



Expediente Nº: E/01606/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA SAD y SEGUR IBÉRICA SA** en virtud de denuncia presentada por el **SINDICATO AUTONOMO DE TRABAJADORES DE EMPRESAS DE SEGURIDAD** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 16 de enero de 2013 tiene entrada en esta Agencia escrito remitido por el delegado sindical del **SINDICATO AUTÓNOMO DE TRABAJADORES DE EMPRESAS DE SEGURIDAD CATALUNYA (ATES)**, en el que se comunica posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en el Centro Deportivo del **REAL CLUB DEPORTIVO ESPAÑOL (RCDE)** sito en *****POBLACIÓN.1 (BARCELONA)** y cuyo titular es la sociedad **REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA SAD** (en adelante el denunciado).

En el mencionado escrito el denunciante manifiesta la instalación de un sistema de videovigilancia en el Centro Deportivo del RCDE y la existencia de un contrato de servicio de seguridad suscrito con la empresa SEGUR IBÉRICA S.A. El sistema se utiliza con la finalidad de control laboral sin haber sido informados los trabajadores ni sus representantes. Se denuncia que por parte del responsable del fichero existe una cesión de imágenes a terceros.

Adjunta a su denuncia copia de carta de despido de uno de los trabajadores.

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 26 de marzo de 2013 se solicita información a la empresa de seguridad SEGUR IBÉRICA S.A con domicilio en Barcelona, resultando la misma devuelta por el servicio de Correos con la indicación de "DESCONOCIDO".
2. Con fecha 26 de marzo de 2013 se solicita información al titular del sistema, resultando la notificación recepcionada con fecha 4 de abril de 2013.
3. Con fecha 19 de abril de 2013 se solicita información a SEGUR IBÉRICA S.A con domicilio en (C/.....1), resultando la notificación recepcionada con fecha 24 de abril de 2013.
4. Con fecha 24 de abril de 2013 se solicita información al departamento jurídico de la mercantil SEGUR IBÉRICA S.A, teniendo entrada en esta Agencia escrito de fecha 13 de junio de 2013 en el que la representante de la sociedad, comunica:

Se adjunta copia del contrato suscrito con fecha 10 de julio de 2009

entre el RCD ESPANYOL DE BARCELONA SAD y SEGUR IBÉRICA S.A, por el que se encomienda a ésta última los servicios de seguridad privada del estadio del citado Club Deportivo (documento Doc.1) y cuyo objeto queda reflejado (cláusula segunda) en los siguientes términos: "...la prestación...de un servicio de vigilancia y protección".

*SEGUR IBÉRICA S.A tiene conocimiento con fecha 30 de octubre de 2012 de las faltas laborales cometidas por uno de sus trabajadores en el desarrollo del servicio de seguridad prestado en el RCDE sito en ***POBLACIÓN.1 (Barcelona). El procedimiento mediante el cual se le informó de los citados hechos, tuvo el siguiente desarrollo:*

- o *Con fecha 12 de noviembre de 2012, el RCDE remite a SEGUR IBÉRICA S.A escrito de fecha 30 de octubre de 2012, por el que pone en conocimiento de esta empresa las irregularidades constatadas por el responsable del fichero, cometidas por el vigilante de seguridad de SEGUR IBÉRICA S.A en el ejercicio de las funciones de seguridad privada contratadas. En este informe se especifican las actuaciones irregulares del vigilante, algunas de ellas indicadas con fecha y hora de ejecución.*
- o *El citado informe motivó el conocimiento por parte de la empresa de seguridad de las faltas laborales cometidas por el vigilante de seguridad, dando lugar a la sanción disciplinaria correspondiente; es decir al despido del citado trabajador. Se acompaña copia del informe emitido con fecha 30 de octubre de 2012 por el Departamento de Seguridad del RCD Espanyol (documento Doc.2), mediante el cual se solicita "Que el vigilante de Seguridad.... cause baja en el servicio en nuestras instalaciones a partir de este momento"...".Debido al visionado del Sistema del Circuito Cerrado de Televisión y analizando las grabaciones que legalmente realizamos..."*
- o *Se procedió a la comunicación del despido del trabajador con fecha 21 de noviembre de 2012,*
- o *No fue preciso que el RCD Espanyol aportase al Juzgado de lo Social la grabación de los hechos para su visionado, ya que en fase de conciliación judicial se pactó con el trabajador la resolución contractual y sus efectos.*

