

Expediente N°: E/04977/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el **HOSPITAL CARLOS HAYA DE MALAGA** en virtud de denuncia presentada por el **SINDICATO JUNTA MEDICA DE CARLOS HAYA** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 13 de mayo de 2013 tiene entrada en esta Agencia escrito del representante legal del sindicato **JUNTA MÉDICA DE CARLOS HAYA** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999, de 13 de diciembre, motivada por cámaras de videovigilancia cuyo titular es la entidad **HOSPITAL CARLOS HAYA DE MALAGA** (en adelante el denunciado) instaladas en "lugares de dominio público que pudieran vulnerar el derecho a la intimidad de los trabajadores del centro", en el complejo hospitalario "**HOSPITAL CARLOS HAYA DE MALAGA**" ubicado en **C.C.C..**

Obra en el expediente copia de la Resolución de Archivo de Actuaciones dictada por esta Agencia Española de Protección de Datos, de fecha 31 de mayo de 2012, dimanante del expediente E/03999/2011, incoado como consecuencia de denuncia presentada contra el propio hospital con fecha 22 de junio de 2011, y que dio lugar a las actuaciones que constan en el expediente tramitado y resuelto en la referida fecha.

Obra en el referido expediente **E/03999/2011**, el anterior informe del Hospital denunciado, remitido a la Agencia el 12 de enero de 2012, así como otro, complementario del anterior, de fecha 20 de marzo de 2012, y registro de entrada en la Agencia de 27 de marzo de 2012.

En la citada denuncia, de fecha 22 de junio de 2011, se expone que por parte del Hospital se ha procedido a la instalación de entre 65 y 70 cámaras de vigilancia, no cumpliéndose los requisitos establecidos legalmente.

De acuerdo con la citada Resolución:

"Respecto a la información facilitada a los trabajadores, del sistema de videovigilancia, se aporta documentación del procedimiento utilizado para informar a los trabajadores, tanto del Servicio Andaluz de Salud, como de empresas externas, así como documentación acreditativa de cumplimiento de precitado procedimiento.

El citado procedimiento de información dispone de una hoja de control de modificaciones en la que se indica que el documento fue creado en junio de 2009 y revisado en octubre de 2010. Pertenece a los procedimientos generales existentes en el Documento de Seguridad de la Información Corporativa del Servicio Andaluz de Salud (S.A.S.) En él se trata el derecho de información al paciente y usuarios, así como información a los trabajadores mediante información expresa a sus Representantes y

mediante Plan de Formación. Se incluye también el derecho de información a los trabajadores de empresas externas. Se adjunta una cláusula informativa, el cartel de zona videovigilada, informes de seguimiento, entre los que se encuentra un informe enviado a los representantes de los trabajadores del SAS (Junta de Personal), controles del procedimiento, indicadores de nivel de cumplimiento (entre los que se encuentra el Plan de Formación a trabajadores del SAS).

Se adjunta también una Nota de Circulación Interior de fecha 28/07/2009 firmada por el Subdirector de Servicios Generales con una cláusula informativa y los formularios de ejercicio de los derechos ARCO.

Asimismo, se incluye una Nota Informativa, de fecha 29/06/2010, remitida por el Ingeniero Técnico de Seguridad a la Junta de Personal, comunicando la existencia de equipos de videovigilancia para “ejercer la vigilancia y protección de bienes muebles e inmuebles, así como la protección de las personas que pueden encontrarse en los mismos”. Este mismo documento se ha enviado también a diversas empresas externas, entre la que se encuentra EULEN SEGURIDAD, a la que se le envió el 3/01/2012). Igualmente, en esta misma fecha, se le hizo entrega del documento de seguridad de la información corporativa de videovigilancia.

Se adjunta igualmente, una lista de unas 775 personas que han asistido a un curso de “Sensibilización Protección de Datos” impartido en 2010 y 2011, así como copia de la Guía de Videovigilancia de la Agencia Española de Protección de Datos.

Por lo tanto el Hospital denunciado, cumple el deber de información, en cuanto al sistema de videovigilancia, recogido en el artículo 5 de la LOPD, anteriormente transcrito.”

En virtud del citado Acuerdo, “A la vista de todo lo expuesto, se procede al archivo del presente expediente de actuaciones previas al no apreciarse por parte del organismo denunciado, vulneración a la actual normativa en materia de protección de datos.”

