

Expediente Nº: E/05301/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **D.D.D. (B.B.B.)** en virtud de denuncia presentada por D. **C.C.C. (COMITE DE EMPRESA B.B.B.)** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 22 de agosto de 2017 tiene entrada en esta Agencia escrito de D. **C.C.C. (COMITE DE EMPRESA B.B.B.)**, (en adelante el denunciante), comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad **B.B.B.** (en adelante el denunciado), instaladas en el establecimiento sito en el **D.D.D.**

El denunciante manifiesta que la entidad denunciada ha instalado cámaras ocultas en las dependencias de la cocina del hotel, sin informar a los representantes de los trabajadores, con captación de sonido. Adjunta una fotografía de una cámara de videovigilancia introducida en una carcasa de plástico similar a las carcasas de detectores de humo.

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

1. Con fecha 17 de octubre de 2017 se solicita información al responsable del establecimiento, teniendo entrada en esta Agencia con fecha 3 de noviembre de 2017 escrito del mismo del que se desprende:

- El sistema de videovigilancia ha sido instalado por la empresa VISOR SISTEMAS, inscrita en la Dirección General de Seguridad el Estado con el número ***Nº.1 Aportan copia del contrato de arrendamiento de servicios de instalación y mantenimiento de fecha 1 de marzo de 2013.
- De la documentación aportada, documento de seguridad, fotografías y planos, se desprende que el sistema de videovigilancia instalado en **D.D.D.** cuenta con 13 cámaras de videovigilancia, fijas sin funcionalidad de zoom ni movimiento.

Las cámaras se encuentran instaladas en: entrada principal, salida de emergencia, jardín, entrada personal, salida de emergencia planta 5, acceso playa, paseo playa, entrada mercancías, salida jardín, entrada baños personal, economato, cocina y sótano.

Según se desprende del plano de ubicación aportado, las cámaras recogen imágenes de espacios privativos del hotel.

La cámara identificada como nº 12, ubicada en la cocina recoge una panorámica de la misma.

- Las cámaras han sido instaladas con la finalidad de reforzar la seguridad de clientes y trabajadores y necesidad empresarial de llevar un control del cumplimiento por parte de los trabajadores de sus obligaciones.
- Aportan detalle del modelo de cartel informativo de la existencia de cámaras de videovigilancia y reportaje fotográfico de la ubicación de los mismos. Los carteles informan de la existencia de una

zona videovigilada y del responsable ante el que se puede ejercer los derechos de protección de datos de carácter personal.

Han sido colocados 5 carteles informativos en: jardín planta 6, entrada playa (2), entrada recepción y entrada de personal.

- Las imágenes se visualizan en un monitor ubicado en la recepción del hotel.
- A las imágenes grabadas solamente tiene acceso personal del hotel: el Director del hotel, el jefe de recepción y el jefe del servicio técnico, los cuales disponen de código de usuario y contraseña.
- Las imágenes son grabadas y se conservan durante un periodo de 30 días.
- El fichero de videovigilancia ha sido inscrito en el Registro General de Protección de Datos con el código **E.E.E.**
- Manifiestan que los trabajadores firman un documento denominado “**A.A.A.**” que incluye la siguiente cláusula: *“Informamos que en el caso de utilizarse sistemas de videovigilancia con finalidad de seguridad y control laboral, así como de controlar el acceso, las zonas vigiladas estarán convenientemente señalizadas. Aportan copia de uno de estos documentos firmado por un trabajador el 1 de diciembre de 2015.*
- Aportan copia de un escrito fechado el 27 de mayo de 2016 dirigido al Comité de Empresa de B.B.B., firmado por la dirección del hotel y por el Comité de empresa con el siguiente contenido:

“Por medio de la presente, la Dirección de esta empresa les recuerda, según lo recogido en el art. 20.3 en relación con el art. 64.1 del Estatuto de los trabajadores, que en nuestras instalaciones ubicadas en (C/...1), se encuentra instalado un sistema de video vigilancia desde el año 2011 cuya función es, entre otras y en lo que a este Comité concierne, vigilar y controlar el cumplimiento por parte de los trabajadores de sus obligaciones y deberes laborales pudiendo recurrir B.B.B. a las imágenes capturadas por las cámaras, al objeto de aplicar el régimen disciplinario previsto en el V Acuerdo Laboral de ámbito estatal para el sector de Hostelería y ponerlas en conocimiento de las autoridades judiciales oportunas.