En la página web de SEGUR IBÉRICA, Portal del empleado, se informa a los trabajadores de la finalidad de los sistemas de videovigilancia en los siguientes términos: ".... que, de acuerdo con lo dispuesto en el artículo 20.3 del Estatuto de los Trabajadores, los sistemas de videovigilancia establecidos en los lugares de trabajo, son utilizados además de para la labor de seguridad privada encomendada, para verificar el cumplimiento y control por el trabajador de sus obligaciones y deberes laborales; pudiendo ser las imágenes grabadas utilizadas para sancionar el incumplimiento de los mismos. Esta doble finalidad de los sistemas de videovigilancia es necesaria e idónea en la actividad desarrollada por los vigilantes, ya que la seguridad privada y el cumplimiento de los deberes laborales

en interés de la misma están intrínsecamente ligadas la seguridad privada y el cumplimiento de los deberes laborales en interés de la misma”.

No obstante, por la propia naturaleza de la relación laboral prestada por los vigilantes de seguridad, éstos conocen sobradamente la existencia de las cámaras instaladas en los lugares vigilados, así como la finalidad de las mismas, entre otras la de controlar el cumplimiento de las obligaciones profesionales.

En documento Doc.3 se acompaña copia del aviso colgado en la web.

No existe un consentimiento expreso firmado por los vigilantes de seguridad para el tratamiento de las imágenes. La legitimación de Secur Ibérica S.A para el tratamiento de datos de carácter personal, como son las imágenes, con fines de vigilancia a través de sistemas de cámaras o videocámaras instalados en el citado centro, viene determinada por la legislación específica existente en materia de Seguridad Privada, como es el RD 195/2010 de 26 de febrero, por el que se modifica el RD 2364/1994 de 9 de diciembre en el que se aprobaba el Reglamento de Seguridad Privada.

En este supuesto, la existencia de las cámaras en las instalaciones del RCDE y en concreto en el cuarto de control en el que los vigilantes de seguridad de la Compañía prestan sus servicios, viene impuesta por la relación contractual suscrita entre SEGUR IBÉRICA y el Club.

Secur Ibérica SL al suscribir el contrato de prestación de servicios con el Club, se hacía cargo de las instalaciones del mismo en las condiciones en las que se encontraba el mismo, es decir con las cámaras de seguridad ya instaladas en sus instalaciones, sin que por parte de la empresa de seguridad se pueda decidir sobre las mismas.

La existencia de cámaras de seguridad en el Estadio de Fútbol responde a la necesidad e idoneidad de las mismas para garantizar la seguridad de las instalaciones y de las personas que acuden a este tipo de actividades deportivas, 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. Cuando el vigilante de seguridad accede a una relación laboral de este tipo, regulada por la Ley de Seguridad Privada, está asumiendo este tratamiento activo y pasivo de las imágenes que captan las cámaras instaladas por el Club Deportivo.

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.

5. Con fechas 24 de mayo y 14 de junio de 2013 se reitera la solicitud de información al responsable del sistema de videovigilancia, teniendo entrada en esta Agencia escrito de fecha 14 de junio de 2013 en el que manifiesta:

*El responsable del sistema de videovigilancia instalado es el **REAL***

CLUB DEPORTIVO ESPANYOL DE BARCELONA SAD.

La instalación del sistema de videovigilancia fue realizada por la empresa PCI SECURITY DOCTORS S.L.

