



Expediente N°: E/04174/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **TELECOR, SA** en virtud de denuncia presentada por D^a. **B.B.B.** y teniendo como base los siguientes

HECHOS

PRIMERO: Fecha de entrada de la denuncia: 12 de junio de 2017

Denunciante: D^a. **B.B.B.**

Denuncia a: **C.C.C.**

Por los siguientes hechos según manifestaciones de la denunciante: Instalación en el establecimiento del **A.A.A.**, de una cámara de videovigilancia, sin señalar, en el interior del almacén, que también es usado por los empleados como vestuario, habiendo sido visualizadas imágenes registradas por la cámara, y en las que aparece la denunciante cambiándose de ropa, por otros empleados de la empresa cuando un técnico se desplazó al establecimiento a extraer las imágenes grabadas.

Que según el denunciante tuvieron lugar a fecha de: En verano de 2016

Y, entre otra, anexa la siguiente documentación:

Vídeo en el que se muestra la cámara del almacén.

Informe de la Inspección de Trabajo a raíz de la denuncia, sobre estos mismos hechos, presentada por la denunciante.

Los antecedentes que constan son los siguientes:

Con fecha 19 de agosto de 2016 y número de registro ***REGISTRO.1 tiene entrada en esta Agencia escrito de la denunciante donde relata los mismos hechos que constan en esta denuncia, pero sin aportar prueba documental alguna, dando lugar a la apertura del expediente de investigación E/04713/2016. Con fecha 30 de agosto de 2016 y número de salida ***REGISTRO.2, esta Agencia le dirige escrito a la denunciante solicitando que aporte indicios documentales de la existencia del sistema de videovigilancia instalado y dándole un plazo de 10 días hábiles para remitir la información solicitada. Al no aportar documentación adicional, con fecha 21 de octubre de 2017 se firmó resolución de archivo de las actuaciones previas iniciadas.

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 13 de julio de 2017 y número de salida ***REGISTRO.3 se solicita información a la sociedad investigada teniendo entrada en esta Agencia con fecha 21 de julio de 2017 y número de registro ***REGISTRO.4 escrito de la representante legal del investigado en el que manifiesta:



1. El responsable del sistema de videovigilancia es la empresa TELECOR, S.A.
2. La instalación de las cámaras la realizó MEGA2 SEGURIDAD, S.L., empresa inscrita en el registro de empresas de seguridad de la Dirección General de Policía con nº ***, aportando copia del contrato de arrendamiento de servicios de seguridad que la sociedad investigada tiene suscrito con la empresa instaladora.
3. Respecto de la finalidad por la cual se han instalado las cámaras, la representante del investigado manifiesta que el establecimiento en cuestión está destinado a la venta de telefonía móvil y sus accesorios, lo que conlleva una serie de riesgos y vulnerabilidades habida cuenta del valor de la mercancía, por lo que es necesario que el local se encuentre protegido mediante cámaras para la vigilancia del mismo.
4. En relación al procedimiento seguido para informar a los trabajadores de la existencia de cámaras de videovigilancia en el local se aporta copia del Sistema de Información para Empleado (S.I.E.) donde se informa a los trabajadores, por parte de la Dirección de la Empresa, de la existencia de sistemas de grabación continuada en el centro comercial y en zonas de trabajo, bien sean de acceso, tránsito, venta, elaboración y almacenamiento, y cuya finalidad es el control de la seguridad de las personas, bienes, instalaciones y mercancías a la venta. Asimismo, se informa de la posibilidad de utilizar el sistema para la detección de acciones irregulares, ya sean realizadas por personas ajenas a la empresa o por los propios trabajadores, utilizándose en ese caso para la imposición de sanciones disciplinarias por incumplimiento del contrato de trabajo.

En el mismo aviso se informa a los trabajadores del plazo de conservación de la imágenes, salvo incidencia, quién accede a las mismas así como de la existencia de hojas para ejercitar los derechos ARCO disponibles en los SAC de los Centros Comerciales.