Por tanto, esta empresa podrá hacer uso de las imágenes grabadas por el sistema de video vigilancia siempre que existan indicios o probadas razones de que por parte de algún miembro de la plantilla existan incumplimientos que presumiblemente puedan derivar en una infracción tipificada en el régimen disciplinario aplicable a la empresa. Todo ello, sin perjuicio de los visionados esporádicos que se puedan realizar por parte de la Dirección de las imágenes capturadas como control rutinario de la actividad diaria de la empresa, siempre con el único fin de vigilar y controlar.

Además, se les recuerda que las imágenes capturadas por este sistema de video vigilancia cumplen con lo regulado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, estando debidamente señalizadas los puntos donde se encuentran las cámaras, respetándose siempre los derechos específicos de los trabajadores, como por ejemplo, a la intimidad, en relación con espacios vetados a la utilización de este tipo de medios como vestuarios, baños, taquillas o zonas de descanso; o el derecho a la propia imagen de los trabajadores, además de la vida privada en el entorno laboral no registrando en particular las conversaciones privadas.”

2. Con 13 de diciembre de 2017 se solicita colaboración a la Comandancia de Puerto Rico de la Guardia Civil (Las Palmas), con objeto de determinar si en la cocina del hotel denunciado han sido instaladas cámaras ocultas y, en su caso, la finalidad de las mismas, teniendo entrada con fecha 22 de enero de 2018 un informe elaborado por Agentes de la citada Comandancia, en el que se pone de manifiesto lo siguiente:

- El día 21 de diciembre de 2017, a petición de la solicitud de colaboración efectuado desde la Inspección de Datos de esta Agencia, dos Agentes de la Guardia Civil se personan en el Hotel D.D.D.

y se trasladan, junto con la Directora del hotel a la cocina, comprobando que hay 4 cámaras de seguridad instaladas en recintos en los que se manipulan alimentos a baja temperatura. Estas cámaras se encuentran dentro de una cubierta de plástico que simula ser un detector de humo.

- Se desconoce si las cámaras están operativas, si bien la Directora manifiesta que se encuentran desconectadas.
- La directora manifiesta desconocer si existe algún grabador de las imágenes de estas cámaras, en cuyo caso podría estar en las dependencias de la empresa de seguridad que realizó la instalación (VISOR SEGURIDAD, S.L.).
- En relación con el motivo por el que han sido instaladas dichas cámaras, la Directora manifiesta que desconoce el motivo y que la instalación fue realizada por la empresa propietaria del hotel.
- Los agentes han solicitado información a la empresa de seguridad VISOR SEGURIDAD, S.L., cuyo escrito de respuesta aportan junto al informe y en el que pone de manifiesto lo siguiente:
 - o Las cámaras fueron instaladas a petición del cliente, ya que les manifestaron que había rumores de posibles robos en dicha área.
 - o Las cámaras no graban sonido. Aportan ficha técnica de las mismas.
 - o Las imágenes se conservaban durante 30 días.
 - o Al sistema accedía la Dirección del Hotel.

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 Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”*. Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”*.

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.”

El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.

Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma."

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

"1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia."

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

De acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas que las hacen identificadas o identificables y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

IV

En el presente expediente D. **C.C.C. (COMITE DE EMPRESA B.B.B.)**, comunica la posible infracción a la Ley Orgánica 15/1999 motivada por la instalación de cámaras de videovigilancia ocultas en las dependencias de la cocina del **D.D.D.**, sin informar a los representantes de los trabajadores.

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

Ahora bien, en esta cuestión, en primer lugar se plantea si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo, al amparo del artículo 6.1 de la LOPD.

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

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto.

Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

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

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

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

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

La concurrencia de estos requisitos resulta de difícil cumplimiento en el ámbito laboral. En consecuencia, vista la dificultad que entraña obtener el consentimiento, la Agencia Española de Protección de Datos, ha entendido que lo procedente es acudir a las normas que legitimen el tratamiento de los datos. Por tanto, en el ámbito laboral, el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en ése articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del Estatuto de los Trabajadores (ET) dispone que *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso”*.

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

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

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral.

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

A este respecto, debe tratarse por separado el sistema de videovigilancia instalado en la entidad, de las cámaras ocultas denunciada ubicadas en las dependencias de la cocina.

En primer lugar, respecto al sistema de videovigilancia, de la documentación aportada, se desprende que se instalaron con una doble finalidad: por un lado, las cámaras han sido instaladas con la finalidad de reforzar la seguridad de clientes y trabajadores y por otro lado, la necesidad empresarial de llevar un control del cumplimiento por parte de los trabajadores de sus obligaciones, al amparo de lo previsto en el art. 20.3 del RD 2/2015 de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

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

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

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

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

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

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

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

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

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

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

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

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

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

“ANEXO-

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

En el caso que nos ocupa, la entidad denunciada aporta fotografías de la existencia de carteles informativos de videovigilancia visibles y ubicados en los accesos a la zona videovigilada: jardín planta 6, entrada playa (2), entrada recepción y entrada de personal. Dichos carteles son acordes al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo, dispone de cláusula informativa, a disposición de los interesados, de conformidad con el artículo 3.b) de la Instrucción 1/2006.

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

Respecto a su vertiente de herramienta para el control laboral, la entidad manifiesta que los trabajadores firman un documento denominado “ **A.A.A.**” que incluye la siguiente cláusula: *“Informamos que en el caso de utilizarse sistemas de videovigilancia con finalidad de seguridad y control laboral, así como de controlar el acceso, las zonas vigiladas estarán convenientemente señalizadas. Aportan copia de uno de estos documentos firmado por un trabajador el 1 de diciembre de 2015.*

Asimismo aportan copia de un escrito fechado el 27 de mayo de 2016 dirigido al Comité de Empresa de B.B.B. firmado por la dirección del hotel y por el Comité de empresa con el siguiente contenido:

“Por medio de la presente, la Dirección de esta empresa les recuerda, según lo recogido en el art. 20.3 en relación con el art. 64.1 del Estatuto de los trabajadores, que en nuestras instalaciones ubicadas en (C/...1), se encuentra instalado un sistema de video vigilancia desde el año 2011 cuya función es, entre otras y en lo que a este Comité concierne, vigilar y controlar el cumplimiento por parte de los trabajadores de sus obligaciones y deberes laborales pudiendo recurrir B.B.B. a las imágenes capturadas por las cámaras, al objeto de aplicar el régimen disciplinario previsto en el V Acuerdo Laboral de ámbito estatal para el sector de Hostelería y ponerlas en conocimiento de las autoridades judiciales oportunas.

Por tanto, esta empresa podrá hacer uso de las imágenes grabadas por el sistema de video vigilancia siempre que existan indicios o probadas razones de que por parte de algún miembro de la plantilla existan incumplimientos que presumiblemente puedan derivar en una infracción tipificada en el régimen disciplinario aplicable a la empresa. Todo ello, sin perjuicio de los visionados esporádicos que se puedan realizar por parte de la Dirección de las imágenes capturadas como control rutinario de la actividad diaria de la empresa, siempre con el único fin de vigilar y controlar.

Además, se les recuerda que las imágenes capturadas por este sistema de video vigilancia cumplen con lo regulado en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, estando debidamente señalizadas los puntos donde se encuentran las cámaras, respetándose siempre los derechos específicos de los trabajadores, como por ejemplo, a la intimidad, en relación con espacios vetados a la utilización de este tipo de medios como vestuarios,

baños, taquillas o zonas de descanso; o el derecho a la propia imagen de los trabajadores, además de la vida privada en el entorno laboral no registrando en particular las conversaciones privadas.”

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

Respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos”

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.

El responsable del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se hace constar en la Instrucción 1/2006 , al señalar en su artículo 7 que *“1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.*

Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real."

En el caso que nos ocupa, consta la inscripción en el Registro General de la Agencia Española de Protección de Datos, por parte de la entidad denunciada, del fichero denominado "VIDEOVIGILANCIA".

Asimismo las imágenes se conservan durante 30 días, de conformidad con el artículo 6 de la citada Instrucción 1/2006, que recoge: *"Los datos serán cancelados en el plazo máximo de un mes desde su captación"*.

De la documentación aportada, documento de seguridad, fotografías y planos, se desprende que el sistema de videovigilancia instalado en **D.D.D.** cuenta con 13 cámaras de videovigilancia, fijas sin funcionalidad de zoom ni movimiento. Las cámaras se encuentran instaladas en: entrada principal, salida de emergencia, jardín, entrada personal, salida de emergencia planta 5, acceso playa, paseo playa, entrada mercancías, salida jardín, entrada baños personal, economato, cocina y sótano. Debe tenerse en cuenta la existencia de una cámara claramente visible en zona de cocina que capta una panorámica de la misma e identificada con el número 12 en las fotografías y planos aportados por la entidad denunciada.

En segundo lugar, respecto a la cámaras ocultas instaladas en las dependencias de la cocina (objeto de denuncia), el día 21 de diciembre de 2017, a petición de la solicitud de colaboración efectuado desde la Inspección de Datos de esta Agencia, dos Agentes de la Guardia Civil se personan en el Hotel D.D.D. y se trasladan, junto con la Directora del hotel a la cocina, comprobando que hay 4 cámaras de seguridad instaladas en recintos en los que se manipulan alimentos a baja temperatura. Estas cámaras se encuentran dentro de una cubierta de plástico que simula ser un detector de humo. Los agentes actuantes desconocen si las cámaras están en funcionamiento, si bien la Directora manifiesta que se encuentran desconectadas. No se encuentra en las instalaciones de la cocina ningún grabador o dispositivo de la señal que pudiesen emitir las cámaras. La directora manifiesta desconocer si existe algún grabador de las imágenes de estas cámaras. En relación con el motivo por el que han sido instaladas dichas cámaras, la Directora manifiesta que desconoce el motivo y que la instalación fue realizada por la empresa propietaria del hotel.

Solicitada por los agentes actuantes información a la empresa de seguridad VISOR SEGURIDAD, S.L.,(empresa de seguridad instaladora del sistema de videovigilancia denunciado, instalado en la cocina), ésta les aporta informe en el que se recoge que, las cámaras fueron instaladas a petición del cliente, ya que les manifestaron que había rumores de posibles robos en dicha área. Las cámaras no graban sonido. Aportan ficha técnica de las mismas. Las imágenes se conservaban durante 30 días.

Por tanto, de la documentación existente se desconoce la existencia o no de grabaciones con las cámaras, objeto de denuncia, ubicadas en el recinto de la cocina y si las hubiera, si éstas han sido utilizadas como prueba en procedimiento judicial.

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

breve duración al existir sospechas fundadas de que la falta de prendas y otros objetos del establecimiento mercantil obedecía a su sustracción por algún trabajador.

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

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

Al tratarse por ello de un supuesto episódico y de corta duración entiende el TSJM que *"sería absurdo exigir a la empresa una comunicación a los trabajadores de la instalación de unas cámaras de grabación advirtiéndoles "en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo", así como la colocación de carteles de publicidad ,pues de esta forma se arruinaría con toda seguridad la finalidad buscada".*

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

Más recientemente la Sentencia del TC 39/2016, de 3 de marzo, dictada con relación a un conflicto entre el uso de cámaras ocultas y los derechos de los trabajadores, ha dado un giro a los

criterios y efectos de la sentencia del TC 29/2013. La sentencia TC 39/2016 tiene origen en el despido de una trabajadora por apropiarse de dinero de caja del comercio en que prestaba sus servicios, conducta captada con cámaras instaladas ocultas por la empresa, no habiendo comunicado a los trabajadores dicha instalación pero sí habiéndose colocado en el escaparate del establecimiento, en lugar visible, el distintivo informativo de que el centro estaba vigilado. En esta sentencia se recoge: "(...) *Se ha cumplido en este caso con la obligación de información previa pues basta a estos efectos con el cumplimiento de los requisitos estos efectos con el cumplimiento de los requisitos específicos de información a través del distintivo de acuerdo con la Instrucción 1/2006. El trabajador conocía que en la empresa se había instalado un sistema de control por videovigilancia, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control. Lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario está obligado a solicitar el consentimiento de los trabajadores afectados. (...)*