En documento **Doc.4** se adjuntan las copias correspondientes a los Anexo 1 y Anexo 2 al contrato nº 430 de fecha 30 de abril de 2010, suscrito entre el responsable del sistema y la citada empresa de seguridad. El objeto del contrato queda modificado en los siguientes términos:

- o Anexo 1 (cláusula segunda): *“el objeto de este contrato es la prestación por parte de LA EMPRESA la prestación de un servicio de mantenimiento preventivo del sistema de alarma, mantenimiento preventivo de CCTV, mantenimiento preventivo de control de accesos y de otras instalaciones, además de conexión a central de alarmas y otros mantenimientos correctivos”.*
- o Anexo 2 (cláusula segunda): *“el objeto de este contrato es la prestación por parte de LA EMPRESA la prestación de un servicio de visionado durante las noches y fines de semana”.*

La única causa que ha motivado la instalación de un sistema de videovigilancia es la seguridad en el Estadio de fútbol donde se desarrollan actos deportivos y otros eventos de forma ocasional, lo que provoca la presencia de una multitud de personas en nuestras instalaciones.

Existen carteles informativos de zona videovigilada ubicados en distintas partes del estadio, permitiendo con ello que toda persona que acceda a las instalaciones del RCD ESPANYOL SAD conozca la existencia de cámaras de videovigilancia.

Se adjunta fotografía del modelo de cartel informativo instalado (documento **Doc.5**) y copia del modelo de formulario informativo sobre el sistema de videovigilancia (documento Doc.6).

El Director de Seguridad del RCD ESPANYOL, como personal relacionado con el RCD ESPANYOL DE BARCELONA SAD, puede acceder al sistema de videovigilancia y a la visualización de las imágenes captadas.

El responsable del sistema mantiene con la compañía SEGUR IBÉRICA SA una relación mercantil en base a la prestación de servicios de seguridad, mediante contrato privado entre ambas partes suscrito con fecha 10 de julio de 2009 y renovado en iguales condiciones hasta la fecha.

Se aportan copias del contrato inicial de arrendamiento de servicios de seguridad suscrito con fecha 10 de julio de 2009 (documento Doc.7) y del contrato celebrado con fecha 27 de agosto de 2012 (documento Doc.8).

Las imágenes se conservan durante un plazo de 30 días y la persona que puede acceder a las mismas es el Director de Seguridad del RCD ESPANYOL DE BARCELONA SAD.

En documento Doc.9 aporta copia de la notificación remitida por la AEPD en relación a la inscripción en el Registro General de Protección de Datos del fichero denominado "CONTROL DE ACCESO A INSTALACIONES" en el que figura como responsable el *RCD ESPANYOL DE BARCELONA SAD*.

Por parte del Director de Seguridad se observó que un empleado de la compañía SEGUR IBÉRICA S.A se encontraba incumpliendo de forma grave su función de seguridad, señalando tal irregularidad a la citada empresa.

No detalla el procedimiento seguido para el visionado de las imágenes y su comunicación con fecha 30 de octubre de 2012 a la empresa de seguridad SEGUR IBÉRICA S.A.

El responsable del sistema, por motivos estrictamente de seguridad, se ha visto obligado a poner un sistema de videovigilancia en el Estadio de Fútbol para velar por la seguridad de quienes acuden al estadio y en general como medida de protección para evitar que puedan acceder en cualquier momento terceras personas no relacionadas con ninguna actividad del Club. En paneles de información repartidos por todo el Estadio se informa de la existencia de cámaras de videovigilancia y todos los empleados del Club tiene conocimiento verbal y por escrito de dicha circunstancia. A mayor abundamiento, podemos señalar que los empleados de las compañías de seguridad contratadas tienen conocimiento de la existencia de cámaras de videovigilancia, pues dicho personal es quien se ocupa de velar por la seguridad del Club y serán las empresas de seguridad contratadas quienes tendrán la información oportuna del sistema a los mismos.

El sistema de videovigilancia está conectado a central de alarmas con la empresa PCI SECURITY DOCTORS S.L. En documento Doc.4 se adjuntan las copias del contrato de prestación de servicios firmado con la misma (Anexo 1 y Anexo 2).

No se adjuntan copias de la documentación acreditativa de que la empresa de seguridad está autorizada por el órgano administrativo ni de la documentación que permita comprobar que la citada empresa de seguridad ha notificado las características de la instalación de videovigilancia a la autoridad competente.

6. Con fecha 14 de junio de 2013 y mediante diligencia de inspección se constata la existencia del fichero denominado VIDEOVIGILANCIA inscrito con el código *****COD.1**, con la finalidad de videovigilancia de las instalaciones y cuyo responsable es RCD ESPANYOL DE BARCELONA SAD.
7. Con fecha 25 de junio de 2013 y mediante diligencia de inspección se constata la existencia de fichero denominado CONTROL DE ACCESO A INSTALACIONES inscrito con el código *****COD.2**, con la finalidad de la gestión del control de accesos a las instalaciones propias corporativas y cuyo responsable figura RCD ESPANYOL DE BARCELONA SAD.
8. Con fecha 11 de julio de 2013 y previa diligencia telefónica de inspección, se solicita a la entidad SEGUR IBÉRICA S.A información detallada y complementaria sobre el procedimiento seguido para informar a sus

trabajadores de la finalidad del sistema de videovigilancia objeto de esta investigación.

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 el SINDICATO AUTÓNOMO DE TRABAJADORES DE EMPRESAS DE SEGURIDAD CATALUNYA (ATES), manifiesta la instalación de un sistema de videovigilancia en el Centro Deportivo del RCDE y la existencia de un contrato de servicio de seguridad suscrito con la empresa SEGUR IBÉRICA S.A, habiéndose utilizado el sistema con la finalidad de control laboral sin haber sido informados los trabajadores ni sus representantes. Se denuncia que por parte del responsable del fichero existe una cesión de imágenes a terceros.

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 negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.”*

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 e) de la Ley 23/1992, de 30 de julio, de Seguridad Privada, que establece *“1. Con sujeción a lo dispuesto en la presente Ley y en las normas reglamentarias que la desarrollen, las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades: a) Vigilancia y protección de bienes, establecimientos, espectáculos, certámenes o convenciones, b) Protección de personas determinadas, previa la autorización correspondiente, c) Depósito, custodia,*

recuento y clasificación de monedas y billetes, títulos-valores y demás objetos que, por su valor económico y expectativas que generen, o por su peligrosidad, puedan requerir protección especial, sin perjuicio de las actividades propias de las entidades financieras, d) Transporte y distribución de los objetos a que se refiere el apartado anterior a través de los distintos medios, realizándolos, en su caso, mediante vehículos cuyas características serán determinadas por el Ministerio del Interior, de forma que no puedan confundirse con los de las Fuerzas Armadas ni con los de las Fuerzas y Cuerpos de Seguridad, e) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, de conformidad con lo dispuesto en la Disposición adicional sexta, f) Explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas y su comunicación a las Fuerzas y Cuerpos de Seguridad, así como prestación de servicios de respuesta cuya realización no sea de la competencia de dichas Fuerzas y Cuerpos, g) Planificación y asesoramiento de las actividades de seguridad contempladas en esta Ley”.

La existencia de cámaras de seguridad en el Estadio de Fútbol responde a la necesidad e idoneidad de las mismas para garantizar la seguridad de las instalaciones y de las personas que acuden a este tipo de actividades deportivas, 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.

En este supuesto, la existencia de las cámaras en las instalaciones del RCDE y en concreto en el cuarto de control en el que los vigilantes de seguridad de la Compañía prestan sus servicios, viene impuesta por la relación contractual suscrita entre SEGUR IBÉRICA y el Club.

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.

Así, según se señala la entidad *SEGUR IBERICA, SEGUR IBÉRICA S.A*, ésta tiene conocimiento con fecha 30 de octubre de 2012 de las faltas laborales cometidas por uno de sus trabajadores en el desarrollo del servicio de seguridad prestado en el RCDE El procedimiento mediante el cual se le informó de los citados hechos, tuvo el siguiente desarrollo:

