de reproducción de imágenes que sean relevantes para el proceso. Así establece, el precitado artículo:

“1. Los medios de prueba de que se podrá hacer uso en juicio son:

- 1. Interrogatorio de las partes.*
- 2. Documentos públicos.*
- 3. Documentos privados.*
- 4. Dictamen de peritos.*

5. *Reconocimiento judicial.*

6. *Interrogatorio de testigos.*

2. *También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso..*

3. *Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias”.*

Por lo tanto, en cuanto a lo aportado en el juicio, dicho cuerpo legal admite la aportación como medio de prueba de *los medios de reproducción de la palabra, el sonido y la imagen*, lo cual implica la posibilidad de tratamiento de datos dentro de dichas propuestas de prueba, debiendo ser el correspondiente órgano jurisdiccional quien se manifieste sobre la legitimidad de lo presentado, por lo que, en el caso de que esta Agencia impusiera una eventual sanción, dicha circunstancia colisionaría con el ejercicio del derecho constitucional a una tutela judicial efectiva.

Además, hemos de tener en cuenta que, la Audiencia Nacional en sentencia de 22 de octubre de 2010 (rec. 409/2009) nos dice, en cuanto a la obtención de medios probatorios y su validez en el procedimiento, pese a no ser solicitadas ni obtenidas por vía judicial, lo siguiente:

“De un lado ha de tenerse en cuenta que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD).

Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, parecer ser, y, así se desprende del acta de juicio, ocurrió en el presente supuesto.

Por otra parte, y si bien es cierto que los procedimientos judiciales tampoco son ajenos a la normativa de protección de datos, tal y como indicamos en la SAN 9-10-2009 (Rec. 37/2009) dado que el derecho de protección de datos, en cuanto derecho fundamental y autónomo previsto en el artículo 18.4 CE , vincula a todos los poderes públicos (Art. 53 CE) y entre ellos al Poder Judicial, tal y como igualmente indica la STS 18-9-2006 Rec. 274/2002 . Sin embargo dicha LOPD debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos.

Además de que el sometimiento de los ficheros judiciales a la LOPD ha de entenderse (según la misma SAN 9-10-2009 Rec. 37/2009) sin menoscabo de la

función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE, hasta el punto de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales." (el subrayado es de la Agencia Española de Protección de Datos).

Así la STC 99/1994 recoge: "La Sentencia de 6 de abril de 1994 corrobora la legitimidad de la prueba consistente en una filmación videográfica si la misma no ha vulnerado algún derecho, es decir, si con ello no se ha violado la intimidad o la dignidad de la persona afectada por la filmación. Es el propio Tribunal Constitucional el que estima admisible la captación de la imagen del sujeto cuando la misma conducta de aquel o las circunstancias en que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que pudieran colisionar con aquél".

Pero es que a mayor abundamiento, la propia Sentencia nº ****/2014 dictada por el Juzgado de los Social nº 15 de Valencia el 27 de febrero de 2014 desestimando la demanda interpuesta por el denunciante por el despido del mismo, recoge en su Fundamento de Derecho Segundo: <<... la representación del actor insistió en el juicio en la impugnación de la prueba de reproducción de los videos, por ilegalidad, que contra esta tesis, la motivación que impulsa la colocación de cámaras, su comunicación a los representantes de los trabajadores y a la AEPD, su localización, encaves donde se desarrollan tareas que en modo alguno afectan a la intimidad, cubren en el caso los requisitos de idoneidad (es medida susceptible de conseguir el objetivo propuesto), necesidad (no hay otra con igual eficacia para conseguir el propósito) y proporcionalidad (genera más beneficios o ventajas para el interés general que perjuicio sobre los bienes eventualmente en conflicto) - por todas STC 207/1996 – dado que en definitiva, comprobado por la empresa que se estaba produciendo sustracción desde su propio entramado, desde luego a todas luces con ocultación, como al fin revelan las grabaciones, es notorio que tales eran el medio indicado e idóneo y al fin necesario de comprobación al que acudir. >>

En la misma línea el Auto del Procedimiento Abreviado 00****/2013 del Juzgado de Instrucción 2 de Torrent fechado el 17/2/2014, recoge, en sus Razonamientos Jurídicos:

<<Las imágenes fueron captadas por cámaras que cumplían toda la normativa administrativa tal y como resulta del oficio remitida por la Agencia Española de Protección de Datos. Estaban situadas en lugares visibles y en cualquier caso el propio imputado en su declaración reconoció que sabía de la existencia de dichas cámaras. Ninguna violación respecto de la intimidad del imputado se ha producido. La jurisprudencia constitucional en el ámbito laboral STC 29/2013 determina que cuando la empresa pretenda valerse de las grabaciones captadas por las cámaras de seguridad para fines de control laboral debe informar previamente a los trabajadores de tal posibilidad, es decir, "en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósitos"....

El imputado conocía perfectamente que estaba siendo grabado, como se ha

dicho. Las cámaras estaban situadas dentro del recinto de la empresa y se cumplieron los requisitos administrativos, la aportación se efectúa al objeto de esclarecer la presunta comisión de una actuación delictiva...

Se puede exigir que el trabajador sea informado de que en el supuesto de que se cometa una infracción disciplinaria pudiera ser utilizado, pero no es necesario que se le informe de manera expresa de que si comete un delito, ya sea contra la empresa o contra cualquier otra persona, puedan ser utilizado dichas imágenes, ni en consecuencia se haya producido vulneración de derecho fundamental alguno por su aportación al proceso.>>

Y en su parte dispositiva, el titular del Juzgado manifiesta:

<<Se desestima el recurso de reforma frente a la providencia de 28 de octubre de 2013, librándose los oficios solicitados y admitiéndose como prueba las imágenes aportadas por la representación de la parte denunciante.>>

A la vista de todo lo expuesto, la captación de las imágenes objeto de denuncia fueron utilizadas como medio de prueba en un procedimiento judicial, siendo plenamente admitidas por el juzgador cumpliendo los requisitos de finalidad y proporcionalidad exigidos por la actual normativa en materia de protección de datos.

Por lo tanto, a la vista de todo lo expuesto, en el presente caso no se aprecia vulneración por parte de la sociedad denunciada de la normativa de protección de datos, por lo que procede el 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 **ALCIÓN PLÁSTICOS S.L.** 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