

Expediente Nº: E/03346/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Fecha de entrada de la denuncia: 27 de abril de 2017

Denunciante: D. **A.A.A.**

Denuncia a: **B.B.B..**

Por los siguientes hechos según manifestaciones del denunciante: Instalación de cámaras de videovigilancia en las oficinas de la sociedad sitas en (C/....., 1), donde se realizan las reuniones del comité de empresa, sin que los representantes de los trabajadores hayan sido informados y sin que exista señalización de la zona videovigilada. Refieren que desconocen si las cámaras también graban audio. Manifiestan no tener constancia de que se haya inscrito el fichero en el Registro General de Protección de Datos ni de que se estén cumpliendo los requisitos exigidos en la normativa de la LOPD.

Que según el denunciante tuvieron lugar a fecha de: En el momento de presentar la denuncia.

Aporta sólo la denuncia.

Requerido el denunciante por esta Agencia, con fecha 29 de mayo de 2015 y número de salida ***SAL.1 para que aporte información adicional que permita extraer indicios documentales sobre la instalación de videovigilancia referida, con fecha 16 de junio de 2017 y número de registro ***SAL.2 tiene entrada en esta Agencia escrito del denunciante en el que facilita la dirección de la instalación e identifica al posible responsable manifestando además, que las imágenes registradas por las cámaras son visibles desde las oficinas que la sociedad ARCELOR-MITTAL tiene ubicadas en ***LOC.1.

Y anexa la siguiente documentación:

Reportaje fotográfico de las cámaras y plano con su ubicación

Plano de situación de las oficinas

Burofax remitido a la sociedad solicitando información del sistema de videovigilancia instalado en las oficinas de la (C/....., 1)

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 3 de julio de 2017 se solicita información a la sociedad investigada teniendo entrada en esta Agencia con fecha 26 de julio de 2017 escrito del investigado en el que manifiesta, como aclaración preliminar, que las cámaras se encuentran desconectadas y fuera de servicio, no grabando ni almacenando imagen alguna. No obstante, da respuesta a los puntos de información solicitados en el requerimiento remitido por esta Agencia, manifestando lo siguiente:

1. El Responsable del sistema de videovigilancia es la sociedad JOFEMENE, S.A. Aclara, ante la información solicitada sobre la relación existente entre B.B.B., JOFEME, S.A. y ARCELOR-MITTAL, que tanto la sociedad investigada como JOFEME, S.A. son dos subcontratas de ARCELOR-MITTAL indicando que, en el supuesto de que las cámaras estuvieran operativas, ninguna empresa, y en particular, ARCELOR-MITTAL, desempeñarían tarea alguna en lo que respecta a la gestión del sistema de videovigilancia careciendo de acceso a los dispositivos del sistema de videovigilancia objeto de denuncia.
2. La preinstalación del sistema de videovigilancia la realizó la empresa A2 electricidad, realizando únicamente las tareas de preinstalación de los dispositivos y sin ocuparse del mantenimiento de los mismos. La sociedad investigada aporta un certificado expedido y firmado por el responsable de la empresa instaladora en el que declara haber instalado el sistema de videovigilancia objeto de denuncia dejándolo desconectado y afirmando que, en una comprobación posterior, realizada por la empresa a mediados de 2015, se verificó que el sistema seguía desconectado y que, por problemas en la instalación, ya no podía funcionar.
3. Respecto de la finalidad por la cual se instalaron las cámaras, el investigado manifiesta que el objetivo de la instalación del sistema de videovigilancia era proteger la propiedad contra robos e intrusiones y evitar hurtos y actos vandálicos que se habían producido en las oficinas en repetidas ocasiones. La colocación de las cámaras y los carteles resultó suficiente para conseguir el efecto disuasorio perseguido, garantizando la seguridad de clientes y trabajadores, motivo por el cual, aunque la instalación no estuviera operativa, decidieron dejarse colocados.
4. En relación al procedimiento seguido para informar a los trabajadores de la existencia de las cámaras, manifiestan que en un lugar visible de la zona videovigilada existe un cartel en el que se informa que existen, a disposición de los interesados, impresos en los que se detalla la información prevista en el artículo 5.1 de la LOPD y que pueden solicitarse en las propias oficinas. Aportan también el formulario informativo sobre la finalidad del sistema de videovigilancia, firmado por los dos empleados que dicen trabajar en las oficinas, en el que manifiestan haber sido informados y expresan su consentimiento al tratamiento.
5. Respecto de la información facilitada al público en general sobre la existencia de cámaras, se aportan fotografías de dos carteles, que señalizan la existencia de las mismas; uno situado a la entrada y otro en el interior de las oficinas, y que responden al modelo de cartel de zona videovigilada. En el detalle del cartel se comprueba que se incluye el nombre del responsable del fichero así como la

dirección en la que ejercitar los derechos ARCO.