- o Con fecha 12 de noviembre de 2012, el RCDE remite a *SEGUR IBÉRICA S.A* escrito de fecha 30 de octubre de 2012, por el que pone en conocimiento de esta empresa las irregularidades constatadas por el responsable del fichero, cometidas por el vigilante de seguridad de *SEGUR IBÉRICA S.A* en el ejercicio de las funciones de seguridad privada contratadas. En este informe se especifican las actuaciones irregulares del vigilante, algunas de ellas indicadas con fecha y hora de ejecución.
- o El citado informe motivó el conocimiento por parte de la empresa de seguridad de las faltas laborales cometidas por el vigilante de seguridad, dando lugar a la sanción disciplinaria correspondiente; es decir al despido del citado trabajador. Se acompaña copia del informe emitido con fecha 30 de octubre de 2012 por el Departamento de Seguridad del RCD Espanyol, mediante el cual se solicita “Que el vigilante de Seguridad.... cause baja en el servicio en nuestras instalaciones a partir de este momento”...”...Debido al visionado del Sistema del Circuito Cerrado de Televisión y analizando las grabaciones que legalmente realizamos...”.

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 del *RCD Espanyol*, 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

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 cartel informativo de zona videovigilada, ubicados en distintas zonas del estadio, informándose sobre la existencia de cámaras, y el responsable del sistema, de acuerdo 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.

Pero es que además respecto a los trabajadores de SEGUR IBÉRICA, en la página web de dicha empresa , Portal del empleado, se informa a los trabajadores de la finalidad de los sistemas de videovigilancia en los siguientes términos: *"... que, de acuerdo con lo dispuesto en el artículo 20.3 del Estatuto de los Trabajadores, los sistemas de videovigilancia establecidos en los lugares de trabajo, son utilizados además de para la labor de seguridad privada encomendada, para verificar el cumplimiento y control por el trabajador de sus obligaciones y deberes laborales; pudiendo ser las imágenes grabadas utilizadas para sancionar el incumplimiento de los mismos. Esta doble finalidad de los sistemas de videovigilancia es necesaria e idónea en la actividad desarrollada por los vigilantes, ya que la seguridad privada y el cumplimiento de los deberes laborales en interés de la misma están intrínsecamente ligadas la seguridad privada y el cumplimiento de los deberes laborales en interés de la misma".*

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 CONTROL DE ACCESO A INSTALACIONES, cuyo responsable es el RCD ESPANYOL DE BARCELONA, S.A.D.

Asimismo, de acuerdo con dicha inscripción, los “Colectivos o categorías de interesados” a los que el fichero se refiere son: “Proveedores, empleados, Clientes y usuarios.”.

V

Por otro lado, en cuanto a la cesión a terceros denunciada, 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.

Pues bien, en el caso que se plantea el responsable de las instalaciones y el sistema de videovigilancia es la entidad REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA; y SEGUR IBÉRICA S.A. es la entidad encargada de los servicios de seguridad privada del estadio, en virtud de contrato suscrito con fecha 10 de julio de 2009 entre el RCD ESPANYOL DE BARCELONA SAD y SEGUR IBÉRICA S.A, y cuyo objeto queda reflejado (cláusula segunda) en los siguientes términos: *“...la prestación... de un servicio de vigilancia y protección”*. Posteriormente con fecha 30 de abril de 2010 se añaden los Anexos 1 y Anexo 2 al contrato, suscrito entre el responsable del sistema y la citada empresa de seguridad, siendo el objeto del contrato modificado en los siguientes términos:

- o Anexo 1 (cláusula segunda): *“el objeto de este contrato es la prestación por parte de LA EMPRESA la prestación de un servicio de mantenimiento preventivo del sistema de alarma, mantenimiento preventivo de CCTV, mantenimiento*

preventivo de control de accesos y de otras instalaciones, además de conexión a central de alarmas y otros mantenimientos correctivos”.

- o Anexo 2 (cláusula segunda): *“el objeto de este contrato es la prestación por parte de LA EMPRESA la prestación de un servicio de visionado durante las noches y fines de semana”.*

Por lo tanto a través del contrato suscrito entre el responsable REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA 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, control y mantenimiento de las cámaras de seguridad. Así la citada empresa actuaría por cuenta del responsable del fichero, en este caso REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA, 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.

