

Expediente N°: E/05863/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **AENA, SA**, en virtud de denuncia presentada por **ALTERNATIVA SINDICAL DE POLICIA, JEFATURA SUPERIOR DE POLICIA DE CATALUÑA** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 29 de junio de 2015 tiene entrada en esta Agencia un escrito de **ALTERNATIVA SINDICAL DE POLICIA** en el que se denuncian dos hechos:

1. Sistema de videovigilancia ubicado en los calabozos, sala de retornados y sala de asilados del Aeropuerto. Consideran que debiera ser considerado un sistema distinto del sistema de videovigilancia que AENA ha dispuesto en el aeropuerto, ya que los carteles informativos situados en las entradas del aeropuerto no suelen ser vistos por las personas que resultan detenidas en las mencionadas salas, donde el tratamiento de imágenes de personas en su interior comporta una sensibilidad añadida. Entienden los denunciantes que el sistema de videovigilancia de dichas salas debiera ser un sistema independiente del general del aeropuerto, con un fichero carteles informativos específicos. Fundamentan lo anterior en base al artículo 3.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad que define las Fuerzas y Cuerpos de Seguridad del Estado y al artículo 2.3 apartado e) que establece que se regirán por sus disposiciones específicas los tratamientos de datos personales procedentes de imágenes obtenidos mediante videocámaras, siendo la disposición específica a aplicar la recogida en 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 definitiva, a juicio de los denunciantes, se trata de un sistema de videovigilancia instalado en dependencias policiales que, aunque dentro del recinto del aeropuerto, deberían regirse por una normativa específica y por lo tanto por un fichero específico.

2. Que el sistema de videovigilancia general del aeropuerto y gestionado por AENA se encuentra inscrito como fichero en la AEPD con la finalidad de videovigilancia/seguridad de las instalaciones de AENA en consonancia con la Orden FOM/2028/2012, de 31 de agosto. Añaden que a pesar de lo anterior, en fecha de 20/4/2015 funcionarios del Cuerpo Nacional de Policía que se encontraban prestando servicios en los filtros fronterizos del Módulo 4 de la Terminal 2 de dicho aeropuerto, fueron advertidos por funcionarios del mismo cuerpo que habían sido grabados por los operadores de las cámaras cuando realizaban su trabajo policial y durante tiempo indeterminado. En opinión de los denunciantes, dichas tomas se utilizan con la finalidad de control laboral cuando la finalidad de dicho sistema es la de la seguridad y el control de acceso a las instalaciones, pero no el control de los funcionarios públicos del Cuerpo Nacional de Policía que presentan sus servicios en dependencias del aeropuerto. Añaden que se trata de cámaras muy potentes ya que disponen de una gran zoom y capacidad de movimiento por lo que pueden enfocar puntos muy concretos como las pantallas de ordenador que utilizan los policías en los controles fronterizos.

Junto a las denuncias se aportaron los siguientes documentos:

1. A pesar de que la denuncia relaciona determinados documentos adjuntos, dichos documentos no constan con la denuncia.

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. En fecha de 30/7/2015 se ha recibido copia del informe de fecha 23.7.2015 emitido por el Comisario Principal Jefe de la BPSP de la Policía Nacional en relación a lo denunciado en el punto SEGUNDO. El informe analiza jurídicamente el hecho denunciado concluyendo la no existencia de vulneración a la normativa aplicable.
2. En fecha de 24/2/2016 se practica acta de inspección al Aeropuerto de Barcelona donde se mantiene reunión con Jefe de Seguridad del Aeropuerto y representante de AENA y con el comisario de Policía Nacional nº ****, en calidad de representante de la Comisaría de Policía Nacional ubicada en el Aeropuerto del Prat. En dicha inspección se averigua lo siguiente:

2.1. Respecto del sistema de videovigilancia instalado en el AEROPUERTO DE BARCELONA el representante de AENA informa de lo siguiente:

