



Expediente Nº: E/03916/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 27 de marzo de 2013 tiene entrada en esta Agencia escrito remitido por D. **A.A.A.** (en adelante el denunciante) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en la parcela sita en la finca **C.C.C., F.F.F., H.H.H. de G.G.G.**, cuyos titulares son D. **B.B.B.** y Dña. **E.E.E.** (en adelante los denunciados).

En su escrito el denunciante manifiesta la instalación de un sistema de videovigilancia en la vivienda propiedad de los denunciados, captando imágenes del camino común que da acceso a la propiedad del denunciante. La instalación se ha realizado sin permiso del denunciante. Existen carteles informativos en los que no se indica los datos del responsable ante quien poder ejercitar los derechos ARCO.

Se adjunta a la denuncia: (1) reportaje fotográfico, (2) copias de los escritos remitidos a los denunciados, solicitando entre otros la retirada de las cámaras y (3) copia de la denuncia interpuesta ante la Guardia Civil de Lora del Rio en relación a la instalación de las cámaras de videovigilancia.

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 18 de julio de 2013 se solicita información a los titulares del sistema, teniendo entrada en esta Agencia escrito de fecha 16 de agosto de 2013 en el que manifiestan:

Ser los responsables del sistema de videovigilancia instalado.

*Los denunciados junto al denunciante, son propietarios en proindiviso de la parcela sita en **C.C.C., F.F.F.** de **G.G.G.**.*

Se adjunta copia de la escritura de propiedad (documento Doc.1).

Dos meses antes de la instalación del sistema se produjeron una serie de robos, destrozos y actos vandálicos en la parte de proindiviso pertenecientes a los denunciados, además de aparecer abierta en varias ocasiones la puerta de la cancela que da acceso a la finca.

Se acompaña reportaje fotográfico acreditativo (fotos 1-19, fotos 36-41)

Por tanto se tomó la decisión de instalar, personalmente y

en el ámbito familiar, dos cámaras de videovigilancia orientadas hacia la piscina y césped, y hacia la cancela de entrada a la finca.

Las cámaras de seguridad grabaron el día 11 de noviembre de 2012 al autor del destrozo de la cancela de entrada. En las fotografías adjuntas nº 20-35 se adjuntan las imágenes extraídas de la cámara de seguridad.

*En Sentencia de 21 de mayo de 2013 dictada por el Juzgado de Primera Instancia e Instrucción nº 2 de Lora del Río, se le condena a D. **A.A.A.** como el autor responsable de una falta de daños... (documento Doc.2).*

Existen carteles informativos de zona videovigilada, en los que no se indican los datos de la persona responsable para el ejercicio de los derechos ARCO. Se encuentran ubicados en la fachada de la casa y en la zona de piscina y césped (documento fotográfico fotos 46-49).

No se dispone de formularios informativos para el ejercicio de los derechos ARCO.

Se adjunta foto aérea de la finca (documento doc.4) en la que se delimita por colores, las parcelas resultantes de la división particular en proindiviso, el camino de acceso común a la finca, la cancela de entrada a la misma y se señala la colocación de las dos cámaras de videovigilancia.

Las cámaras instaladas, no disponen de zoom ni posibilidad de movimiento. En documento Doc.5 se acompaña reportaje fotográfico de las cámaras (fotos 50-51) y del espacio que captan siguiendo el ángulo de orientación de las mismas (fotos 52-53).

Existe un monitor donde se visualizaban las imágenes (fotos 54-56) ubicado en el interior de la vivienda, cuyo acceso estaba restringido a los denunciados.

Las imágenes se han grabado en disco duro, con un tiempo de conservación de siete días y transcurrido el mismo se borran. El acceso a las grabaciones estaba limitado a los denunciados.

Desde el 11 de noviembre de 2012, fecha en la cual se constató la autoría de los destrozos en la cancela de acceso a la finca y una vez puestas a disposición del juez las imágenes captadas, el sistema se desconectó y no ha vuelto a funcionar.

2. Con fecha 20 de septiembre de 2013 se solicita colaboración a la JEFATURA DE POLICÍA LOCAL DE LORA DEL RÍO, con objeto de realizar las actuaciones oportunas encaminadas a determinar los aspectos del sistema de videovigilancia denunciado.

Teniendo entrada en esta Agencia escrito de fecha 26 de septiembre de 2013 en el que el Jefe de Policía Local informa:

*Personados agentes de esa Policía Local en la finca D.D.D., se entrevistan con D. **B.B.B.**, el cual muestra a los agentes la ubicación de las cámaras denunciadas;*

manifestándoles que instaló las cámaras en su día, debido a una serie de daños sufridos de manera continuada sobre las plantas y la cancela de entrada.

Los citados hechos pudieron ser constatados por los agentes.

En el lugar donde se encontraba instalado el sistema de videovigilancia se observa en la parte superior dos cajas de registro de luz, a las cuales se les ha practicado un pequeño orificio, y donde en su interior se ubicaban las cámaras de pequeño tamaño. Se orientan hacia el camino común y la cancela de entrada a la citada finca.

Posteriormente en el interior de la vivienda, el inspeccionado muestra a los agentes el equipo de grabación. Se trata de un ordenador-grabador y monitor.

Depositadas sobre la mesa, se encuentran dos cámaras de pequeño tamaño; las cuales y según manifiesta el inspeccionado, son las cámaras que se encontraban instaladas en el lugar antes citado.

El equipo, a la llegada de los agentes, se encuentra desconectado. Se pone en marcha en ese momento y se puede observar cómo en el mismo, no hay imagen alguna; debido a la retirada del sistema de cámaras. Se adjunta fotografía acreditativa (foto 3).

Se acompaña documento gráfico del lugar donde se encontraban instaladas las cámaras de videovigilancia (foto 2) así como de los equipos utilizados para la grabación de imágenes (foto 1).

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 D. **A.A.A.** denuncia la instalación de un sistema de videovigilancia en la parcela sita en la finca **C.C.C., F.F.F., H.H.H.** de **G.G.G.**), cuyos responsables son D. **B.B.B.** y Dña. **E.E.E.**, captando imágenes del camino común que da acceso a la propiedad del denunciante. La instalación se ha realizado sin permiso del denunciante. Existen carteles informativos en los que no se indica los datos del responsable ante quien poder ejercitar los derechos ARCO.

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.

Así, hasta la entrada en vigor, el 27 de diciembre de 2009, de la Ley 25/2009, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y sus ejercicio (conocida como “Ley Ómnibus”), la legitimación para el tratamiento por particulares y empresas de imágenes captadas a través de dispositivos de videovigilancia sólo era posible en caso de que dichos sistemas hubieran sido contratados con empresas de seguridad privada, debidamente acreditadas ante el Ministerio del Interior, al que además debía notificarse el contrato que se hubiese celebrado, conforme a lo exigido por la Ley 23/1992, de 30 de julio de Seguridad Privada.

La Ley 25/2009 ha suprimido para la mayor parte de los casos estas exigencias, al liberalizar la comercialización, entrega, instalación y mantenimiento de estos dispositivos, de forma que ya no será necesario acudir para su puesta en funcionamiento a una empresa de seguridad privada ni cumplir las obligaciones de notificación del contrato al Ministerio del Interior.

En concreto el artículo 14 de la nueva Ley modifica el artículo 5.1 e) de la Ley 23/1992, de 30 de julio de Seguridad Privada, añadiendo una Disposición Adicional Sexta a la Ley de Seguridad Privada con la siguiente redacción:

“Disposición Adicional Sexta. Exclusión de las empresas relacionadas con equipos técnicos de seguridad:

Los prestadores de servicios y las filiales de empresas de seguridad que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarma, quedan excluidas de la legislación de seguridad privada, siempre y cuando no se dediquen a ninguno de los otros fines definidos en el artículo 5, sin perjuicio de otras legislaciones

específicas que pudieran resultarles de aplicación."

La interpretación de la mencionada disposición determina que cualquier particular o empresa cuya actividad no sea la propia de una empresa de seguridad privada podrá; "vender, entregar, instalar y mantener equipos técnicos de seguridad" sin necesidad de cumplir las exigencias previstas en la Ley de Seguridad Privada para tales empresas. De este modo, dado que la Ley permite la instalación y mantenimiento de dichos equipos por empresas distintas a las de seguridad privada, legitima a quienes adquieran de estos dispositivos para tratar los datos personales derivado de la captación de las imágenes sin necesidad de acudir a empresas de seguridad privada, siendo dicho tratamiento conforme a lo previsto en la Ley Orgánica de Protección de Datos de Carácter Personal.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma, que no es el caso que nos ocupa, sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora; esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho Departamento.

En el caso que nos ocupa, la parcela en la que se instalaron las dos cámaras de videovigilancia pertenecen proindiviso a los dos denunciados y al denunciante. Meses antes de la instalación del sistema se produjeron una serie de robos, destrozos y actos vandálicos en la parte de proindiviso pertenecientes a los denunciados, además de aparecer abierta en varias ocasiones la puerta de la cancela que da acceso a la finca. Por lo que se decidió por parte de los dos denunciados instalar las dos cámaras de videovigilancia orientadas hacia la piscina y césped, y hacia la cancela de entrada a la finca.

Por tanto la existencia de cámaras de seguridad en la parcela respondía a la necesidad e idoneidad de las mismas para garantizar la seguridad de las instalaciones, así como evitar actuaciones de vandalismo, que se habían venido produciendo en la parte del proindiviso de los denunciados, siendo fundamental la misión realizadas por las cámaras.

A este respecto, la propia sentencia dictada por el Juzgado de Primera Instancia e Instrucción nº Dos de Lora del Ríos, en fecha 27 de mayo de 2013, en el JF Nº 105/2013, recoge en el Fundamento de Derecho Tercero respecto a la denuncia efectuada por el ahora denunciante contra los denunciados por la instalación de las citadas cámaras: *"(...) dicho ánimo tendencial para restringir la libertad ajena no se aprecia tampoco con las cámaras colocadas en la finca, dado que las mismas, como bien señala (...) tienen una finalidad de seguridad de la finca. Así la misma testigo reseña acto seguido que aun así dichas cámaras la intimidan, intimidación compartida con su pareja y denunciante, sin embargo, dicha sensación pertenece al fuero íntimo de las personas, no pudiendo juzgarse los hechos desde la percepción propia del presunto perjudicado sino a la luz de un observador ajeno y objetivo. Así este juzgador, que ha podido analizar la abundante documental aportada por ambas partes, no entiende, habida cuenta de la disposición de las cámaras- en el camino de entrada a la finca-la disposición del camino-que pasa enfrente de las casas de los dos hermanos del denunciante- y de los hechos acaecidos con anterioridad y posterioridad-robos, quema*

de una palmera y la ruptura por el propio denunciante del candado (como reconoce en la vista), hacen más que justificable la existencia de dichas cámaras así como de los carteles anunciando las mismas con un efecto puramente intimidatorio de todo visitante ajeno con intereses espúreos, como igualmente reproduce en su parte de terreno el denunciante, quien también goza de los mismos carteles”.

Por tanto, las cámaras denunciadas responden a una finalidad de seguridad probada, estando orientadas las mismas una hacia la cancela de entrada a la finca y otra hacia la piscina y césped propiedad de los denunciados.

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 queda incardinado en la esfera del interés legítimo de los denunciados, por cuanto los mismos tiene un evidente interés en la instalación y mantenimiento de cámaras de seguridad; y la finalidad es también legítima, sin que se oponga a norma u obligación de ningún tipo.

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

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

En consonancia con lo anterior, el Tribunal Supremo en Sentencia de 8 de febrero de 2012 anuló el artículo 10.2.b) del RD 1720/2007, de 21 de diciembre por considerar que el Reglamento vulneraba la regulación contenida en la Directiva. Así, la Audiencia Nacional realiza una ponderación caso por caso entre el interés legítimo del responsable del tratamiento y los derechos y libertades fundamentales de los afectados, como en Sentencias de la Sección Primera de la Sala de lo Contencioso Administrativo de 5 de marzo y 31 de mayo de 2012.

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

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

IV

Por otro lado, respecto a las manifestaciones del denunciante de que el denunciado ha enseñado las imágenes captadas por las cámaras a dos personas, hay que señalar que el artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), establece que *“El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo”*.

El deber de secreto que incumbe a los responsables de los ficheros y a quienes intervienen en cualquier fase del tratamiento, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados o tratados no pueda revelar ni dar a conocer su contenido teniendo el *“deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo”*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la protección de datos a que se refiere la Sentencia del Tribunal Constitucional 292/2000 y, por lo que ahora interesa, comporta que los datos personales no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley.

Este deber de guardar secreto, que incumbe a los responsables de ficheros y a quienes intervengan en cualquier fase del tratamiento, incluye el deber de guardarlos, y lo contempla como obligación que subsistirá aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Ahora bien, en el supuesto denunciado ha de tenerse en cuenta que el Tribunal Constitucional viene manteniendo que los principios y garantías del procedimiento judicial penal son, en principio y con las oportunas modulaciones, aplicables al procedimiento administrativo sancionador, dado que también este es manifestación del ordenamiento punitivo del Estado, resultando clara la plena virtualidad del principio de presunción de inocencia. En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que*

nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”.

De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), establece que *“Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia.”*

Asimismo, se debe tener en cuenta, en relación con el principio de presunción de inocencia lo que establece el artículo 137 de LRJPAC:

“1. Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario.”

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y comprobado la existencia de una prueba de cargo acreditativa de los hechos que motivan esta imputación.

En este punto procede traer a colación la Sentencia de la Audiencia Nacional de fecha 25/05/2001 que señala que *“de la valoración de la prueba obrante en el expediente administrativo se llega a la conclusión que no ha quedado debidamente acreditado este hecho integrador del tipo, es decir no se prueba que el Banco entregara al Sr... el respectivo extracto, suscitándole este hecho concreto serias dudas, frente a la exigible certidumbre”*. Y concluye afirmando que *sin negar que pudieron producirse los hechos como indica la denunciante, tampoco puede rechazarse la posibilidad que el extracto no le fuera entregado al marido por el Banco, sino que aquel lo obtuviera aprovechando alguna visita al domicilio o mediante la actuación de algún familiar, dicho ello en términos de pura hipótesis”*.

De acuerdo con la citada doctrina jurisprudencial cabe concluir que, en el presente caso, no se han aportado evidencias firmes de los que pueda deducirse que los denunciados, hayan vulnerado el deber de secreto.

La Constitución Española, considera, en su artículo 24.2, el derecho a la presunción de inocencia como un derecho fundamental:

“2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia” (el subrayado es de la Agencia Española de Protección de Datos).

Conforme a lo anterior, el Tribunal Supremo señala, en su Sentencia de fecha 26/10/98, el derecho a la presunción de inocencia *“no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para*

que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”

En tal sentido, el Tribunal Constitucional, en su Sentencia 24/1997, establece que *“los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:*

a) La prueba indiciaria ha de partir de hechos plenamente probados.

b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)” (el subrayado es de la Agencia Española de Protección de Datos).

En el presente caso, en las actuaciones previas de investigación realizadas por los Servicios de Inspección de esta Agencia, no se ha podido obtener pruebas que corroboren y acrediten que los denunciados vulneraran el deber de secreto al que se refiere el artículo 10 de la LOPD.

V

Por otro lado, se plantearía en el presente supuesto, la aportación de las grabaciones efectuadas por los denunciados, en el seno de un procedimiento judicial, como prueba del autor de los daños producidos en la cancela de acceso a la finca. En este punto hemos de 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. 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 transcrito, 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 el 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 manifieste sobre la legitimidad de lo presentado, no constando en el presente caso, pronunciamiento en contra en este sentido, sino todo lo contrario, por lo que, en el caso de que esta Agencia impusiera una eventual sanción por estos hechos, dicha circunstancia colisionaría con el ejercicio del derecho constitucional a una tutela judicial efectiva.

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

VI

Por otro lado, de conformidad con la doctrina del Tribunal Constitucional, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo [RTC 1995\66], F.5; 55/1996, de 28 de marzo [RTC 1996\55], FF. 6, 7, 8 y 9; 207/1996, de 16 de diciembre [RTC1996\207], F.4.e) y 37/1998, de 17 de febrero [RTC 1998\37], F.8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra

medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La medida adoptada por los denunciados resultaba idónea y necesaria ya que se trataba de recabar pruebas de los daños que se venían produciendo en sus bienes para su aportación a un procedimiento judicial; y es equilibrada pues la grabación se limita a una determinada zona, y a un intervalo reducido de tiempo, en los momentos en los que se produce los daños.

De conformidad con la normativa expuesta, la captación de imágenes a través de videocámaras constituye un tratamiento de datos personales. Sin embargo, en el supuesto que nos ocupa, la captación de las imágenes objeto de denuncia fueron utilizadas como medio de prueba en un procedimiento judicial cumpliendo los requisitos de finalidad y proporcionalidad exigidos por la actual normativa en materia de protección de datos.

A mayor abundamiento, desde el 11 de noviembre de 2012, fecha en la cual se constató la autoría de los destrozos en la cancela de acceso a la finca y una vez puestas a disposición del juez las imágenes captadas, el sistema se desconectó y no ha vuelto a funcionar.

A este respecto, con fecha 20 de septiembre de 2013 se solicitó colaboración a la JEFATURA DE POLICÍA LOCAL DE LORA DEL RÍO, con objeto de realizar las actuaciones oportunas encaminadas a determinar los aspectos del sistema de videovigilancia denunciado, teniendo entrada en esta Agencia escrito de fecha 26 de septiembre de 2013 en el que el Jefe de Policía Local informa que :

Personados agentes de esa Policía Local en la finca D.D.D., se entrevistan con D. B.B.B., el cual muestra a los agentes la ubicación de las cámaras denunciadas; manifestándoles que instaló las cámaras en su día, debido a una serie de daños sufridos de manera continuada sobre las plantas y la cancela de entrada.

Los citados hechos pudieron ser constatados por los agentes.

En el lugar donde se encontraba instalado el sistema de videovigilancia se observa en la parte superior dos cajas de registro de luz, a las cuales se les ha practicado un pequeño orificio, y donde en su interior se ubicaban las cámaras de pequeño tamaño. Se orientan hacia el camino común y la cancela de entrada a la citada finca.

Posteriormente en el interior de la vivienda, el inspeccionado muestra a los agentes el equipo de grabación. Se trata de un ordenador-grabador y monitor.

Depositadas sobre la mesa, se encuentran dos cámaras de pequeño tamaño; las cuales y según manifiesta el inspeccionado, son las cámaras que se encontraban instaladas en el lugar antes citado.

El equipo, a la llegada de los agentes, se encuentra desconectado. Se pone en marcha en ese momento y se puede observar cómo en el mismo, no hay imagen alguna; debido a la retirada del sistema de cámaras.

Por lo tanto, el denunciado una vez obtenidas las pruebas del autor de los daños sufridos en la cancela procedió a la retirada del sistema.

Por último respecto a las manifestaciones del denunciado respecto a la cámara instalada por el denunciante, se le informa que si lo estima procedente podrá interponer la correspondiente denuncia en esta Agencia, aportando las pruebas que tenga por convenientes.

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

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 D. **B.B.B.**, a D^a. **E.E.E.** y a D. **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.



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