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”.*

Asimismo dada la relación contractual entre REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA y SEGUR IBÉRICA S.A., para la que el trabajador despedido prestaba sus servicios en las instalaciones de aquella, estaría justificada la información que REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA pudiera suministrar sobre la conducta del trabajador, (contraria a las condiciones contractuales pactadas entre ambos), que de acuerdo con el Estatuto de los Trabajadores le 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.

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

VI

En cuanto a la alegación de que los trabajadores no han sido informados de la finalidad de las cámaras, no cabe sino reiterar que, de acuerdo con la información obrante en el expediente, dicho sistema de videovigilancia tenía por objeto la seguridad.

En consecuencia, el seguimiento realizado a dichos efectos no se circunscribe

dentro del marco de un sistema de videocámaras con fines de control empresarial cuya finalidad principal sea captar y grabar las imágenes de los trabajadores, sino en el ámbito de la utilización de dicho sistema para fines de seguridad, ajenos al desarrollo de la actividad laboral.

Ello no obsta para que, según se pone de manifiesto en las actuaciones, las imágenes obtenidas provocaran, asimismo, el despido del trabajador por parte de la empresa de seguridad.

De este modo, junto con la finalidad propia de las videocámaras instaladas, vinculadas a la seguridad, no puede desconocerse que, en determinados supuestos -como el que es objeto de las presentes actuaciones-, de la captación legítima de las imágenes por parte del responsable del fichero con relevancia en materia de seguridad, puedan derivar consecuencias de índole diversa, tanto en el ámbito penal, como administrativo, o incluso laboral.

En el presente caso, del contenido de las actuaciones se desprende que el motivo del visionado del vídeo por parte del responsable del sistema fue diversos incumplimientos producidos por un trabajador de la empresa de seguridad contratada, en su jornada de trabajo, con abandono reiterado de su puesto o incumplimiento de protocolos, por lo que podemos entender que el REAL CLUB DEPORTIVO no utilizó las imágenes captadas por las video cámaras para el control laboral de los trabajadores de la empresa de seguridad, sino por estrictos motivos de seguridad, quedando condicionada la procedencia o no del despido a los procedimientos correspondientes, dilucidándose en este expediente únicamente la utilización de las imágenes para proceder al mismo.

Cuestión distinta sería la utilización de las imágenes para cuestiones estrictamente laborales como la alegada de incumplir la idoneidad de su presencia, en cuanto al vestuario, no vinculadas con seguridad, que en su caso derivaron en despido. Finalidad para cuyo uso se requiere como establece el Tribunal Constitucional en su sentencia 24/2013 de 11 de febrero (F.J 8): *“la 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”*. Ahora bien, en este caso, como ya ha sido establecido anteriormente, también los trabajadores fueron informados en la página web de SEGUR IBÉRICA, Portal del empleado, de la finalidad de los sistemas de videovigilancia en los siguientes términos: *“.... que, de acuerdo con lo dispuesto en el artículo 20.3 del Estatuto de los Trabajadores, los sistemas de videovigilancia establecidos en los lugares de trabajo, son utilizados además de para la labor de seguridad privada encomendada, para verificar el cumplimiento y control por el trabajador de sus obligaciones y deberes laborales; pudiendo ser las imágenes grabadas utilizadas para sancionar el incumplimiento de los mismos. Esta doble finalidad de los sistemas de videovigilancia es necesaria e idónea en la actividad desarrollada por los vigilantes, ya que la seguridad privada y el cumplimiento de los deberes laborales en interés de la misma están intrínsecamente ligadas la seguridad privada y el cumplimiento de los deberes laborales en interés de la misma”*.

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 del REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA SAD 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:

- o **PROCEDER AL ARCHIVO** de las presentes actuaciones.
- o **NOTIFICAR** la presente Resolución a **REAL CLUB DEPORTIVO ESPANYOL DE BARCELONA SAD**, a **SEGUR IBÉRICA SA** y a **SINDICATO AUTONOMO DE TRABAJADORES DE EMPRESAS DE SEGURIDAD**.

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