

Expediente Nº: E/02237/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Fecha de entrada de la denuncia: 16 de marzo de 2017

Denunciante: D. **C.C.C.**

Denuncia a: **D.D.D..**

Por los siguientes hechos según manifestaciones del denunciante: Instalación de cámaras de videovigilancia en el local comercial de restauración en el que trabaja y que enfocan el espacio ocupado por los trabajadores, sin existir carteles informativos que lo señalicen y no haber sido informados los trabajadores de la finalidad de la instalación. Además de grabar imágenes, el denunciante refiere que las cámaras tienen la posibilidad de grabar sonido. Denuncia otro establecimiento, propiedad de la empresa, por idénticos hechos y circunstancias.

Y, entre otra, anexa la siguiente documentación:

Fotografías de las cámaras denunciadas.

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 14 de junio de 2017 y número de salida ***REGISTRO.1 se solicita información al titular de la mercantil teniendo entrada en esta Agencia con fechas 6 de julio de 2017 y número de registro ***REGISTRO.2 y 7 de julio de 2017 y números de registro ***REGISTRO.3, ***REGISTRO.4 y ***REGISTRO.5 escritos del investigado en el que manifiesta:

1. El Responsable del sistema de videovigilancia es la mercantil **D.D.D.. UNIPERSONAL**, con instalaciones en los locales que dispone en las direcciones **B.B.B.** y **A.A.A..**
2. La instalación del sistema de videovigilancia la realizó la empresa **SECURITAS DIRECT ESPAÑA, S.A.**, inscrita en el registro de empresas de seguridad de la Dirección General de Policía con número *** y que ha proporcionado una solución, según se extrae de las manifestaciones del investigado y del detalle de las condiciones del contrato facilitado, basada en cámaras de grabación por eventos, ya sea por detección de movimiento o de audio, con grabación en servidores en "la Nube" y conectadas a una Central Receptora de Alarmas.
3. Respecto de la finalidad por la cual se han instalado las cámaras, el denunciado manifiesta que el motivo por el que se ha procedido a la instalación del sistema de videovigilancia es la desaparición de mercancía en el almacén y en las zonas de trabajo y ante falta de pruebas se ha optado por esta medida para esclarecer los hechos y evitar que vuelvan a repetirse.

4. En relación al procedimiento utilizado para informar a los empleados de la instalación de las cámaras y su finalidad, el investigado refiere que han sido los propios trabajadores, ante la situación referida anteriormente, los que, a través de sus encargados, han solicitado la instalación de algún mecanismo para resolver el problema porque aunque, y según manifiesta el investigado, nunca se ha exigido responsabilidades a los empleados, los propios trabajadores asumen que es un problema que es necesario resolver. Además de la existencia de carteles para señalar la existencia de las cámaras, que responden al modelo de cartel de zona videovigilada y que están situados en el interior del local y en el espacio de trabajo, el investigado aporta, como documentación acreditativa de haber seguido el procedimiento de información a los empleados, copia de un documento, que según figura, está firmado por el administrador de la empresa y el representante de los trabajadores, y en el que se informa de que las cámaras serán utilizadas con un fin de videovigilancia además de para el control de la calidad y el rendimiento laboral de los trabajadores y, llegado el caso, para la detección y sanción de actos delictivos o faltas laborales recogidas en el convenio colectivo que regula la actividad de la sociedad.
5. Aunque el investigado manifiesta que las cámaras están orientadas sólo al área en el que los trabajadores realizan sus tareas y no captan espacio ni de la zona destinada a clientes ni del exterior, existen carteles informativos a la entrada de los dos locales, situados en la cristalería, que señalizan la existencia de cámaras y que responden al modelo de cartel de zona videovigilada. Existen además los dos carteles referidos en el punto anterior, situados en el interior de las instalaciones, en concreto en la zona destinada a los trabajadores. En el detalle del cartel aportado puede apreciarse que se identifica al responsable del sistema de videovigilancia y dónde ejercer los derechos de acceso, cancelación y oposición.
Aporta además copia del formulario informativo sobre el sistema de videovigilancia al que se refiere el artículo 3.b de la Instrucción 1/2006. Nada se indica del procedimiento para distribuir dicho formulario ante una solicitud del mismo.
6. En relación a los lugares en los que se encuentran ubicadas las cámaras de videovigilancia, aporta planos de situación para los dos establecimientos, en los que se marca el emplazamiento concreto de las cámaras así como fotografía de todas y cada una de ellas. Indica que las cámaras no disponen de zoom ni de posibilidad de movimiento pero sí que graban sonido, dado que, como ya se ha indicado, el modelo de las cámaras facilitadas por la empresa instaladora y de acuerdo a la solución de seguridad contratada, funciona por activación ante eventos, ya sea movimiento o detección de sonidos.