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 12 de noviembre de 2013 y número de salida 301880/2013, por parte de la Inspección de Datos de ésta Agencia, se solicita información al responsable del Centro Hospitalario, acerca de los posibles “cambios realizados en el sistema de videovigilancia instalado en el HOSPITAL CARLOS HAYA DE MÁLAGA en relación al anterior informe remitido a ésta Agencia en fecha 12/01/2012”.

Con fecha de registro de entrada 9/12/2013, tiene entrada en ésta Agencia “Informe Técnico” correspondiente a nuestra nueva solicitud, en la que:

*“Se indica que el sistema de Videovigilancia del Hospital Regional Universitario Carlos Haya de Málaga, no ha sufrido cambios y/o modificaciones algunas desde la emisión del último informe a la Agencia Española de Protección de Datos, el pasado día 19/03/2012. Con registro de Salida en el HRUCH nº *****, fecha 20/03/2012, hora 12:35:55”.*

Según se aprecia, el citado informe, de fecha 20 de marzo de 2012, y registro de entrada en la Agencia de 27 de marzo de 2012, obra incorporado –asimismo- en el expediente **E/03999/2011**, habiendo servido de base para la Resolución del mismo.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 presente expediente de actuaciones previas parte de los mismos hechos denunciados en el expediente E/03999/2011, con fecha de entrada en esta Agencia el 22 de junio de 2011, la existencia de un sistema de videovigilancia en el HOSPITAL CARLOS HAYA DE MALAGA que pudiera vulnerar la normativa de protección de datos.

Dicho expediente de actuaciones E/03999/2011, se resolvió con el archivo del mismo en fecha 31 de mayo de 2012, tal y como se transcribe a continuación:

<<HECHOS

SEGUNDO: *Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:*

El representante del HOSPITAL REGIONAL UNIVERSITARIO CARLOS HAYA, mediante escrito con fecha de entrada en la Agencia de 27/01/2012, manifiesta lo siguiente como consecuencia de la solicitud de información remitida por la inspectora responsable de las presentes actuaciones:

*1.El Hospital y sus centros dependientes (Hospital General, Hospital Materno Infantil, Hospital Civil y Centro de Alta Resolución y Especialidades José Estrada) son centros de titularidad pública perteneciente al Servicio Andaluz de Salud, que se encuadra en la Consejería de Salud de la Junta de Andalucía. Todos los centros del Servicio de Salud tienen el mismo CIF *****.*

2.El sistema de videovigilancia se instaló en la década de los 90, habiendo sido instalado, ampliado y mantenido por diversas empresas de seguridad privada, siendo la última EULEN SEGURIDAD, SA, que presta sus servicios desde el 1/09/2009 hasta la

actualidad. Se adjunta copia del último contrato en vigor, de fecha 1/12/2011 (Anexo 1).

Dicha empresa se encarga de la seguridad y vigilancia de los bienes muebles e inmuebles que conforman el conjunto del Hospital, así como el mantenimiento de los sistemas técnicos de seguridad instalados en el Centro, entre ellos el de videovigilancia.

Observaciones: En el contrato de fecha 30/11/2011 aportado se indica que queda sujeto a los Pliegos de Cláusulas Administrativas Particulares y Prescripciones Técnicas correspondientes.

Se adjunta también copia del contrato “de protección de datos” de fecha 1/12/2011, entre cuyas cláusulas se encuentran varias que hacen referencia a la condición de Encargado del Tratamiento de EULEN SEGURIDAD.

3.El sistema se instaló fundamentalmente para obtener un mayor grado de calidad del servicio, mejor organización, mejor control de recursos humanos y materiales, vigilancia de los controles de acceso a los edificios y dependencias con el fin de garantizar la seguridad del personal que presta sus servicios a los ciudadanos que acceden a las instalaciones y equipamiento.

4.Se adjunta en el Anexo 2 listado de fotografías de los diferentes accesos a los edificios, donde puede constatarse la ubicación de los correspondientes carteles informativos.

Observaciones

Se adjuntan 37 fotografías de otros tantos accesos a los centros del complejo hospitalario.

5.Se adjuntan en los Anexos 3 a 7, los modelos de formularios informativos a disposición de los ciudadanos: cláusula informativa, formulario para el ejercicio de los derechos ARCO. El procedimiento establecido para distribuir los formularios ante una solicitud se difunde mediante una nota interior de fecha 28/07/2009 a las Subdirecciones de Atención al Ciudadano y Recursos Humanos (Anexo 21).

Observaciones

En los citados Anexos se encuentra la siguiente documentación: Nota de Circulación Interior, nota informativa, formularios para ejercer los derechos ARCO.

