



Expediente N°: E/03579/2014

## RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidades **AEROPUERTOS ESPAÑOLES DE SEGURIDAD AEREA S.A.**, y **SEGUR IBERICA S.A.**, en virtud de denuncia presentada por D. **A.A.A. Y OTROS** y teniendo como base los siguientes

### HECHOS

**PRIMERO:** Con fecha 20 de marzo de 2014 tiene entrada en esta Agencia escrito remitido por D. **A.A.A. (REPRESENTANTE DEL SECRETARIADO CONFEDERAL NACIONAL del SINDICATO INTERSINDICAL CANARIA)**, D. **B.B.B. (PRESIDENTE DEL COMITÉ DE EMPRESA DE SEGURIBÉRICA S.A. en el centro de trabajo del Aeropuerto Tenerife Norte)**, D. **C.C.C. (DELEGADO DEL COMITÉ DE EMPRESA SEGUR IBERICA S.A.)** Y D. **D.D.D. (DELEGADO DE PREVENCIÓN DE RIESGOS LABORALES Y EN REPRESENTACIÓN DE INTERSINDICAL CANARIA)** (en adelante los denunciantes) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por los tratamientos de imágenes llevados a cabo en el **AEROPUERTO TENERIFE NORTE** sito en **AEROPUERTO DE LOS RODEOS, TENERIFE NORTE, LOS RODEOS** por la empresa **SEGUR IBÉRICA S.A** y **AEROPUERTOS ESPAÑOLES DE SEGURIDAD AÉREA S.A** (en adelante los denunciados).

En su escrito los denunciantes manifiestan que la empresa **SEGUR IBÉRICA S.A.**, a raíz de la comunicación de la imposición de tres sanciones a trabajadores (con la categoría de vigilantes de seguridad) por una serie de supuestos acontecidos el día 4 de febrero de 2014, ha llevado a cabo una visualización del sistema de cámaras con fines ajenos a la seguridad aeroportuaria. Asimismo se ha podido observar cómo personal no autorizado visualizaba las grabaciones, ubicadas en el cuarto de Registro de discos duros de las grabaciones de CCTV, cuyo acceso (bajo el control del respectivo Jefe de Equipo) se encuentra limitado y protegido mediante un código asignado a los usuarios autorizados respectivamente por el Departamento de Seguridad de **AENA**.

Adjuntan a su denuncia: (1) Copia del escrito de Escritura de Elevación a Público de Acuerdos Sociales adoptados con fecha 2 de abril de 2011 por el Congreso Confederal Nacional de la Confederación Intersindical Canaria, (2) Copia del Acta de Constitución del Comité de Empresa del centro de trabajo de **SEGUR IBÉRICA S.A.**, Vigilantes de Seguridad Aeropuerto Tenerife Norte, (3) Tres copias de “*cartas de sanción a trabajadores de la empresa*” remitidas por **SEGUR IBÉRICA SA** al Comité de Empresa del Aeropuerto Tenerife Norte y en las que con fecha 24 de febrero de 2014 se les comunica respectivamente a los trabajadores afectados: “*la decisión de sancionarles por la comisión de faltas laborales MUY GRAVES (tipificadas en el art. 53.4 del Convenio Colectivo Nacional de Empresas de Seguridad) detectadas durante la Auditoría efectuada los días 4, 5 y 6 de febrero de 2014 por la Agencia Estatal de Seguridad Aérea y puestas de manifiesto en las grabaciones de los hechos, dejando constancia las imágenes de los mismos*”.