En el local situado en B.B.B., existe una única cámara, colocada en la pared y enfocada, según refiere el investigado y se indica en el plano, hacia la zona de trabajo y en concreto hacia los hornos. En la respuesta al requerimiento no aporta fotografía de la imagen captada por la cámara porque, según manifestaciones del personal a cargo del local e incorporado mediante Diligencia a las actuaciones de inspección, la aplicación a través de la cual visualizan las imágenes no funciona adecuadamente en el caso de esa cámara y no muestra imagen alguna, estando pendientes de que la empresa instaladora vaya a revisarla. Con fecha 4 de octubre de 2017 y número de salida ***REGISTRO.6 se solicita a la sociedad investigada que, entre otras cuestiones, aporte la imagen pendiente, teniendo entrada en esta Agencia, con fecha 7 de noviembre de 2017 y número de registro ***REGISTRO.7 escrito de respuesta en el que el investigado facilita la imagen de la captura pendiente comprobándose que la cámara del local B.B.B. está

enfocada hacia unas neveras y mesa de trabajo captando, en el lateral derecho, lo que parecen unos hornos.

En el local situado en A.A.A., existen dos cámaras; una situada en el almacén y que según fotografía aportada, capta imágenes de las mercancías y productos almacenados en el interior, y otra en la pared de la zona de trabajo y enfocada, según el plano de situación facilitado, hacia el horno, captando imágenes del área en donde los empleados desarrollan su actividad.

7. En lo que respecta al sistema de monitorización, el denunciado afirma que las imágenes capturadas por el sistema de videovigilancia sólo pueden visualizarse en la aplicación My Cam, software propietario de SECURITAS DIRECT S.A., que está instalada en el móvil del propietario de los dos locales de la sociedad investigada.
8. El sistema graba las imágenes capturadas por las cámaras y las almacena, según refiere el investigado, en un servidor “en la nube” facilitado por la empresa de seguridad, pudiendo conservarse habida cuenta de la solución de seguridad que tiene contratada la sociedad y según se describe en las condiciones del contrato, bien en una tarjeta de memoria, bien en servidores en la nube hasta un máximo de 8 horas de grabación para cada cámara, pudiendo descargarse dichas grabaciones al dispositivo móvil del usuario de la aplicación, tal y como figura en el manual de instrucciones aportado. Preguntado el investigado para que aclare el modo de operación del registro de las grabaciones que tiene configurado refiere, en la respuesta al requerimiento de fecha 10 de octubre de 2017, que las imágenes se almacenan en servidores en la nube pudiendo ser visionadas por un máximo de tres días. Según manifiesta la sociedad investigada, a dichas imágenes únicamente accede el responsable del sistema de videovigilancia a través de la aplicación móvil y aunque refiere que SECURITAS DIRECT no tiene acceso a las grabaciones de las cámaras, según se desprende de las características del contrato para la solución contratada, la empresa de seguridad podría acceder en el supuesto de que se produjera un salto de alarma a objeto de verificarlo. Preguntado el investigado para aclarar estos términos sobre si el sistema de videovigilancia está conectado a una Central Receptora de Alarmas, nada refiere sobre esta cuestión.