6.En el Anexo 8 se detalla el nº de cámaras, lugares en los que se encuentran, disponibilidad de zoom, posibilidad de movimiento y cuántas de ellas son exteriores. No hay cámaras instaladas en el exterior de ninguno de los centros del complejo.

Algunas cámaras están instaladas en el interior del recinto de algunos centros, concretamente en el Hospital General, Hospital Materno Infantil y Hospital Civil, aunque sin posibilidad de acceso al exterior (vía pública) del recinto. Se adjuntan planos de los recintos interiores de los centros del Hospital en los que se ubican cámaras.

Anexo 9: Recinto interior del Hospital General

Anexo 10: Recinto interior del Hospital Materno Infantil.

Anexo 11: Recinto interior del Hospital Civil.

Anexo 12: Plano del recinto interior del centro de Alta Resolución y Especialidades José Estrada.

Sólo una de las cámaras instaladas en los recintos interiores tiene incorporado zoom y posibilidad de movimiento. Es la nº 29 y se encuentra en el Hospital General. Sin embargo, actualmente no pueden ser utilizadas estas funciones por los usuarios del sistema de videovigilancia.

Observaciones

En la relación de cámaras aportada se puede comprobar que en el Hospital General hay 12 cámaras que captan imágenes del recinto y 32 que las captan del interior. De todas ellas, sólo una dispone de zoom (la numerada como cámara 29, ubicada en la subida exterior del Pabellón de Gobierno). Esta misma cámara también es la única que tiene posibilidad de movimiento.

En el Hospital Materno Infantil se dispone de 4 cámaras en el recinto y 12 interiores. Ninguna dispone de zoom o movimiento.

En el Hospital Civil hay 4 cámaras en el recinto y 13 interiores. Ninguna dispone de zoom o movimiento.

En el Centro de Alta Resolución y Especialidades José Estrada hay 4 cámaras interiores. Ninguna dispone de zoom o movimiento.

7.En el Anexo 13 se facilitan las fotografías de las cámaras instaladas en el interior del recinto y en el 14, fotografías de las imágenes captadas por cada una de las cámaras interiores, visualizadas sobre el monitor de videovigilancia.

8.Se adjuntan fotografías de las dependencias donde se utilizan monitores. (Anexo 15 Hospital General y Anexo 16 Hospital Materno Infantil). Así mismo en los Anexos 17 y 18 se adjuntan planos de las dependencias donde se ubican (Hospital General y Hospital Materno Infantil respectivamente). En el Hospital General se visualizan 32 cámaras y en el Materno Infantil 15.

9.NO es posible el acceso a las imágenes por terceros no autorizados ni en el Hospital General ni en el Hospital Materno Infantil, ya que existe en cada puesto un vigilante de seguridad encargado de realizar el visionado y garantizar la no accesibilidad de terceros no autorizados a las imágenes. Además, en ambos casos, el diseño y disposición de los monitores no permite el visionado de las imágenes desde ningún ángulo excepto desde la ubicación del propio vigilante de seguridad, y en el caso de que éste deba abandonar temporalmente su puesto por motivos justificados y contemplados en la prestación del servicio, existe un dispositivo que permite la desconexión de los monitores, accionado mediante una llave que custodia el propio vigilante.

10.Las medidas de seguridad del Hospital General y del Hospital Materno Infantil, son las siguientes:

-Vigilancia por vigilantes de seguridad durante las 24 horas del día, los 365 días al

año.

- Sistema de alimentación eléctrico de emergencia alternativo al habitual.
- Sistema de detección de incendios.
- Sistema de protección contra incendio, tales como extintores, bocas de incendio equipadas, ...
- Salidas de emergencias alternativas a las existentes.
- Cámaras de videovigilancia ubicadas en los accesos.
- Cámaras de videovigilancia ubicadas en las dependencias.

Observaciones

No se citan medidas de conformidad con el Reglamento de Seguridad.

11.El perfil de las personas con acceso al sistema son cargos funcionales del complejo hospitalario, tales como Director Gerente, Director de Servicios Generales, Subdirector de Servicios Generales, Ingeniero Técnico Industrial e Ingeniero Técnico responsable de Seguridad, tal y como se detalla en el anexo técnico nº 13 del documento de seguridad de la información corporativa de videovigilancia del HRUCH. Así mismo, la empresa de Seguridad Privada tiene permiso de acceso, en virtud del contrato de servicios y contrato de nombramiento de encargado de tratamiento (Anexo 1). Los perfiles son los mismos ya indicados.