**SEGUNDO:** Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el

esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Con fecha 3 de julio de 2014 se solicita información a la mercantil **SEGUR IBÉRICA S.A** en relación el contrato habilitante para la prestación del servicio de Seguridad en el **AEROPUERTO DE LOS RODEOS TENERIFE NORTE** suscrito con **AENA** y la información relativa al tratamiento de las imágenes captadas por el sistema en el ejercicio de las funciones de sus trabajadores, junto a las medidas de seguridad adoptadas durante el desarrollo del mismo.
2. Con fecha 3 de julio de 2014 se solicita información a la entidad **AEROPUERTOS ESPAÑOLES DE SEGURIDAD AÉREA S.A**, en calidad de responsable del sistema de videovigilancia instalado en el **AEROPUERTO DE LOS RODEOS, TENERIFE NORTE**, teniendo entrada en esta Agencia escrito de fecha 29 de julio de 2014 en el que la Adjunta a la Dirección de Asesoría Jurídica y Gestión Patrimonial manifiesta:

*La mercantil **AENA AEROPUERTOS S.A** es la responsable del sistema de videovigilancia instalado.*

*Tanto en el Programa Nacional de Seguridad (Capítulo 2 “Seguridad en los aeropuertos”) como en los Programas de Seguridad de los Aeropuertos, en aplicación del mismo Programa Nacional de Seguridad, amparan la instalación y aplicación de estos sistemas de vigilancia además de las patrullas físicas y uso de la vigilancia privada.*

*La Ley 5/2014 de 4 de abril de Seguridad Privada, desarrolla un nuevo marco jurídico para este sector y actividad.*

Se adjunta recopilatorio de la normativa de aplicación (documento Anexo 1).

*Los sistemas de seguridad en el citado Aeropuerto llevan instalados más de 15 años y en constante evolución. La empresa que realizó la instalación originalmente fue **IKUSI SIS S.A** y desde el año 2010 hasta la actualidad han intervenido las siguientes empresas: **IKUSI, TECOSA y SIMAVE**.*

En documento Anexo 2 se adjunta copia del contrato suscrito con la empresa instaladora IKUSI con fecha 25/06/2012, cuyo objeto es: “Suministro con instalación de un control de accesos para el Aeropuerto de Tenerife Norte”.

*La finalidad del sistema de videovigilancia responde a la Seguridad Aeroportuaria y la garantía en la aplicación óptima de las medidas de seguridad de la aviación civil reflejadas en el Programa Nacional de Seguridad para la Aviación Civil (PNS).*

*Para poder cumplir con la exigencia normativa del PNS, las Fuerzas y Cuerpos de Seguridad del Estado tienen una responsabilidad que implica que se pongan a su disposición todos los medios disponibles en los aeropuertos para garantizar la seguridad de las instalaciones.*

*Existen carteles informativos de zona videovigilada, en los*

*cuales se indica a “Aena” como responsable del fichero de los datos recogidos por las cámaras, informando de la dirección donde poder ejercitar los derechos ARCO.*

*Se encuentran ubicados respectivamente en la Zona de Bandejas del Filtro Interinsular, Filtro Nacional y Control C.*

*El escrito incluye reportaje fotográfico.*

*Asimismo en documento Anexo 3 se adjunta el modelo de formulario informativo debidamente cumplimentado, existente a disposición del público en el Aeropuerto.*

*Los monitores de visualización se ubican en el centro de control CCTV, localizado en la dependencia aeroportuaria CTRL-C (se aportan fotografías del lugar y del CCTV).*

*El acceso a la sala CCTV está restringido a los vigilantes de seguridad de la empresa SEGUR IBÉRICA, los cuales custodian la llave de entrada. La autorización de este personal a la sala va implícita en el servicio de vigilancia contratado.*

*Además en el CCTV hay un vigilante 24H que también controla el acceso a la sala.*

*La visualización de las imágenes además está autorizada al siguiente personal:*

- o Ejecutivos de servicio. Tienen acceso desde la oficina situada en una zona restringida y bajo llave. Acceden al software de visualización mediante usuario y contraseña.*
- o Director del Aeropuerto, Jefe de la Oficina de Seguridad, Técnico de Seguridad y Empleados de mantenimiento (SIMAVE). Este personal accede a las visualizaciones desde sus respectivas oficinas dotadas con medidas de seguridad, mediante la validación de usuario y contraseña.*

*Puntualmente, previa petición a la Oficina Local de Seguridad, existen accesos de las FFCCS quedando registrados en el Parte Diario de Vigilante.*

*La entrega de las grabaciones a las FFCCS o a un Juzgado, se realiza en todo caso previa petición de oficio (LO 2/1986).*

*Se relaciona el personal con acceso al sistema de videovigilancia:*

- o Vigilantes contratados por la empresa de seguridad SEGUR IBÉRICA, así como su responsable en el Aeropuerto (Responsable del Expediente de Seguridad).*

*El servicio de vigilancia contratado con SEGUIR IBÉRICA S.A está contratado para realizar las funciones de seguridad aeroportuaria. Entre sus funciones destacan:*

*Inspección de pasajeros y equipajes en filtros de seguridad.*

*Inspección de equipajes de bodega.*

*Vigilancia perimetral del recinto aeroportuario.*

*Vigilancia y control de accesos a zonas restringidas.*

*Seguridad de Terminales y Zonas de Acceso Controladas.*

*Coordinación de seguridad: centro de control remoto y servicios asociados.*

Se acompaña copia del contrato suscrito por la empresa de seguridad y **AENA AEROPUERTOS S.A.**, con fecha 24/05/2013, en el seno del expediente número SEG \*\*\*/12 y cuyo objeto es: “la prestación por parte de **SEGUIR IBÉRICA S.A** de un servicio de Vigilancia y Protección” (documento Anexo 4).

- o *Por cuestiones inherentes al expediente de mantenimiento del sistema, pueden acceder el personal de mantenimiento de la empresa **SIMAVE**.*

Se acompaña copia del contrato suscrito entre las partes con fecha 20/12/2012, cuyo objeto se señala: “Mantenimiento de sistemas de seguridad para el control de accesos y video vigilancia del Aeropuerto de Tenerife Norte” (documento Anexo 5).

- o *Por parte de AENA: Director del Aeropuerto, Jefe de Departamento de Operaciones, Servicios y Seguridad, Jefa de la Sección de Seguridad Aeroportuaria, Técnico de Seguridad y Ejecutivos.*

*La grabación de imágenes se almacena por un lado analógicamente en un grabador y digitalmente en cabinas de disco, con un tiempo de conservación como máximo de un mes desde la fecha de captación.*

*El sistema de vídeo digital incluye los racks de almacenamiento de datos y el sistema de cámaras analógicas incluye el sistema de almacenamiento (grabación).*

*En el puesto CCTV existen, entre otras, una matriz de pantallas que permite visualizar las cámaras digitales y analógicas además de un puesto BVMS con un servicio de vídeo digital (vídeo en directo o visualización de grabaciones) y concentrador de alarmas conectadas del CCTV DIGITAL.*

*El acceso tanto a las grabaciones analógicas como digitales se lleva a cabo en recintos cerrados bajo llave custodiadas por los Jefes de equipo de vigilantes y en la Oficina Local de Seguridad (OLS). Lógicamente el acceso queda registrado.*

*El acceso a las grabaciones está autorizado al siguiente personal:*

- o *Empleados de la empresa de seguridad **SEGUR IBÉRICA**, para realizar las labores de consulta y vigilancia.*
- o *Empleados de la empresa de mantenimiento **SIMAVE**.*
- o *Personal de AENA (del Dpto. de Operaciones, Servicios y Seguridad, Dirección, Ejecutivos) para*

*consulta y control en tiempo real de la operativa del Aeropuerto.*

- o *Policía Judicial, Guardia Civil y Cuerpo Nacional de Policía, bajo petición oficial según establece la Ley Orgánica 2/1986.*

*AENA, como empresa de derecho privado, dispone de fichero de titularidad privada inscrito en el Registro General de Protección de Datos, denominado VIDEOVIGILANCIA, con código de inscripción \*\*\*CÓD.1. Se acompaña documentación acreditativa (documento Anexo 6).*

*Se aporta copia del “Documento de Seguridad de Aena Aeropuertos S.A” (documento Anexo 7).*

*Las medidas de seguridad adoptadas en el uso y tratamiento de los datos captados con fines de videovigilancia se corresponden con las relativas al nivel Básico, recogidas en el Documento de Seguridad aludido.*

*Respecto al procedimiento seguido en el visionado y tratamiento de las imágenes captadas por el sistema con fecha 4 de febrero de 2014, durante el desarrollo de la Auditoría de la Agencia Estatal de Seguridad Aérea, AENA manifiesta:*

- o *Durante la citada Auditoría, Aena no realizó ningún tipo de tratamiento en las imágenes captadas, ya que los incumplimientos detectados por los auditores en los filtros de seguridad fueron comunicados en una reunión realizada al final de la auditoría junto con el resto de posibles no conformidades relacionadas con la Seguridad Aeroportuaria. Entre las no conformidades detectadas en los filtros de seguridad, y en referencia a la que trata sobre este asunto, los auditores informaron la hora exacta y el filtro donde ocurrieron los hechos, aunque no identificaron a los vigilantes que cometieron los fallos.*
- o *Aena (y así lo tiene establecido en su Pliego de Prescripciones Técnicas), comunica los incumplimientos que se detectan a lo largo de la ejecución del servicio del Pliego y realiza medidas correctoras a los incumplimientos independientemente de la identidad del vigilante. La empresa de seguridad, a su vez tomará las medidas oportunas para solventar las incidencias ya sea en su gestión o prestación del servicio.*

*El sistema de videovigilancia está conectado a central de alarmas con la empresa IKUSI SIS S.A.*

*No se acompaña copia del contrato suscrito respecto al servicio de central de alarmas.*

*Se adjunta la documentación acreditativa de que la citada empresa de seguridad está autorizada por el Ministerio del Interior (Anexo 8) y de la notificación de las características de la instalación a la DGP (documento Anexo 9).*

Respecto al procedimiento empleado para informar a los trabajadores de la finalidad por la cual se han instalado las cámaras de videovigilancia, **AENA** manifiesta que: *"...Todo el personal de nueva incorporación recibe el Documento de Política Informativa de Protección de Datos o Comunicación sobre tratamiento de datos de carácter personal y deber de secreto documento (Anexo 10). Cada nuevo trabajador firma acusando recibo, un modelo en el que se le indican las políticas de la empresa (entre ellas la de protección de datos)".*

3. Con fecha 24 de octubre de 2014 se reitera el requerimiento de información remitido a **SEGUR IBÉRICA S.A.**, teniendo constancia de la recepción de dicha notificación con fecha 9 de octubre de 2014 según consta en el documento de recibo de Correos.
4. Con fecha 11 de febrero de 2014 se reitera la solicitud de información remitida a la sede social de **SEGUR IBÉRICA S.A.**, sin que hasta la fecha de firma del presente informe haya tenido entrada en esta Agencia escrito de respuesta.

## **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**

Con carácter previo, procede situar la materia de videovigilancia en su contexto normativo.

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.” (el subrayado es de la Agencia Española de Protección de Datos).*

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.

### III

En el presente expediente se denuncia a **SEGUR IBÉRICA S.A** y a **AEROPUERTOS ESPAÑOLES DE SEGURIDAD AÉREA, S.A.** manifestando que la empresa **SEGUR IBÉRICA S.A**, a raíz de la comunicación de la imposición de tres sanciones a trabajadores (con la categoría de vigilantes de seguridad) por una serie de supuestos acontecidos el día 4 de febrero de 2014, ha llevado a cabo una visualización del sistema de cámaras instalado en el citado aeropuerto, con fines ajenos a la seguridad aeroportuaria

Pues bien, el artículo 6.1 de la LOPD dispone lo siguiente:

*“1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”. (El subrayado es de esta Agencia)*

Por su parte, el apartado 2 del mencionado artículo contiene una serie de excepciones a la regla general contenida en el 6.1, estableciendo que *“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 comercial, 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.”*

La Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, establece, entre otros requisitos, la necesidad de legitimación para que el tratamiento de los datos de carácter personal sea lícito, y así lo dispone el artículo 2 de la citada Instrucción, anteriormente transcrito.

Prima facie, el tratamiento de imágenes por razones de seguridad se encuentra amparado, en el artículo 5.1 f) de la Ley 5/2014, de 4 de abril, de Seguridad Privada, que establece: “1. Constituyen actividades de seguridad privada las siguientes: a) La vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos. b) El acompañamiento, defensa y protección de personas físicas determinadas, incluidas las que ostenten la condición legal de autoridad. c) El depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores, joyas, metales preciosos, antigüedades, obras de arte u otros objetos que, por su valor económico, histórico o cultural, y expectativas que generen, puedan requerir vigilancia y protección especial. d) El depósito y custodia de explosivos, armas, cartuchería metálica, sustancias, materias, mercancías y cualesquiera objetos que por su peligrosidad precisen de vigilancia y protección especial. e) El transporte y distribución de los objetos a que se refieren los dos párrafos anteriores. f) La instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia. g) La explotación de centrales para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma, así como la monitorización de cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de Seguridad competentes en estos casos. h) La investigación privada en relación a personas, hechos o delitos sólo perseguibles a instancia de parte”.

En primer lugar, debe tenerse en cuenta el tipo de instalaciones (aeropuerto,) en el que se encuentra el sistema de videovigilancia y la importancia del mismo y que por lo tanto, la finalidad del sistema de videovigilancia instalado en el aeropuerto es la de poder controlar todos los accesos al aeropuerto. Tanto en el Programa Nacional de Seguridad (Capítulo 2 “Seguridad en los aeropuertos”) como en los Programas de Seguridad de los Aeropuertos, en aplicación del mismo Programa Nacional de Seguridad, amparan la instalación y aplicación de estos sistemas de vigilancia además de las patrullas físicas y uso de la vigilancia privada.

La existencia de cámaras de seguridad en el Aeropuerto responde a la necesidad e idoneidad de las mismas para garantizar *la Seguridad Aeroportuaria y la garantía en la aplicación óptima de las medidas de seguridad de la aviación civil reflejadas en el Programa Nacional de Seguridad para la Aviación Civil (PNS)*, siendo fundamental tanto las cámaras como el servicio que prestan las personas encargadas de visionar las mismas. El tratamiento de las imágenes tanto activo (grabando todo lo que ocurre en las instalaciones) como pasivo (siendo grabado dentro de las instalaciones) de las imágenes, es un elemento inherente a la condición de vigilante de seguridad.

La finalidad del tratamiento de las imágenes es la seguridad de las instalaciones vigiladas, pero parte esencial de esta seguridad es el cumplimiento de las obligaciones del personal a cargo de los equipos de grabación.

De otra parte, dicho tipo de tratamiento de datos resulta conforme con el artículo 10. 2 a) del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que señala que *“No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando (...) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:*

*- El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.”*

De la documentación obrante en el expediente, se extrae que, en el presente supuesto, el tratamiento de datos por medio de cámaras y/o videocámaras con fines de seguridad queda incardinado en la esfera del interés legítimo de la entidad denunciada, por cuanto la misma tiene un evidente interés en la instalación y mantenimiento de cámaras de seguridad; y la finalidad de seguridad es también legítima, sin que se oponga a norma u obligación de ningún tipo.

El interés legítimo es un presupuesto legitimador del tratamiento de datos personales. Así, el artículo 7 de la Directiva 95/46/CE, de 24 de octubre determina: *“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: (...) f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del Art. 1 de la presente Directiva.: en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales”.*

En este sentido, la Sentencia del Tribunal de Justicia de las Comunidades Europeas de 24 de noviembre de 2011, que resuelve una cuestión prejudicial planteada por el Tribunal Supremo, ha clarificado que el artículo 7.f) de la Directiva 95/46/CE tiene efecto directo.

En consonancia con lo anterior, el Tribunal Supremo en Sentencia de 8 de febrero de 2012 anuló el artículo 10.2.b) del RD 1720/2007, de 21 de diciembre por considerar que el Reglamento vulneraba la regulación contenida en la Directiva. Así, la Audiencia

Nacional realiza una ponderación caso por caso entre el interés legítimo del responsable del tratamiento y los derechos y libertades fundamentales de los afectados, como en Sentencias de la Sección Primera de la Sala de lo Contencioso Administrativo de 5 de marzo y 31 de mayo de 2012.