Aporta además copia del formulario informativo sobre el sistema de videovigilancia al que se refiere el artículo 3.b de la Instrucción 1/2006, indicando que existe un cartel informativo, situado en un lugar visible de la zona videovigilada, en el que se informa de la existencia de impresos informativos a disposición de los interesados que quieran solicitarlos y que están disponibles en las propias oficinas en las que se encuentran las cámaras.

6. En relación a los lugares en los que se encuentran ubicadas las cámaras de videovigilancia, aporta plano de situación en el que se marca el emplazamiento concreto de las dos cámaras que hay en las oficinas, facilitando imagen de ambas. No se aporta imagen de lo registrado por las cámaras porque la sociedad investigada insiste en que el sistema no está operativo y que las cámaras sólo se mantienen en el emplazamiento en el que están a efectos de disuadir de la comisión de posibles robos y actos vandálicos. No obstante aclara que las cámaras que forman parte del sistema carecen de zoom, de posibilidad de movimiento y de capacidad de registrar sonido. Refiere que una de las cámaras está situada en la parte trasera izquierda de las instalaciones, enfocada hacia la entrada a las oficinas y una parte de una mesa y la otra está colocada en la parte trasera derecha de las oficinas y enfocada hacia la entrada.
7. En lo que respecta al sistema de monitorización, el investigado afirma que no existen monitores o dispositivos equivalentes en los que puedan visualizarse las imágenes al igual que afirma que no se almacena imagen alguna en un sistema de grabación, reiterando que el sistema de videovigilancia no se encuentra conectado ni operativo. No obstante, consultado el Registro General de Protección de Datos, se comprueba, tal y como figura en Diligencia incorporada a las actuaciones de inspección, que existe un fichero registrado, con código de inscripción número **C.C.C.** que se corresponde con el fichero "Videovigilancia" y cuyo responsable es la sociedad investigada.

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

El artículo 126.1, apartado segundo, 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 (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

III

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.

IV

En el caso que nos ocupa, D. **A.A.A.** denuncia a la entidad **B.B.B.**, por la instalación de cámaras de videovigilancia en las oficinas de la sociedad sitas en (C/....., 1), donde se realizan las reuniones del comité de empresa, sin que los representantes

de los trabajadores hayan sido informados y sin que exista señalización de la zona videovigilada. Manifiestan no tener constancia de que se haya inscrito el fichero en el Registro General de Protección de Datos ni de que se estén cumpliendo los requisitos exigidos en la normativa de la LOPD.

Ante dicha denuncia, la Inspección de Datos de esta Agencia solicita información a la denunciada, para el esclarecimiento de los hechos denunciados, manifestando ésta que las cámaras se encuentran desconectadas y fuera de servicio, no grabando ni almacenando imagen alguna. La preinstalación del sistema de videovigilancia la realizó la empresa A2 electricidad, realizando únicamente las tareas de preinstalación de los dispositivos y sin ocuparse del mantenimiento de los mismos. En prueba de ello, la sociedad investigada aporta un certificado expedido y firmado por el responsable de la empresa instaladora en el que declara haber instalado el sistema de videovigilancia objeto de denuncia dejándolo desconectado y afirmando que, en una comprobación posterior, realizada por la empresa a mediados de 2015, se verificó que el sistema seguía desconectado y que, por problemas en la instalación, ya no podía funcionar.

Por lo tanto, no puede obviarse que al Derecho Administrativo Sancionador le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad de los principios de presunción de inocencia. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del *ius puniendi* en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”*.