12.El sistema de grabación está formado por videograbadores conectados a las cámaras, que almacenan las imágenes en disco duro. El acceso a las imágenes le corresponde a la empresa de seguridad, como encargada del tratamiento del sistema.

13.El plazo de almacenamiento de las imágenes en los diferentes videograbadores nunca es superior a un mes.

14.Ubicación de los locales donde se sitúan los dispositivos de grabación:

- Hospital General. Planta sótano del Pabellón "A", local junto al Mortuorio.
- Hospital Materno Infantil. Planta baja edificio, local junto a la entrada del Laboratorio.
- Hospital Civil. Planta baja, local junto a Rehabilitación
- Centro de Resolución de Especialidades. Planta tercera, local junto a Sala de Reuniones.

15.Medidas de seguridad en las dependencias donde se ubican los videograbadores, son:

- Sistema de alimentación eléctrico de emergencia alternativo al habitual.
- Sistema de detección de incendios.
- Sistema de protección contra incendio, mediante extintores, bocas de incendio equipadas,...
- Cámaras de videovigilancia ubicadas en los accesos. Cámaras de videovigilancia ubicadas en su interior. Dependencias con alarma anti-intrusismo. Sala técnica con cerradura y permanentemente cerrada. - Acceso restringido a su interior solo a personal autorizado.
- Procedimiento de acceso solo a personal autorizado a estas dependencias.

No se citan medidas de conformidad con el Reglamento de Seguridad.

16.El código de inscripción del fichero relativo a la videovigilancia es el 2100681167, creado por la Secretaria General del Servicio Andaluz de Salud.

Se ha comprobado que el fichero inscrito con el código indicado es el denominado "Videovigilancia", con fecha de inscripción de 9/03/2010.

17.En el Anexo 22 se encuentra copia del documento de seguridad de la información corporativa de videovigilancia.

Observaciones

El citado documento consta de 38 páginas y trata aspectos de la seguridad relacionados con su organización, funciones y obligaciones del personal (de todo el personal, del responsable de la información de videovigilancia, del de sistemas y tecnologías de la información, del de bases de datos, del de aplicaciones, etc...), definición de perfiles, procedimientos de información, de gestión de derechos ARCO y de relaciones contractuales con empresas externas con acceso a la información corporativa. También procedimientos de accesos al sistema, gestión de soportes, uso de los ficheros en soporte papel, uso del correo electrónico, etc.

18.En el Hospital Regional Universitario Carlos Haya (HRUCH) de Málaga, no existe en la actualidad ningún sistema de videovigilancia conectado a central de alarmas.

19.Se adjunta en el Anexo nº 19, procedimiento utilizado para Informar a trabajadores, tanto del Servicio Andaluz de Salud, como de empresas externas, así como documentación acreditativa de cumplimiento de precitado procedimiento.

El citado procedimiento de información dispone de una hoja de control de modificaciones en la que se indica que el documento fue creado en junio de 2009 y revisado en octubre de 2010. Pertenece a los procedimientos generales existentes en el Documento de Seguridad de la Información Corporativa del Servicio Andaluz de Salud (S.A.S.)

En él se trata el derecho de información al paciente y usuarios, así como información a los trabajadores mediante información expresa a sus Representantes y mediante Plan de Formación. Se incluye también el derecho de información a los trabajadores de empresas externas. Se adjunta una cláusula informativa, el cartel de zona videovigilada, informes de seguimiento, entre los que se encuentra un informe enviado a los representantes de los trabajadores del SAS (Junta de Personal), controles del procedimiento, indicadores de nivel de cumplimiento (entre los que se encuentra el Plan de Formación a trabajadores del SAS).

Se adjunta también una Nota de Circulación Interior de fecha 28/07/2009 firmada por el Subdirector de Servicios Generales con una cláusula informativa y los formularios de ejercicio de los derechos ARCO.

Así mismo se incluye una Nota Informativa, de fecha 29/06/2010, remitida por el Ingeniero Técnico de Seguridad a la Junta de Personal, comunicando la existencia de equipos de videovigilancia para “ejercer la vigilancia y protección de bienes muebles e inmuebles, así como la protección de las personas que pueden encontrarse en los mismos”. Este mismo documento se ha enviado también a diversas empresas externas, entre la que se encuentra EULEN SEGURIDAD, a la que se le envió el 3/01/2012). Igualmente, en esta misma fecha, se le hizo entrega del documento de seguridad de la información corporativa de videovigilancia.