En consecuencia, teniendo la trabajadora información previa de la instalación de la cámaras de videovigilancia, a través del correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el artículo 18.4 CE."

En consecuencia esta sentencia del TC estima que no se ha violado el derecho de protección de datos porque, dada la existencia de relación laboral entre las partes, no era preciso el consentimiento individual de los trabajadores, ni el colectivo, para la adopción de una medida de control de la actividad laboral y que la obligación de informar previamente del dispositivo instalado quedaba cumplida con la colocación del correspondiente distintivo avisando de su existencia, razón por la que acaba concluyendo que el proceder de la empresa supera el juicio de proporcionalidad.

La doctrina de esta sentencia ya la ha aplicado la Sala IV del Tribunal Supremo en sentencia de 7 de julio de 2016 (R. 3233/2010) en la que el Tribunal declara la validez de una prueba videográfica que motivó el despido disciplinario de una trabajadora, que había sido grabada hurtando productos de la empresa. Pues bien, el Tribunal declara la validez de la prueba utilizada, y concluye que en este caso existió un uso apropiado de la videovigilancia implantada, por los siguientes motivos: existían carteles que anunciaban la existencia de cámaras de videovigilancia; la trabajadora conocía en qué lugar se encontraban; las cámaras estaban instaladas en zonas comunes de trabajo; la grabación de conductas tuvo como detonante las múltiples pérdidas sufridas por la empresa. Por todo ello, el TS considera que la medida adoptada por la empresa superó el juicio de proporcionalidad, al ser idónea, necesaria y equilibrada.

Esta Agencia es conocedora de la reciente sentencia del 9 de enero de 2018, dictada por el Tribunal Europeo de Derecho Humanos (TEDH) en el que se condena al Estado Español a indemnizar por daño moral sufrido a las demandantes por no haber sido informadas debidamente de la existencia de cámaras ocultas en su centro de trabajo. Se trata de unas cajeras de supermercado que cometen hurtos de forma periódica y la empresa instala cámaras dirigidas a la salida del supermercado, a las cajas registradoras y la parte posterior de éstas (donde las cajeras almacenaban la mercancía por la que no se pagaba). La empresa informó al Comité de empresa y a los trabajadores acerca de las primeras pero no de las segundas, que se encontraban ocultas, que fueron las que captaron los hurtos que dieron lugar al despido de las trabajadoras. Sin embargo, aunque el caso pueda resultar en varias cuestiones similar al que se plantea en el presente expediente, existen algunas cuestiones que lo diferencian sustancialmente: en primer lugar el TEDH

aprecia, en la citada sentencia, que la proporcionalidad de las cámaras ocultas se destruye porque la medida no había sido selectiva, como sí había sucedido en otros casos previamente analizados por el Tribunal (Sentencia Kopke V. Alemania), es decir se captaban a todos los empleados y de forma continuada durante un largo periodo de tiempo; sin embargo en el caso que nos ocupa, la zona donde se encontraban las cámaras estaban limitadas a la zona de trabajo de la cocina, donde existía ya una cámara claramente visible (identificada con el número 12 por la entidad), y por lo tanto captaban a los empleados que ejercitaban su trabajo en dicha zona, respetando espacios vetados donde pueda desarrollarse la intimidad de los trabajadores. Además se desconoce si existen o no grabaciones realizadas por las mismas y de haberlas, si han sido aportadas como prueba a procedimiento judicial en el ejercicio de la tutela judicial efectiva.

A la vista de lo expuesto y en base a las sentencias descritas, 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:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **D.D.D. (B.B.B..) y 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