

Expediente Nº: E/03171/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **INFOSYSTEM, C.B. (A.A.A. Y B.B.B.)** en virtud de denuncia presentada por D^a. **C.C.C.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 22 de abril de 2016 tiene entrada en esta Agencia escrito de D^a. **C.C.C.** (en adelante la denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad **INFOSYSTEM, C.B.** (en adelante el denunciado) instaladas en **(C/...1)**. La denunciante manifiesta que la entidad denunciada ha instalado cámaras que enfocan su puesto de trabajo y la zona de entrada y atención al público, sin haber sido informada previamente.

Adjunta: reportaje fotográfico.

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 abril de 2016 se solicita información al responsable del establecimiento teniendo entrada en esta Agencia con fecha 30 de junio escrito de un comunero del denunciado en el que manifiesta:

1. No tiene instalado ningún sistema de videovigilancia sino un sistema de alarma contratado con la empresa **SECURITAS DIRECT**. Aporta copia del contrato y certificado de instalación.
2. El sistema de alarma solo funciona cuando se activa y se cierra la tienda. Consta con un detector de movimiento que capta imágenes si se activa la alarma.
3. Aporta fotografías de los elementos del sistema y del cartel instalado por la empresa.
 - a. Se comprueba que estas fotografías coinciden con las aportadas por la denunciante.
4. Aporta certificado de la empresa instaladora de que la grabación de imágenes se produce por salto de la alarma con captación de movimiento del fotodetector.

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

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 los establecido en el artículo 3 de la Ley Orgánica 15/1999...”.

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

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

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

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

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

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

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

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

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

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

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

III

En el presente caso, D^a. **C.C.C.** denuncia la instalación de cámaras de videovigilancia que enfocan su puesto de trabajo, sin haber sido informada previamente.

Por lo tanto, la denuncia formulada se refiere a la instalación de cámaras en un centro de trabajo, por lo que procede establecer los requisitos necesarios a los efectos de la normativa de protección de datos.

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

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

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

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

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

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

El apartado 2 del artículo 6 de la LOPD exime del necesario consentimiento cuando los datos se refieran “a las partes de un contrato o precontrato 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 en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en éste articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del texto refundido de la Ley 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 humana y teniendo en cuenta la capacidad real de los trabajadores con discapacidad”.

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

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

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, 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, como establece la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero de 2013, debe ir precedido de *“una información previa y expresa, precisa, clara e inequívoca a los trabadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, 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”*.

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.

Por lo tanto la entidad denunciada podría utilizar cámaras de videovigilancia tanto

con una finalidad de seguridad de las personas e instalaciones como a efectos de control laboral siempre y cuando se cumpla, en uno y otro caso, con el deber de información en la forma descrita.

Una vez realizadas las aclaraciones precedentes; la Inspección de Datos de esta Agencia solicita información al denunciado, teniendo entrada contestación del mismo manifestando que no tiene instalado ningún sistema de videovigilancia sino un sistema de alarma contratado con la empresa **SECURITAS DIRECT**. Aporta copia del contrato y certificado de instalación. Así, El sistema de alarma solo funciona cuando se activa y se cierra la tienda. Consta con un detector de movimiento que capta imágenes por foto y se activa la alarma. Aporta fotografías de los elementos del sistema y del cartel instalado por la empresa.

Asimismo aporta certificado de la empresa instaladora de que *“este tipo de elementos solo realizan grabación de imágenes cuando se produce un salto de alarma con captación de movimiento del fotodetector, ya que en el momento en que el sensor capta movimiento, estando la alarma conectada, realiza las fotografías para identificar el motivo del salto (...)”*.

Asimismo atendiendo a la información de la empresa instaladora SECÚRITAS DIRECT, se desprende que:

El sistema de seguridad homologado por el Ministerio del Interior, cuenta con elementos de protección electrónicos a través de Verificación por imágenes, para cumplimiento de las exigencias normativas del artículo 48 del Reglamento de Seguridad Privada y artículo 8 de la Orden INT 316/2011 de 1 de febrero sobre funcionamiento de sistemas de alarma en el ámbito de la Seguridad Privada, compuesto por los siguientes elementos de detección contra intrusión:

- o Elemento de detección Magnético, ubicado en la zona descrita como “Almacén”.*
- o Elemento de detección Fotodetector, ubicado en la zona descrita como “Entrada”.*
- o Elemento de detección Fotodetector ubicado en la zona descrita como “Tienda”.*

Cuando el sistema de seguridad se encuentra armado/conectado por el cliente, los elementos de detección que incorporan verificación por vídeo (imagen) de acuerdo con las exigencias descritas en el artículo 8 de la Orden citada, captan movimiento (funciona como detector volumétrico) y además capta y graba cinco fotogramas seguidos para comprobación de la realidad del salto de alarma producido en el inmueble protegido.

SECÚRITAS DIRECT ESPAÑA S.A.U tendrá a su cargo la custodia de las imágenes obtenidas como consecuencia de los saltos de alarma generados por

el sistema de seguridad (...)

*De conformidad con la Ley Orgánica 15/99 de Protección de Datos y la normativa de desarrollo, el cliente ha autorizado a SECÚRITAS DIRECT el tratamiento de datos de carácter personal, que serán incluidos en un fichero denominado "FICHERO CLIENTES", siendo inscrito en el Registro General de Protección de Datos con el código nº ***CÓD.1".*

Por lo tanto, a la vista de la documentación se desprende que el sistema de captación de seguridad denunciado, no consta de cámaras o dispositivos de captación y grabaciones de imágenes instaladas en modo local, es decir dicho sistema no capta imágenes de manera ininterrumpida sino que solamente capta o graba una imagen, en caso de que el sistema de alarma salte a consecuencia de una posible intrusión en la zona que protege el detector. Así, cuando el sistema de seguridad se encuentra armado/conectado por el cliente, los elementos de detección que incorporan verificación por vídeo (imagen), captan movimiento (funciona como detector volumétrico) y además capta y graba cinco fotogramas seguidos para comprobación de la realidad del salto de alarma producido en el inmueble protegido. A tal efecto SECÚRITAS DIRECT ESPAÑA S.A.U tenía a su cargo la custodia de las imágenes obtenidas como consecuencia de los saltos de alarma generados por el sistema de seguridad y por tanto, tiene inscrito el fichero denominado "FICHERO CLIENTES", en el Registro General de Protección de Datos.

A la vista de lo expuesto, el sistema instalado no cumple una finalidad de control laboral, ni se informa, en consecuencia, del uso de sus imágenes a tal fin.

A la vista de todo lo expuesto, se procede al archivo del presente expediente de actuaciones previas al no apreciarse vulneración a la actual normativa en materia de protección de datos.

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 **INFOSYSTEM, C.B. (A.A.A. Y B.B.B.)** y a D^a. **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