Se adjunta una lista de unas 775 personas que han asistido a un curso de “Sensibilización Protección de Datos” impartido en 2010 y 2011, así como copia de la Guía de Videovigilancia de la Agencia Española de Protección de Datos.

20. En la actualidad existen dos dependencias donde se ubican monitores, que posibilitan el visionado y control operativo de la videovigilancia, uno en el Área de Urgencias Generales del Hospital General y otro en el Área de Urgencias de Maternidad del Hospital Materno Infantil.

21. Respecto a las cámaras instaladas en el Centro de Control Operativo de Videovigilancia y la Central Receptora de Alarmas:

-El HRUCH no dispone de ninguna dependencia que se utilice como central receptora de alarmas.

-En los ya citados Anexos 16 y 17 se adjuntan planos de las dependencias.

-En la dependencia del Hospital General se ubica una cámara y en la dependencia del Hospital Materno Infantil se dispone una cámara en la entrada del Área de Urgencias de Maternidad.

-La finalidad de su instalación, en el marco general del propósito de la instalación

del sistema de videovigilancia, concretamente en el ámbito de los accesos a Urgencias Generales y de Maternidad del complejo hospitalario, es la de constituir el soporte tecnológico necesario para garantizar la seguridad de todos los usuarios y profesionales del HRUCH, los cuales accedan y/o desarrollen su labor profesional en estas áreas, de modo que se facilite con su implementación el apoyo y soporte imprescindibles para custodiar y velar por el orden y seguridad ante situaciones antisociales que puedan acontecer en estas dependencias específicas del complejo hospitalario, concretamente la vigilancia en el control de acceso a los edificios y dependencias en los que se ubica el Hospital Regional Universitario Carlos Haya, con el fin de garantizar la seguridad del personal que presta servicios a los ciudadanos que acceden a las instalaciones y equipamiento.

-Las cámaras instaladas en estas dependencias no disponen de zoom ni posibilidad de movimiento.

- En el Anexo 20 se facilitan las fotografías de las diferentes cámaras de seguridad instaladas en estas dependencias, con indicación expresa del nº con el cual se identifica en la planimetría de situación.

- En el Anexo 13 se detallan y relacionan fotografías de las imágenes que capta cada una de las cámaras interiores del recinto de cada centro, visualizadas sobre el monitor de videovigilancia, indicándose el nº de cámara que capta dicha imagen.

Dado que el denunciante aporta como “Foto 5” una fotografía que podría captar imágenes de la vía pública, es por lo que se solicita al HOSPITAL REGIONAL UNIVERSITARIO CARLOS HAYA DE MALAGA información al respecto.

El representante del HOSPITAL REGIONAL UNIVERSITARIO CARLOS HAYA, mediante escrito con fecha de entrada en la Agencia de 27/03/2012, manifiesta lo siguiente:

- *La ubicación concreta de la cámara que aparece en la fotografía, dado que desconocen su procedencia y si ha sido manipulada ó no, suponen que es la señalizada como nº29 en el Plano del Anexo 9 del Informe emitido por el HRUCH en fecha 25/01/2012 (que ha tenido entrada el día 27/01/12) .*
- *Se ratifica la información anteriormente remitida, tal y como se detalla en el informe emitido por el HRUCH en fecha 25/01/2012, en el cual se cita literalmente "...solo existe una única cámara que tenga Incorporado zoom y posibilidad de movimiento, concretamente la cámara nº 29 instalada en el recinto del Hospital General, aunque actualmente no pueden ser utilizadas estas funciones...", ya que el dispositivo que controla el zoom y el movimiento de la precitada cámara se encuentra desmontado y almacenado en armario metálico y despacho bajo llave, tal y como se puede constatar en fotos nº 1, 2 y 3 que se adjuntan, pudiéndose verificar además en la fotografía nº4 que en el puesto de control de videovigilancia del Hospital General no existe ningún mecanismo ni dispositivo que permita el zoom o el movimiento de dicha cámara.*
- *Se adjunta fotografía nº5 del visionado actual de la cámara, coincidente con la aportada en el Informe emitido por el HRUCH en fecha 25/01/2012.*
- *Conforme a lo ya expresado, no existe actualmente posibilidad de utilizar el zoom o mover la cámara de referencia.*

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 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, se denuncia por el representante de la Sección Sindical CCOO en el HRUCH, la instalación de un sistema de videovigilancia en el citado Hospital que podría vulnerar la normativa de protección de datos.

