

Expediente N°: E/07244/2012

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha de 25 de septiembre de 2012 tiene entrada en esta Agencia un escrito de D. **A.A.A.** y Dña. **B.B.B.** en calidad de Presidente y Secretario del Comité de Empresa (en adelante los denunciantes) del centro de trabajo de la entidad **AREAS SA** (en adelante el denunciado) en el Aeropuerto de Palma, en el que manifiestan la instalación de un dispositivo router añadido a la instalación del circuito cerrado de captación de imágenes con sus características y limitaciones técnicas inherentes a la confidencialidad de las imágenes obtenidas.

Los denunciantes declaran haber remitido al denunciado escrito en el que le comunican:

- Tras el archivo de actuaciones del expediente de la Agencia Española de Protección de Datos con referencia **E/02170/2008** relativo a la instalación de un circuito cerrado de captación de imágenes en el Centro de Trabajo (en varios puntos de venta) en el que se constató:

d) que “no existen monitores en los centros donde se puedan visualizar las imágenes captadas por las videocámaras”

h) que “las imágenes son visualizadas por el responsable del fichero y son grabadas y guardadas en el sistema instalado”

i) que de la documentación técnica del sistema de grabación y transmisión de imágenes “se desprende que permite la visualización remota vía Internet”

- Que la visualización “vía Internet” supone difusión a un circuito abierto y universal y que supuestamente debe tratarse de un error en el que debería hacerse constar que las imágenes se visualizan “vía Intranet”.

Los denunciantes manifiestan que las imágenes solamente pueden ser visualizadas remotamente vía Intranet y que la existencia de un router implica la externalización de imágenes del circuito cerrado permitiendo su acceso a cualquier persona interna o ajena a la empresa de seguridad responsable que disponga de llave de acceso (password).

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes

extremos:

Con fecha 27 de mayo de 2013 se solicita información al denunciado con relación al sistema de videovigilancia instalado en el Aeropuerto de Son Sant Joan (Palma), tras la instalación del dispositivo router o equipos encaminadores:

- Personas que disponen de acceso a las imágenes captadas por el sistema de videovigilancia tal y como aparece recogido en el documento de seguridad del correspondiente fichero.
- Procedimiento habilitado para garantizar que únicamente las personas autorizadas puedan acceder a las imágenes incluso cuando la transmisión de las imágenes se realice a través de Internet.

En respuesta a la solicitud de información remitida desde esta Agencia el denunciado ha remitido escrito de respuesta con fecha 14 de junio en el que se pone de manifiesto:

- Las personas con acceso a las imágenes grabadas por el sistema de video vigilancia son los operadores y supervisor de la empresa de seguridad G.P.I.S. con CIF *****, personal acreditado con tarjeta de identificación profesional emitida por el Ministerio del Interior y contratada al respecto para dicho fin (adjunta contrato suscrito con dicha entidad).

A las imágenes grabadas también accede el Responsable de Seguridad de la empresa AREAS SA como responsable del fichero.

Las imágenes se visualizan y almacenan en la sede de la empresa de seguridad contratada para dicho fin.

- El procedimiento para el acceso a las imágenes es el siguiente:
 - o El sistema se compone de un Rack de comunicaciones (con llave de seguridad) en el que se almacena un videograbador de seguridad marca VisualTools y un router con línea Telefónica para el traspaso de datos. La contraseña del route se modifica en el momento de su conexión con la empresa de seguridad.
 - o Las imágenes son grabadas a través de las cámaras y estas emiten las mismas al videograbador de seguridad que las encripta y traslada a través de la línea del router a la empresa de seguridad para su descryptación por un software propiedad de la empresa de seguridad con licencias y medidas de seguridad precisa para su visionado.
 - o El acceso a las imágenes se realiza mediante pantalla de acceso con password de 20 dígitos que se modifica cada tres meses por parte del Responsable de Seguridad de AREAS y el Supervisor de la empresa contratada.
 - o La estructura del sistema es completamente cerrada ya que del videograbador a las cámaras analógicas disponen de cableado RG-59 que impide el acceso a las imágenes.
 - o La estructura del sistema es idéntica a la que anteriormente se ha comunicado a esta Agencia y las imágenes grabadas se destruyen cada mes exceptuando las imágenes aportadas a procedimientos

judiciales que se conservan en la empresa de seguridad en zona protegida según reglamento.

