Expediente Nº: E/03357/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ***SEGUR IBÉRICA S.A., y SERVICIO GALEGO DE SALUD (SERGAS)*** en virtud de denuncia presentada por Dª. ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 20 de mayo de 2014 tiene entrada en esta Agencia escrito de Dª.***A.A.A.*** (en adelante la denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad ***SERVICIO GALEGO DE SALUD (SERGAS)*** instaladas en ***"HOSPITAL UNIVERSITARIO XERAL DE VIGO"*** ubicado en ***(C/.....1)*** bajo el servicio de control de la entidad ***SEGUR IBÉRICA S.A.***

La denunciante manifiesta que:

1. *Que quien suscribe mantiene una relación laboral con SEGUR IBÉRICA, S.A. desde el año 2009.*
2. *Que SEGUR IBÉRICA, S.A. con domicilio en calle (C/.....2) entreplanta, del municipio de A Coruña, es una empresa dedicada a la seguridad privada, que presta sus servicios a entidades públicas y privadas, y en lo que nos atañe, presta servicios de seguridad privada para el SERVICIO GALEGO DE SALUD (SERGAS).*
3. Que el SERVICIO GALEGO DE SALUD (SERGAS) cuenta con sistemas de videovigilancia con fines de seguridad instalados en los distintos complejos hospitalarios y otros centros dependientes, entre ellos, Complexo Hospitalario Universitario Xeral Cies de Vigo, encuadrado en el COMPLEXO HOSPITALARIO DE VIGO (CHUVI), cuyas cámaras se hallan señalizadas (adjunto documento nº1) y el correspondiente fichero, inscrito ante la Agencia Española de Protección de Datos.
4. *Por lo expuesto, entiende la denunciante que SERVICIO GALEGO DE SALUD (SERGAS) es el RESPONSABLE DEL FICHERO, siendo SEGUR IBÉRICA, S.A., EL ENCARGADO DE TRATAMIENTO.*

La denunciante denuncia los siguientes hechos:

1. El pasado 5 de noviembre de 2013 SEGUR IBÉRICA, S.A. sancionó a la denunciante por falta laboral grave aduciendo que "(.) usted había sido vista utilizando el teléfono móvil cuando se encontraba en el pasillo (...) descuidando por completo sus funciones", adjunto escrito de comunicación de sanción al trabajador. (Documento nº2)

2. Quien suscribe se opuso a la sanción impuesta siguiendo para ello el procedimiento previsto, esto es, presentación de papeleta de conciliación ante el SMAC, posterior demanda ante el JUZGADO DE SOCIAL DE VIGO y celebración de JUICIO ORAL, aporto documentación acreditativa del procedimiento descrito. (Documento nº3).

3. Que es en el curso de la vista oral cuando las partes presentan los medios de

prueba, y fue en este momento procesal cuando SEGUR IBERICA, S.A. procedió a la muestra de una grabación extraída de las cámaras de seguridad instaladas en el Complexo Hospitalario Universitario Xeral Cies de Vigo en las que se mostraban imágenes de la trabajadora, captadas en el centro de trabajo y encaminadas a demostrar la falta laboral grave que se dirimía en la vista oral.

4. De la captación de estas imágenes para fines de CONTROL LABORAL no se informó a ninguno de los trabajadores de SEGUR IBÉRICA, S.A., asimismo, desconoce esta parte:

A) Si la extracción de estas imágenes del sistema de grabación del SERVICIO GALEGO DE SALUD (SERGAS), su traslado y posterior tratamiento para fines no declarados fue autorizado por EL RESPONSABLE DEL FICHERO,

B) Si el acceso a las imágenes se realizó por personal autorizado expresamente por el responsable del fichero. En el caso del SERVICIO GALEGO DE SALUD (SERGAS) cualquier acceso a las imágenes o grabaciones debe ser autorizado y registrado por el COORDINADOR DE SEGURIDAD Y firmado por LA GERENCIA.