- 2.1.1.El AEROPUERTO DE BARCELONA es un recinto aeroportuario cerrado por una valla perimetral excepto en los accesos por carretera, donde se señala, mediante los correspondientes carteles, que se accede al interior de dicho recinto.
- 2.1.2.El recinto aeroportuario alberga diversos edificios como las terminales de pasajeros, almacenes, edificios administrativos, pistas de despegue y aterrizaje para los aviones, viales interiores y demás infraestructuras y servicios necesarios para la operativa aeroportuaria.
- 2.1.3.Además de las instalaciones anteriormente citadas también se encuentran en el interior del aeropuerto dependencias gestionadas por los diversos cuerpos de seguridad del Estado. Policía Nacional, Guardia Civil y Mossos d'Esquadra.
- 2.1.4.El recinto aeroportuario se encuentra sujeto a diversa normativa entre la que cabe señalar el denominado PROGRAMA NACIONAL DE SEGURIDAD PARA LA AVIACIÓN CIVIL, elaborado por la AGENCIA ESTATAL DE SEGURIDAD dependiente del MINISTERIO DE FOMENTO y de obligado cumplimiento en el citado recinto. Dicho programa recoge la necesidad de dotar de sistemas de videovigilancia al recinto aeroportuario.
- 2.1.5.De esta manera, el aeropuerto de Barcelona cuenta con un sistema de videovigilancia formado por más de 2500 cámaras que vigilan el interior del recinto aeroportuario. Parte de las cámaras cubren la seguridad del interior de edificios y parte las zonas externas a edificios, incluidos los viales interiores para el tránsito de vehículos, recogiendo, en todo caso, imágenes

del interior del recinto aeroportuario. El sistema de videovigilancia descrito también recoge imágenes de las zonas descritas en el punto 2.1.3.

- 2.1.6. Las cámaras se visualizan en un centro de control ubicado dentro del propio recinto almacenándose por un periodo de 30 días. El mencionado centro de control se encuentra dividido en diferentes salas de forma que una de ellas es gestionada por empleados de la empresa de seguridad contratada al efecto por AENA y que actualmente es la empresa SEGURISA, SA existiendo otras salas contiguas correspondientes a los diferentes cuerpos y fuerzas de seguridad del Estado desde donde personal de dichos cuerpos dispone de acceso y control sobre las cámaras del sistema de videovigilancia de AENA que cubren sus correspondientes zonas de su competencia.
- 2.1.7. El contrato de prestación de servicios suscrito entre AENA y SEGURISA recoge compromiso de confidencialidad. Adicionalmente, AENA obliga a que SEGURISA exija a sus vigilantes que firmen un compromiso de confidencialidad. Se recaba copia del escrito dirigido por AENA a SEGURISA a tal efecto así como copia del modelo de compromiso de seguridad que SEGURISA exige a sus vigilantes (documento DOC. 1 anexo al acta de inspección).
- 2.1.8. El acceso que realizan los diferentes cuerpos de seguridad del Estado desde sus respectivas salas se realiza en modo visualización ya sea a imágenes en directo o grabadas en los 30 días anteriores, quedando restringido la extracción de grabaciones a la solicitud previa y por escrito a AENA ya que son sus técnicos los únicos con derechos de acceso para poder realizar dichas extracciones.
- 2.1.9. El control sobre el movimiento de las cámaras no fijas así como del zoom de las cámaras que cuentan con dicha posibilidad puede ser realizado por cualquiera de los diferentes usuarios con acceso a dichas cámaras, quedando asignado el control al usuario que se conecte primero a dicha cámara. El sistema no almacena histórico sobre que usuario se conectó a una determinada cámara ni sobre el usuario que estableció una orientación concreta ni el zoom de la cámara.
- 2.1.10. Respecto de las personas que pueden acceder al sistema de videovigilancia instalado, manifiestan que existe un acceso restringido a las mismas y que únicamente las personas que por sus funciones necesitan de dicho acceso disponen del mismo. Algunas cámaras, como se verá más adelante, cuentan con un nivel de acceso especialmente restringido.
- 2.1.11. El código de inscripción del fichero de videovigilancia en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos es el ***CÓD.1
- 2.1.12. Al objeto de informar a los ciudadanos acerca de la existencia del sistema de videovigilancia se ha dispuesto de numerosos carteles informativos ubicados en las entradas a diferentes edificios del Aeropuerto así como por el interior de todo el recinto, pasillos de tránsito, etc y en concreto en las salas de estancia de los pasajeros.
- 2.1.13. El acceso a las imágenes del sistema de videovigilancia del Aeropuerto, del que es responsable AENA, por parte de las fuerzas y cuerpos de

seguridad del Estado se encuentra sujeto a un protocolo establecido tras la consulta realizada por AENA a la Agencia Española de Protección de Datos que dio como consecuencia el informe de fecha 2/9/2013 y del que se recaba copia (documento DOC. 2 anexo al acta de inspección).

2.2. Respecto de la visualización de imágenes de agentes de policía que prestan servicios en los denominados “filtros fronterizos” los representantes de AENA y de Policía Nacional informan de lo siguiente:

- 2.2.1. Los denominados “filtros fronterizos” corresponden a las zonas donde se realizan los controles de documentación a los pasajeros con un origen o destino internacional.
- 2.2.2. Dichos controles son realizados por agentes de Policía Nacional en zonas especialmente habilitadas para ello y en las que se ubican cabinas donde los agentes revisan la documentación de cara a permitir o no el tránsito de los pasajeros.
- 2.2.3. Las cámaras que cubren estas zonas son utilizadas por parte de AENA y de Policía Nacional al objeto del control de la seguridad en general y del control de las aglomeraciones de pasajeros en particular, dado que a veces se producen colas de pasajeros en dichos filtros, en cuyo caso los responsables policiales y de seguridad del aeropuerto toman las medidas correspondientes para disminuir dichas aglomeraciones reasignando recursos de una zonas a otras.
- 2.2.4. Estas zonas se encuentran cubiertas por cámaras que permiten el control a distancia de la orientación de la cámara así como del zoom óptico, pudiendo ser controladas tanto por vigilantes de SEGURISA como por agentes de Policía Nacional y de otros cuerpos de seguridad si las zonas de cobertura de dichas cámaras entran en las zonas de su competencia.
- 2.2.5. En relación a las imágenes captadas por la cámara 0172 el día 20/4/2015 entre las 22.10 y las 22.14 y relativas a la zona fronteriza ubicada en la Terminal 2, Módulo 4 del Aeropuerto, el representante de AENA manifiesta que no les consta solicitud alguna de extracción de dichas imágenes, por lo que no se dispone de las mismas al haber sido canceladas transcurridos los 30 días siguientes. Tampoco les consta la solicitud de ejercicio de los derechos reconocidos en la normativa de protección de datos sobre dichas imágenes.
- 2.2.6. Los inspectores solicitan el acceso a la imagen captada por la cámara 0172 recabándose copia de la imagen captada por dicha cámara en el momento de realizar el acceso (documento DOC. 3 anexo al acta de inspección) apreciándose una vista panorámica del área donde se realiza el denominado “filtro fronterizo”. Los inspectores constatan que sobre dicha cámara existe control remoto de posición en 360º así como la posibilidad de zoom óptico que permite enfocar de cerca cualquier objeto ubicado en su zona de cobertura, por lo que técnicamente es posible obtener planos cercanos de una persona ubicada en dicha zona.
- 2.2.7. El representante de Policía Nacional manifiesta a preguntas de los inspectores que en ningún caso Policía Nacional utiliza las imágenes de dichas cámaras para el control laboral de sus agentes, siendo la finalidad

del tratamiento de las imágenes de las cámaras a las que tienen acceso la seguridad en general y la gestión de las aglomeraciones que, como consecuencia de los filtros se producen, en particular.

2.3. Respecto de la videovigilancia instalada en las dependencias policiales del aeropuerto, los representantes de AENA y de Policía Nacional informan de lo siguiente:

- 2.3.1. Policía Nacional cuenta con una comisaria ubicada en el interior del Aeropuerto. Dicha comisaria cuenta con tres dependencias especiales: Calabozos, Sala de Asilados y Sala de no admitidos cuya gestión entra dentro de sus competencias.
- 2.3.2. Calabozos: Zona habilitada para albergar a personas que se encuentran en situación de detenidos y dispone de varias celdas y un pasillo común. En dicha estancia se ha ubicado una cámara fija y sin zoom que visualiza únicamente el pasillo común. Los inspectores recaban copia de pantalla con la imagen captada por dicha cámara (documento DOC 4 anexo al acta de inspección).
- 2.3.3. Sala de Asilados: Zona habilitada para albergar a personas que se encuentran en situación de solicitud de asilo y que dispone de varias salas entorno a una zona común. En dicha estancia se ha ubicado una cámara fija y sin zoom que visualiza únicamente la zona común. Los inspectores recaban copia de pantalla con la imagen captada por dicha cámara (documento DOC 5 anexo al acta de inspección).
- 2.3.4. Sala de no admitidos (anteriormente denominada sala de retornados): Zona habilitada para albergar a personas cuyo acceso a territorio español no ha sido aprobado y se encuentran a la espera de que la compañía aérea que le trasladó hasta el Aeropuerto gestione su regreso al lugar de origen. Dicha estancia dispone de varias salas entorno a una zona común. En dicha estancia se ha ubicado una cámara fija y sin zoom que visualiza únicamente la zona común. Los inspectores recaban copia de pantalla con la imagen captada por dicha cámara (documento DOC 6 anexo al acta de inspección).
- 2.3.5. Si bien las tres cámaras anteriores forman parte del sistema de videovigilancia del Aeropuerto y están sujetas a las mismas reglas generales, presentan unas especiales características específicas ya que el acceso a las imágenes ha sido restringido para que sea visualizado por los agentes de Policía Nacional encargados de la vigilancia de las mencionadas dependencias y de forma excepcional por técnicos de seguridad de AENA a los efectos de poder realizar extracciones de aquellas imágenes que Policía Nacional requiera puntualmente.
- 2.3.6. El acceso a las dependencias policiales donde se ubican las cámaras anteriores se realiza a través de zonas y pasillos del aeropuerto en los que se ubican carteles que informan de la existencia del sistema de videovigilancia. Los inspectores constatan y recaban fotografías (documento DOC 7 anexo al acta de inspección) de ambas zonas del pasillo que da acceso a las mencionadas dependencias policiales.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

En primer lugar procede situar el contexto normativo en materia de videovigilancia. Así el artículo 1 de la LOPD dispone: *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma señala: *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*.

El artículo 5.1. f) del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*.

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

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa*

existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático". Sigue señalando: "Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999..."

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

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

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

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

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

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

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

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

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

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

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

III

En el presente expediente se denuncia por **ALTERNATIVA SINDICAL DE POLICIA** por un lado que, el sistema de videovigilancia del Aeropuerto del Prat de Barcelona, ubicado en los calabozos, sala de retornados y sala de asilados, aunque dentro del recinto del aeropuerto, debería regirse por una normativa específica y por lo tanto por un fichero específico y ser considerado distinto del sistema de videovigilancia que AENA ha dispuesto en el aeropuerto, ya que los carteles informativos situados en las entradas del aeropuerto no suelen ser vistos por las personas que resultan detenidas en las mencionadas salas; y por otro lado que el sistema de videovigilancia general del aeropuerto y gestionado por AENA se encuentra inscrito como fichero en la AEPD con la finalidad de videovigilancia/seguridad y a pesar de lo anterior, dichas imágenes se utilizan con fines de control de los funcionarios públicos del Cuerpo Nacional de Policía que prestan sus servicios en dependencias del aeropuerto.

Con carácter previo debe señalarse el tipo de instalación en el que se encuentra el sistema de videovigilancia y la importancia del mismo: el aeropuerto del Prat en Barcelona. El recinto aeroportuario se encuentra sujeto a diversa normativa entre la que cabe señalar el denominado Programa Nacional de Seguridad para la Aviación Civil, elaborado por la Agencia Estatal de Seguridad, dependiendo del Ministerio de Fomento y de obligado cumplimiento en el citado recinto. Dicho programa recoge la necesidad de dotar de sistemas de videovigilancia al recinto aeroportuario.

Una vez realizado dicho inciso, respecto a la primera cuestión denunciada, procede entrar a valorar el cumplimiento del deber de información e inscripción de ficheros por parte de la entidad denunciada, respecto al sistema de videovigilancia instalado en el aeropuerto del Prat.

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

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

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

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

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

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

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

En cuanto al modo en que hay de facilitarse la información recogida en el artículo

5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

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

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

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

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

“ANEXO-

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

En el caso que nos ocupa, mediante inspección realizada por los Servicios de Inspección de esta Agencia, en fecha 24 de febrero de 2016, al aeropuerto denunciado, se desprende la existencia de numerosos carteles informativos ubicados en las entradas a diferentes edificios del aeropuerto así como por el interior de todo el recinto, pasillos de tránsito, etc, y en las salas de estancia de los pasajeros. Dichos carteles son acordes al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD.

A este respecto cabe decir que el aeropuerto del Prat es un recinto aeroportuario cerrado por una valla perimetral excepto en los accesos por carretera, donde se señala, mediante los correspondientes carteles, que se accede al interior de dicho recinto. Dicho recinto alberga diversos edificios como las terminales de pasajeros, almacenes, edificios administrativos, pistas de despegue y aterrizaje para los aviones, viales interiores y demás infraestructuras y servicios necesarios para la operativa aeroportuaria. Además de estas instalaciones, también se encuentran en el interior dependencias de los diversos cuerpos de seguridad del Estado. Policía Nacional, Guardia Civil y Mossos d'Escuadra, entendiéndose que no existe ningún inconveniente que dichas instalaciones policiales formen parte también del único sistema de videovigilancia que dispone el aeropuerto, siempre que se cumpla la normativa de protección de datos.

Asimismo y concretamente respecto a las cámaras ubicadas en la zona de dependencias policiales donde se ubican los calabozos, sala de asilados y sala de no admitidos se constata por los inspectores actuantes que en el acceso a dichas dependencias se realiza a través de zonas y pasillos en los que se ubican los citados carteles informativos.

Respecto a la ubicación del cartel informativo, no es necesario que se coloque debajo de cada cámara siendo suficiente conforme a lo dispuesto en el artículo 3 a) de la Instrucción 1/2006, colocar el distintivo informativo en lugar suficientemente visible, tanto en espacios abiertos como cerrados, y en el caso que nos ocupa dicha norma se cumple, por lo tanto la citada entidad cumple con el deber de información de la existencia de un sistema de videovigilancia dentro de sus instalaciones.

Debe recordarse que, como ya ha sido desarrollado en varios informes jurídicos de esta Agencia, la Agencia carece de competencias para la autorización de sistemas de videovigilancia, siendo su competencia la de velar para que el tratamiento de datos derivados de la existencia de dichos sistemas resulte acorde a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de carácter personal, y la Instrucción 1/2006, de 8 de noviembre de esta Agencia.

Las cámaras de videovigilancia se visualizan en un centro de control ubicado dentro del propio recinto y se encuentra dividido en diferentes salas de forma que una de ellas es gestionada por empleados de la empresa de seguridad contratada al efecto por AENA y que actualmente es la empresa SEGURISA, SA existiendo otras salas contiguas correspondientes a los diferentes cuerpos y fuerzas de seguridad del Estado desde donde personal de dichos cuerpos dispone de acceso y control sobre las cámaras del sistema de videovigilancia de AENA que cubren sus correspondientes zonas de su competencia.

A este respecto, el contrato de prestación de servicios suscrito entre AENA y SEGURISA recoge compromiso de confidencialidad. Adicionalmente, AENA obliga a que SEGURISA exija a sus vigilantes que firmen un compromiso de confidencialidad.

El acceso que realizan los diferentes cuerpos de seguridad del Estado desde sus respectivas salas se realiza en modo visualización ya sea a imágenes en directo o grabadas en los 30 días anteriores, quedando restringido la extracción de grabaciones a la solicitud previa y por escrito a AENA ya que son sus técnicos los únicos con derechos de acceso para poder realizar dichas extracciones.

Asimismo las captaciones que realizan las cámaras en dichas dependencias policiales son las siguientes: en la zona de calabozo hay una cámara fija y sin zoom que visualiza únicamente el pasillo común; en la zona de asilados hay una cámara fija y sin zoom que visualiza únicamente la zona común y Sala de no admitidos (anteriormente denominada sala de retornados) hay una cámara fija y sin zoom que visualiza únicamente la zona común. Por lo tanto las imágenes captadas no infringen el principio de proporcionalidad de los datos previsto en el artículo 4.1 de la Ley Orgánica de Protección de Datos, cuando se habla de que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Si bien las tres cámaras anteriores forman parte del sistema de videovigilancia del Aeropuerto y están sujetas a las mismas reglas generales, presentan unas especiales características específicas ya que el acceso a las imágenes ha sido restringido para que sea visualizado por los agentes de Policía Nacional encargados de la vigilancia de las mencionadas dependencias y de forma excepcional por técnicos de seguridad de AENA

a los efectos de poder realizar extracciones de aquellas imágenes que Policía Nacional requiera puntualmente.

Por tanto, siguiendo el criterio de la citada Instrucción 1/2006, no puede considerarse, en el presente caso, que la instalación de las videocámaras en los términos expuestos vulnere los principios de calidad, proporcionalidad y finalidad del tratamiento.

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

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

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

de Datos, para su inscripción en el Registro General de la misma.

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

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

El artículo 20.1 de la LOPD, establece que la creación, modificación o supresión de ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente. Por su parte el artículo 53.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, determina que cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

Pues bien, consta la Orden FOM/2028/2012, de 31 de agosto, publicado en el BOE de fecha 26 de septiembre de 2012 y la inscripción en el Registro de Protección de Datos de esta Agencia del fichero "VIDEOVIGILANCIA DE AENA" con última modificación el 07/11/2012.

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

A la vista de toda la información documentación recabada durante la Inspección realizada por los Servicios de Inspección de esta Agencia en fecha 24/02/2016 se desprende que el aeropuerto cumpliría la normativa de protección de datos, no existiendo inconveniente que el sistema de videovigilancia instalado capte todas las dependencias ubicadas en el aeropuerto, incluyendo las dependencias policiales.

III

Respecto a la segunda cuestión planteada relativa a que el sistema de videovigilancia general del aeropuerto y gestionado por AENA se encuentra inscrito como fichero en la AEPD con la finalidad de videovigilancia/seguridad y a pesar de lo anterior, dichas imágenes se utilizan con fines de control de los funcionarios públicos del Cuerpo Nacional de Policía que presentan sus servicios en dependencias del aeropuerto, cabe decir que, en esta cuestión, en primer lugar se plantea si es necesario el consentimiento inequívoco de los trabajadores cuando se instalan cámaras de videovigilancia en el centro de trabajo, al amparo del artículo 6.1 de la LOPD.

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

manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen”.

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

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

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

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

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

El apartado 2 del artículo 6 de la LOPD exime del necesario consentimiento cuando los datos se refieran *“a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento...”*

En el ámbito laboral, el Ordenamiento el Ordenamiento Jurídico Español, regula en el Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo de 24 de Octubre de 1995, los poderes de Dirección del empresario y es en éste articulado donde hallamos la oportuna legitimación.

El artículo 20.3 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (ET) dispone que : *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores con discapacidad”.*

De todo ello se desprende que el empresario, en este caso la entidad denunciada, se halla legitimada para tratar las imágenes de los trabajadores en el ámbito laboral, al amparo del artículo 20.3 del ET. Ahora bien, esta legitimación no es absoluta y exige por parte del empresario la obligación de informar de dicho tratamiento a los

trabajadores(cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la LOPD.).

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

En el primer caso, es decir cuando el objetivo de la instalación de las cámaras va dirigido al cumplimiento por los trabajadores de sus deberes laborales, sería necesario por parte del empresario, garantizar el derecho de información en la recogida de las imágenes, mediante información a los trabajadores del alcance específico que se va a dar a las mismas para el control laboral, como establece la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero de 2013, debe ir precedido de *“una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”*.