De acuerdo con este planteamiento, la Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público recoge en su artículo 28.1: *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa”*

Conforme señala el Tribunal Supremo (STS 26/10/98) el derecho a la presunción de inocencia *“no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”*

El Tribunal Constitucional, en su Sentencia 24/1997, tiene establecido que *“los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:*

a) La prueba indiciaria ha de partir de hechos plenamente probados.

b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras).”

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que *“Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate.”*

En definitiva, aquellos principios impiden imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan esta imputación o de la intervención en los mismos del presunto infractor.

En el presente caso, al encontrarse las cámaras que componen el sistema desconectadas e inoperativas, no se ha acreditado la captación o grabación de imágenes de datos personales por parte de la denunciada, contraviniendo la normativa de protección de datos, por lo que procede el archivo del presente expediente de actuaciones previas.

No obstante, y dado que se plantea por el denunciante el tratamiento sin consentimiento de los datos de los trabajadores, debe plantearse si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo, al amparo del artículo 6.1 de la LOPD.

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

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la

AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

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

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

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

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

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

En el ámbito laboral, el Ordenamiento el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, 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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.”*

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

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

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, se aplicaría toda

la normativa y jurisprudencia recogida “ut supra”, es decir sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral.

En el segundo caso, es decir cuando la finalidad es de vigilancia y protección de las instalaciones y personal de la empresa, es necesario el cumplimiento de la LOPD, el Reglamento de Desarrollo de la LOPD y la Instrucción 1/2006. Por lo tanto, debería cumplirse, entre otros, el deber de información recogido en el artículo 5 de la LOPD, disponiendo de distintivos informativos de zona de videovigilancia acordes a la Instrucción 1/2006 e impresos informativos.

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.»

Respecto de la información facilitada al público en general sobre la existencia de cámaras, se aportan fotografías de dos carteles, que señalizan la existencia de las mismas; uno situado a la entrada y otro en el interior de las oficinas, y que responden al modelo de cartel de zona videovigilada. En el detalle del cartel se comprueba que se incluye el nombre del responsable del fichero así como la dirección en la que ejercitar los derechos ARCO.

Aporta además copia del formulario informativo sobre el sistema de videovigilancia al que se refiere el artículo 3.b de la Instrucción 1/2006, indicando que existe un cartel informativo, situado en un lugar visible de la zona videovigilada, en el que se informa de la existencia de impresos informativos a disposición de los interesados que quieran solicitarlos y que están disponibles en las propias oficinas en las que se encuentran las cámaras.

En relación al procedimiento seguido para informar a los trabajadores de la existencia de las cámaras, manifiestan que en un lugar visible de la zona videovigilada existe un cartel en el que se informa que existen, a disposición de los interesados, impresos en los que se detalla la información prevista en el artículo 5.1 de la LOPD y que pueden solicitarse en las propias oficinas. Aportan también el formulario informativo sobre la finalidad del sistema de videovigilancia, firmado por los dos empleados que dicen trabajar en las oficinas, en el que manifiestan haber sido informados y expresan su consentimiento al tratamiento.

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 los clientes de la entidad como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado, aun cuando como, ya se ha señalado, se encuentre inoperativo.

Sin embargo, ello no implica que en el ámbito laboral quepa todo tratamiento de datos personales para el control por el empresario del cumplimiento de los deberes laborales del trabajador. Es decir, una cosa es la finalidad del tratamiento, que en este caso sería la prevista en el art. 20.3 ET, y otra la necesaria aplicación del principio de proporcionalidad consagrado en el art. 4.1 LOPD únicamente permitiendo el tratamiento de datos *“adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”*.

En definitiva, aun cuando el artículo 20.3 del ET. faculta al empresario para adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, esta adopción debe tener en cuenta obligatoriamente los derechos específicos de los trabajadores respetando los derechos a la intimidad y el derecho fundamental a la protección de datos en relación con espacios vetados a la utilización de este tipo de medios como vestuarios, baños, taquillas o zonas de descanso y dentro de las zonas de descanso estaría incluida el comedor de los trabajadores.

Por último, 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.”

A este respecto, consta la inscripción del fichero denominado "VIDEOVIGILANCIA" en el Registro General de la Agencia Española de Protección de Datos, con fecha inicial 18/12/2013 y modificada el 23/01/2014, siendo su finalidad la videovigilancia de las instalaciones.

A la vista de lo expuesto se procede al 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:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **JOFEMENE S.A.** y 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 los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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