



Expediente Nº: E/03225/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **SECRETARÍA GENERAL DEL SERVICIO ANDALUZ DE SALUD - HOSPITAL REINA SOFIA** en virtud de denuncia presentada por **VARIOS DENUNCIANTES** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 25 de febrero de 2014 tienen entrada en esta Agencia escritos remitidos por **VARIOS TRABAJADORES**, comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en las instalaciones del **HOSPITAL UNIVERSITARIO REINA SOFÍA** sito en **(C/...1)** de **CÓRDOBA** y cuyo titular es **SECRETARÍA GENERAL DEL SERVICIO ANDALUZ DE SALUD** (en adelante el denunciado).

En los mencionados escritos se manifiesta: *“la instalación de un sistema de cámaras de videovigilancia en el área común del Taller de Mantenimiento, sito en el complejo del Hospital Universitario Reina Sofía, entre cuyas finalidades se presume el control laboral, sin información previa al personal que presta sus servicios en dicha zona”.*

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 30 de junio de 2016 se solicita información al responsable del sistema.

Del análisis de las manifestaciones y documentación recibida con fechas 21 y 28 de julio de 2016, se desprende lo siguiente:

La SECRETARÍA GENERAL DEL SERVICIO ANDALUZ DE SALUD es la titular y responsable del fichero denominado VIDEOVIGILANCIA, publicado en BOJA nº 18 de 28 de enero de 2010, según lo dispuesto en la Orden de 28 de diciembre de 2009 por la que se crea entre otros ficheros, el denominado “Videovigilancia” con datos de carácter personal del Servicio Andaluz de Salud.

Se inscribe en el Registro General de Protección de Datos con el código *****CÓD.1.**

La finalidad declarada, es la vigilancia en el control de acceso a los edificios y dependencias en los que se ubica el Servicio Andaluz de Salud con el fin de garantizar la seguridad entre otros del personal que presta servicios, de los ciudadanos que acceden, de las instalaciones y del equipamiento.

Adicionalmente se delega la gestión de los ficheros de videovigilancia en las Direcciones Gerencias de los Centros, por lo que en este caso concreto, por

delegación,> la responsabilidad del fichero recae en el HOSPITAL UNIVERSITARIO REINA SOFÍA (HURS).

Se acompaña documentación acreditativa en el Anexo 1.

El sistema de videovigilancia forma parte del Servicio de Vigilancia y Seguridad del Complejo Hospitalario, que actualmente está desempeñado por la empresa SECURITAS SEGURIDAD ESPAÑA S.A. El contrato de servicio contempla la instalación y el mantenimiento de los equipos de videovigilancia.

En documento Anexo 7 se adjunta copia del contrato de servicio suscrito entre las partes con fecha 31 de julio de 2014 y en documento Anexo 2 consta la autorización emitida por la DGP que habilita a la citada empresa de seguridad.

Existen carteles informativos de zona videovigilada ubicados en las zonas próximas a las cámaras y en las zonas comunes de todos los centros que componen el Complejo Hospitalario.

Se adjunta reportaje fotográfico (Anexo 3)

El Hospital dispone de un procedimiento operativo estandarizado POE-SEG-001 para el ejercicio de los derechos ARCO, en el cual se contempla el procedimiento de acceso a los sistemas de videovigilancia e incluye el modelo de cláusula informativa sobre el tratamiento de datos con la finalidad de seguridad a través de sistema de videovigilancia.

En documento Anexo 4 se incorpora copia del Procedimiento corporativo ARCO para la atención a la ciudadanía y del procedimiento operativo estandarizado, específico del HURS documento operativo de fecha 30 de septiembre de 2010.

Respecto al sistema de cámaras instalado, se distribuye entre los distintos centros que integran el Complejo Hospitalario, a saber: Consultas externas, Edificio de Gobierno, Hospital General, Hospital Materno Infantil, Hospital Los Morales, Hospital Provincial, Anatomía Patológica y Talleres, Lavandería y Galerías Sótano, Quirófanos y vestuarios Hospital General, Parking Personal, Edificio 061 y Galerías (Urgencias), Videosafe Central térmica (punto limpio), Gases medicinales, Videofase Club de Diálisis, Centro de transformación, Tanatorio, Nueva Plataforma Logística, IMIBIC, CARE y CRTS.

Actualmente se encuentran en funcionamiento un total de 450 cámaras, cuya orientación cubre las diversas áreas de accesos, pasillos, zonas comunes y zonas técnicas.

Del análisis de la documentación gráfica adjunta (Anexo 5), relativa al sistema de cámaras instalado con las imágenes captadas por cada una de ellas y los planos de situación en cada uno de los centros del Complejo Hospitalario, cabe distinguir:

- o 71 cámaras se localizan en diversas áreas exteriores, distribuidas entre los 13 módulos que integran el Complejo Hospitalario. Captan espacios de las vías públicas que los comunican y de las áreas exteriores adyacentes a los mismos.*
- o El resto de cámaras recogen áreas interiores de los respectivos módulos y de las zonas exteriores inmediatas.*

Los monitores de visualización se localizan en el puesto permanente de Seguridad.

Se acompaña reportaje fotográfico (Anexo 6).

El personal con acceso al sistema pertenece a la empresa externa que presta el servicio de Vigilancia y Seguridad en el Complejo Hospitalario.

En documento Anexo 7 se aporta copia del contrato de servicio suscrito entre las partes con fecha 31 de julio de 2014.

El sistema de grabación de imágenes está compuesto por CCTV con cámaras analógicas conectadas a videograbadores distribuidos en los diferentes recintos conectados a la red informática corporativa HURS. Todos los videograbadores se gestionan para la monitorización de las cámaras en el centro de control de seguridad, mediante PC's que incorporan el software de gestión con palabra clave y password.

Las imágenes se almacenan durante 15 días, no sobrepasando en ningún caso el plazo máximo establecido en la LOPD.

El sistema de videovigilancia no se encuentra conectado a central de alarmas.

En relación al sistema de cámaras ubicado en el ÁREA COMÚN DEL TALLER DE MANTENIMIENTO, se menciona que su instalación es debida a determinadas incidencias ocurridas en la zona, de las cuales se adjuntan escritos emitidos por el Maestro Industrial así como escrito de solicitud de instalación de cámaras de videovigilancia formulado por el Jefe de Servicio de Mantenimiento, de fecha 1 de diciembre de 2015, solicitando la instalación de cámaras de videovigilancia en base a desapariciones de diverso material (Anexo 8).

En Anexo 9 se adjunta reportaje fotográfico de las cámaras instaladas en dicha zona y de las imágenes captadas por cada una de ellas, de cuyo análisis se observa:

- o Cuatro cámaras exteriores perimetrales, cuyas imágenes captan la vía de acceso y entrada a los talleres (dirección reprografía y punto limpio).*
- o Tres cámaras interiores, que recogen diversos espacios de pasillo, mostrador y talleres de mantenimiento.*
- o La existencia de cartel informativo de zona videovigilada instalado en el interior del Taller, en el que se indica como responsable la Admón. del Hospital Universitario Reina Sofía ante quien poder ejercitar los derechos ARCO.*
- o El procedimiento empleado para informar a los trabajadores que prestan sus servicios en el área de Mantenimiento, se realizó mediante:*

La programación y ejecución de actividades formativas, tanto a nivel general del HURS como específicos para las



categorías profesionales que se integran en el Servicio de Mantenimiento, cuyo contenido estuvo orientado al Plan de Concienciación de Protección de Datos

Se acompaña documentación acreditativa, con el calendario de los cursos impartidos durante el período 2008-2011 y el material docente impartido relativo a videovigilancia (Anexo 10).

La cartelería informativa de la instalación de cámaras de videovigilancia en las zonas afectadas.

La información verbal a los trabajadores de las incidencias por las cuales se solicitó e instalaron las cámaras de videovigilancia.

Asimismo, ante la demanda de información sobre la legalidad de los equipos instalados en el área de Mantenimiento, el Responsable de Seguridad formuló un informe de fecha 2012, cuyo objeto es el análisis de las prácticas comentadas por los trabajadores de SS.GG desde el punto de vista de la privacidad y de la LOPD, tratando de dar respuesta a las cuestiones planteadas por los mismos (Anexo 11).

Además, con carácter general el Responsable de Seguridad de la información en el HURS redactó, con fecha 3 de julio de 2014, un "Resumen de Condiciones para la instalación de cámaras de videovigilancia con fines de control empresarial" (Anexo 12).

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 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.

III

En el presente expediente varios trabajadores denuncian la instalación de un sistema de cámaras de videovigilancia en el área común del Taller de Mantenimiento, sito en el complejo del Hospital Universitario Reina Sofía, entre cuyas finalidades se presume el control laboral, sin consentimiento ni información previa al personal que presta sus servicios en dicha zona.

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.

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

En el ámbito laboral, el Ordenamiento el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 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 Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley 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 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 trabajadores 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.

En el caso que nos ocupa, al sistema de cámaras instalado, se distribuye entre los distintos centros que integran el Complejo Hospitalario, a saber: Consultas externas, Edificio de Gobierno, Hospital General, Hospital Materno Infantil, Hospital Los Morales, Hospital Provincial, Anatomía Patológica y Talleres, Lavandería y Galerías Sótano, Quirófanos y vestuarios Hospital General, Parking Personal, Edificio 061 y Galerías (Urgencias), Videosafe Central térmica (punto limpio), Gases medicinales, Videofase Club de Diálisis, Centro de transformación, Tanatorio, Nueva Plataforma Logística, IMIBIC, CARE y CRTS. Actualmente se encuentran en funcionamiento un total de 450 cámaras, cuya orientación cubre las diversas áreas de accesos, pasillos, zonas comunes y zonas técnicas.

