



Procedimiento N° PS/00528/2012

RESOLUCIÓN: R/03155/2012

En el procedimiento sancionador PS/00528/2012, instruido por la Agencia Española de Protección de Datos a la entidad **LA VIMETERA, S.L.**, vista la denuncia presentada por el **Departamento de Interior de la Generalidad de Cataluña** y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 16 de julio de 2012 tuvo entrada en esta Agencia informe del Departamento de Interior de la Generalidad de Cataluña, (en lo sucesivo el denunciante) poniendo de manifiesto que a raíz de la inspección policial practicada con fecha 29 de mayo de 2012 en el establecimiento PARADISE, ubicado en la Avda. **B.B.B.** (Girona), los Mozos de Escuadra actuantes comprobaron que en el interior de dicho local se estaba produciendo un tratamiento de datos de carácter personal con cámaras de videovigilancia que podía constituir infracción a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal Datos (en lo sucesivo LOPD).

SEGUNDO: Del contenido de dicho informe de fecha 30 de mayo de 2012, también suscrito por los Mozos de Escuadra que practicaron la reseñada actuación policial en el mencionado local, y de la copia del Acta de Inspección que acompaña al mismo, la cual fue levantada por dichos Mozos en el momento de la realización de la inspección al local, se acreditan los siguientes hechos:

- La mercantil LA VIMETERA, S.L., con CIF ***** y domicilio social en c/ **A.A.A.** (Girona), es titular del establecimiento PARADISE, ubicado en la Avda. **B.B.B.** (Girona),
- Durante la inspección efectuada en dicho establecimiento con fecha 29 de mayo de 2012, los Mozos de Escuadra actuantes comprobaron que el Club "PARADISE" contaba con un sistema de seguridad integrado por 16 cámaras de videovigilancia, un monitor emplazado en el despacho del director del local desde el que se visualizaban las imágenes captadas por dichas cámaras en tiempo real y de un grabador de la marca Samsung.
- En el momento de la inspección las cámaras del local estaban conectadas a un servidor informático situado en el despacho del director del Club. Dicho dispositivo tenía encendidos los pilotos de señalización de funcionamiento.



- El establecimiento cuenta con carteles que informan sobre la existencia de cámaras de videovigilancia.
- Según informó el director del local las imágenes captadas se graban y almacenan por un período de diez días.
- Los Mozos de Escuadra actuantes constataron a través del monitor emplazado en el despacho del director que dos de dichas cámaras de videovigilancia, emplazadas en una habitación con taquillas situada a la entrada del local, captaban imágenes correspondientes a unas quince mujeres que prestan sus servicios en dicho local mientras se estaban desvistiendo de su ropa de calle y poniendo su ropa de trabajo en dicha dependencia.

TERCERO: Con fechas 17 y 21 de septiembre de 2012 se verifica que la mercantil LA VIMETERA, S.L. no tiene inscrito en el Registro General de Protección de Datos ningún fichero de videovigilancia a su nombre.

CUARTO: Con fecha 24 de septiembre de 2012 el Director de la Agencia Española de Protección de Datos (en adelante AEPD) acordó iniciar un procedimiento sancionador a la entidad LA VIMETERA, S.L. por la presunta comisión de las infracciones de los artículos 4.1 y 26.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), estando tipificada como infracción grave en el artículo 44.3.c) de la citada Ley Orgánica la primera de las infracciones citadas y tipificada como infracción leve en el artículo 44.2.b) de dicha norma la segunda de las infracciones reseñadas. Dicho Acuerdo de inicio se notificó a la entidad imputada con fecha 28 de septiembre de 2012, según figura en el Acuse de Recibo del Servicio de Correos justificativo de tal entrega.

QUINTO: Transcurrido el plazo concedido para formular alegaciones al acuerdo de inicio sin que conste que la entidad imputada haya ejercido dicho derecho, el citado acuerdo se considera propuesta de resolución, por lo que procede a elevar el procedimiento a la resolución del Director de la Agencia Española de Protección de Datos, en virtud de lo previsto en el artículo 13.2 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora.

HECHOS PROBADOS

PRIMERO: Con fecha 29 de mayo de 2012 los Mozos de Escuadra de la Generalidad de Cataluña practicaron en el establecimiento denominado PARADISE, ubicado en la Avda. **B.B.B.** (Girona), una inspección a raíz de la cual constataron que el local contaba con un sistema de videovigilancia integrado por 16 cámaras de videovigilancia, un monitor emplazado en el despacho del director del local desde el que se visualizaban las imágenes captadas por dichas cámaras en tiempo real y de un grabador de la marca



Samsung. (folios 1 y 2)

SEGUNDO: La mercantil LA VIMETERA, S.L. figura como titular del mencionado establecimiento PARADISE. (folio 1)

TERCERO: Los Mozos de Escuadra actuantes visualizaron a través del monitor situado en el despacho del director del citado local que las dos cámaras de videovigilancia, colocadas en una habitación con taquillas utilizada como vestidor, y que estaba situada a la entrada del local, captaban imágenes correspondientes a unas quince mujeres que prestan sus servicios en dicho Club mientras éstas se estaban desvistiendo de su ropa de calle y poniendo su ropa de trabajo. (folios 1 y 2)

CUARTO: Las imágenes captadas por el sistema de videovigilancia instalado en el Club PARADISE eran grabadas y almacenadas por un período de diez días, sin que el fichero de videovigilancia resultante de dicho tratamiento de datos personales constara como inscrito a nombre de la mercantil LA VIMETERA, S.L. en el Registro General de Protección de Datos de la AEPD. (folios 1, 2, y 6 al 10)

QUINTO: Consta que con fecha 26 de octubre de 2010 la mercantil LA VIMETERA, S.L. procedió a inscribir un fichero de videovigilancia con código ***COD.1, en el Registro General de Protección de Datos de la AEPD, figurando como finalidad y usos previstos del mismo "Videovigilancia de las instalaciones". (folio 20)

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

El artículo 13.2 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora., dispone que *"El acuerdo de iniciación se comunicará al instructor, con traslado de cuantas actuaciones existan al respecto, y se notificará al denunciante, en su caso, y a los interesados, entendiéndose en todo caso por tal al inculpado. En la notificación se advertirá a los interesados que, de no efectuar alegaciones sobre el contenido de la iniciación del procedimiento en el plazo previsto en el [artículo 16.1](#), la iniciación podrá ser considerada propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, con los efectos previstos en los [artículos 18](#) y [19 del Reglamento](#)."*

De conformidad con lo expuesto, el acuerdo de iniciación correctamente notificado podrá ser considerado directamente propuesta de resolución cuando contenga un pronunciamiento preciso a cerca de la responsabilidad imputada. Para ello son necesarios varios requisitos:

- Que dicha posibilidad sea advertida expresamente al inculpado en el acuerdo



de notificación.

- Que el acuerdo de iniciación cumpla todas las exigencias que sobre el contenido se exigen en el apartado primero del citado artículo.
- Que el inculpado no presente alegaciones en plazo sobre el contenido de la iniciación.
- Que como consecuencia de la instrucción no resulte modificada la determinación inicial de los hechos, de su posible calificación, de las sanciones imponible o de las responsabilidades susceptibles de sanción. (Art. 16.3 del citado Real decreto.

La STS de 19 de diciembre de 2001 (RJ 2001, 2617) recaída en recurso de casación en interés de ley, interpretando el artículo 13.2 arriba transcrito, declara que basta que el interesado no haya formulado alegaciones sobre el contenido del boletín de denuncia que inicia el procedimiento, para que no sea preceptiva la notificación de la propuesta de resolución, ni necesario, en consecuencia, el trámite de audiencia, al servir el acuerdo de iniciación como propuesta de resolución.

En el presente caso, se han observado las prescripciones citadas al respecto, por lo es conforme a derecho considerar el citado acuerdo de iniciación como propuesta de resolución.

III

Con carácter previo al análisis del fondo del asunto, debe señalarse que el artículo 1 de la LOPD dispone que *“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”*.

La LOPD viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento, con la salvedad de las excepciones legalmente previstas.

En cuanto al ámbito de aplicación de la citada norma, 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”*. Por ello resulta preciso determinar que ha de entenderse por tratamiento de datos y dato de carácter personal.

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”*. 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.



El concepto de dato de carácter personal se define en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*.

Por su parte el artículo 5.1 del Reglamento de desarrollo de la LOPD, aprobado por 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, recoge en sus apartados f) y o) las definiciones de “datos de carácter personal” y “persona identificable”. Así, se considera “datos de carácter personal”: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”* y “persona identificable” como: *“toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas”*.