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

En el caso que nos ocupa, la finalidad del sistema de videovigilancia es la seguridad de las personas e instalaciones interiores del aeropuerto y parte de las zonas externas a edificios, incluidos los viales interiores para el tránsito de vehículos. Por lo tanto su finalidad es la vigilancia y seguridad sin que se aporten pruebas por el denunciante que acredite que se utilicen para una finalidad distinta a la que se tiene declarada, como sería el control laboral.

En relación a las imágenes captadas por la cámara 0172 el día 20/4/2015 entre las 22.10 y las 22.14, objeto de denuncia, y relativas a la zona fronteriza ubicada en la Terminal 2, Módulo 4 del Aeropuerto, el representante de AENA manifiesta que no les consta solicitud alguna de extracción de dichas imágenes, por lo que no se dispone de las mismas al haber sido canceladas transcurridos los 30 días siguientes. Tampoco les consta la solicitud de ejercicio de los derechos reconocidos en la normativa de protección de datos sobre dichas imágenes.

Los inspectores solicitan el acceso a la imagen captada por la cámara 0172 recabándose copia de la imagen captada por dicha cámara en el momento de realizar el acceso apreciándose una vista panorámica del área donde se realiza el denominado “filtro fronterizo”. Los inspectores constatan que sobre dicha cámara existe control remoto de posición en 360º así como la posibilidad de zoom óptico que permite enfocar de cerca cualquier objeto ubicado en su zona de cobertura.

El representante de Policía Nacional manifiesta a preguntas de los inspectores que en ningún caso la Policía Nacional utiliza las imágenes de dichas cámaras para el

control laboral de sus agentes, siendo la finalidad del tratamiento de las imágenes de las cámaras a las que tienen acceso la seguridad en general y la gestión de las aglomeraciones que, como consecuencia de los filtros se producen, en particular.

Asimismo respecto de esta cuestión, se planteó denuncia por parte del Sindicato Policial ALTERNATIVA SINDICAL DE POLICÍA a la UCOT, elaborándose informe al respecto, que concluía con la no existencia de vulneración a la normativa aplicable, de fecha 23/07/2015 por parte del Comisario Principal, Jefe de la BPSP en el que se recoge: *"La cuestión es determinar si existe algún tipo de irregularidad, como afirman los denunciantes, en el uso de las imágenes captadas y/o grabadas por una de las cámaras-consideran que no está justificado que una de las cámaras les grabe de forma fija, porque ello afecta a sus derechos-lo que de ser cierto implicaría haber utilizado el sistema de videovigilancia para una finalidad distinta a la prevista y declarada, cual es la de vigilar las instalaciones para proteger a las personas y los bienes, con vulneración de la legislación vigente.*

Pues bien, de lo actuado no resultan elementos o indicios racionales de que se hay hecho un mal uso de las imágenes captadas por el sistema, y el hecho de que la cámara grabe de forma reiterada o incluso continua, durante un determinado lapso de tiempo, a una persona que esté dentro del campo de visión del dispositivo, no implica en sí mismo un uso desproporcionado ni injustificado de la vigilancia, siempre que, como es este caso, el campo de grabación esté en una zona pública perfectamente identificada.

Otra cuestión diferente hubiera sido si las imágenes captadas se hubieran difundido, cedido a terceros indebidamente, sin consentimiento, o se utilizaran para otra finalidad distinta de la declarada, por ej, el control laboral de los empleados, si previamente no se hubiera comunicado a las personas afectadas. Ello no impide que los afectados puedan, como se ha señalado, ejercer sus derechos, de forma individual, ante el depositario de las imágenes".

Por lo tanto la entidad denunciada cumpliría como ya se ha desarrollado, con el deber de información recogido en el artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD, informando tanto a las personas que puedan acceder a las instalaciones como a sus trabajadores de la existencia y finalidad del sistema de videovigilancia instalado, sin que conste su utilización a efectos de control laboral ni se informe, en consecuencia, del uso de sus imágenes a tal fin.

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

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

3. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
4. **NOTIFICAR** la presente Resolución a **AENA, SA**, y a **ALTERNATIVA SINDICAL DE POLICIA**.

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 la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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.

Mar España Martí

Directora de la Agencia Española de Protección de Datos