La denuncia planteada se refiere a las cámaras instaladas en el taller de mantenimiento. A este respecto la entidad manifiesta que su instalación fue debida a determinadas incidencias ocurridas en la zona, de las cuales se adjuntan escritos emitidos por el Maestro Industrial así como escrito de solicitud de instalación de cámaras de videovigilancia formulado por el Jefe de Servicio de Mantenimiento, de fecha 1 de diciembre de 2015, solicitando la instalación de cámaras de videovigilancia en base a desapariciones de diverso material

Por lo tanto la finalidad de la instalación del sistema en la citada zona era la seguridad ante la desaparición de determinados materiales de dicha zona.

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 carteles informativos de la existencia de las cámaras, acorde al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD, en las zonas próximas a las cámaras y en las zonas comunes de todos los centros que componen el Complejo Hospitalario. Asimismo, se aporta fotografía de la existencia de cartel informativo de zona videovigilada instalado en el interior del taller.

El Hospital dispone de un procedimiento operativo estandarizado POE-SEG-001 para el ejercicio de los derechos ARCO, en el cual se contempla el procedimiento de acceso a los sistemas de videovigilancia e incluye el modelo de cláusula informativa sobre el tratamiento de datos con la finalidad de seguridad a través de sistema de videovigilancia.

Igualmente se aporta cláusula informativa a disposición de los interesados, de conformidad con el artículo 3 b) de la citada Instrucción. En dicha cláusula se recoge



“Que sus datos personales se incorporarán a un fichero denominado “VIDEOVIGILANCIA” del que es responsable este organismo (...) y serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia”.

Respecto al procedimiento empleado para informar a los trabajadores de la finalidad por la cual se han instalado las cámaras, manifiestan que se realizó mediante:

La programación y ejecución de actividades formativas, tanto a nivel general del HURS como específicos para las categorías profesionales que se integran en el Servicio de Mantenimiento, cuyo contenido estuvo orientado al Plan de Concienciación de Protección de Datos. Se acompaña documentación acreditativa, con el calendario de los cursos impartidos durante el período 2008-2011 y el material docente impartido relativo a videovigilancia.

Asimismo, ante la demanda de información sobre la legalidad de los equipos instalados en el área de Mantenimiento, el Responsable de Seguridad formuló un informe de fecha 2012, cuyo objeto es el análisis de las prácticas comentadas por los trabajadores de SS.GG desde el punto de vista de la privacidad y de la LOPD, tratando de dar respuesta a las cuestiones planteadas por los mismos.

Ahora bien, en este informe del responsable de seguridad ya se recogía que *“no constaba que se hubiera llevado a cabo información personal a todos los trabajadores, sugiriendo que se llevase a cabo una información a todos los trabajadores del hospital (en todo caso, al menos a los trabajadores de mantenimiento) mediante formación on line. Otra Opción sería la difusión a través de sesiones presenciales a través de los cargos intermedios”.*

No obstante no consta ni se han presentado pruebas por parte de los denunciantes que acredite que el sistema de videovigilancia sea utilizado para fines distintos que la propia seguridad de las instalaciones, personal y equipamiento del centro. Igualmente dicha cuestión deberá ser tenida en cuenta por la citada entidad para que en el caso que se quiera realizar un control laboral a través de las cámaras, cuestión que como se ha recogido no requiere el consentimiento del trabajador, se proceda a informar a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral, con *“una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida”.*

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 puedan acceder a las instalaciones como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado, sin que conste su utilización a efectos de control laboral ni se informe, en consecuencia, del uso de sus imágenes a tal fin.

IV

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.”

El artículo 20.1 de la LOPD, establece que la creación, modificación o supresión de ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario Oficial

correspondiente. Por su parte el artículo 53.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, determina que cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

En el caso que nos ocupa, la Secretaría General del Servicio Andaluz de Salud es la titular y responsable del fichero denominado VIDEOVIGILANCIA, publicado en BOJA nº 18 de 28 de enero de 2010, según lo dispuesto en la Orden de 28 de diciembre de 2009 por la que se crea entre otros ficheros, el denominado "Videovigilancia" con datos de carácter personal del Servicio Andaluz de Salud.

Consta inscrito en el Registro General de Protección de Datos el fichero denominado "VIDEOVIGILANCIA" en fecha 09/03/2010 y modificado el 05/11/2013.

La finalidad declarada, es la vigilancia en el control de acceso a los edificios y dependencias en los que se ubica el Servicio Andaluz de Salud con el fin de garantizar la seguridad entre otros del personal que presta servicios, de los ciudadanos que acceden, de las instalaciones y del equipamiento.

Asimismo, las imágenes se almacenan durante 15 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".

Por lo tanto, a la vista de todo lo expuesto, se procede el 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 y el ANEXO I a **SECRETARÍA GENERAL DEL SERVICIO ANDALUZ DE SALUD - HOSPITAL REINA SOFIA**
- 3. NOTIFICAR** a cada uno de los **DENUNCIANTES** la presente Resolución y exclusivamente el Anexo que le corresponda, en el que se incluye su identificación.

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 el artículo 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