En primer lugar, procede entrar a valorar el cumplimiento del deber de información e inscripción de ficheros por parte del organismo denunciado.

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 presente caso, se aporta por el centro hospitalario, fotografías de la

existencia de cartel informativo de zona videovigilada instalado en 31 accesos al complejo hospitalario, acordes al previsto en el artículo 3.a) de la Instrucción 1/2006, en relación con el artículo 5 de la LOPD. También se aporta copia del formulario informativo a disposición de los interesados, de conformidad con el artículo 3.b) de la citada Instrucción, y formularios para el ejercicio de los derechos ARCO. El procedimiento establecido para distribuir los formularios ante una solicitud se difunde mediante una nota interior de fecha 28 de julio de 2009, a las Subdirecciones de Atención al Ciudadano y Recursos Humanos.

Respecto a la información facilitada a los trabajadores, del sistema de videovigilancia, se aporta documentación del procedimiento utilizado para informar a los trabajadores, tanto del Servicio Andaluz de Salud, como de empresas externas, así como documentación acreditativa de cumplimiento de precitado procedimiento.

El citado procedimiento de información dispone de una hoja de control de modificaciones en la que se indica que el documento fue creado en junio de 2009 y revisado en octubre de 2010. Pertenece a los procedimientos generales existentes en el Documento de Seguridad de la Información Corporativa del Servicio Andaluz de Salud (S.A.S.) En él se trata el derecho de información al paciente y usuarios, así como información a los trabajadores mediante información expresa a sus Representantes y mediante Plan de Formación. Se incluye también el derecho de información a los trabajadores de empresas externas. Se adjunta una cláusula informativa, el cartel de zona videovigilada, informes de seguimiento, entre los que se encuentra un informe enviado a los representantes de los trabajadores del SAS (Junta de Personal), controles del procedimiento, indicadores de nivel de cumplimiento (entre los que se encuentra el Plan de Formación a trabajadores del SAS).

Se adjunta también una Nota de Circulación Interior de fecha 28/07/2009 firmada por el Subdirector de Servicios Generales con una cláusula informativa y los formularios de ejercicio de los derechos ARCO.

Asimismo, se incluye una Nota Informativa, de fecha 29/06/2010, remitida por el Ingeniero Técnico de Seguridad a la Junta de Personal, comunicando la existencia de equipos de videovigilancia para “ejercer la vigilancia y protección de bienes muebles e inmuebles, así como la protección de las personas que pueden encontrarse en los mismos”. Este mismo documento se ha enviado también a diversas empresas externas, entre la que se encuentra EULEN SEGURIDAD, a la que se le envió el 3/01/2012). Igualmente, en esta misma fecha, se le hizo entrega del documento de seguridad de la información corporativa de videovigilancia.

Se adjunta igualmente, una lista de unas 775 personas que han asistido a un curso de “Sensibilización Protección de Datos” impartido en 2010 y 2011, así como copia de la Guía de Videovigilancia de la Agencia Española de Protección de Datos.

Por lo tanto el Hospital denunciado, cumple el deber de información, en cuanto al sistema de videovigilancia, recogido en el artículo 5 de la LOPD, anteriormente transcrito.

Por otro lado, 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 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.

Pues bien, consta inscrito el fichero denominado VIDEOVIGILANCIA en el Registro General de la Agencia Española de Protección de datos, creado por la Secretaría General del Servicio Andaluz de Salud mediante Orden de 28 de diciembre de 2009 por la que se crean ficheros, entre ellos videovigilancia, publicado en BOJA nº 18 de fecha 28 de enero de 2010.

Asimismo, el sistema de grabación está compuesto por una serie de videograbadores que tiene conectado mediante cable las diferentes cámaras de vigilancia. Estos videograbadores almacenan las imágenes en disco duro. El plazo de almacenamiento de las imágenes en los diferentes videograbadores nunca es superior a un mes, de conformidad con el artículo 6 de la Instrucción 1/2006, que señala: "Los datos serán cancelados en el plazo máximo de un mes desde su captación".

IV

Una vez analizado el deber de información e inscripción de ficheros, procede analizar el apartado 1 y 2 del artículo 6 de la LOPD, que disponen:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Respecto a la legitimación en el tratamiento de las imágenes, la respuesta se encuentra en el artículo 2 de la Instrucción 1/2006, que establece que: "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”.