Aportan los siguientes documentos:

1. Certificado de autenticidad de los registros de grabaciones en equipos de videovigilancia emitido por la entidad VISUAL TOOLS en el que se hace constar que:
 - Las imágenes almacenadas, la fecha y la hora de las mismas en los grabadores digitales modelos VX4, VX8 y VX16 no pueden ser alteradas tanto si se verifican desde el propio equipo o desde la red con el software Supervisor del fabricante.
 - El sistema de grabación de imágenes es únicamente accesible desde GUI controlado con diferentes niveles de acceso y claves de acceso específicas.
 - La seguridad de los videograbadores VX se soporta en los siguientes aspectos técnicos:
 - o Sistema operativo LINUX empotrado.
 - o Uso de versión DEBIAN GNU/LINUX de reconocida calidad en lo que se refiere a la seguridad.
 - o Existencia de tres únicos puertos TCP/IP abiertos (22, 80 Y 8554).
 - o El sistema permite únicamente su acceso mediante GUI controlado que en remoto utiliza mecanismos de autenticación con sistema challenge con hash que imposibilitan el robo de contraseñas dado que las contraseñas nunca viajan en claro.
 - o La comunicación entre el sistema VX y el supervisor se realiza con autenticación segura que imposibilitan la suplantación del equipo VX por otro dispositivo.
2. Certificado de la entidad VISUAL TOOLS en el que se pone de manifiesto que el sistema de grabación en disco duro modelo VX/VX Suministrado a la empresa AREAS SA para su instalación en el Aeropuerto de Palma de Mallorca cumple en su totalidad con el artículo 120 apartado 1º del Reglamento de Seguridad Privada (Real Decreto 2364/94 de 9 de diciembre).
3. Informe de auditoría de cumplimiento LOPD de febrero de 2013 en el que se incluye la auditoría del fichero de videovigilancia a la empresa de seguridad G.P.I.S.

FUNDAMENTOS DE DERECHO

I

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

II

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

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

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

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

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

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

de la ciudadanía en el sistema democrático”. Sigue señalando: “Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”.

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

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

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

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

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

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

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 D. **A.A.A.** y Dña. **B.B.B.** en calidad de Presidente y Secretario del Comité de Empresa del centro de trabajo de la entidad **AREAS SA** (en adelante el denunciado) en el Aeropuerto de Palma, denuncian la instalación de un dispositivo router a la instalación existente del circuito cerrado de captación de imágenes, lo que implica según manifiesta, la externalización de imágenes del circuito cerrado permitiendo su acceso a cualquier persona interna o ajena a la empresa de seguridad responsable que disponga de llave de acceso (password).

En primer lugar, cabe decir que la LOPD proporciona, como ya ha sido recogido “ut supra”, un amplísimo concepto de tratamiento de datos personales. Serán tratamiento de datos personales las 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. La Directiva 95/46/CE es aún más minuciosa en la enumeración de las operaciones o procedimientos que constituyen tratamiento: recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como bloqueo, supresión o destrucción.

En definitiva, la divulgación o difusión de imágenes de una persona constituye un tratamiento de datos de carácter personal en el sentido expresado en la LOPD y en la Directiva comunitaria.

Ahora bien, y entrando en el fondo de la cuestión planteada relativa a la divulgación de la imagen de los trabajadores de la empresa vía internet sin el consentimiento de éstos, hay que señalar que el artículo 9 de la Ley Orgánica 15/1999, regula la Seguridad de los datos, concretando lo siguiente:

“1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban

reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley”.

El citado artículo 9 de la LOPD establece el “*principio de seguridad de los datos*” imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el “*acceso no autorizado*” por parte de terceros.

Por lo tanto todo, el responsable del fichero y en su caso el encargado del tratamiento deben adoptar las medidas de índole técnica y organizativas necesarias previstas en la LOPD y su Reglamento de desarrollo, que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Con carácter general los ficheros de videovigilancia suelen tener un nivel básico. No obstante el responsable del fichero debe tener en cuenta que deberá evaluar el nivel de seguridad teniendo en cuenta lo dispuesto por el artículo 81 del Reglamento en función del contenido y finalidad del fichero.

El responsable deberá informar a las personas con acceso a los datos sobre sus obligaciones de seguridad y su deber de secreto en los términos del artículo 8 de la Instrucción que recoge: “*El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.*”

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga acceso a los datos deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior”:

Pues bien, una vez establecida la normativa precedente debe decirse que no existe inconveniente en la visualización o grabación de las imágenes a distancia siempre que la entidad denunciada cumpla todos los requisitos en materia de seguridad, recogidos en la normativa de protección de datos.

Así, con fecha 27 de mayo de 2013 se solicita información al denunciado con relación a diversos aspectos del sistema de videovigilancia instalado en el centro de trabajo de la entidad **AREAS, S.A.**, en el Aeropuerto de Son Sant Joan (Palma), tras la instalación del dispositivo router o equipos encaminadores:

- Personas que disponen de acceso a las imágenes captadas por el sistema de videovigilancia tal y como aparece recogido en el documento de seguridad del correspondiente fichero.
- Procedimiento habilitado para garantizar que únicamente las personas autorizadas puedan acceder a las imágenes incluso cuando la transmisión de las imágenes se realice a través de Internet.

En respuesta a la solicitud de información remitida desde esta Agencia el denunciado ha remitido escrito de respuesta con fecha 14 de junio de 2013 en el que se pone de manifiesto que el sistema está compuesto por un rack de comunicaciones (con llave de seguridad); en su interior se encuentra un videograbador de seguridad, un SAI que alimenta el sistema y un router aportado a la contratación de la línea a Telefónica para el traspaso de datos; la contraseña del router es variada en el momento de su conexión con la empresa de seguridad por personal técnico de la misma. Las imágenes son grabadas a través de las cámaras y éstas emiten las mismas al videograbador de seguridad quien las inscripta y traslada a través de la línea del router a la empresa de seguridad para su descryptación por un software propiedad de la empresa de seguridad con sus licencias y las medidas de seguridad precisas para su visionado. Para acceder a ellas se realiza a través de una pantalla y un acceso de 20 dígitos (que se cambia cada tres meses por parte del responsable de Seguridad de **AREAS** y el Supervisor de la empresa contratada) por lo que al desconocer el password nadie tiene acceso a los datos grabados ni a la configuración del sistema. La estructura del sistema es completamente cerrada ya que del videograbador a las cámaras analógicas están cableadas mediante RG-59 evitando que se pueda acceder a ellas. Así las imágenes que se almacenan en el videograbador están encriptadas y solo se pueden trasladar a otro equipo mediante un software propiedad de la empresa **G.P.I.S.** contratada con sus licencias, de la misma empresa fabricante del videograbador.

Las personas con acceso a las imágenes grabadas por el sistema de video vigilancia son los operadores y supervisor de la empresa de seguridad G.P.I.S., personal acreditado con tarjeta de identificación profesional emitida por el Ministerio del Interior y contratada al respecto para dicho fin (adjunta contrato suscrito con dicha entidad). A las imágenes grabadas también accede el Responsable de Seguridad de la empresa **AREAS SA** como responsable del fichero.

Las imágenes se visualizan y almacenan en la sede de la empresa de seguridad contratada para dicho fin y esta tiene adscrito cvomntrato de confidencialidad con la entidad **AREAS S.A.**.

En prueba de todos ello, la entidad denunciada aporta:

1. Certificado de autenticidad de los registros de grabaciones en equipos de videovigilancia emitido por la entidad VISUAL TOOLS en el que se hace constar que:

- Las imágenes almacenadas, la fecha y la hora de las mismas en los grabadores digitales modelos VX4, VX8 y VX16 no pueden ser alteradas tanto si se verifican desde el propio equipo o desde la red con el software Supervisor del fabricante.
- El sistema de grabación de imágenes es únicamente accesible desde GUI controlado con diferentes niveles de acceso y claves de acceso específicas.
- La seguridad de los videograbadores VX se soporta en los siguientes aspectos técnicos:
 - o Sistema operativo LINUX empotrado.



- o Uso de versión DEBIAN GNU/LINUX de reconocida calidad en lo que se refiere a la seguridad.
 - o Existencia de tres únicos puertos TCP/IP abiertos (22, 80 Y 8554).
 - o El sistema permite únicamente su acceso mediante GUI controlado que en remoto utiliza mecanismos de autenticación con sistema challenge con hash que imposibilitan el robo de contraseñas dado que las contraseñas nunca viajan en claro.
 - o La comunicación entre el sistema VX y el supervisor se realiza con autenticación segura que imposibilitan la suplantación del equipo VX por otro dispositivo.
2. Certificado de la entidad VISUAL TOOLS en el que se pone de manifiesto que el sistema de grabación en disco duro modelo VX/VX Suministrado a la empresa AREAS SA para su instalación en el Aeropuerto de Palma de Mallorca cumple en su totalidad con el artículo 120 apartado 1º del Reglamento de Seguridad Privada (Real Decreto 2364/94 de 9 de diciembre).
 3. Informe de auditoría de cumplimiento de la LOPD de febrero de 2013 en el que se incluye la auditoría del fichero de videovigilancia a la empresa de seguridad **G.P.I.S**, recogiendo dicha auditoria que las instalaciones y tratamiento de la citada entidad se adecuan a la legislación actual aplicable en seguridad de tratamiento de datos de carácter personal.

Por lo tanto cabe concluir que, de lo anteriormente expuesto, se desprende que la entidad denunciada cumple la medidas de seguridad exigibles al fichero de videovigilancia del que es titular no produciéndose, como se denuncia, una difusión de las imágenes obtenidas por el sistema de videovigilancia, vía Internet, por lo que se procede al archivo del presente expediente de actuaciones previas.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **AREAS S.A** y a D. **A.A.A.** y D^a. **B.B.B.** .

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