5. Respecto de la información facilitada sobre la existencia de cámaras, además del aviso a los empleados al que hace referencia el punto anterior, se aporta fotografía de un cartel, situado a la entrada del establecimiento comercial, que señalizan la existencia de las mismas; y que responden al modelo de cartel de zona videovigilada. En el modelo de cartel que aportan se identifica al Responsable del Fichero y la dirección donde ejercer los derechos ARCO, aunque en el cartel físico situado a la entrada de la tienda, debido a la distancia a la que está tomada la fotografía y la falta de enfoque, no puede apreciarse el detalle del mismo sin ser posible constatar que la información coincide con la facilitada en el modelo.

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 está a disposición de los ciudadanos en la propia tienda.

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 cámaras así como fotografía de todas ellas.

Existen un total de dos cámaras en el establecimiento comercial; una situada en la parte destinada a exposición y venta, justo detrás del mostrador, y otra situada en el almacén de la tienda, frente a la puerta de acceso, sobre el botiquín de prevención de riesgos laborales y claramente visible, según se aprecia en la fotografía aportada por el



investigado y en el video aportado en la denuncia. El denunciado manifiesta que ambas cámaras son fijas.

Tal y como puede apreciarse a partir de la imagen del monitor que se aporta con capturas de las imágenes que captan las cámaras que conforman el sistema de videovigilancia, la cámara situada en la parte abierta al público del establecimiento comercial capta imágenes de la zona de exposición y venta del interior de la tienda y parte del pasillo de paso del Centro Comercial que discurre frente al local, apreciándose, en la parte superior de la imagen, una zona de ocio infantil. La cámara del interior del almacén capta imágenes del interior del mismo distinguiéndose bultos apilados y una serie de estanterías donde se guardan distintos objetos y productos. En relación a esta última cámara la representante de la sociedad investigada insiste en manifestar que el uso del espacio donde se ubica esta cámara es el de almacenaje de la mercancía existente y no el de vestuario, por lo que, cuando los empleados acceden a esta zona y hacen uso del mismo de una manera diferente a la que tiene asignada, conociendo además que existe una cámara, lo hacen bajo su propia responsabilidad.

7. En lo que respecta al sistema de monitorización, la representante del investigado aporta una fotografía de la pantalla de los que parece un centro de control y monitorización refiriendo que se trata de la Sala de CCTV de las Oficinas Centrales de la sociedad. Manifiesta que el acceso al sistema de videovigilancia para las empresas del Grupo El Corte Inglés, al que pertenece la sociedad investigada, está reservado al personal de la empresa MEGA2 SEGURIDAD, S.L., aportando copia de un contrato de arrendamiento de servicios de seguridad suscrito entre El Corte Inglés, S.A. y la referida empresa de seguridad.
8. El sistema graba las imágenes capturadas por las cámaras de forma cíclica y temporal, conservándose por un período de 7 días, salvo incidencia. La representante de la sociedad investigada manifiesta que, para acceder a las grabaciones es preciso estar identificado como personal autorizado y hacerlo mediante una clave. Refieren que la captura, transmisión y almacenamiento de las grabaciones se realiza mediante un sistema propietario, denominado PSS (Pro Surveillance System) de la empresa Dahua Technology, en dos grabadores que están ubicados en dependencias reservadas impidiendo así su difusión y visualización por personal no autorizado. Indican que la persona autorizada para acceder a las grabaciones es el Delegado de Seguridad Central para TELECOR.

Sin embargo, apreciadas discrepancias entre esta manifestación y lo referido tanto en la denuncia como en el Informe de la Inspección de Trabajo en relación a la visita de un técnico al establecimiento comercial para extraer manualmente las imágenes registradas por las cámaras, con fecha 28 de agosto de 2017 y número de salida ***REGISTRO.5 se requiere de nuevo a la sociedad investigada para identificar la ubicación física de los grabadores y aclarar los términos en que se realizó la extracción de las imágenes del sistema de videovigilancia. Con fecha 19 de septiembre de 2017 y número de salida ***REGISTRO.6 tiene entrada en esta Agencia escrito del investigado en el que refiere un error formal en su respuesta inicial, aclarando que existe un único grabador situado en el propio local de C.C.C. del Centro Comercial y para cuyo acceso se requiere usuario y contraseña, disponiéndose, por otro lado, de un visor software remoto de dicho grabador y al que se accede desde el Centro de Control de las Oficinas Centrales.