Así, hasta la entrada en vigor, el pasado 27 de diciembre de 2009, de la Ley 25/2009, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y sus ejercicio (conocida como “Ley Ómnibus”), la legitimación del tratamiento de los datos de carácter personal en materia de videovigilancia, a excepción de los casos, prácticamente imposibles dada su dificultad práctica, en los que se hubiera obtenido el consentimiento inequívoco de cada una de las personas que resulten captadas o grabadas como consecuencia del uso de las cámaras, puede proceder, en función del ámbito de aplicación, bien de la Ley 23/1992, de 30 de julio, de Seguridad Privada (en adelante LSP), o bien de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Así hasta la entrada en vigor de la citada Ley 25/2009, la legitimación para el tratamiento la legitimación para el tratamiento por particulares y empresas de imágenes captadas a través de dispositivos de videovigilancia sólo era posible en caso de que dichos sistemas hubieran sido contratados con empresas de seguridad privada, debidamente acreditadas ante el Ministerio del Interior, al que además debía notificarse el contrato que se hubiese celebrado, conforme a lo exigido por la Ley 23/1992, de 30 de julio de Seguridad Privada.

La Ley 25/2009 ha suprimido para la mayor parte de los casos estas exigencias, al liberalizar la comercialización, entrega, instalación y mantenimiento de estos dispositivos, de forma que ya no será necesario acudir para su puesta en funcionamiento a una empresa de seguridad privada ni cumplir las obligaciones de notificación del contrato al Ministerio del Interior..

En concreto el artículo 14 de la nueva Ley modifica el artículo 5.1 e) de la Ley 23/1992, de 30 de julio de Seguridad Privada, añadiendo una Disposición Adicional Sexta a la Ley de Seguridad Privada con la siguiente redacción:

“Disposición Adicional Sexta. Exclusión de las empresas relacionadas con equipos técnicos de seguridad:

Los prestadores de servicios y las filiales de empresas de seguridad que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarma, quedan excluidas de la legislación de seguridad privada, siempre y cuando no se dediquen a ninguno de los otros fines definidos en el artículo 5, sin perjuicio de otras legislaciones específicas que pudieran resultarles de aplicación.”

La interpretación de la mencionada disposición determina que cualquier particular o empresa cuya actividad no sea la propia de una empresa de seguridad privada

podrá; “vender, entregar, instalar y mantener equipos técnicos de seguridad” sin necesidad de cumplir las exigencias previstas en la Ley de Seguridad Privada para tales empresas. De este modo, dado que la Ley permite la instalación y mantenimiento de dichos equipos por empresas distintas a las de seguridad privada, legitima a quienes adquieran de estos dispositivos para tratar los datos personales derivado de la captación de las imágenes sin necesidad de acudir a empresas de seguridad privada, siendo dicho tratamiento conforme a lo previsto en la Ley Orgánica de Protección de Datos de Carácter Personal.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma, sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora; esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho Departamento.

En todo caso, el tratamiento de las imágenes deberá cumplir los restantes requisitos exigibles en materia de protección de datos de Carácter Personal, recogidos en la Ley Orgánica y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, como son, entre otros, los relativos a que las imágenes que se capten sean las necesarias y no excesivas para la finalidad perseguida; el deber de informar a los interesados, tanto a través de la colocación de carteles informativos como mediante la puesta a disposición de aquéllos de impresos en que se detalle la información; la notificación de la existencia de los ficheros a la Agencia Española de Protección de Datos; o la implantación de medidas de seguridad.

En el caso que nos ocupa, el HRUCH no dispone de ninguna dependencia que se utilice como central receptora de alarmas.

El HRUCH tiene formalizado contrato de servicios con la empresa de seguridad EULEN SEGURIDAD S.A., que presta sus servicios desde el 1/09/2009 hasta la actualidad. Aporta copia del último contrato en vigor, de fecha 30/11/2011. EULEN, es la encargada de la seguridad y vigilancia de los bienes muebles e inmuebles que conforman el conjunto del hospital, así como el mantenimiento de los sistemas técnicos de seguridad instalados en el mismo, entre ellos el sistema de videovigilancia. Asimismo, el citado Hospital tiene formalizado contrato para el tratamiento de datos personales, con la citada empresa, como encargada del tratamiento, de conformidad con lo dispuesto en el artículo 12 de la LOPD.