Aunque no se aporta código de inscripción del fichero en 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, bajo la denominación “Videovigilancia”, con código de inscripción **E.E.E.**

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

conciene 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 presente caso, D. **C.C.C.** denuncia la instalación de cámaras de videovigilancia en el local comercial de restauración en el que trabaja y que enfocan al espacio ocupado por los trabajadores, sin existir carteles informativos que lo señalicen y no haber sido informados los trabajadores de la finalidad de la instalación. Denuncia otro establecimiento, propiedad de la empresa, por idénticos hechos y circunstancias.

En primer lugar, se debe proceder a analizar el cumplimiento del deber de información e inscripción de fichero, por parte de la entidad denunciada.

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

“1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante”.

En cuanto al modo en que hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

“Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.”

“ANEXO-

1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.”

En el caso que nos ocupa, existen carteles informativos a la entrada de los dos locales, situados en la cristalería, que señalizan la existencia de cámaras y que responden al modelo de cartel de zona videovigilada. Existen además carteles situados en el interior de las instalaciones de los dos locales, en concreto en la zona destinada a los trabajadores. En el detalle del cartel aportado puede apreciarse que se identifica al responsable del sistema de videovigilancia y dónde ejercer los derechos de acceso, cancelación y oposición. 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.

Aporta además copia del formulario informativo sobre el sistema de videovigilancia al que se refiere el artículo 3.b de la Instrucción 1/2006, a disposición de los interesados.

En relación al procedimiento para informar a los trabajadores de la finalidad para la que se han instalado las cámaras de videovigilancia, el investigado manifiesta que además de la existencia de carteles para señalar la existencia de las cámaras, que responden al modelo de cartel de zona videovigilada y que están situados en el interior del local y en el espacio de trabajo, aporta, copia de un documento, que según figura, está firmado por el administrador de la empresa y el representante de los trabajadores, y en el que se informa de que las cámaras serán utilizadas con un fin de videovigilancia (finalidad de dar cumplimiento al operativo de seguridad y para prevenir riesgos que afecten a la seguridad y protección de las personas, locales y bienes patrimoniales), además de para el control de la calidad y el rendimiento laboral de los trabajadores así como verificación del cumplimiento de sus obligaciones y deberes laborales y, llegado el caso, para la detección y sanción de actos delictivos o faltas laborales recogidas en el convenio colectivo que regula la actividad de la sociedad.

Por lo tanto, el sistema de videovigilancia instalado cumple una doble finalidad de seguridad de las instalaciones y protección de las personas y bienes, así como cumplimiento de las obligaciones y deberes laborales de sus empleados.

A la vista de la documentación presentada por la entidad denunciada, ésta informa tanto a sus trabajadores, como a las personas que accedan a las instalaciones de los establecimientos, de la existencia de un sistema de videovigilancia y de la finalidad del mismo.

Hay que tener en cuenta que todo tratamiento de datos personales ha de estar legitimado por alguna de las causas del art. 6 LOPD. Pues bien, la captación y grabación de las imágenes de los empleados del centro con un fin de control laboral aparece amparado por el art. 6 LOPD, al existir una habilitación legal para el control laboral pretendido que es de carácter imperativo para “las partes de un contrato... de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento”.

El artículo 20.3 del Texto Refundido del Estatuto de los Trabajadores(ET),

aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre, 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”*.

En este sentido, el artículo 20.3 ET en relación con el art. 6 LOPD legitimaría, en principio, a la empleadora para tratar las imágenes de los trabajadores en el ámbito laboral con carácter general. Así, el tratamiento de datos realizado en el centro de trabajo por medio de cámaras de videovigilancia está exceptuado del consentimiento de los empleados, por la habilitación legal que le confiere al empresario el art. 20.3 del Estatuto de los Trabajadores, que comprende entre otras, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales. Esta facultad ha de producirse en todo caso, como es lógico, dentro del debido respeto a la dignidad del trabajador, como expresamente nos recuerda la normativa laboral (arts. 4.2. e y 20.3 LET). El Tribunal Constitucional, STCO 98/2000, de 10 de abril de 2000, destaca en su fundamento jurídico 6 que *“La jurisprudencia de este Tribunal ha insistido reiteradamente en la plena efectividad de los derechos fundamentales del trabajador en el marco de la relación laboral, ya que ésta no puede implicar en modo alguno la privación de tales derechos para quienes prestan servicio en las organizaciones productivas, que no son ajenas a los principios y derechos constitucionales. Sin embargo no basta la mera manifestación del ejercicio del poder de control por el empleador para que el derecho del trabajador se vea sacrificado. Estas limitaciones empresariales tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes. Se trata, en definitiva, de la aplicación del principio de proporcionalidad.”*

