Procedimiento Nº PS/00048/2010

RESOLUCIÓN: R/00959/2010

En el procedimiento sancionador PS/00048/2010, instruido por la Agencia Española de Protección de Datos a la entidad ***LIDL SUPERMERCADOS S.A.U.***, vista la denuncia presentada por D. ***A.A.A.*** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 17 de marzo de 2008 tiene entrada en esta Agencia un escrito de D. A.A.A., en el que declara que la cadena de supermercados "LIDL" y, en concreto, el establecimiento sito en la (C/.....), no cumple la normativa reguladora sobre videograbaciones y derechos de los ciudadanos al respecto. Manifiesta que en los carteles informativos, únicamente se ve la leyenda *"Sistema video grabación"* puesta bajo un monitor que hay en el pasillo de entrada a la zona de compra y, donde se visualizan imágenes que graba alguna cámara. En el resto de la tienda no es visible ningún tipo de aviso o letrero al respecto de las grabaciones, ni derechos de los ciudadanos a su acceso.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se solicita información y documentación a Lidl Supermercados, S.A.U., en adelante LIDL, en relación con el sistema de videovigilancia instalado en el establecimiento sito en la (C/.....).

1. En el escrito de respuesta al citado requerimiento con fecha de entrada en esta Agencia el día 20/10/2008, el representante de LIDL realiza las siguientes manifestaciones:

a. Las cámaras de videovigilancia instaladas en la tienda están ubicadas en los siguientes puntos:

   Sala de ventas, tanto en pasillos como en zona de caja.

   Almacén

   Oficina

b. Estas cámaras fueron instaladas con la finalidad de controlar todos los accesos del centro, garantizar la seguridad tanto de clientes como de trabajadores de la empresa, y prevenir, controlar y detectar hurtos, robos y otros posibles delitos.

c. Los carteles informativos se encuentran colocados en los siguientes puntos de la tienda:

   Puerta de entrada de clientes

   Muelle del almacén y debajo de un monitor situado en la entrada de la tienda.

   Asimismo disponen de formulario informativo que se encuentra a disposición de nuestros clientes.

d. La empresa que realizó la instalación de las videocámaras es Siemens Building Technologies Security, S.A. con la que tienen suscrito un contrato en fecha 1/01/2008.

2. El representante de LIDL aporta la siguiente documentación:

    a. Copia del modelo de cartel informativo en los que consta la imagen de una videocámara bajo la leyenda "ZONA VIDEOVIGILADA". Bajo dicha imagen se informa de la dirección postal ante la que se pueden ejercer los derechos establecidos en la LO 15/1999 de Protección de Datos de Carácter Personal.

    b. Modelo de cláusula informativa con el siguiente contenido:

"*Art. 3, apartado B. 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.*

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

Que sus datos personales se incorporarán al fichero denominado "VIDEOVIGILANCIA" y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia. Que el destinatario de sus datos personales es:

LIDL Supermercados, S.A.U., Ref.: Protección de datos, (C/.....).

Que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante el responsable del fichero.

Que el responsable del fichero tratamiento es LIDL Supermercados, S.A.U., ubicado en (C/.....)."

    c. Copia del contrato suscrito el día 1/1/2008 entre LIDL y Siemens Building Technologies Security, S.A. con objeto de la prestación del servicio de instalación, mantenimiento y explotación de centrales de alarma.

    d. Copia de la resolución del Comisario Jefe de la Unidad Central de Seguridad Privada de la que se desprende que Siemens Building Technologies Security, S.A. se encuentra inscrita en el Registro de Empresas de Seguridad, con el número de inscripción ***.

3. De las fotografías aportadas por el denunciante se desprende que en el comercio denunciado dispone de monitores que reproducen las imágenes captadas por las cámaras de video vigilancia, estando disponible su visualización al público. Este hecho podría suponer una infracción del artículo 4.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

4. Consta en el registro General de Protección de Datos la inscripción de un fichero denominado "*VIDEOVIGILANCIA"* con el código ######## y con la descripción "*CONTROL DE EDIFICIOS PARKINGS Y TIENDAS CON CAMARAS DE VIDEOVIGILANCIA"* cuyo responsable es la empresa Lidl Supermercados, S.A.U.

TERCERO: En fecha 10 de febrero de 2010 el Director de la Agencia Española de Protección de Datos, acordó iniciar procedimiento sancionador a LIDL SUPERMERCADOS, S.L., por la posible infracción de los artículos 4.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en los sucesivo LOPD), tipificada como graves en el artículo 44.3.d) de dicha norma, pudiendo ser sancionada con multa de 60.101,21 € a 300.506,05 €, de acuerdo con el artículo 45.2 de la citada Ley Orgánica.

CUARTO: Notificado con fecha 17 de febrero de 2010 dicho acuerdo de inicio, en fecha 5 de marzo

de 2010 , se recibe escrito de D. B.B.B. y C.C.C., en nombre y representación de LIDL SUPERMERCADOS, S.A.U., formulando, en síntesis, las siguientes alegaciones al Acuerdo de Inicio:

- Que la finalidad de instalación de las cámaras es "controlar todos los accesos del centro, garantizar la seguridad tanto de clientes como de trabajadores de la empresa, y prevenir, controlar y detectar hurtos, robos y otros posibles delitos". Sólo las finalidades de seguridad, y no otras, fueron las que llevaron a la implantación del sistema de cámaras de vigilancia.
- Que la instalación de las cámaras no supuso el medio inicial para llevar a cabo las finalidades indicadas, como se desprende de observar la fecha de notificación del correspondiente fichero a la AEPD, puesta en relación con la fecha de constitución e inicio de la actividad comercial de LIDL.
- Que la utilización del sistema respecta el principio legal de proporcionalidad, dado que la medida es idónea para conseguir el fin que es la vigilancia y seguridad para las personas que se hallan en el interior de la tienda; es una medida necesaria por cuanto se habían probado otras no suficientemente eficaces para lograr la seguridad de dichas personas y es una medida ponderada y equilibrada para la consecución del interés perseguido.
- Que el tratamiento de las imágenes lo lleva a cabo una empresa de seguridad privada, la cual ha asesorado a LIDL en la colocación, emplazamiento, instalación y demás elementos del funcionamiento del sistema de videovigilancia.
- Que según manifiesta el Informe Jurídico de esta Agencia 468/2006, la aplicación de los principios anteriormente señalados es especialmente relevante cuando la finalidad perseguida no es la de la vigilancia y seguridad, sino la del control de los hábitos de consumo.
- Que en vista de lo expuesto se solicita el archivo del expediente de referencia.