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 misma Directiva 95/46/CE en su Considerando 14 afirma: *“(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;”*.

Es claro, pues, que para el legislador comunitario la imagen personal es un dato de carácter personal sujeto al régimen de protección establecido en la Directiva cuando se efectúe tratamiento sobre ella.

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

De conformidad con la normativa expuesta, la captación y grabación de imágenes a través de videocámaras con fines de vigilancia y control constituye un tratamiento de datos personales que cae bajo la órbita de la normativa de protección de datos de carácter personal, toda vez que la información que captan las videocámaras contiene, entre otra información, datos concernientes a personas identificadas o identificables situadas en el entorno videovigilado y sobre las que suministran



información relativa a la imagen personal de éstas, el lugar de su captación y la actividad o conducta desarrollada por los individuos a las que las imágenes se refieren.

Este tipo de tratamiento se encuentra regulado de forma específica en 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 (en lo sucesivo Instrucción 1/2006), en cuyo artículo 1.1 se señala lo siguiente:

“Artículo 1.1. 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.”

Con arreglo a lo anteriormente expuesto, cabe concluir que, en el supuesto presente, las videocámaras que componen el sistema de seguridad del establecimiento realizan tratamientos de datos de carácter personal ya que, por un lado, la grabación, captación, transmisión, conservación, y almacenamiento de imágenes constituye un tratamiento de datos, y, por otro, la imagen de los afectados, de acuerdo con los preceptos transcritos, constituye un dato de carácter personal, toda vez que la información que las cámaras captan para su visualización y grabación concierne a personas físicas y suministra información sobre la imagen personal de éstas, el lugar de la captación y la actividad desarrollada por los individuos a los que las imágenes se refieren, por lo que tal actuación se encuentra enmarcada en el ámbito competencial de la LOPD.

IV

De acuerdo con lo dispuesto en el 43.1 de la LOPD se encuentran sujetos al régimen sancionador establecido en la LOPD “*los responsables de los ficheros*” y “*los encargados de los tratamientos*”. Ahora bien, la LOPD recoge y diferencia las figuras del responsable del fichero y del responsable del tratamiento. Efectivamente, el artículo 3.d) de la LOPD, innovando respecto de la Ley Orgánica 5/1992, incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. Así conforme al citado artículo 3.d) el responsable del fichero o del tratamiento es “*la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*” .

Por lo que debe entenderse que la expresión “*responsables de los ficheros*”, contenida en el precitado artículo 43.1 de la LOPD, se refiere tanto a los responsables del fichero como a los responsables de los tratamientos.



En el presente caso, de conformidad con las citadas definiciones legales y con la normativa expuesta, LA VIMETERA, S.L. es la entidad responsable del tratamiento de datos personales efectuado a través de las cámaras de videovigilancia instaladas en el interior del establecimiento "PARADISE", todo ello en su condición de persona jurídica que ha decidido sobre la finalidad, contenido y uso del citado tratamiento y, por tanto, está sujeta al régimen de responsabilidad recogido en el Título VII de la LOPD.

V

Dicho tratamiento precisa que se cumpla el principio del consentimiento recogido en el artículo 6 de la LOPD, cuyos apartados 1 y 2 disponen que:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

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.

En relación con dicho principio, el artículo 2 de la citada Instrucción 1/2006 establece respecto a la legitimación en el tratamiento de las imágenes que:

"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".

En el caso que nos ocupa, la habilitación legal para el tratamiento de las imágenes de las personas físicas con fines de vigilancia procede de la Ley 25/2009, de 27/12, de modificación de diversas leyes para su adaptación a la Ley 17/2009, de 23/11, sobre el libre acceso a las actividades de servicios, ya que no consta que el sistema de videovigilancia se encuentre conectado a una central de alarma, supuesto en el que su instalación y la captación y/o tratamiento de imágenes estaría sujeta, además de a la LOPD, a las condiciones derivadas de la Ley 32/92 de 30 de julio, de Seguridad Privada y su Reglamento de Desarrollo.

En todo caso, el tratamiento de las imágenes a través de cámaras de videovigilancia deberá cumplir los restantes requisitos exigibles en materia de Protección de Datos de Carácter Personal, recogidos en la Ley Orgánica y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos.

VI



En primer lugar se imputa a la entidad denunciada una infracción a lo previsto en el artículo 4.1 de la LOPD, cuyo tenor literal señala 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”*

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 de carácter personal, lo que exige respetar la normativa existente en materia de protección de datos, garantizándose por el artículo 4.1 y 2 de la LOPD el cumplimiento del principio de proporcionalidad y finalidad en todo tratamiento de datos personales.

La STC 254/1993, de 20 de julio, señaló que *“el derecho fundamental a la protección de datos persigue, en suma, garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino; o dicho de otro modo, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno; mientras que el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos (..)”*.

El citado artículo 4.1 de la LOPD consagra el principio de pertinencia en el tratamiento de los datos de carácter personal, que impide el tratamiento de aquellos que no sean necesarios o proporcionados a la finalidad que justifica el mismo, debiendo restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de éstos. En consecuencia, el tratamiento del dato ha de ser *“pertinente”* al fin perseguido, por lo que únicamente pueden ser sometidos a tratamiento aquellos datos que sean estrictamente necesarios para la finalidad perseguida. Por otra parte, el cumplimiento del principio de proporcionalidad no sólo debe producirse en el ámbito de la recogida de los datos, sino asimismo de respetarse en el posterior tratamiento que se realice de los mismos.

Este criterio, se encuentra recogido también en el artículo 6 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24/10/1995, 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, y aparece también reflejado en el Convenio 108, cuyo artículo 5 c) indica que *“los datos de carácter personal que sean objeto de un tratamiento automatizado (...) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado”*.

El mencionado precepto debe ponerse en correlación con lo previsto en el apartado 2 del mismo artículo 4 de la LOPD, según el cual: *“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.”*. Las finalidades a las que alude este apartado 2 han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley.

De este modo, el uso de las instalaciones de cámaras y videocámaras debe seguir ciertas reglas que rigen todo el proceso desde su captación, transmisión, almacenamiento, reproducción hasta su cancelación.

De lo expuesto se deduce que el artículo 4.1 de la LOPD resulta aplicable al



supuesto de hecho que se discute, en concreto, en lo relativo al tratamiento de datos de carácter personal derivado de la captación, visualización y grabación de imágenes recogidas por las dos cámaras de videovigilancia instaladas en una dependencia del local con taquillas, la cual es utilizada como vestidor por las mujeres que prestan sus servicios en el citado Club PARADISE. Así, este tratamiento de datos viene realizándose sin tener en cuenta que debe existir una relación de proporcionalidad entre la finalidad de seguridad perseguida a través del sistema de videovigilancia instalado en el local y el modo y tipo de datos que se recogen a través de las cámaras. Así, resulta fundamental que la habitación en que están colocadas las dos cámaras citadas se utiliza como vestidor por personas que desarrollan en dicho espacio actividades privadas, tales como vestirse y desvestirse.

Es por ello que la instalación de dichas cámaras con fines de videovigilancia en la mencionada habitación supone una intromisión a la intimidad y a la imagen de dichas personas, además de una vulneración a la normativa de protección de datos. Téngase en cuenta que, independientemente de que se trate de un establecimiento de pública concurrencia, se están captando imágenes de una serie de personas mientras realizan actividades de naturaleza privada e íntima, las cuales no sólo eran accesibles en tiempo real al director del Club a través del monitor situado en su despacho, sino que también eran grabadas manteniéndose almacenadas en un fichero por espacio de diez días. Estas circunstancias suponen un tratamiento automatizado de datos de carácter personal particularmente invasivo e intrusivo para la intimidad de las personas afectadas por el mismo y especialmente agresivo con su dignidad, por lo que se considera que no es un tratamiento adecuado y pertinente en relación con el ámbito y finalidad de seguridad y control de instalaciones y personas a las que responde la colocación del sistema de videovigilancia.

Por su parte el artículo 4 de la Instrucción 1/2006 se pronuncia del siguiente modo en cuanto a los principios de calidad, proporcionalidad y finalidad del tratamiento:

“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”.

También en la exposición de motivos de la referida Instrucción 1/2006 se hace referencia a esta proporcionalidad en la instalación de estos sistemas, indicándose:

“En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el



principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la [Sentencia del Tribunal Constitucional 207/1996](#) determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones <<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)>>».

Asimismo la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalan sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, tales como la instalación de sistemas de vigilancia en espacios comunes, o aseos del lugar de trabajo. Por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.»

A la vista de lo expuesto, el tratamiento realizado de las imágenes procedentes de la habitación con taquillas situada a la entrada del establecimiento se considera excesivo, inadecuado y no pertinente en relación con el ámbito y la finalidad de videovigilancia a la que responde la instalación de las dos cámaras, incumpléndose con ello el principio de proporcionalidad que deben regir el tratamiento de datos personales.

VII

Sobre este particular hay que señalar que los responsables del tratamiento de datos de carácter personal derivado de la colocación de cámaras de videovigilancia deben ponderar los derechos y garantizar el cumplimiento estricto del principio de proporcionalidad, no resultando admisible la instalación de cámaras en lugares como vestidores, gimnasios, balnerarios ni en cualquier otro espacio en el que puedan captarse imágenes susceptibles de afectar a los derechos a la intimidad, a la propia imagen y a la protección de datos. Por lo tanto, el tipo de tratamiento de datos de carácter personal que deriva de la colocación de dos cámaras de videovigilancia en



una zona especialmente sensible del Club PARADISE no supera el juicio de proporcionalidad.

La proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de las personas.

En este sentido, el Dictamen 4/2004, apartado D) del Grupo del artículo 29 de la Directiva 95/46/CE, relativo al tratamiento de datos personales mediante vigilancia por videocámara, adoptado el 11 de febrero de 2004, señala lo siguiente :

“D) Proporcionalidad del recurso a la vigilancia por videocámara.

El principio según el cual los datos deberán ser adecuados y proporcionales al fin perseguido significa, en primer lugar, que el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir: con fines que realmente justifiquen el recurso a tales sistemas. Dicho principio de proporcionalidad supone que se pueden utilizar estos sistemas cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no requieran captación de imágenes (por ejemplo, la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, sistemas mejores y más potentes de alumbrado nocturno en las calles, etc.) resulten claramente insuficientes o inaplicables en relación con los fines legítimos mencionados anteriormente.

El mismo principio también es aplicable a la selección de la tecnología adecuada, los criterios de utilización del equipo en concreto y la especificación de disposiciones para el tratamiento de datos en relación también con las normas de acceso y el período de retención. Deberá evitarse, por ejemplo, que un organismo administrativo pueda instalar equipos de vigilancia por videocámara en relación con infracciones de menor importancia (por ejemplo, para reforzar la prohibición de fumar en los colegios y otros lugares públicos o la prohibición de tirar colillas y papeles al suelo en los lugares públicos). Dicho de otro modo, es necesario aplicar, caso por caso, el principio de idoneidad con respecto a los fines perseguidos, lo que implica una especie de obligación de minimización de los datos por parte del responsable del tratamiento. Si bien un sistema proporcionado de vigilancia por videocámara y alerta puede considerarse lícito cuando se producen varios episodios de violencia en una zona próxima a un estadio o se cometen agresiones repetidas a bordo de autobuses en zonas periféricas o cerca de las paradas de autobús, no ocurre lo mismo cuando se trata de un sistema destinado a evitar que se insulte a los conductores de autobús o que se ensucien los vehículos (tal y como le ha sido descrito a una autoridad de protección de datos), a identificar a ciudadanos responsables de infracciones de menor importancia, como dejar las bolsas de basura fuera del cubo o en zonas en las que está prohibido tirar basura, o a detectar a personas responsables de robos ocasionales en piscinas cubiertas. La proporcionalidad deberá evaluarse basándose en criterios más estrictos en lo que se refiere a lugares cerrados al público. El intercambio de información y experiencias entre las autoridades competentes de los diferentes Estados miembros puede ser útil en este sentido. Las consideraciones anteriores se refieren, en concreto, al uso cada vez más frecuente de vigilancia por videocámara con fines de autodefensa y protección de la propiedad (sobre todo, cerca de edificios públicos y oficinas, incluidas



las áreas circundantes). Para este tipo de utilización se requiere la evaluación, desde un punto de vista más general, de los efectos indirectos derivados del recurso masivo a la vigilancia por videocámara (es decir, si la instalación de varios dispositivos es realmente un factor disuasorio o si los infractores o vándalos pueden, simplemente, desplazarse a otras zonas y actividades).

Es decir, aunque pueda resultar justificable el uso de técnicas de videovigilancia por motivos de seguridad, en ningún caso resulta admisible la instalación de cámaras en espacios protegidos en los que se desarrollen actividades cuya práctica pueda afectar a la imagen o la vida privada, y ello en atención a la naturaleza de los derechos fundamentales que pueden verse afectados, entre los que se encuentra el de la protección de datos. Así, el responsable del tratamiento debe valorar esta circunstancia a fin de respetar tales derechos y adoptar otros medios de prevención y protección menos intrusivos y lesivos para los afectados y, en todo caso, especialmente respetuosos con su dignidad.

Por lo tanto, en este supuesto aunque la medida utilizada por la entidad titular del establecimiento en dicha dependencia fuera susceptible de cumplir el objetivo de seguridad de las instalaciones y personas, no es ponderada ni equilibrada.

En conclusión, la conducta analizada supone una vulneración por parte de la mercantil denunciada de lo previsto en el aludido artículo 4.1 de la LOPD.

VIII

La infracción del artículo 4.1 de la LOPD se incardina en el artículo 44.3.c) de la LOPD, en la redacción dada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, (en adelante LES), publicada en el B.O.E. nº 55 de 05/03/2011, que establece como infracción grave: *c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.*

A la vista de lo expuesto LA VIMETERA, S.L. resulta responsable de una infracción del artículo 4.1 de la LOPD, habida cuenta que el tratamiento de datos de carácter personal derivado de la captación, visualización, grabación y almacenamiento de las imágenes recogidas por las dos cámaras de videovigilancia instaladas en una habitación del local utilizada como vestidor resulta excesivo y no pertinente al fin de seguridad perseguido con dicha medida, pudiendo ser sancionada por ello con multa de 40.001 a 300.000 €, de acuerdo con el artículo 45.2 de la LOPD en su redacción dada por la LES en su Disposición Final quincuagésima sexta, “tres”.

IX

En segundo lugar también se imputa a la entidad denunciada una infracción a lo previsto en el artículo 26.1 de la LOPD por la falta de inscripción del fichero de videovigilancia resultante de la grabación de las imágenes recogidas por las cámaras que integran el sistema de videovigilancia instalado en el Club PARADISE.

En el Acta de Inspección e informe evacuado por los agentes actuantes figura



que el director del local, el Sr. **C.C.C.**, informó a los Mozos de Escuadra durante la realización de la inspección efectuada en el mencionado local que las imágenes captadas se grababan y almacenaban por un período de diez días, constatándose por esta Agencia con fechas 17 y 21 de septiembre de 2012 que la mercantil titular del establecimiento no tenía inscrito en el Registro General de Protección de Datos el fichero de videovigilancia resultante de dicho tratamiento.

Los hechos descritos suponen una infracción del artículo 26.1 de la LOPD, el cual 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 Española de Protección de Datos”.

Sobre este particular el artículo 7 de la mencionada Instrucción 1/2006, relativo a “Notificación de ficheros”, dispone 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 e 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.”

Por tanto, en este supuesto existe constancia de que las imágenes captadas por las cámaras se graban y dan lugar a la creación de un fichero de datos personales de videovigilancia, cuya inscripción en el Registro General de Protección de Datos no se ha producido, según se ha podido constatar en la tramitación del procedimiento sancionador, hasta 22 de noviembre de 2012.

Es decir, aunque la entidad imputada ha subsanado la falta de inscripción del mencionado fichero de videovigilancia, sin embargo ha quedado acreditado que dicha regularización se llevó a cabo con posterioridad a la notificación del acuerdo de inicio del presente procedimiento sancionador (28 de septiembre de 2012), motivo por el cual nos encontramos frente a la comisión de una infracción consumada como mínimo hasta la fecha en que se llevó a cabo la inscripción en el mencionado Registro (22 de noviembre de 2012).

X

El artículo 44 .2.b), en redacción dada por la disposición final quincuagésima sexta de la Ley 2/2011, considera como infracción leve: *“b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave”.*

La entidad imputada ha cometido la infracción descrita, por cuanto no atendió a la obligación impuesta en el artículo 26.1 de la citada Ley Orgánica hasta que procedió a la regularización de la situación imputada, pudiendo ser sancionada, con multa de 900 a



40.000 euros, de acuerdo con el artículo 45.1 de la citada Ley Orgánica y con la modificación efectuada por la LES.

XI

El artículo 45.6 de la vigente LOPD dispone que: *“Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurren los siguientes presupuestos:*

- a) *Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.*
- b) *Que el infractor no hubiese sido sancionado o apercibido con anterioridad.*

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento”.

En este caso se debe indicar que al acordar el inicio del procedimiento sancionador se consideró que, no obstante concurrir los presupuestos establecidos en los apartados a) y b) del mencionado precepto, no procedía apercibir a la entidad imputada en atención no sólo a que se trata de una medida excepcional sino, y fundamentalmente, debido a la naturaleza de los hechos constatados. Así, se valoró que LA VIMETERA, S.L., a través de las dos cámaras de videovigilancia colocadas en la habitación con taquillas utilizada como vestidor, estaba realizando un tratamiento de datos de carácter personal en un espacio especialmente sensible por el tipo de imágenes que se captaban y grababan en el mismo.

XII

Los apartados 1 al 5 del artículo 45 de la LOPD, en la redacción dada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, en su disposición final quincuagésima sexta, número “tres”, establecen lo siguiente:

- “1 Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.*
- 2. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.*
- 3. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.*
- 4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:*
 - a) *El carácter continuado de la infracción.*
 - b) *El volumen de los tratamientos efectuados.*



- c) *La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.*
- d) *El volumen de negocio o actividad del infractor.*
- e) *Los beneficios obtenidos como consecuencia de la comisión de la infracción.*
- f) *El grado de intencionalidad.*
- g) *La reincidencia por comisión de infracciones de la misma naturaleza.*
- h) *La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.*
- i) *La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.*
- j) *Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.*

5 *El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:*

- a) *Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.*
- b) *Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.*
- c) *Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.*
- d) *Cuando el infractor haya reconocido espontáneamente su culpabilidad.*
- e) *Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.»*

El apartado 45.5 de la LOPD deriva del principio de proporcionalidad de la sanción y permite establecer "la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate", pero para ello es necesario la concurrencia de una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, o bien, de alguna otra de las circunstancias que el mismo precepto cita.

En el presente caso, ha quedado probada la responsabilidad de la entidad imputada en la comisión de las dos infracciones cuya autoría se le imputa, debiendo tenerse en consideración, a los efectos de la aplicación del artículo 45.5 de la LOPD, el tratamiento automatizado en cuestión, particularmente invasivo e intrusivo con la intimidad de las personas afectas por el mismo y especialmente agresivo con su dignidad. Junto a ello debe subrayarse, a los efectos de la aplicación del artículo 45.4 de



la LOPD, el carácter continuado de la infracción, el grado de intencionalidad y el volumen de negocio y actividad del infractor que se autodefine en su página web como el mayor Club de Europa.

En sentido contrario, habría que añadir que LA VIMETERA, S.L. ha subsanado de forma diligente la situación derivada de la falta de inscripción del fichero de videovigilancia en el Registro General de Protección de Datos, ya que procedió a inscribir dicho fichero después de serle notificado el acuerdo de inicio de procedimiento sancionador.

Teniendo en cuenta los criterios de graduación de las sanciones previstos en el artículo 45.4 y 5 de la LOPD, se estima procedente sancionar a la entidad imputada con sendas multas de 50.000 € y 1.100 € por las infracciones a lo previsto en los artículos 4.1 y 26.1 de la LOPD, respectivamente .

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: IMPONER a la entidad **LA VIMETERA, S.L.**, por una infracción del artículo 4.1 de la LOPD, tipificada como grave en el artículo 44.3.c) de dicha norma, una multa de **50.000 € (Cincuenta mil euros)**, de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.

SEGUNDO: IMPONER a la entidad **LA VIMETERA, S.L.**, por una infracción del artículo 26.1 de la LOPD, tipificada como leve en el artículo 44.2.b) de dicha norma, una multa de **1.100 € (Mil cien euros)** de conformidad con lo establecido en los apartados 1, 4 y 5 del artículo 45 de la citada Ley Orgánica.

TERCERO: NOTIFICAR la presente resolución a **LA VIMETERA, S.L.** y al **Departamento de Interior de la Generalidad de Cataluña**.

CUARTO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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.