C) Si se vulneraron las medidas de seguridad y plazos de conservación desarrollados por a ley 23/1992 de 30 de julio, se seguridad privada, su reglamento de desarrollo, LOPD e Instrucción 1/2006.

5. Que siendo SEGUR IBÉRICA S.A el ENCARGADO DE TRATAMIENTO, no consta a quien suscribe la cesión autorizada de las imágenes por parte del RESPONSABLE DEL FICHERO para fines distintos de los contratados, y mucho menos para su utilización en el marco de un procedimiento laboral en el que el RESPONSABLE DEL FICHERO no es parte.

Aporta copia de DNI, fotos de carteles informativos, copia de comunicación de sanción al trabajador de 5 de noviembre de 2013 por parte de SEGUR IBERICA, S.A., copia delL procedimiento de conciliación ante el Servicio de Mediación, Arbitraje y Conciliación (SMAC), demanda ante el Juzgado de lo Social de Vigo y celebración de juicio oral, con fallo desestimatorio de la demanda de impugnación de sanción interpuesta por la denunciante contra SEGUR IBERICA, S.A.

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 4 de junio de 2014 se solicita información al ***HOSPITAL UNIVERSITARIO XERAL CIES*** y al ***SERVICIO GALEGO DE SALUD (SERGAS)*** teniendo entrada en esta Agencia con fecha 25 de junio escrito del SERGAS, Gerente de Gestión de Integrada de Vigo en el que manifiesta:

1. *El responsable del sistema de videovigilancia instalado en el Hospital Xeral de Vigo es Xerencia de Xestión Integrada de Vigo.*
2. *Realizó la instalación del sistema de videovigilancia: Sistemas de Seguridade A1, S.L.,*
3. *Causas que han motivado la instalación de las cámaras: "Garantizar 'que solo las personas expresamente autorizadas puedan acceder a las áreas restringidas, verificando su identidad de forma automatizada; disponer de los*

medios necesarios para gestionar posibles incidentes de seguridad".

4. *Se adjunta cartel donde se informa de la existencia de cámaras de videovigilancia y se identifica al responsable: "Xerente do CHUVI, (C/.....1)". Los carteles se ubican en la zona que abarca cada cámara. (Anexo 1).*
5. *Se adjunta modelo del formulario informativo, donde se indica que el destinatario de los datos personales es SEGUR IBÉRICA S.A. y el responsable del fichero es XERENTE DE XESTIÓN INTEGRADA DE VIGO, (C/.....1). (Anexo 2).*
6. *Se adjunta detalle del número de cámaras instaladas, numeradas e indicando las que tienen el sistema DOMO. Se adjuntan planos de situación. (Anexo 3).*
    a. Tres cámaras son domo del total de dieciséis. Las cámaras 1, 2, 3, 4, 5 y 7 están ubicadas enfocando hacia zona exterior pero dentro del recinto del hospital, de modo que la vía captada forma parte del complejo hospitalario.

Se adjunta diligencia con plano de GoogleMaps donde se han situado estas seis cámaras.

7. *Se adjuntan fotografías de cada cámara numerada y fotografías de las imágenes que capta. (Anexo 4).*
8. *Se adjunta fotografía de los monitores donde se visualizan las imágenes de las cámaras. (Anexo 5).*

En la fotografía se aprecia lo que parece ser una sala de control, con tres monitores.

9. *Se adjunta relación de las personas pertenecientes a la empresa de seguridad "Segur Ibérica S.A.", que pueden acceder al sistema de videovigilancia; especificando las que estuvieron el día del incidente. (Anexo 6).*

Entre las personas identificadas en el turno de mañana del 30 de octubre de 2012 se encuentra la denunciada.