En el supuesto objeto del presente expediente, los derechos y libertades fundamentales de los afectados –esto es, las personas cuyas imágenes son captadas, grabadas y visionadas por las cámaras de seguridad de la entidad denunciada– no se ven lesionados hasta el punto de prevalecer sobre el interés legítimo de dicha empresa relacionado con la seguridad.

En definitiva, el interés legítimo supone la legitimación de AENA, y de quien ésta ha designado para el tratamiento de imágenes, siempre que se cumplan las garantías establecidas en la Instrucción 1/2006 antes mencionada, destacando en particular el deber de información y los derechos de las personas a que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

#### IV

Por otro lado, en cuanto al acceso al visionado de las imágenes por parte de **SEGUR IBERICA**, para analizar esta cuestión, debe partirse de los conceptos de responsable y encargado del tratamiento contenidos en la Ley Orgánica 15/1999.

Así, será responsable del fichero o del tratamiento, conforme al artículo 3 d) de la Ley, *“la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”*. Por su parte, es encargado del tratamiento, según el artículo 3 g), *“la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento”*.

A este respecto el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), establece como regla general el previo consentimiento del interesado para la comunicación de datos personales a un tercero. Así dispone en su apartado 1 lo siguiente: *“1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.”*

El artículo 3. i) de la citada norma define la *“cesión o comunicación de datos”* como *“toda revelación de datos realizada a una persona distinta del interesado”*.

No obstante lo anterior, la propia LOPD habilita, en su artículo 12, el acceso de terceros a los datos personales cuando el acceso a los datos se realice para prestar un

servicio al responsable del fichero o del tratamiento, al señalar en su apartado 1: *“1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.”*

El citado artículo 12.1 de la LOPD permite, por tanto, el acceso a datos de carácter personal a la persona o entidad que presta un servicio al responsable del fichero, sin que, por mandato expreso de la ley, pueda considerarse dicho acceso como una cesión o comunicación de datos.

A este respecto existe contrato suscrito entre SEGUR IBERICA y AENA con fecha 24/05/2013 cuyo objeto es la prestación por parte de SEGUR de un servicio de vigilancia y protección, recogiendo el Anexo D del citado contrato, que la empresa adjudicataria tendrá la consideración de encargada del tratamiento de los ficheros responsabilidad de AENA obligándose de acuerdo al artículo 12 de la LOPD, a utilizar dichos datos exclusivamente para la ejecución del contrato y llevar a cabo el tratamiento de los datos de carácter personal suministrados por AENA conforme a las instrucciones especificadas en el mismo.

Por lo tanto a través del contrato suscrito entre el responsable AENA y el encargado SEGUR IBÉRICA S.A., éste trata los datos conforme a las instrucciones del responsable, entre cuyas faenas encomendadas se encuentra la visualización y control de las cámaras de seguridad. Así la citada empresa actuaría por cuenta del responsable del fichero, en este caso AENA, no entendiéndose la existencia de una cesión de datos ilegítima, siendo el acceso a los datos por parte de SEGUR IBÉRICA S.A., necesarios para la prestación de un servicio al responsable del tratamiento.

Así, respecto al procedimiento seguido en el visionado y tratamiento de las imágenes captadas por el sistema con fecha 4 de febrero de 2014, durante el desarrollo de la Auditoría de la Agencia Estatal de Seguridad Aérea, AENA manifiesta:

- o *Durante la citada Auditoría, Aena no realizó ningún tipo de tratamiento en las imágenes captadas, ya que los incumplimientos detectados por los auditores en los filtros de seguridad fueron comunicados en una reunión realizada al final de la auditoría junto con el resto de posibles no conformidades relacionadas con la Seguridad Aeroportuaria. Entre las no conformidades detectadas en los filtros de seguridad, y en referencia a la que trata sobre este asunto, los auditores informaron la hora exacta y el filtro donde ocurrieron los hechos, aunque no identificaron a los vigilantes que cometieron los fallos.*
- o *Aena (y así lo tiene establecido en su Pliego de Prescripciones Técnicas), comunica los incumplimientos que se detectan a lo largo de la ejecución del servicio del Pliego y realiza medidas correctoras a los incumplimientos independientemente de la identidad del vigilante. La*