QUINTO: Con fecha 16 de marzo de 2010, por parten del instructor del procedimiento se inició el período de práctica de pruebas, dando por reproducidos a efectos probatorios la denuncia interpuesta por D. A.A.A. y su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante LIDL SUPERMERCADOS S.A.U., y el Informe de actuaciones previas de Inspección que forman parte del expediente E/00739/2008.

Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00048/2010 presentadas por LIDL SUPERMERCADOS S.A.U., y la documentación que a ellas acompaña.

SEXTO: En fecha 20 de abril de 2010, el Instructor del Procedimiento emitió Propuesta de Resolución, en la que se propone que por el Director de la Agencia Española de Protección de Datos, se sancione a LIDL SUPERMERCADOS S.A.U., con multa de 6.000 € (seis mil euros), por la infracción del artículo 4.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, dándose traslado a ésta para que en el plazo máximo de quince días hábiles presentara alegaciones.

SÉPTIMO: En fecha 11 de mayo de de 2010 , se recibe escrito de D. D.D.D., en nombre y representación de LIDL SUPERMERCADOS, S.A.U., formulando, en síntesis, las siguientes alegaciones a la Propuesta de Resolución:

- Se ratifican en las alegaciones realizadas al Acuerdo de Inicio respecto a las cuestiones relativas a la finalidad de instalación de las videocámaras, el análisis de la proporcionalidad, necesidad y adecuación, en relación al sistema de videovigilancia.

- Que tratándose de la mera emisión de imágenes en circuito cerrado, que no se graban ni se conservan entienden que no se lleva a cabo tratamiento alguno de datos. Asimismo manifiestan que la ley define como tratamiento de datos, la recogida, grabación, conservación o elaboración de datos.

- Que la medida cumple los tres requisitos del principio de proporcionalidad es decir, en primer lugar es idónea para conseguir el fin perseguido, que es el de la vigilancia; en segundo lugar es necesaria, por cuanto se había probado otras medidas no suficientemente eficaces para lograr la seguridad de las personas; y en tercer lugar, es una medida ponderada y equilibrada para la consecución del interés perseguido.

- Que las medidas son consideradas aceptables respecto a las cámaras situadas a la “Entrada clientes”, además de otros emplazamientos, en Resoluciones de la AEPD, como por ejemplo la del expediente E/01149/2008.

-Que se muestran conformes con el fundamento de la “disminución cualificada de culpabilidad de la imputada”.

- Que en relación a la licitud y proporcionalidad de esas medidas de vigilancia y seguridad, otras Resoluciones de la AEPD, como la del Expediente E/01449/2008, se han resuelto con el archivo de las actuaciones porque el sistema de videovigilancia fue instalado por motivos de seguridad, por empresa de seguridad autorizada por el Ministerio del Interior y el tratamiento resulta legítimo.

- Que a la vista de lo expuesto se dicte resolución en la que se declare el archivo del expediente de referencia.

OCTAVO: De las actuaciones llevadas a cabo en el presente procedimiento, han quedado acreditados los siguientes hechos probados

HECHOS PROBADOS

PRIMERO: Consta que con fecha de 17 de marzo de 2008 tiene entrada en esta Agencia un escrito de D. A.A.A., en el que declara que la cadena de supermercados "LIDL" y, en concreto, el establecimiento sito en la (C/.....), no cumple la normativa reguladora sobre videograbaciones y derechos de los ciudadanos al respecto. Manifiesta que en los carteles informativos, únicamente se ve la leyenda *"Sistema video grabación"* puesta bajo un monitor que hay en el pasillo de entrada a la zona de compra y, donde se visualizan imágenes que graba alguna cámara. (Folio 1 a 4).

SEGUNDO: La representación de LIDL manifiesta que las cámaras de videovigilancia instaladas en la tienda están ubicadas en los siguientes puntos: sala de ventas, tanto en pasillos como en zona de caja, almacén y oficina, y que la finalidad de sus instalación fue controlar todos los accesos del centro, garantizar la seguridad tanto de clientes como de trabajadores de la empresa, y prevenir, controlar y detectar hurtos, robos y otros posibles delitos.(Folio 38)

TERCERO: La representación de LIDL informa que los carteles informativos se encuentran colocados en los siguientes puntos de la tienda: puerta de entrada de clientes, muelle del almacén y debajo de un monitor situado en la entrada de la tienda. Adjunta copia del mismo, siendo acorde al previsto en la Instrucción 1/2006, de 8 de noviembre de la Agencia Española de Protección de Datos. Asimismo aporta cláusula informativa prevista en el artículo 3 b) de la citada Instrucción. (Folio 40 a 42).

CUARTO: La empresa que realizó la instalación de las videocámaras es Siemens Building Technologies Security, S.A., con la que tienen suscrito un contrato en fecha 1/01/2008. Aporta copia del contrato suscrito entre LIDL y Siemens Building Technologies Security, S.A. con objeto de la prestación del servicio de instalación, mantenimiento y explotación de centrales de alarma. Asimismo, se aporta copia de la resolución del Comisario Jefe de la Unidad Central de Seguridad Privada de la que se desprende que Siemens Building Technologies Security, S.A. se encuentra inscrita en el Registro de Empresas de Seguridad, con el número de inscripción ***.(Folio 43 a 53).

QUINTO: De las fotografías aportadas por el denunciante se desprende que el comercio denunciado dispone a la entrada del mismo, de un monitor que reproduce las imágenes captadas por las cámaras de videovigilancia, estando disponible su visualización al público. (Folio 3 y 4).

SEXTO: Consta en el registro General de Protección de Datos la inscripción de un fichero denominado "*VIDEOVIGILANCIA"* con el código ######## y con la descripción "*CONTROL DE EDIFICIOS PARKINGS Y TIENDAS CON CAMARAS DE VIDEOVIGILANCIA"* cuyo responsable es la empresa Lidl Supermercados, S.A.U.(Folio 79 a 81).

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

Con carácter previo al análisis del artículo 4.1 de LOPD, cuya vulneración se imputa a Lidl Supermercados, S.A.U. (en adelante LIDL), hay que señalar que dicha Ley Orgánica 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.

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".*

El artículo 2.1 de la misma señala como ámbito de aplicación de la citada norma que: *"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 identificable*s".

De acuerdo con lo anterior, resulta preciso determinar, en primer lugar, que ha de entenderse por dato de carácter personal. El artículo 3.a) de la LOPD considera dato de carácter personal "*cualquier información concerniente a personas físicas identificadas o identificables*".

Por su parte el artículo 5.1 del Reglamento de desarrollo de al LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, recoge en sus aparatados 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":* "*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*".

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.

En el 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, 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.

El Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la citada Directiva 95/46/CE, en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, formula distintos criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas.

Para determinar si el supuesto que se analiza implica el tratamiento de datos relacionados con personas identificables, el citado Grupo considera que los datos constituidos por imagen y sonido son personales aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la captación de imágenes y las herramientas de comunicación utilizadas. A efectos de la Directiva, se añade, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dispositivos

específicos.

En segundo lugar, debe analizarse el concepto de tratamiento de datos, este concepto se recoge en el artículo 3.c) de la LOPD, que define 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*", recogiéndose en el artículo 5.1.f) del reseñado Real Decreto 1720/2007, de 21 de diciembre, como tal *"cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, 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.

En el ámbito comunitario, la 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.

En nuestro país la STC 14/2003, de 30 de enero, entró en el análisis de esta cuestión. El Tribunal Constitucional tras recordar que, en su dimensión constitucional, el derecho a la propia imagen proclamado en el artículo 18.1 CE se configura como un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que puede tener difusión pública, consideró que la facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad-informativa, comercial, científica, cultural, etc.- perseguida por quien la capta o difunde. (SSTC 81/2001, de 26 de marzo, FJ 2; 139/2001, de 18 de junio, FJ 4; 83/2002, de 22 de abril, FJ 4).

Desde la perspectiva de la protección de datos de carácter personal, esta Sentencia del Tribunal Constitucional considera que la fotografía es un dato de carácter personal sujeto al régimen legal de protección, doctrina extensible a todos los medios de reproducción de imagen.

Por su parte, 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 sus artículos 1.1 y 2 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."

"Artículo 2.

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 acuerdo con los preceptos transcritos, la cámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere.

El Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la citada Directiva 95/46/CE, en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, formula distintos criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas.

Para determinar si el supuesto que se analiza implica el tratamiento de datos relacionados con personas identificables, el citado Grupo considera que los datos constituidos por imagen y sonido son personales aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la captación de imágenes y las herramientas de comunicación utilizadas. A efectos de la Directiva, se añade, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dispositivos específicos.

Así las cosas, la captación y grabación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, ya que constituye un tratamiento de datos de carácter personal siempre que dichas imágenes contengan *"cualquier información concerniente a personas físicas identificadas o identificables",* es decir, que permita la identificación de las personas que aparecen en las mismas.

En este supuesto, el sistema de videovigilancia y seguridad instalado en el local comercial ubicado en la (C/.....) permitía la visualización en tiempo real de las zonas acotadas objeto de protección y la grabación de la imagen de los afectados por este tipo de tratamiento. Dicho sistema estaba compuesto por diferentes cámaras instaladas en la sala de ventas (tanto

pasillos como zona de caja), almacén y oficina. Asimismo tiene un monitor a la entrada del establecimiento y a la vista de todo el público que accede al mismo, donde se visualizan las imágenes de las cámaras. Es decir, ya que a efectos de la LOPD la imagen de una persona constituye un dato de carácter personal, nos encontramos ante un tratamiento que cae bajo la órbita de la normativa de protección de datos de carácter personal, toda vez que la información captada, visualizada y grabada, contiene entre otra información, datos concernientes a personas identificadas o identificables dado el entorno en el que se recogen y graban, 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.

Así, de conformidad con la normativa y jurisprudencia expuesta, la captación y grabación de imágenes a través de videocámaras, como es el caso que nos ocupa, constituye un tratamiento de datos personales, cuyo responsable se identifica, en el presente caso, con LIDL SUPERMERCADOS, S.A.U., toda vez que es éste el que decide sobre la finalidad, contenido y uso del citado tratamiento.

III

Asimismo, la vigente LOPD atribuye la condición de responsables de las infracciones a lo previsto en dicha norma a los responsables de los ficheros (artículo 43), concepto que debe integrarse con la definición que de los mismos recoge el artículo 3.d) de la misma. Este precepto, innovando respecto de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal, incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. Conforme al citado artículo 3.d) de la LOPD, 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".*

El artículo 5.1 q) del RDLOPD considera como tal a la "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo 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."