10. *Las imágenes se graban en un videograbador, guardándose durante diez días y destruyéndose en el onceavo.*

El nombre del fichero inscrito en el Registro General de Protección de Datos es: "Seguridad física y control de accesos", creado por disposición general en el Diario Oficial de Galicia, núm. 23 del 03 de febrero de 2009; nombre de la disposición: "Orden del 13 de enero de 2009 por la que se crean determinados ficheros de datos de carácter personal en la Consejería de Sanidad y en el Servicio Gallego de Salud".

Mediante diligencia se ha comprobado la inscripción en el Registro General de esta Agencia de un fichero denominado **SEGURIDAD FISICA Y CONTROL DE ACCESOS** inscrito con el código número ******COD.1***, cuyo responsable es **SERVICIO GALLEGO DE SALUD** con CIF ************* y Disposición General de creación Boletín 23 de 3/3/2009 del Diario Oficial de Galicia.

Con fecha 4 de junio de 2014 se solicita información a ***SEGUR IBERICA S.A.*** en la sede de Madrid y con fecha 22 de julio en la sede de La Coruña, ambas con indicación de "ENTREGADO" por el Servicio de Correos, no habiendo obtenido respuesta a fecha del presente informe.

En concreto se solicitaba información sobre:

- el procedimiento empleado para informar a los trabajadores de su empresa, así como del COMPLEXO HOSPITALARIO DE VIGO (CHUVI) de la finalidad por la cual se han instalado las cámaras de videovigilancia y adjuntar la documentación acreditativa del cumplimiento del citado procedimiento.

- Detalle de las personas que pueden acceder al sistema de videovigilancia instalado. Si el acceso está permitido a terceros, adjuntar copia del contrato correspondiente. Deberá especificarse claramente qué personas o personas accedieron a las imágenes grabadas el pasado 30 de octubre de 2013 en relación con un incidente que tuvo lugar en el centro de trabajo, y que dio lugar a la imposición de una sanción disciplinaria a una trabajadora del COMPLEXO HOSPITALARIO DE VIGO (CHUVI).

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 los 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.

III

En el presente expediente Dª. ***A.A.A.***, vigilante de seguridad de la empresa ***SEGUR IBÉRICA S.A.***, comunica posible infracción a la Ley Orgánica 15/1999 motivada por la utilización por parte de la empresa ***SEGUR IBÉRICA***, de las grabaciones realizadas por las cámaras de videovigilancia cuyo responsable es el ***SERVICIO GALEGO DE SALUD(SERGAS***), instaladas en el complejo hospitalario Universitario Xeral Cies de Vigo. La denunciante manifiesta que las grabaciones realizadas el día 30 de octubre de 2013 por el citado sistema de videovigilancia fueron aportadas por la empresa SEGUR IBÉRICA, para la que la denunciante presta sus servicios, en el Juzgado de lo Social de Vigo como prueba de la falta laboral grave que se dirimía en el citado Juzgado.

En primer lugar, hay que tener en cuenta, el tipo de instalaciones en el que se encuentra el sistema de videovigilancia y la importancia del mismo y que por lo tanto, la finalidad del sistema de videovigilancia instalado en el complejo hospitalario es la de garantizar que solo las personas expresamente autorizadas puedan acceder a las áreas restringidas, verificando su identidad de forma automática, así como disponer de los medios necesarios para gestionar posibles incidentes de seguridad.

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 complejo hospitalario responde a su necesidad e idoneidad para garantizar la seguridad y protección de las instalaciones, bienes y personas, 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, como se ya se ha recogido, es la de garantizar el control de acceso de las personas y la seguridad, pero parte esencial de esta seguridad es el cumplimento de las obligaciones del personal a cargo de la empresa de seguridad contratada al respecto.

IV

Una vez realizada la precisión anterior, para analizar la cuestión planteada, de cesión de imágenes, debe partirse de los conceptos de responsable y encargado del

tratamiento contenidos en la Ley Orgánica 15/1999.

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

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

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

No obstante lo anterior, la propia LOPD habilita, en su artículo 12, el acceso de terceros a los datos personales cuando el acceso a los datos se realice para prestar un servicio al responsable del fichero o del tratamiento, al señalar en su apartado 1: *"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento."*

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

A este respecto, el responsable del sistema de videovigilancia instalado en el Hospital Xeral de Vigo es el SERVICIO GALLEGO DE SALUD, y SEGUR IBÉRICA es la empresa que tiene encargada la seguridad y vigilancia del citado centro hospitalario, para la que la denunciante presta sus servicios.

Por lo tanto, a través del contrato suscrito entre el responsable SERVICIO GALLEGO DE SALUD y el encargado SEGUR IBÉRICA, éste trata los datos conforme a las instrucciones del responsable, entre cuyas faenas encomendadas se encuentra la seguridad del centro hospitalario garantizando que solo las personas expresamente autorizadas puedan acceder a las áreas restringidas y gestionar posibles incidentes de seguridad. De tal forma que el incumplimiento de la normativa de seguridad establecida, podría dar lugar a una penalización contractual a SEGUR IBÉRICA como encargada de su cumplimiento. Así la citada empresa actuaría por cuenta del responsable del fichero, no entendiéndose la existencia de una cesión de datos ilegítima, siendo el acceso a los datos por parte de SEGUR IBÉRICA necesarios para la prestación de un servicio al responsable del tratamiento.

Por otro lado, respecto a que las cámaras se han utilizado por parte de SEGUR IBÉRICA para una finalidad distinta a la que le es propia, cabe decir que la finalidad del sistema de videovigilancia denunciado no tiene como finalidad controlar la prestación de servicios de los trabajadores (vigilantes de seguridad) de SEGUR IBÉRICA sino como ya se ha dicho la finalidad del sistema de videovigilancia es la seguridad del centro

hospitalario, verificando el acceso de las personas.

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

V

En cuanto a las manifestaciones de la denunciante relativas a que la captación de las imágenes para fines de control laboral no se informó a ningún trabajador de SEGUR IBÉRICA, no cabe sino reiterar que, de acuerdo con la información obrante en el expediente, dicho sistema de videovigilancia tenía por objeto la seguridad y no el control laboral de los trabajadores.

Debe tenerse en cuenta que, en el presente caso lo que procede examinar no es la utilización del sistema de videovigilancia del centro hospitalario para el control laboral del denunciante, sino el hecho de que la imagen del denunciante, como trabajador de la empresa de seguridad que presta su servicios para el citado centro, fuera objeto de captación, grabación y tratamiento en el marco del sistema de videovigilancia implantado por el mismo con fines de seguridad.

Debe significarse que los hechos captados por las cámaras y que derivaron en efectos laborales, se relacionan con cuestiones de seguridad imputadas a la denunciante y captadas por las cámaras. Así, la propia Sentencia nº 00226/2014, dictada por el Juzgado de los SOCIAL Nº 5 DE Vigo, en fecha 26 de marzo de 2014 se recoge en su Fundamento de Derecho Segundo: *"(…) es de significar que la secuencia fáctica anteriormente relatada deriva de la prueba documental unida a las actuaciones, de la grabación reproducida en el acto del juicio y de las testificales depuestas a instancia de empresa y trabajadora demandante en las que nítidamente se observa a ésta ensimismada en la utilización de un móvil que el inspector de servicios de servicios ha descartado que se corresponda con el modelo facilitado por la empresa, sin que a lo largo de unos dos minutos y medio se preocupe de realizar una mínima vigilancia o control sobre las personas que acceden al edificios, desviando toda su atención hacia el teléfono móvil, lo cual denota una clara desatención en el desempeño de sus atribuciones, porte que no pasa desapercibido para algún facultativo que mira a la actora con cierta cara de asombro. De igual modo a través de la documental aportada y la testifical depuesta ha quedado certificada que la actora es contumaz en tales actitudes… "*

Por lo tanto se le imputaba a la denunciante una falta de vigilancia o control de las personas que acceden al edificio, por lo tanto motivos de seguridad estrictamente.

Debe recordarse que el sistema de videovigilancia instalado en el centro hospitalario no ha quedado acreditado que tenga como objeto realizar el control laboral de los trabajadores sino garantizar que solo las personas expresamente autorizadas puedan acceder a las áreas restringidas, verificando su identidad de forma automatizada; así como gestionar posibles incidentes de seguridad.

El seguimiento y utilización de las imágenes de las videocámaras se produjo en consecuencia para fines de seguridad, detectando a través de las mismas un problema de seguridad provocado por la denunciante en su desempeño laboral.

Ello no obsta para que, según se pone de manifiesto en las actuaciones, las imágenes obtenidas, fueran aportadas por la empresa de seguridad, para la que presta sus servicios la denunciante, para demostrar los hechos de los que se le acusaba en el ámbito laboral derivado del problema de seguridad creado.

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 puedan derivar consecuencias de índole diversa, tanto en el ámbito penal, como administrativo, o incluso laboral, circunstancia que se produce con más habitualidad en el colectivo de vigilantes de seguridad por la índole del trabajo desempeñado.

VI

Se deben estudiar las implicaciones que lo denunciado presenta al respecto del derecho a la protección de datos en relación con el derecho a la tutela judicial efectiva de los protagonistas, por lo que partiremos de un análisis general relativo a la conexión de dichos derechos. Así, al respecto del derecho a la tutela judicial efectiva, nuestra norma suprema en el artículo 24 de la Constitución Española, en sus apartados 1 y 2, dispone lo siguiente:

"1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que en ningún caso, pueda producirse indefensión.

2. Asimismo, todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa."

Así, constitucionalmente se consagra el derecho de los ciudadanos, ya sean personas físicas o jurídicas, a la tutela judicial efectiva y al derecho a utilizar los medios de prueba que consideren adecuados para el sostenimiento de su pretensión en sede judicial. Sin embargo, de dicha previsión, surge una colisión entre el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva de los jueces y tribunales referida, contenido en el artículo 24 de la Constitución, anteriormente trascrito, dadas a los bienes jurídicos afectados en su aplicación.

Por ello, ante tales situaciones, el Legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio Legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula la materia protegida.

En efecto, la exigibilidad del consentimiento del titular de los datos que pudieran ser objeto de un tratamiento en un procedimiento judicial, para dicho tratamiento de sus datos, supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que una persona pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos o la dependencia en su aplicación a quien manejara la titularidad del dato, implicaría, lógicamente, una merma en la posibilidad de aportación por el interesado de *"los medios de prueba pertinentes para su defensa",* vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) *"el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".*

Por otro lado, junto a lo dispuesto en el artículo 6.2 de la LOPD, el artículo 11 de la LOPD, recoge otras excepciones, a la exigencia del consentimiento:

"1.- Los datos de carácter personal objeto de 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.

2.-El consentimiento exigido en el apartado anterior no será preciso:

a.-Cuando la cesión esté autorizada en una ley.(…)

d.-Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.(…)"(el subrayado es de la Agencia Española de Protección de Datos).

En este sentido, entraría en liza lo dispuesto en el artículo 299 de la Ley 1/2000, de 7 de enero de Enjuiciamiento Civil, que admite la aportación como medio de prueba, de medios de reproducción de imágenes que sean relevantes para el proceso. Así establece, el precitado artículo:

"1. Los medios de prueba de que se podrá hacer uso en juicio son:

1. Interrogatorio de las partes.
2. Documentos públicos.
3. Documentos privados.
4. Dictamen de peritos.
5. Reconocimiento judicial.
6. Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso..

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias".

Por lo tanto, en cuanto a lo aportado en un juicio, dicho cuerpo legal admite la aportación como medio de prueba de los medios de reproducción de la palabra, el sonido y la imagen, lo cual implica la posibilidad de tratamiento de datos dentro de dichas propuestas de prueba, debiendo ser el correspondiente órgano jurisdiccional quien se manifestara sobre la legitimidad de lo presentado. Además, hemos de tener en cuenta que, la Audiencia Nacional en sentencia de 22 de octubre de 2010 (rec. 409/2009) nos dice, en cuanto a la obtención de medios probatorios y su validez en el procedimiento, pese a no ser solicitadas ni obtenidas por vía judicial, lo siguiente:

"De un lado ha de tenerse en cuenta que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD).

Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien inicialmente no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, parecer ser, y así se desprende del acta de juicio, ocurrió en el presente supuesto.

Por otra parte, y si bien es cierto que los procedimientos judiciales tampoco son ajenos a la normativa de protección de datos, tal y como indicamos en la SAN 9-10-2009 (Rec. 37/2009) dado que el derecho de protección de datos, en cuanto derecho fundamental y autónomo previsto en el artículo 18.4 CE , vincula a todos los poderes públicos (Art. 53 CE) y entre ellos al Poder Judicial, tal y como igualmente indica la STS 18-9-2006 Rec. 274/2002 . Sin embargo dicha LOPD debe ser aplicada con gran cautela, y en la medida en que resulte compatible con las funciones propias (jurisdiccionales y no jurisdiccionales) de los referidos órganos judiciales, pues la singularidad de la actividad jurisdiccional y los intereses que en ella subyacen, exigen en ocasiones una limitación o modulación de los derechos y garantías de los ciudadanos.

Además de que el sometimiento de los ficheros judiciales a la LOPD ha de entenderse (según la misma SAN 9-10-2009 Rec. 37/2009) sin menoscabo de la función jurisdiccional y, por tanto, atinente a lo que debe considerarse como "aspecto accesorio" o administrativo de la función jurisdiccional, centrándonos concretamente en el procedimiento judicial, existen también en él una serie de intereses y garantías que ostentan un trascendente valor en dicho proceso, tales como el del verdadero esclarecimiento de los hechos o el legítimo ejercicio del derecho de defensa de las partes, que han de ser ponderados en aquellos casos en que dichos intereses y garantías confluyen con el derecho contemplado en el artículo 18.4 CE , hasta el punto

de que pueden llegar a implicar una importante limitación de tal derecho de protección de datos personales."

Así las cosas, es el órgano judicial correspondiente quien se debe manifestar sobre la legitimidad de la prueba aportada, y en el caso que nos ocupa se ha manifestado sobre su legitimidad en la propia sentencia dictada, dado que fue admitida y constituyó prueba fundamental para determinar la sentencia que se dicta al respecto.

VII

Por último, 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 por el Servicio Gallego de Salud, fotografías de la existencia de carteles informativos de zona videovigilada, ubicados en las zonas que abarcan cada cámara, 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.

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."

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 de 13 de enero de 2009 de la Consellería de Sanidad, publicada en el Boletín Oficial de Comunidades nº 23 de fecha 3 de febrero de 2009, por la que se crean determinados ficheros de datos de carácter personal en la Consellería de Sanidad y en el Servicio Gallego de SALUD, en el que figura el de "Seguridad física y control de accesos".

Asimismo en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos, consta debidamente inscrito en fecha 20 de abril de 2009, el fichero denominado "SEGURIDAD FÍSICA Y CONTROL DE ACCESO" cuyo responsable es el ***SERVICIO GALLEGO DE SALUD.***

Asimismo, de acuerdo con dicha inscripción, los "Colectivos o categorías de interesados" a los que el fichero se refiere son: *"Clientes y usuarios, empleados, proveedores, personas que acceden a las sedes y establecimientos".*

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

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 ***SEGUR IBÉRICA S.A., SERVICIO GALEGO DE SALUD (SERGAS)*** y a ***A.A.A..***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

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