V

Por último, respecto al cumplimiento por parte del centro denunciado de las medidas de seguridad, cabe decir que se aporta por el mismo copia del documento de seguridad de la información corporativa de videovigilancia. El citado documento consta de 38 páginas y trata aspectos de la seguridad relacionados con su organización, funciones y obligaciones del personal (de todo el personal, del responsable de la información de videovigilancia, del de sistemas y tecnologías de la información, del de

bases de datos, del de aplicaciones, etc...), definición de perfiles, procedimientos de información, de gestión de derechos ARCO y de relaciones contractuales con empresas externas con acceso a la información corporativa. También procedimientos de accesos al sistema, gestión de soportes, uso de los ficheros en soporte papel, uso del correo electrónico, etc.

Asimismo, no es posible el acceso a las imágenes por terceros no autorizados ni en el Hospital General ni en el Hospital Materno Infantil, ya que existe en cada puesto un vigilante de seguridad encargado de realizar el visionado y garantizar la no accesibilidad de terceros no autorizados a las imágenes. Además, en ambos casos, el diseño y disposición de los monitores no permite el visionado de las imágenes desde ningún ángulo excepto desde la ubicación del propio vigilante de seguridad, y en el caso de que éste deba abandonar temporalmente su puesto por motivos justificados y contemplados en la prestación del servicio, existe un dispositivo que permite la desconexión de los monitores, accionado mediante una llave que custodia el propio vigilante.

El perfil de las personas con acceso al sistema son cargos funcionales del complejo hospitalario, tales como Director Gerente, Director de Servicios Generales, Subdirector de Servicios Generales, Ingeniero Técnico Industrial e Ingeniero Técnico responsable de Seguridad, tal y como se detalla en el anexo técnico nº 13 del documento de seguridad de la información corporativa de videovigilancia del HRUCH. Así mismo, la empresa de Seguridad Privada tiene permiso de acceso, en virtud del contrato de servicios y contrato de nombramiento de encargado de tratamiento.

Respecto a las medidas de seguridad en las dependencias donde se ubican los videograbadores, son: sistema de alimentación eléctrico de emergencia alternativo al habitual, sistema de detección de incendios, sistema de protección contra incendio, mediante extintores, bocas de incendio equipadas,...; cámaras de videovigilancia ubicadas en los accesos, cámaras de videovigilancia ubicadas en su interior, dependencias con alarma anti-intrusismo, sala técnica con cerradura y permanentemente cerrada, acceso restringido a su interior solo a personal autorizado, procedimiento de acceso solo a personal autorizado a estas dependencias.

Finalmente señalar que la denuncia realizada por el representante de la Sección Sindical CCOO del Hospital Regional Universitario Carlos Haya de Málaga, respecto a EULEN SEGURIDAD, se está tramitando actualmente en otro expediente de actuaciones previas E/00333/2012, siéndole comunicada, en su día, la resolución que se adopte en el citado expediente.

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

III

Ante la existencia de una nueva denuncia con fecha de entrada en esta Agencia 13 de mayo de 2013, contra el Hospital denunciado, por los mismos hechos

denunciados en el E/ 03999/2011, con fecha de resolución de archivo 31 de mayo de 2012, por parte de la Inspección de Datos de ésta Agencia, se solicita información en fecha 12 de noviembre de 2013, al responsable del Centro Hospitalario, acerca de los posibles *“cambios realizados en el sistema de videovigilancia instalado en el HOSPITAL CARLOS HAYA DE MÁLAGA en relación al anterior informe remitido a ésta Agencia en fecha 12/01/2012”*.

Con fecha de registro de entrada 9/12/2013, tiene entrada en ésta Agencia “Informe Técnico” correspondiente a nuestra nueva solicitud, en la que: *“Se indica que el sistema de Videovigilancia del Hospital Regional Universitario Carlos Haya de Málaga, no ha sufrido cambios y/o modificaciones algunas desde la emisión del último informe a la Agencia Española de Protección de Datos, el pasado día 19/03/2012. Con registro de Salida en el HRUCH nº *****, fecha 20/03/2012, hora 12:35:55”*.

Por lo tanto, dado que el presente expediente E/04977/2013, parte de los mismos hechos, y denunciado que el E/03999/2011, habiéndose procedido a la resolución de archivo del E/03999/2011, por los motivos transcritos, y no habiéndose producido ninguna modificación en el sistema de videovigilancia del hospital, desde el informe realizado de fecha 19 de marzo de 2012, así como ante la ausencia de nueva información que pudiera modificar la resolución transcrita, se procede al archivo del presente expediente de actuaciones previas.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución al **HOSPITAL CARLOS HAYA DE MALAGA** y al **SINDICATO JUNTA MEDICA DE CARLOS HAYA**.

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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

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 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos