



Expediente N°: E/02038/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **EL RECREO DE XXXX S.L** en virtud de denuncia presentada por D. **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 11 de marzo de 2016 tiene entrada en esta Agencia escrito remitido por D. **A.A.A.** (en adelante el denunciante) comunicando, una posible infracción a la Ley Orgánica 15/1999 motivada por la existencia de cámaras de videovigilancia en el establecimiento con denominación comercial **EL RECREO DE XXXX** sito en C/ **XXXX Nº 28**, de **MADRID** y cuyo titular es la entidad **EL RECREO DE XXXX S.L.U** (en adelante el denunciado).

En su escrito, el denunciante manifiesta: *“la instalación de un sistema de videovigilancia en el interior del establecimiento “El Recreo de XXXX”. Los carteles informativos de zona videovigilada no detallan al responsable del sistema. No se dispone de formularios informativos sobre el tratamiento de datos personales con fines de vigilancia. Informa que con fecha 12 de noviembre de 2015 el sistema grabó imágenes de su persona implicada en un altercado que sucedió en el local, que fueron presentadas como prueba en el juicio por delito leve *****/15 celebrado en el Juzgado de Instrucción nº 18 de Madrid. En el móvil del administrador de la sociedad denunciada, se guarda copia de las mismas. Se desconoce si existe fichero de videovigilancia inscrito en el Registro de Protección de Datos”.*

Adjunta a su denuncia, fotografía de un cartel que informa de la “conexión a central de alarmas con verificación de vídeo y audio”.

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 fechas de 17 de mayo y 18 de julio de 2016 se solicita información al responsable del sistema.

Del análisis de las manifestaciones y documentación aportada por el mismo, con fechas de entrada en esta Agencia 8 de julio y 3 de agosto de 2016, se desprende:

*La mercantil **EL RECREO DE XXXX S.L.U** es responsable y titular del sistema de videovigilancia instalado en el local **EL RECREO DE XXXX** sito en C/ **XXXX Nº 28**, de **MADRID**.*

*La empresa **SERVIATEL** realizó la instalación del sistema.*

Existen carteles informativos de zona videovigilada, localizados en el acceso al establecimiento y en el interior

del mismo.

En documento **Doc.2** se acompaña reportaje fotográfico.

Asimismo, el establecimiento dispone de formularios informativos sobre el tratamiento de datos personales con fines de vigilancia a través de cámaras.

Se adjunta copia del modelo de cláusula informativa, debidamente cumplimentado (Doc.3).

El sistema está compuesto por un total de seis cámaras sin zoom, ubicadas en el interior del local (zonas de barra, almacén, cocina y público) según se indica en el plano de situación adjunto (Doc.1).

En documento Doc.4 se acompaña reportaje fotográfico de las cámaras y de las imágenes captadas por las mismas, visualizadas en el monitor del sistema, de cuyo análisis se observa:

- o *La cámara CAM 1 recoge la imagen del interior del establecimiento, distinguiéndose la puerta cristalera de acceso al local y su fachada acristalada.*
- o *El resto de cámaras captan diversos espacios interiores del local.*

Las imágenes se graban y se eliminan automáticamente transcurridos nueve días.

El sistema de grabación se localiza en un despacho con medidas de seguridad. Su acceso está limitado al administrador y dueño del establecimiento.

Se adjunta reportaje fotográfico (Doc.6).

*Existe fichero de VIDEOVIGILANCIA inscrito en el Registro General de Protección de Datos con el código ***CÓD.1.*

Se acompaña documento acreditativo (Doc.5).

Respecto a las imágenes captadas en el altercado producido en el interior del establecimiento con fecha 12 de noviembre de 2015, manifiesta que las mismas se aportaron al Despacho de Abogados "Vergara 25 S.L" para su custodia y remisión al organismo judicial correspondiente.

FUNDAMENTOS DE DERECHO

I

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

II

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

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

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”*. Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”*.

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

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

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

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

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

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

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

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

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

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

III

En el presente expediente, D. **A.A.A.** denuncia la instalación de un sistema de videovigilancia en el interior del establecimiento “*El Recreo de XXXX*” que pudiera vulnerar la normativa de protección de datos, habiendo presentado el denunciado grabaciones del sistema como prueba, dos meses después de ser grabadas, en el juicio por delito leve *****/15 celebrado en el Juzgado de Instrucción nº 18 de Madrid.

En primer lugar, debe entrarse a valorar el cumplimiento del deber de información e inscripción de ficheros, por parte del establecimiento denunciado.

El tratamiento de las imágenes por parte del responsable, obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1

de la LOPD el cual reza lo siguiente:

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

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

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

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

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

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

En cuanto al modo en que hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

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

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

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

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

“ANEXO-

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

En el caso que nos ocupa, se aporta por el denunciado fotografía de la existencia de carteles informativos de la existencia de las cámaras, ubicados en el cristal de la puerta de entrada al establecimiento y en el interior del mismo. Dichos carteles son acordes al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo aporta modelo de cláusula informativa a disposición de los interesados, de conformidad con el artículo 3 b) de la citada Instrucción.

Por tanto, el establecimiento denunciado cumple el deber de información respecto al sistema de videovigilancia.

Por otro lado, respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos”

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.

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

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

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

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

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

En el caso que nos ocupa, consta inscrito, en el Registro General de la Agencia Española de Protección de Datos, entre otros, el fichero denominado VIDEOVIGILANCIA, cuyo responsable es **“EL RECREO DE XXXX S.L”**.

Por otro lado, el sistema está compuesto por un total de seis cámaras sin zoom, ubicadas en el interior del local (zonas de barra, almacén, cocina y público). De las fotografías aportadas de las imágenes captadas por cada una de las cámaras se desprende que la cámara CAM 1 recoge la imagen del interior del establecimiento, distinguiéndose la puerta cristalera de acceso al local y su fachada acristalada; y el resto de cámaras captan diversos espacios interiores del local. A este respecto, el artículo 4.1 y 2 de la LOPD, garantiza el cumplimiento del principio de proporcionalidad en todo tratamiento de datos personales, cuando señala que:

“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”.

En este sentido, se pronuncia la Instrucción 1/2006, cuando señala en el artículo 4, lo siguiente:

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida”.

No obstante, en algunas ocasiones la protección de los espacios privados sólo es posible si las cámaras se ubican en espacios como las fachadas. A veces, también resulta necesario captar los accesos, puertas o entradas, de modo que aunque la cámara se encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en la porción de vía pública que inevitablemente se capta. Por otra parte, las videocámaras deberán orientarse de modo tal que su objeto de vigilancia principal sea el entorno privado y la captación de imágenes de la vía pública sea la mínima imprescindible

Precisamente la redacción del artículo 4 de la Instrucción 1/2006, no viene sino a recoger el principio de proporcionalidad del artículo 4 de la LOPD.

A la vista de lo expuesto, las imágenes captadas por las citadas cámaras no infringirían el principio de proporcionalidad de los datos previsto en el artículo 4.1 de la Ley Orgánica de Protección de Datos, cuando se habla de que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

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

IV

Una vez analizadas las cuestiones precedentes, debe entrarse en el fondo de la cuestión planteada, relativa a la aportación por parte del denunciado de las grabaciones obtenidas por el sistema de videovigilancia, como prueba en el juicio por delito leve *****/15 celebrado en el Juzgado de Instrucción nº 18 de Madrid, dos meses después de ser grabadas.

Por tanto, 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. En relación con los hechos denunciados, debe tenerse en cuenta que, al iniciarse un procedimiento jurisdiccional, para dilucidar la legitimidad de la pretensión del demandante, sería de aplicación lo relativo al derecho a la tutela judicial efectiva y a la utilización de prueba en el procedimiento, que consagra nuestro texto constitucional en su artículo 24:

“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.

La utilización de medios de prueba que impliquen un tratamiento de datos de la contraparte en el procedimiento, supone, en principio, una colisión de derechos constitucionales. 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 tanto, normativamente se ha establecido la correspondiente previsión, referida a la utilización de medios probatorios por las partes para el procedimiento seguido en cada caso. Así habría que señalarse que el artículo 299 de la Ley 1/2000, de 7 de enero de Enjuiciamiento Civil (en adelante LEC), admite la aportación como medio de prueba de informes periciales, lo cual se ve complementado con lo establecido en el artículo 11.2 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (en adelante la LOPD), referido a la no exigencia de consentimiento del titular del dato para su comunicación, cuando la: *“cesión esté autorizada en una ley”* y, por otro lado *“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.(...)”*. Así, a este respecto, el artículo 299 de la LEC establece, como hemos dicho, lo siguiente:

“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.*

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

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, 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.

Junto a lo anterior sería de aplicación lo expuesto en, la sentencia de sentencia de 22 de octubre de 2010 (rec. 409/2009) de la Audiencia Nacional, que ofrece una interpretación extensiva al artículo 11.2.d) de la LOPD, que alude a la falta de necesidad de consentimiento para el tratamiento de datos solicitados directamente por los jueces y tribunales, extendiéndolo a aquéllos datos aportados por las partes al proceso y no solicitado por el tribunal. En concreto, la SAN señala 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.”

En el caso que nos ocupa, el denunciado aportó como prueba en defensa de sus

derechos e intereses legítimos, grabaciones realizadas con las cámaras al procedimiento judicial sustanciado al respecto.

A este respecto, la Sentencia del TS 67/2014 de 28 enero, declara que “la STS 485/2013, de 5 de junio, considera que el material fotográfico y videográfico obtenido en el ámbito público y sin intromisión indebida en la intimidad personal o familiar tiene un valor probatorio innegable. La doctrina jurisprudencial de esta Sala en sentencias de 6 de mayo de 1993, 7 de febrero, 6 de abril, 31 de mayo de 1994, 18 de diciembre de 1995, 27 de febrero de 1996, 5 de mayo de 1997, 968/1998 de 17 de julio, 188/1999, de 15 de febrero, 1207/1999, de 23 de julio, 387/2001, de 13 de marzo, 27 de septiembre de 2002, 180/2012 de 14 de marzo, entre otras muchas)ha considerado legítima y no vulneradora de derechos fundamentales los espacios o vías públicas, estimando que la captación de imágenes de actividades que pueden ser constitutivas de acciones delictivas se encuentra autorizada por la ley en el curso de una investigación criminal, siempre que se limiten la grabación de lo que ocurre en espacios públicos fuera del recinto inviolable del domicilio o de, lugares específicos donde tiene lugar el ejercicio de la intimidad. (...).

Por último, se plantea la aportación de las grabaciones a procedimiento judicial dos meses después de ser grabadas. A este respecto, debe decirse que la Agencia se ha pronunciado en diversas ocasiones sobre esta cuestión, señalando que respecto al plazo, sobre el que han de conservarse las imágenes, la elección de dicho plazo, no es arbitraria y sino que encuentra su fundamento tanto en la Instrucción 1/1996, sobre ficheros automatizados establecidos con la finalidad de acceder de controlar el acceso a los edificios, que en su norma quinta prescribe que “Los datos de carácter personal deberán ser destruidos cuando haya transcurrido el plazo de un mes, contado a partir del momento en que fueron recabados”.

Ahora bien, la cuestión se plantea ante la existencia de alguna incidencia respecto de la grabación, como es el caso de la resolución que ahora se recurre. Así, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal viene a señalar que la cancelación dará lugar al bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que “la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”.

Este precepto, a su vez, se complementa con la previsión contenida en el transcrito artículo 16.5 de la Ley Orgánica 15/1999. En relación con esta cuestión, ya se indicaba en informes de esta Agencia de fecha 30 de julio de 2004 y 1 de agosto de 2005 lo siguiente:

“(...) la Ley Orgánica 15/1999 viene regular el bloqueo de los datos de carácter personal en su artículo 16.3, al establecer que “la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”.

Este precepto, a su vez, se complementa con la previsión contenida en el artículo 16.5 que indica que “los datos de carácter personal deberán ser conservados

durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado”.

Del análisis conjunto de las normas citadas se desprende que existirán supuestos en los que si bien deberá procederse a la cancelación de los datos, al haber dejado de ser necesarios para la finalidad que justificó su tratamiento, como sucederá cuando se haya producido la completa consumación del contrato que vincula al responsable del tratamiento con sus clientes, dicha cancelación deberá producirse mediante el bloqueo de los datos de carácter personal sometidos a tratamiento que, produciendo unos efectos similares al borrado físico de los datos, salvo en determinadas circunstancias, descritas por el artículo 16.3 de la Ley Orgánica, no implicará automáticamente ese borrado.

Así, el artículo 16.3 viene a reconocer, en consonancia con lo previsto en el artículo 16.5 de la Ley, que existirán determinados supuestos en los que la propia relación jurídica que vincula al afectado con el responsable del fichero y que determina, en definitiva, el tratamiento del dato de carácter personal cuya cancelación se pretende, así como las obligaciones de toda índole que pudieran derivarse de la citada relación jurídica y que aparecen impuestas por la Ley, impedirá que la cancelación se materialice de forma inmediata en un borrado físico de los datos.

En cuanto a las causas que podrán motivar la conservación del dato, sujeto a su previo bloqueo, y al margen de la relación jurídica con el afectado, a la que se refiere el artículo 16.5 de la Ley Orgánica 15/1999, éstas deberán fundarse en lo dispuesto “en las disposiciones aplicables” o a la “atención de las posibles responsabilidades nacidas del tratamiento”, tal y como prevé la meritada Ley.

En este sentido, para la determinación del período de bloqueo de los datos debe tenerse en cuenta que la Sentencia del tribunal Constitucional 292/2000, de 30 de noviembre, viene a imponer, expresamente, el principio de reserva de Ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho (como sería la derivada del artículo 16.3 de la Ley) deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Así, a título de ejemplo, podría considerarse que el bloqueo habrá de efectuarse durante los plazos de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento, en los términos previstos por la legislación civil o mercantil que resulte de aplicación, así como el plazo de cuatro años de prescripción de las deudas tributarias, en cuanto los datos puedan revestir trascendencia desde el punto de vista tributario (habida cuenta de la obligación de conservación que impone el artículo 111 de la Ley General Tributarias y el plazo legal de prescripción de cuatro años previsto en el artículo 24 de la Ley de Derechos y Garantías de los Contribuyentes).

En todo caso, debe recordarse que el mantenimiento del dato bloqueado, supone una excepción al borrado físico del mismo que, en definitiva, es el fin último de la cancelación (tal y como prevé el propio artículo 16.3, al indicar que “cumplido el citado plazo deberá procederse a la supresión”).

En consecuencia, a nuestro juicio, la cancelación no supone automáticamente en todo caso un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia

relación jurídica que vincula al responsable del fichero con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento.

En lo atinente a la determinación de los períodos en que el dato habrá de permanecer bloqueado, en relación con lo dispuesto en el artículo 16.3, resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, como ya se ha indicado con anterioridad, los plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con su cliente, así como los derivados de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave. (...)"

Por último, en cuanto al modo de llevar a cabo el bloqueo, deberá efectuarse de forma tal que no sea posible el acceso a los datos por parte del personal que tuviera habitualmente tal acceso, por ejemplo, el personal que preste sus servicios en el centro consultante, limitándose el acceso a una persona con la máxima responsabilidad y en virtud de la existencia de un requerimiento judicial o administrativo a tal efecto. De este modo, pese a permanecer el tratamiento de los datos, el acceso a los mismos quedaría enteramente restringido a las personas a las que se ha hecho referencia."

Por lo tanto, en el supuesto que nos ocupa, la captación de las imágenes objeto de denuncia, fueron aportadas como medio de prueba en un procedimiento judicial, estando amparadas la conservación de las imágenes, en el artículo 16.3 de la LOPD, que señala que *"la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión"*.

Por último, respecto a las manifestaciones del denunciante relativas a la copia realizada de las grabaciones en el teléfono móvil del denunciado, a los efectos de su visionado en el juicio, cabe decir que la normativa de protección de datos exige que el responsable del fichero y en su caso el encargado del tratamiento adopten las medidas de índole técnica y organizativas necesarias previstas en la LOPD y su Reglamento de desarrollo, que garanticen la seguridad de las imágenes y eviten su alteración, pérdida, tratamiento o acceso no autorizado; por lo tanto y en la medida de que no consta que dichos requisitos hayan sido vulnerados, no existiría inconveniente al respecto.

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

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **EL RECREO DE XXXX S.L** 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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

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

Mar España Martí
Directora de la Agencia Española de Protección de Datos