*empresa de seguridad, a su vez tomará las medidas oportunas para solventar las incidencias ya sea en su gestión o prestación del servicio.*

Por lo tanto, fue a través de la Auditoría de la Agencia Estatal de Seguridad Aérea realizada el 4 de febrero de 2015 cuando se detectan varios incumplimientos y fallos en los filtros de seguridad por parte de personal de SEGUR que fueron comunicados por AENA a ésta al efecto de que tomara las medidas oportunas para solventar las incidencias.

Asimismo, dada la relación contractual entre **AENA y SEGUR IBÉRICA S.A.**, para el que los trabajadores sancionados prestan sus servicios en las instalaciones de aquella, estaría justificada la información que AENA pudiera suministrar sobre la actuación de los trabajadores de **SEGUR** (contraria a las condiciones contractuales pactadas entre ambos), y que de acuerdo con el artículo 53.4 del Convenio Colectivo Nacional de Empresas de Seguridad sería constitutivo de la comisión de faltas laborales muy graves, siendo **SEGUR** a la que corresponde valorar el cumplimiento de los deberes por parte de sus trabajadores y, en su caso, proponer y corregir las conductas contrarias al correcto desarrollo de sus obligaciones. **AENA** no realiza ningún control sobre el personal de la entidad **SEGUR IBÉRICA**, sino únicamente el cumplimiento del servicio contratado.

Debe tenerse en cuenta que en el propio contrato firmado entre ambas entidades se recoge la penalización que recaería sobre **SEGUR** por incumplimientos contractuales en materia de seguridad aeroportuaria.

Junto a ello, no cabe duda de que las imputaciones derivadas a los trabajadores sancionados, (cuestión que no compete a esta Agencia resolver) revisten, teniendo en cuenta el trabajo que desempeñan, una indudable relevancia en materia de seguridad, subsumible en el fin declarado para el archivo de videovigilancia.

Por lo tanto, no se considera que la utilización de las cámaras para la finalidad denunciada incumpla lo establecido en el artículo 12.4 de la LOPD que establece: *“En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”.*

## V

Seguidamente, procede analizar si el tratamiento de las imágenes realizado cumplía o no con los restantes requisitos exigibles en materia de protección de datos de carácter personal, recogidos en la Ley Orgánica 15/1999, de 13 de diciembre, y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, como son, entre otros, 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.

A este respecto, el artículo 5.1 de la LOPD, que obliga a que se cumpla con el deber de informar a los afectados, dispone que:

*“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 debe facilitarse la información recogida en el artículo 5 de la LOPD, el artículo 3 de la Instrucción 1/2006, 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, según consta en el expediente, se aporta fotografía de la existencia de carteles informativos de zona videovigilada, ubicados en la Zona de bandeja del Filtro Interinsular, Filtro nacional y Control C. Dichos carteles son acordes al artículo 3. a) de la Instrucción 1/2006. Asimismo, se aporta modelo de cláusula informativa a disposición de los interesados de conformidad con el artículo 3. b) de la citada Instrucción.

En consecuencia, el sistema de captación de imágenes por medio de cámaras o

videocámaras al que se refieren las presentes actuaciones cumple con el deber de información recogido en el artículo 5 de la LOPD.

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 recoge 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.”*

Pues bien, en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos, consta debidamente inscrito el fichero denominado VIDEOVIGILANCIA, cuyo responsable es **AENA AEROPUERTOS S.A.**

A la vista de todo lo expuesto se procede al archivo del presente expediente, al no apreciarse vulneración a la normativa de protección de datos, por parte **AENA AEROPUERTOS S.A.** ni por **SEGUR IBÉRICA SA.**

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 a **AEROPUERTOS ESPAÑOLES DE SEGURIDAD AEREA S.A., SEGUR IBERICA S.A.,** y a D. **A.A.A. Y OTROS.**

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.

José Luis Rodríguez Álvarez

Director de la Agencia Española de Protección de Datos