Ahora bien, esta legitimación no es absoluta y exige que el empresario informe de dicho tratamiento a los trabajadores (cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD.).

Sin embargo, 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.

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.

V

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 inscrito en el Registro General de Protección de datos de esta Agencia el fichero denominado “VIDEOVIGILANCIA” en fecha 12/11/2010, cuyo responsable es D.D.D..

VI

Por último, en relación a los lugares en los que se encuentran ubicadas las cámaras de videovigilancia, aporta la entidad denunciada planos de situación para los dos establecimientos, en los que se marca el emplazamiento concreto de las cámaras así como fotografía de todas y cada una de ellas. En el local situado en **B.B.B.**, existe una única cámara, colocada en la pared y captando la imagen de una zona de neveras y mesa de trabajo captando, en el lateral derecho, lo que parecen unos hornos. En el local situado en **A.A.A.**, existen dos cámaras; una situada en el almacén y que según fotografía aportada, capta imágenes de las mercancías y productos almacenados en el interior, y otra en la pared de la zona de trabajo y enfocada, según el plano de situación facilitado, hacia el horno, captando imágenes del área en donde los empleados desarrollan su actividad.

El artículo 4.1 de la LOPD, garantiza el cumplimiento del principio de proporcionalidad en todo tratamiento de datos personales, cuando señala que:

“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”.

Dicho artículo 4 de la LOPD, con la denominación “Calidad de datos” es el primer precepto del título II dedicado a los “Principios de calidad de datos”, que derivan del derecho fundamental a la protección de datos. En el apartado 1 del artículo 4 de la LOPD se establece que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, de acuerdo con una serie de criterios, que se resumen en el principio de proporcionalidad. Por consiguiente consagrándose el “principio de pertinencia en el tratamiento de los datos de carácter personal”, que impide el tratamiento de aquellos que no sean necesarios o proporcionados a la finalidad que justifica el tratamiento, debiendo restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de los mismos. En consecuencia, el tratamiento del dato ha de ser pertinente y no excesivo en relación con el fin perseguido. Únicamente pueden ser sometidos a tratamiento aquellos datos que sean estrictamente necesarios para la finalidad perseguida. Por otra parte, el cumplimiento del principio de proporcionalidad no sólo debe producirse en el ámbito de la recogida de los datos, sino asimismo de respetarse en el posterior tratamiento que se realice de los mismos.

Este criterio se encuentra recogido también en el artículo 6 de la Directiva 95/46/CE, aparece también reflejado en el Convenio 108, cuyo artículo 5 c) indica que “los datos de carácter personal que sean objeto de un tratamiento automatizado (...) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado”.

El mencionado precepto debe ponerse en correlación con lo previsto en el apartado 2 del citado artículo 4, según el cual: “Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.”. Las finalidades a las que alude este apartado 2 han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley.

En el presente caso, de la documentación fotográfica aportada por la entidad denunciada se desprende que las cámaras instaladas en ambos locales tienen como finalidad evitar la desaparición de mercancía en el almacén y en las zonas de trabajo. Las cámaras instaladas se encuentran en las zonas de trabajo de ambos locales, existiendo un tratamiento proporcional que justificaría su instalación, de acuerdo al fin pretendido.

A la vista de lo aportado, las imágenes captadas no infringirían el principio de proporcionalidad de los datos previsto en el artículo 4.1 de la Ley Orgánica de Protección de Datos, cuando se habla de que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

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

Por lo tanto, 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 **MELCRIS S.L.** y D. **C.C.C.**

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