9. En relación al procedimiento seguido para la extracción de las imágenes registradas por las cámaras, la sociedad investigada refiere que, un técnico de la



empresa MEGA2 SEGURIDAD, S.L., encargada de los servicios de seguridad, se personó en el establecimiento comercial para extraer las imágenes de lo ocurrido a raíz de la denuncia de un hurto. Refiere que, aunque la forma habitual de proceder es visualizar las imágenes en remoto, debido a una incidencia en el sistema de control remoto no fue posible visualizar las imágenes de esta manera, personándose el técnico en el establecimiento comercial para extraer las imágenes y después entregarlas al Delegado de Seguridad que es la persona autorizada para su visualización.

El motivo por el que la extracción de dichas imágenes y la visualización de las mismas se hizo en presencia de otros empleados de la tienda, tal y cómo figura en la denuncia y en el Informe de la Inspección de Trabajo, no ha podido ser constatado después de realizadas las actuaciones de inspección, dado que la sociedad investigada no ha aclarado esa cuestión en la respuesta al requerimiento practicado por esta Agencia.

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 presente caso, D^a. **B.B.B.** denuncia la instalación en el establecimiento del **A.A.A.**, de una cámara de videovigilancia, sin señalar, en el interior del almacén, que también es usado por los empleados como vestuario, habiendo sido visualizadas imágenes registradas por la cámara de su persona.

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, se aportan fotografías de la existencia de cartel informativo de la existencia de las cámaras, situado a la entrada del establecimiento comercial. Dicho cartel es acorde 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, indicando que está a disposición de los ciudadanos en la propia tienda.

Ahora bien, en cuanto a la ubicación del cartel informativo, no es necesario que se coloque un cartel debajo de cada cámara, siendo suficiente conforme a lo dispuesto en el artículo 3 a) de la Instrucción 1/2006, *“Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados”* y en el caso que nos ocupa existe cartel a la entrada del establecimiento, que informa de la existencia de un sistema de videovigilancia.

En relación al procedimiento seguido para informar a los trabajadores de la



existencia de cámaras de videovigilancia en el local, se aporta copia del Sistema de Información para Empleado (S.I.E.) donde se informa a los trabajadores, por parte de la Dirección de la Empresa, de la existencia de sistemas de grabación continuada en el centro comercial y en zonas de trabajo, bien sean de acceso, tránsito, venta, elaboración y almacenamiento, y cuya finalidad es el control de la seguridad de las personas, bienes, instalaciones y mercancías a la venta. Asimismo, se informa de la posibilidad de utilizar el sistema para la detección de acciones irregulares, ya sean realizadas por personas ajenas a la empresa o por los propios trabajadores, utilizándose en ese caso para la imposición de sanciones disciplinarias por incumplimiento del contrato de trabajo.

En el mismo aviso se informa a los trabajadores del plazo de conservación de la imágenes, salvo incidencia, quién accede a las mismas así como de la existencia de hojas para ejercitar los derechos ARCO disponibles en los SAC de los Centros Comerciales.

Ahora bien, dado que la denuncia se centra en la falta de información a los trabajadores de la entidad, debe realizarse una serie de consideraciones respecto a la captación de imágenes en el entorno laboral.

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 negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento”*.

En el ámbito laboral, el Ordenamiento el Ordenamiento Jurídico Español, regula el aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre, los poderes de Dirección del empresario y es en ése articulado donde hallamos la oportuna legitimación.

El tratamiento de datos realizado en el centro de trabajo por medio de cámaras de video vigilancia 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, (ET), aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre, que 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. Y así lo ha venido reiterando la jurisprudencia en lo que a empleados públicos se refiere amparado en el art. 6.2 LOPD, como en Sentencia de la Sala Tercera del Tribunal Supremo de 2 de julio de 2007 (Rec. 5017/2003) que señala que el control del cumplimiento del horario de trabajo a que vienen obligados los empleados públicos es inherente a la relación que une a estos con la Administración en cuestión, y no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Asimismo, la Sentencia de la misma Sala de 2 de julio de 2007(Rec. 5017/2003) indica: *“Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa*



obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos".

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. 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"*.

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."*

La entidad denunciada como responsable del tratamiento, debe tener en cuenta la relación de proporcionalidad entre la finalidad perseguida y el modo en el que se tratan los datos, a fin de garantizar el cumplimiento de los principios de proporcionalidad y finalidad previstos por los apartados 1 y 2 del mencionado artículo 4 de la LOPD, siendo obligación del responsable del tratamiento adecuar el uso de los datos personales de modo que el impacto en los derechos de los afectados sea el mínimo posible.

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 el presente caso, de la documentación aportada se desprende que el citado establecimiento tiene cartel y formulario que informan de la existencia de un sistema de videovigilancia de conformidad con el artículo 3 a) y b) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo los trabajadores han sido informados de la

existencia de cámaras de videovigilancia en el local en el Sistema de Información para Empleado (S.I.E.) donde se recoge la finalidad de las mismas.

Por lo tanto, la entidad denunciada informa tanto los clientes, que acceden al establecimiento, como a sus trabajadores de la existencia de un sistema de videovigilancia, y su finalidad.

Ahora bien, respecto a la cuestión que se plantea relativa a la captación de imágenes de trabajadores en una zona de almacén que los mismos utilizan como vestuarios, cabe señalar que la cámara situada en el almacén, tal y como se aprecia en el vídeo de la denuncia y en las fotografías aportadas por la sociedad investigada en su escrito de respuesta, no es una cámara oculta. Se identifica claramente su ubicación al encontrarse justo frente a la puerta de acceso sobre el armario del botiquín de prevención de riesgos.

Asimismo, de la documentación aportada se desprende que el almacén donde se cambian los trabajadores, no es un recinto habilitado por la entidad para ser un vestuario, por lo que los trabajadores son conocedores tanto de la existencia de la cámara como que dicho recinto no es un área designada de vestuario. El uso de dicho espacio, donde se ubica la cámara objeto de denuncia, es el de almacenaje de la mercancía existente y no de vestuario. Cuestión distinta, que no entra dentro del área de competencia de esta Agencia, son las supuestas infracciones que a las disposiciones de seguridad y salud en los lugares de trabajo, así como laborales, pudiera suponer la inexistencia de vestuarios en dicho establecimiento.

Por último, el sistema graba las imágenes capturadas por las cámaras de forma cíclica y temporal, conservándose por un período de 7 días, salvo incidencia, constando inscrito el fichero denominado "VIDEOVIGILANCIA", en el Registro General de la Agencia Española de Protección de Datos.

La representante de la sociedad investigada aclara que existe un único grabador situado en el propio local de C.C.C.. del Centro Comercial y para cuyo acceso se requiere usuario y contraseña, disponiéndose, por otro lado, de un visor software remoto de dicho grabador y al que se accede desde el Centro de Control de las Oficinas Centrales.

En relación al procedimiento seguido para la extracción de las imágenes registradas por las cámaras, la sociedad investigada refiere que, un técnico de la empresa MEGA2 SEGURIDAD, S.L., encargada de los servicios de seguridad, se personó en el establecimiento comercial debido a un incidente de seguridad ocurrido en dicho local y del que consta una denuncia por hurto, siendo necesario visualizar las imágenes de lo sucedido ese día. Refiere que, aunque la forma habitual de proceder es visualizar las imágenes en remoto, debido a una incidencia en el sistema de control remoto no fue posible visualizar las imágenes de esta manera, personándose el técnico en el establecimiento comercial para extraer las imágenes y después entregarlas al Delegado de Seguridad que es la persona autorizada para su visualización.

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 **TELECOR, SA** y D^a. **B.B.B.**

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