Así de conformidad con las definiciones recogidas en la normativa de protección de datos expuesta, la entidad LIDL es, por un lado, la responsable del tratamiento de las imágenes que incluyan datos de carácter personal que son captadas y transmitidas por las cámaras que integran el sistema de seguridad privada instalado con fines de videovigilancia, habiendo sido también responsable del tratamiento de datos derivado de la visualización en tiempo real de dichas imágenes que se producía a través del monitor situado a la entrada del establecimiento, y, por otro lado, es también la responsable del fichero de videovigilancia resultante de la grabación de las imágenes conservadas en el videograbador digital de la instalación, estando, por tanto, dicha sociedad sujeta al régimen de responsabilidad recogido en el Título VII de la LOPD. Esta afirmación encuentra su justificación en que, con independencia de las características particulares del sistema instalado, dicha mercantil decidió la realización de un tratamiento de datos personales, ya que resolvió la instalación de un sistema de cámaras o videocámaras que captan las imágenes de las personas que se encuentran en el ángulo de visión de aquéllas, y decidió, igualmente, que la finalidad, contenido y uso del citado tratamiento sería la vigilancia y control con fines de seguridad.

IV

Respecto al alegato formulado por LIDL relativo a que tiene contratado una empresa de seguridad privada autorizada quien le ha asesorado en la colocación, emplazamiento, instalación y demás elementos del funcionamiento del sistema de videovigilancia, hay que señalar que el apartado 1 del artículo 6 de la LOPD, y el apartado 2 del mismo precepto 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*.

Respecto a la legitimación en el tratamiento de las imágenes, la respuesta se encuentra en el artículo 2 de la Instrucción 1/2006, que establece 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 respectar en todo caso los requisitos exigidos por la legislación vigente en la materia".

Así, hasta la entrada en vigor, el pasado 27 de diciembre de 2009, de la Ley 25/2009, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y sus ejercicio(conocida como "Ley Ómnibus"), la legitimación del tratamiento de los datos de carácter personal en materia de videovigilancia, a excepción de los casos, prácticamente imposibles dada su dificultad práctica, en los que se hubiera obtenido el consentimiento inequívoco de cada una de las personas que resulten captadas o grabadas como consecuencia del uso de las cámaras, puede proceder, en función del ámbito de aplicación, bien de la Ley 23/1992, de 30 de julio, de Seguridad Privada (en adelante LSP), o bien de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

Así hasta la entrada en vigor de la citada Ley 25/2009 , la legitimación para el tratamiento por particulares y empresas de imágenes captadas a través de dispositivos de videovigilancia sólo era posible en caso de que dichos sistemas hubieran sido contratados con empresas de seguridad privada, debidamente acreditadas ante el Ministerio del Interior, al que además debía notificarse el contrato que se hubiese celebrado, conforme a lo exigido por la Ley 23/1992, de 30 de julio de Seguridad Privada.

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

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

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

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

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

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

En todo caso, el tratamiento de las imágenes 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, como son, entre otros, los relativos a que las imágenes que se capten sean las necesarias y no excesivas para la finalidad perseguida; el deber de informar a los interesados, tanto a través de la colocación de carteles informativos como mediante la puesta a disposición de aquéllos de impresos en que se detalle la información; la notificación de la existencia de los ficheros a la Agencia Española de Protección de Datos; o la implantación de medidas de seguridad.

Así en el caso que nos ocupa, LIDL, tiene formalizado con fecha 1 de enero de 2008, contrato de instalación, mantenimiento y explotación de centrales de alarma, del sistema de videovigilancia, con la empresa de seguridad autorizada Siemens Building Technologies Security, S.A, sociedad inscrita en el registro de Empresas de Seguridad de la Dirección General de la Policía con el nº ***.

A la vista de tal circunstancia se señala que aunque el tratamiento de los datos de las personas cuyas imágenes eran captadas por las cámaras de videovigilancia instaladas en el interior del Supermercado se encontrara habilitado por la LSP, este hecho no autorizaría a la visualización de las imágenes en la forma en que se producía en la fecha de los hechos denunciados, al no ser proporcional al fin perseguido, tal y como se desarrollara seguidamente al justificar la vulneración del artículo 4.1 de la LOPD.

Por otro lado, hay que señalar que para que pueda afirmarse la responsabilidad es imprescindible que pueda imputarse al hecho constitutivo de infracción a una persona (principio de personalidad).

El principio de personalidad de la sanción ha sido consagrado por el Tribunal Constitucional en la STC 219/1988, como principio de responsabilidad por hechos propios. El respeto al principio

de personalidad exige un nexo casual entre el hecho constitutivo de la infracción y la persona responsable.

La cuestión radica en analizar la especial configuración que el hecho infractor tiene en Derecho Administrativo Sancionador. La tipificación de las infracciones administrativas trata en definitiva, por lo general, de proteger el cumplimiento del Ordenamiento Jurídico, y de sancionar, por tanto, su incumplimiento, a diferencia de lo que ocurre con las infracciones penales, que sancionan la lesión o puesta en peligro de un bien jurídico protegido, sin que haya, por lo general una norma sustantiva subyacente que imponga la obligación que haya sido vulnerada.

Si en consecuencia, el hecho infractor consiste en un incumplimiento de la norma (y no es una lesión aun bien jurídico), sólo el titular de tal obligación estará, en principio capacitado para cometer la infracción. La exigencia de responsabilidad a quien no sea titular de la obligación incumplida vulneraría, por tanto, el principio de personalidad, pues no corresponde al no titular cumplir la obligación, ni por ende, se le puede hacer responder de su incumplimiento. Ello explica que, a efectos de determinar la imputación de una infracción a una persona determinada, lo relevante sea la indagación previa de la titularidad de la obligación que subyace al tipo.

En definitiva, no cabe imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan esta imputación o de la intervención en los mismos del presunto infractor. Así, en el caso que nos ocupa, LIDL, en base al principio de personalidad es responsable de la comisión de la infracción del artículo 4.1 de la LOPD, al ser ella la que ha decidido la instalación, finalidad, uso y contenido del tratamiento de las imágenes captadas por las cámaras.

V

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 al responsable del tratamiento respetar la normativa existente en materia de protección de datos y cumplir el principio de proporcionalidad recogido en el artículo 4.1 de la LOPD, cuya vulneración se imputa a LIDL en este procedimiento sancionador, y cuyo tenor literal dispone 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"*

El artículo 4 de la LOPD, con la denominación *"Calidad de datos"* es el primer precepto del título II dedicado a los *"Principios de calidad de datos",* que derivan del derecho fundamental a la protección de datos.

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 (..)".*

Al objeto de preservar ese derecho fundamental, la LOPD establece una serie de principios generales en esta materia, que se regulan en los artículos 4 a 12 de la LOPD, entre los que se encuentran la calidad de datos, el derecho a la información, el consentimiento del afectado, la seguridad de los datos, el deber de secreto y el acceso a los datos por cuenta de terceros. Los principios generales de protección de datos constituyen el contenido esencial de protección de datos

y configuran un sistema de tutela que garantiza una utilización racional y razonable de los datos personales. Por ello a través de la configuración de estos principios el legislador aspira a constituir un sistema preventivo de tutela de la persona frente al tratamiento de sus datos.

La reciente SAN, Sección 1ª, de 25 de julio de 2006 (rec. 210/2005) establece que *"dichos principios sirven para delimitar el marco en el que debe desenvolverse cualquier uso o cesión de datos de carácter personal y para integrar la definición de los tipos de infracción definidos en el artículo 44 de la LOPD, pues este aborda la tipificación de las distintas infracciones mediante una remisión a los principios definidos en la propia ley".*

En el apartado 1 del artículo 4 de la LOPD comienza sentando que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, de acuerdo con una serie de criterios, que se resumen en el principio de proporcionalidad.

Este 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 tratamiento, debiendo restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de los mismos. En consecuencia, el tratamiento del dato ha de ser pertinente y no excesivo en relación con el fin perseguido. 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 que además debe 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, 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 citado artículo 4, 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.

Así LIDL alega que el sistema de videovigilancia instalado cumple los tres requisitos del principio de proporcionalidad al ser idóneo para la vigilancia y seguridad de las personas que se encuentran en el interior de la tienda; necesario por cuanto se habían probado otras no suficientemente eficaces para lograr la seguridad de las personas y equilibrada para le consecución del interés perseguido. Sin embargo, si el tratamiento del dato ha de ser "pertinente" al fin perseguido y la finalidad ha de estar "determinada", difícilmente se puede defender, como pretende la mercantil imputada, que el irregular tratamiento dado por LIDL a las imágenes captadas por las cámaras de videovigilancia instaladas, haya respetado el principio de proporcionalidad con el funcionamiento del monitor situado a la entrada del supermercado.

En este supuesto se ha probado que las imágenes captadas por las cámaras que integraban el sistema de videovigilancia podían ser visionadas en tiempo real por cualquier persona que accediera al establecimiento a través del monitor colocado en la entrada del local al que estaban conectadas las citadas cámaras, siendo visionadas también por cualquier persona que se acercara al lugar en que estaba emplazado dicho dispositivo. El referido monitor, permitía que las

imágenes recogidas se visualizaran en tiempo real. Por lo tanto, dicho tratamiento ha supuesto una vulneración del principio de proporcionalidad previsto en el artículo 4.1 de la LOPD, habida cuenta que la exposición de las imágenes captadas en la forma descrita en modo alguno puede considerarse como proporcionado y necesario, para la finalidad de seguridad y vigilancia pretendida ni responde, tampoco, a una intervención mínima en lo que respecta a los derechos a la intimidad y a la protección de datos de carácter personal de los afectados por dicho tratamiento, como argumenta la entidad denunciada.

VI

El Grupo de protección de las personas, ya citado, en lo que respecta al tratamiento de datos personales, en su Dictamen 4/2004, mencionaba en cuanto a las obligaciones y precauciones que deberán respetarse por los responsables del tratamiento de los datos, entre otras, la de evitar las referencias inadecuadas a la intimidad; especificar de forma clara e inequívoca los fines perseguidos con el tratamiento y otras características de la política de privacidad (momento en que se borran las imágenes, peticiones de acceso); obtención del consentimiento del interesado basado en una información clara; mantener la necesaria proporcionalidad entre los datos y el fin perseguido, obligándose al empleo de sistemas idóneos con respecto a dicho fin y a minimizar los datos por parte del responsable del tratamiento; datos que han de ser adecuados, pertinentes y no excesivos y deberán retenerse durante un plazo en consonancia con las características específicas de cada caso.

Así, el uso de las instalaciones de cámaras y videocámaras debe seguir ciertas reglas que rigen todo el proceso desde su captación, visualización, almacenamiento y reproducción hasta su cancelación. LIDL debió tener en cuenta que debía existir una relación de proporcionalidad entre la finalidad perseguida y el modo en el que se trataban los datos, garantizándose por los apartados 1 y 2 del mencionado artículo 4 de la LOPD el cumplimiento del principio de proporcionalidad y finalidad en todo tratamiento de datos personales.

En este sentido el artículo 4 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras establece:

"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 explicitas, 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".

Igualmente hay que valorar, tal y como se indica en la Instrucción 1/2006, de 8 de noviembre, que *"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)".

A la vista de lo anterior, LIDL vulneró el artículo 4.1 de la LOPD al decidir que las imágenes captadas fueran transmitidas en un monitor colgado del techo del local comercial, en la entrada al supermercado, que por su ubicación posibilitaba que todas las personas que pasaban junto al mismo visionaran las imágenes que transmitía, las cuales incluían datos de las personas que estaban siendo enfocadas por las cámaras de videovigilancia, produciéndose de este modo un tratamiento excesivo, no pertinente e inadecuado de datos de carácter personal en relación con la finalidad de protección y seguridad para las que se recogían y que no hacia preciso que la toma de imágenes se difundiera de tal modo, siendo obligación del responsable del tratamiento adecuar el uso de la instalación de modo que el impacto en los derechos de los afectados sea el mínimo posible.

VII

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, apartados D) y E), 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).

E) Proporcionalidad en la realización de actividades de vigilancia por videocámara

El principio según el cual los datos deben ser adecuados, pertinentes y no excesivos implica la evaluación minuciosa de la proporcionalidad de las medidas relativas al tratamiento de datos, una vez que la legalidad del mismo haya quedado validada. Las medidas para la grabación se establecerán teniendo en cuenta, en primer lugar, los siguientes aspectos: a) El ángulo visual con arreglo a los fines perseguidos (por ejemplo, si la vigilancia se realiza en un lugar público, el ángulo deberá establecerse de manera que no permita visualizar detalles o rasgos físicos que resulten irrelevantes para los fines perseguidos, o zonas situadas en el interior de lugares privados cercanos, en particular, si se utiliza el zoom). b) El tipo de equipo que se utilizará para filmar, es decir, fijo o móvil. c) Medidas reales de instalación, es decir, situación de las cámaras, utilización de plano fijo o cámaras móviles, etc. d) Posibilidad de aumentar las imágenes o realizar primeros planos, durante la grabación o después, es decir, una vez que se han almacenado las imágenes, y posibilidad de desenfocar o borrar imágenes individuales. e) Congelación de imágenes. f) Conexión con un «centro» para enviar señales de alarma sonoras o visuales. g) Medidas que se toman como resultado de la vigilancia por videocámara, es decir, cierre de entradas, convocatoria del personal de vigilancia, etc.

En segundo lugar, deberá tenerse en cuenta la decisión que se va a tomar en cuanto a la retención de las imágenes y el plazo (éste último deberá ser bastante breve y estar en consonancia con las características específicas de cada caso). Si bien en algunos casos un sistema que sólo permita la visualización de imágenes en circuito cerrado, sin necesidad de grabar, puede ser suficiente (por ejemplo, en el caso de las cajas de un supermercado), en otros (por ejemplo, para proteger lugares privados), puede que esté justificado grabar imágenes durante unas cuantas horas y borrarlas automáticamente, sin exceder nunca el final del día o, como mucho, el final de la semana. Obviamente, esta regla tiene excepciones, como cuando se emite una señal de alarma o se realiza una petición que merece especial atención; en esos casos, hay motivos suficientes para esperar, durante un período breve, una posible decisión por parte de las autoridades policiales o judiciales. Por poner otro ejemplo, un sistema cuyo objetivo es detectar el acceso no autorizado de vehículos a centros urbanos y zonas de tráfico restringido, sólo deberá grabar imágenes en caso de que se cometa una infracción. La cuestión de la proporcionalidad también deberá tenerse en cuenta debidamente siempre que se considere que son necesarios períodos de retención más breves, que no deberán superar una semana (por ejemplo, imágenes de vigilancia por videocámara que puedan utilizarse para identificar a las personas que frecuentan un banco antes de que se cometa un robo).

En tercer lugar, deberá prestarse atención a los casos en los que se facilita la identificación de una persona mediante la asociación de imágenes del rostro de dicha persona con otra información relativa a conductas actividades reproducidas (por ejemplo, en caso de asociación de imágenes y actividades realizadas por los clientes de un banco en un momento fácilmente identificable). En este sentido, deberá tenerse en cuenta la clara diferencia que existe entre la retención temporal de imágenes de vigilancia por videocámara captadas con un equipo situado a la entrada de un banco y la creación de bancos de datos que incluyan fotos y huellas dactilares facilitadas por los clientes del banco con su consentimiento, lo que supone una intrusión en mayor medida. Por último, deberá prestarse atención a las decisiones que se tomen con respecto tanto a la posible comunicación de los datos a terceras partes (lo que, en principio, no deberá implicar a entidades que no estén relacionadas con las actividades de vigilancia por videocámara) como a su posible revelación, total o parcial, en el extranjero o, incluso, en la red (también a la luz de las disposiciones relativas a la protección adecuada; véase el artículo 25 y siguientes de la Directiva). Obviamente, el requisito según el cual las imágenes deberán ser pertinentes y no excesivas, también se refiere a la combinación de información procedente de diferentes responsables del tratamiento de sistemas de vigilancia por videocámara. Las garantías mencionadas más arriba pretenden implantar, también de manera operacional, el principio al que se hace referencia en la normativa nacional de varios países: el principio de moderación en el uso de datos personales (cuyo objetivo consiste en evitar o reducir al mínimo posible el tratamiento de datos personales). Este principio debería aplicarse en todos los sectores, teniendo en cuenta, también, el hecho de que muchos objetivos pueden alcanzarse realmente sin recurrir a datos personales, o utilizando datos realmente anónimos, a pesar de que, inicialmente, pueda parecer necesario utilizar información personal. Las consideraciones anteriores también son aplicables cuando se da la necesidad justificada de racionalizar los recursos comerciales o de mejorar los servicios prestados a los usuarios" .

En el caso analizado, la forma en la que la entidad responsable del tratamiento permitió la visualización de las imágenes captadas por las cámaras de videovigilancia, y las de las personas incluidas en las mismas, supone que LIDL no adoptó las medidas de índole técnica y organizativa necesarias para evitar el acceso desproporcionado a las mismas, tales como la designación de una o varias personas concretas que fueran las únicas que tuvieran acceso a las imágenes y fueran conocedores de sus obligaciones.

Por consiguiente existe un tratamiento excesivo y no proporcional de las imágenes en relación con el ámbito y las finalidades que podrían justificaban su recogida, toda vez que la seguridad pretendida podría haberse obtenido por medios menos intrusivos para la intimidad de las personas afectadas, en todo caso habilitando a personas concretas (usuarios autorizados) que tuvieran acceso a las imágenes en forma controlada.

VIII

Respecto a las alegaciones realizadas por la entidad denunciada, relativas a que la mera emisión de imágenes en circuito cerrado, que no se graban no suponen un tratamiento de datos, hay que señalar las cámaras de videovigilancia aunque no graben, recogen imágenes, lo que en definitiva supone un tratamiento de datos, según lo dispuesto en el artículo 3. c) de la LOPD, donde se define el tratamiento de datos como *"operaciones y procedimientos técnicos de carácter automatizado o no, que permiten la recogida, grabación, conservación, elaboración, modificación, bloque y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

Así, en el apartado c) del artículo 37 de la LOPD, se recoge como función de la Agencia la de dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la Ley. En el artículo 5 del Estatuto de la Agencia se desarrolla esta previsión, distinguiendo entre la colaboración con los órganos competentes en lo que afecta al desarrollo normativo de la propia Ley, esto es, con el Gobierno para el desarrollo reglamentario, y la potestad normativa propia, dictando instrucciones y recomendaciones precisas para adecuar los tratamientos a los principios de la LOPD, así como recomendaciones de aplicación de disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros, correspondiendo esta potestad reglamentaria al Director de la Agencia.

Por lo tanto, en el ejercicio de la competencia que le atribuye el citado artículo 37.1.c) de la LOPD, la Agencia Española de Protección de Datos dictó la Instrucción 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de la citada Ley Orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas con tales procedimientos.

Así el criterio establecido respecto a esta materia en la LOPD, se complementa con lo dispuesto en el artículo 1 de la Instrucción 1/2006 donde se delimita el ámbito subjetivo de ésta señalando que:

"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 daros personales relacionados con aquéllas".

Por otro lado, el artículo 5.1. t) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define el tratamiento de datos como *"cualquier operación*

o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

Así, esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la LOPD, de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la ley se ha demostrado que precisan de un mayor desarrollo normativo.

La propia Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, define en el artículo 2b) el tratamiento de datos personales como *"cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción."*

Para mayor abundamiento la Sentencia de la Audiencia Nacional de 24/01/2003, al tratar la cuestión de lo que se entiende por tratamiento de datos, manifiesta*: "El artículo 3.c) de la Ley Orgánica 15/1999 define el "tratamiento de datos" como operaciones y operaciones y procedimientos técnicos de carácter automatizado o no, que permiten la recogida, grabación, conservación, elaboración, modificación, bloque y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Partiendo de esta definición, esta Sala considera que no cabe excluir que haya existido, por el hecho de que las imágenes cambiantes cada quince segundos no queden guardadas ni registradas en archivo alguno, pues según el precepto que acabamos de transcribir el tratamiento no exige la conservación de los datos, bastando con su recogida o grabación…".*

Así pues, cabe afirmar que los hechos por lo que se incoa el presente procedimiento sancionador, están perfectamente tipificados en una norma con rango legal como es la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y el criterio establecido respecto a esta materia en la citada ley, se complementa con lo dispuesto en la Instrucción 1/2006.

Por lo tanto a la vista de la jurisprudencia y normativa expuesta, el visionado a tiempo real constituye una captación de la imagen, de ahí la afirmación al considerar dicha actuación un tratamiento de datos de carácter personal.

IX

Respecto a las alegaciones realizadas por LIDL, citando el Informe Jurídico 468/2006, hay que señalar que en el citado informe se recoge el cumplimiento del principio de finalidad y proporcionalidad en el tratamiento de los datos, señalando *que "la aplicación de estos principios resulta especialmente relevante cuando la finalidad perseguida no es la de vigilancia y seguridad, sino como en el presente caso el control de los hábitos de consumo de las personas*". Lo que quiere decir este informe, y no la interpretación realizada por la mercantil denunciada, es que la proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas

de videovigilancia, ya sea su finalidad las funciones de vigilancia y control, como es el supuesto que nos ocupa, ya sean funciones de análisis de los hábitos de consumo de las personas, como es el caso del informe citado; debiendo respetarse el citado principio tanto en la recogida de los datos como en el posterior tratamiento de los mismos, tal y como se ha desarrollado en los Fundamentos de Derecho anteriores. Por lo tanto el tratamiento que realizó LIDL mediante el visionado a tiempo real de las imágenes que captaban las cámaras, por cualquier persona que accediera al establecimiento, a través del monitor ubicado a la entrada del mismo supone una vulneración del principio de proporcionalidad del artículo 4.1. de la LOPD.

Por último, respecto a la invocación del expediente resulto en esta Agencia E/01449/2008, como casos idénticos al que nos ocupa, cabe decir que no existe, una identidad de sujetos, hechos y fundamentos para realizar una aplicación analógica del mismo al caso concreto que nos ocupa, toda vez en aquel expediente se denunciaba el incumplimiento del artículo 5 de la LOPD por parte de la sociedad denunciada, resolviéndose con el archivo del mismo, al quedar acreditado que aquella cumplía con el citado deber, sin que en el mismo se acreditase un incumplimiento del artículo 4.1 de la LOPD, como se produce en el procedimiento que nos ocupa..

A la vista de todo lo expuesto, deben desestimarse las alegaciones formuladas por ***LIDL SUPERMERCADOS S.A.U.***

X

El artículo 44.3.d) de la LOPD tipifica como infracción grave: "Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave".

En relación al tipo de infracción establecido en el citado artículo 44.3.d), la Audiencia Nacional, en Sentencia de 27/10/2004, ha declarado*: "Sucede así que, como ya dijimos en la Sentencia de 8 de octubre de 2003 (recurso 1.821/01) el mencionado artículo 44.3 d) de la Ley Orgánica 15/1999, aún no siendo, ciertamente, un modelo a seguir en lo que se refiere a claridad y precisión a la hora de tipificar una conducta infractora, no alberga una formulación genérica y carente de contenido como afirma la demandante. La definición de la conducta típica mediante la expresión "tratar los datos de carácter personal .." no puede ser tachada de falta de contenido pues nos remite directamente a cualquiera de las concretas actividades que el artículo 3.d) de la propia Ley incluye en la definición de "tratamiento de datos" (recogida, grabación, conservación, elaboración, ... de datos de carácter personal). Y tampoco cabe tachar de excesivamente genérico o impreciso el inciso relativo a que el tratamiento o uso de los datos se realice "... con conculcación de los principios y garantías establecidos en la presente Ley...", pues tales principios y garantías debidamente acotados en el Título II del propio texto legal bajo las rúbricas de Principios de la Protección de Datos (artículos 4 a 12) y Derechos de las Personas (artículos 13 a 19)".*

En el presente caso, la descripción de conductas que establece el artículo 44.3.d) de la LOPD cumple las exigencias derivadas del principio de tipicidad, toda vez que del expresado precepto se desprende con claridad cuál es la conducta prohibida. El tipo aplicable considera infracción grave *"tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley",* por tanto, se está describiendo una conducta - el tratamiento de datos personales o su uso posterior – que precisa, para configurar el tipo, que la misma suponga vulneración de los principios y garantías establecidos por la LOPD.

Conviene recordar que desde el punto de vista material, la culpabilidad consiste en la capacidad que tiene el sujeto obligado para obrar de modo distinto y, por tanto, de acuerdo con el ordenamiento jurídico. En este caso, la entidad LIDL, en su condición de responsable del tratamiento, ha incurrido en infracción grave descrita.

Así, se ha probado que LIDL ha vulnerado un principio básico del derecho fundamental a la protección de datos, en concreto el principio de calidad de los datos en lo que se refiere al uso proporcional de los mismos, al permitir que los datos de carácter personal (imágenes) captados por las mencionadas cámaras estuvieran accesibles y visibles a todo el personal y clientes del supermercado a través del monitor instalado en el mismo, actuación que no responde a la intervención mínima que exige la ponderación entre la finalidad de vigilancia y control de bienes y personas y la posible afectación por la utilización de las mencionadas videocámaras al derecho al honor, a la propia imagen, a la intimidad de las personas y a la normativa de protección de datos, hecho que vulnera el principio de calidad de los datos recogido en el artículo 4.1 de la LOPD

De conformidad con lo expuesto en los Fundamentos de Derecho anteriores ambas conductas encuentran su tipificación en el señalado artículo 44.3.d) de la mencionada Ley Orgánica 15/1999.

XI

El artículo 45. 2. 4. y 5 de la LOPD establece lo siguiente:

*2. Las infracciones graves serán sancionadas con multa de 60.101,21 € a ***.506,05 €.*

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, 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 relación con la aplicación del artículo 45.5 de la LOPD, la Audiencia Nacional ha señalado, entre otras, en Sentencia de 21/01/2004 de la Audiencia Nacional, en su recurso 1939/2001, que dicho precepto <<…*no es sino manifestación del llamado principio de proporcionalidad (artículo 131.1 de la LRJPAC), incluido en el más general del prohibición de exceso, reconocido por la jurisprudencia como principio general del Derecho. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas, atendidas las circunstancias del caso concreto. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos*.>>

La aplicación con carácter excepcional del artículo 45.5 exige la concurrencia de al menos uno de los siguientes requisitos: a) Disminución de la culpabilidad del imputado y b) Disminución de la antijuridicidad del hecho.

En el presente caso, aunque ha quedado acreditada la comisión por parte de LIDL de la infracción grave imputada a dicha empresa, en lo que respecta a la actuación infractora se estima

que concurren una serie de circunstancias que suponen una disminución cualificada de la culpabilidad de la sociedad imputada respecto del artículo 4.1 de la LOPD.

Si bien se ha producido un tratamiento de datos personales inadecuado y excesivo, sin embargo, en el presente caso ha de tenerse en cuenta que el sistema de videocámaras instalado tenía como finalidad el control y protección de bienes y personas del establecimiento, debiendo valorarse también que LIDL ha acreditado que dicho sistema fue instalado por una empresa de seguridad privada, tiene carteles informativos de videovigilancia y cláusula informativa acordes a la Instrucción 1/2006, así como inscrito el fichero de videovigilancia en el Registro General de Protección de Datos de esta Agencia. Por todo ello, se considera que procede la aplicación del artículo 45.5 de la LOPD.

Asimismo, teniendo en cuenta los criterios de graduación de las sanciones previstos en el artículo 45.4 de la LOPD y, en especial, la falta de intencionalidad en la conducta mostrada por LIDL, procede la imposición, a la mencionada sociedad, una sanción de 6.000 euros por la infracción grave imputada al artículo 44.3.d) de la citada LOPD.

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 ***LIDL SUPERMERCADOS S.A.U.***, por una infracción del artículo 4.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 6.000 € (seis mil euros) de conformidad con lo establecido en el artículo 45.2.4 y 5 de la citada Ley Orgánica.

SEGUNDO: NOTIFICAR la presente resolución a ***LIDL SUPERMERCADOS S.A.U.*** y a D. ***A.A.A.***.

TERCERO: 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 000000000 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.

Madrid, 17 de mayo de 2010

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte