Procedimiento Nº PS/00538/2010

RESOLUCIÓN: R/00326/2011

En el procedimiento sancionador PS/00538/2010, instruido por la Agencia Española de Protección de Datos a la entidad ***HIPERCOR, S.A..***, vista la denuncia presentada por Don ***A.A.A.*** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 3 de noviembre de 2009, tuvo entrada en esta Agencia un escrito de Don ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia que el establecimiento Hipercor Bahía, ubicado en la Carretera de Cártama, Km. 2 de Málaga, (en lo sucesivo el denunciado) dispone de un sistema de videovigilancia que captura imágenes de la vía pública que incumplirían la normativa de protección de datos.

El denunciante manifiesta que el centro denunciado tiene cámaras de videovigilancia, tanto en el interior del comercio como en el exterior. Dichas cámaras exteriores están instaladas en las esquinas de las cornisas que dan a la calle y en el perímetro exterior del centro comercial que recoge las imágenes de las calles y aceras colindantes. Las del exterior son tipo DOMO con un giro de 360°. A su vez, tiene una cámara disimulada como farola en el acceso al Parking del mismo tipo DOMO sin tener ningún cartel informativo.

Adjunto a su escrito de denuncia aporta un reportaje fotográfico en el que se aprecia la existencia de cámaras de vídeo en las cornisas del edificio.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 6 de septiembre de 2010, por los inspectores de la Agencia se giró visita de Inspección al centro comercial HIPERCOR BAHÍA DE MÁLAGA durante la cual se pusieron de manifiesto los siguientes hechos:

a. La sociedad propietaria del centro comercial HIPERCOR BAHÍA DE MÁLAGA es HIPERCOR, S.A.., la cual también es responsable del sistema del videovigilancia instalado.

b. EL sistema de videovigilancia instalado en el Centro Comercial tiene como finalidad exclusiva la seguridad del personal, los clientes y de las instalaciones.
c. El sistema de videovigilancia lo constituye un total de 109 cámaras

distribuidas por los departamentos del centro comercial y 9 de ellas se encuentran ubicadas en la parte exterior del inmueble de forma que permitan la visualización del perímetro exterior del mismo. Éstas últimas son de tipo DOMO con movilidad que permite la visualización de 360º.

d. Las imágenes son visualizadas en un centro de control que se ubica en el mismo Centro Comercial y tienen acceso a las mismas, además del responsable de seguridad y directivos del Centro Comercial, los vigilantes de la empresa de seguridad que HIPERCOR, S.A.. tiene contratada.

e. Las imágenes son conservadas por un periodo máximo de 7 días, disponiendo para ello de 11 grabadores digitales. Así mismo, HIPERCOR, S.A.. ha creado un fichero denominado VIDEOVIGILANCIA, inscrito en el Registro General de Protección de Datos con el código ###COD1.

f. Con respecto a la instalación de cámaras en el exterior del edificio, las empresas del grupo HIPERCOR enviaron una comunicación dirigida por el Director de Seguridad de la compañía a la Secretaría de Estado de Interior con fecha 12 de mayo de 2009, por la que se solicita concesión de la correspondiente autorización administrativa para la grabación de imágenes en la vía pública, en todos y cada uno de los centros comerciales que la compañía tiene en el territorio español, con la finalidad de prevenir la comisión de delitos y, si éstos se produjeran, poder utilizar dichas imágenes para la identificación del autor o autores de los mismos, así como ayudar en la organización de los planes de evacuación y desalojo de los edificios. A este respecto se recibió respuesta de la Secretaria de Estado, en el que se comunican que no tienen capacidad legal para autorizar a empresas la instalación de cámaras de video que recojan imágenes de la vía pública.

g. En cada uno de los accesos al edificio hay un cartel informativo de zona videovigilada, en el que se identifica al responsable del fichero ante quién pueden ejercitarse los derechos recogidos en el artículo 5 de la L.O. 15/1999.

h. En el exterior del Centro Comercial existen un total de nueve cámaras de tipo DOMO y en las fachadas exteriores del edificio se encuentran pegados carteles informativos de la existencia de un sistema de videovigilancia.

i. En el interior del Centro Comercial existen instaladas numerosas cámaras de videovigilancia.

j. En el momento de la inspección se encuentra personal de seguridad visualizando las imágenes que capturan en tiempo real las videocámaras del sistema de videovigilancia, a través de varios monitores. El sistema dispone de un programa informático que permite la gestión de las cámaras y las imágenes capturadas.

k. Las cámaras números 42, 43 y 44, ubicadas en la parte exterior del edificio, disponen de funcionalidad de ZOOM y un ángulo de giro de 360º y recogen imágenes de parte de la vía pública apreciándose en las mismas personas

identificables que transitan.

2. El Centro Comercial Dispone de un Servicio de Seguridad Privado que presta la empresa SECURITAS SEGURIDAD ESPAÑA, S.A. cuyo personal utiliza el sistema de videovigilancia en las labores de seguridad. El contrato de prestación de dicho servicio ha sido contratado por EL CORTE INGLES, S.A., con fecha 15/1/2005 cuya copia ha aportado el representante de la entidad a la inspección de datos. En dicho contrato consta que el pago del servicio lo realiza un 59% EL CORTE INGLES, S.A. y un 41% HIPERCOR, S.A.. aunque el contrato sólo lo suscribe el primero.

TERCERO: En el acuerdo de inicio del presente procedimiento se informó que, de la información contenida en las actuaciones previas de investigación, y sin perjuicio de lo que se derivara de la instrucción del presente expediente sancionador, se desprendía que la entidad **HIPERCOR, S.A..** dispone de un sistema de videovigilancia instalado en el establecimiento Hipercor Bahía, ubicado en la Carretera de Cártama Km. 2 de Málaga, que captura imágenes de la vía pública, que es competencia exclusiva de los Cuerpos y Fuerzas de la Seguridad del Estado, por lo que no dispondría de habilitación legal para el tratamiento de imágenes y precisando, por tanto, del consentimiento de los afectados, según se recoge en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal .

CUARTO: Con fecha 28 de septiembre de 2010, el Director de la Agencia Española de Protección de Datos acordó iniciar, procedimiento sancionador a **HIPERCOR, S.A..**, por presunta infracción del artículo 6 de la Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.d) de dicha norma, pudiendo ser sancionado con multa de 60.101,21 € a 300.506,05 €, de acuerdo con el artículo 45.2 de la misma Ley Orgánica.

QUINTO: Notificado el acuerdo de inicio, HIPERCOR, S.A.. mediante escrito de fecha 22 de octubre de 2010, formuló alegaciones, significando lo siguiente:

1. Que la finalidad de la instalación del sistema de videovigilancia de Hipercor no tiene por finalidad el tratamiento de imágenes de terceros que pasen por las inmediaciones de los establecimientos, sino la protección de dichos establecimientos frente a cualquier actuación violenta por parte de terceros contra los mismos incluyendo, la prevención de actos terroristas que ha sufrido en el pasado.

2. Que el sistema de videovigilancia del establecimiento denunciado ha sido instalado por una empresa de seguridad autorizada, por lo que el tratamiento de los datos se encuentra habilitado por la Ley de Seguridad Privada, no siendo necesario el consentimiento del afectado.

3. Que el único medio de llevar a cabo una correcta vigilancia de sus establecimientos es mediante la instalación de sistemas de videovigilancia, que sólo permiten ver la vía pública en el espacio inmediatamente aledaño a las fachadas del establecimiento, con la finalidad de evitar actos delictivos.

4. Que por la propia naturaleza del lugar y finalidad de instalación del sistema de videovigilancia, se obtengan imágenes de las personas que pasan por el perímetro de dichos centro comercial no implica el uso de las mismas con ninguna finalidad, si no

ocurre ningún hecho delictivo contra los bienes o intereses de Hipercor.

5. Que los medios utilizados para la protección de los bienes de Hipercor son legítimos y proporcionales al fin perseguido.

6. Que la instalación de videovigilancia cumple los tres requisitos de proporcionalidad: cumple el juicio de idoneidad puesto que el objetivo se ha conseguido al evitar múltiples actos vandálicos; es necesaria en el sentido que no existen otras medidas más moderadas para la consecución del fin perseguido, y es equilibrada en el sentido de que produce más beneficios al interés general que perjuicios a un interés particular. A este tenor precisan *" Los inspectores de la Agencia comprueban que, aunque las cámaras DOMO disponen técnicamente de un ángulo de giro de 360°, el campo de visualización de las imágenes ha sido limitado a la fachada y zona adyacente según se muestra en las fotografías impresas adjuntas al acta. Es decir, mi representada, sin que nadie le diga nada al respecto, porque conoce la normativa vigente en esta materia, ha adoptado, de motu propio, la decisión de limitar el campo de visión y captura de imágenes a la zona estrictamente necesaria para la seguridad de sus establecimientos".*

7. Que la Agencia no precisa cual es el espacio mínimo imprescindible de captación de personas identificables en la vía pública.

8. Que en el procedimiento sancionador nº PS/353/2008, la Agencia reconoció la habilitación legal para el tratamiento de los datos resultantes de la instalación de videovigilancia, no siendo necesario el consentimiento del afectado.

Por todo lo anterior, solicitó que se acuerde el archivo del expediente incoado.

Por su parte, con fecha 7 de octubre de 2010, el denunciante presentó escrito por el que solicitaba actuar como interesado en el presente procedimiento.-

SEXTO: Con fecha 4 de noviembre de 2010, se inició el período de práctica de pruebas, en el que se dieron por reproducidos a efectos probatorios la denuncia interpuesta por Don ***A.A.A.*** y su documentación, los documentos obtenidos y generados por los Servicios de Inspección ante HIPERCOR, S.A.., y el Informe de actuaciones previas de Inspección que forman parte del expediente E/03632/2009.

También se dieron por reproducidas las alegaciones de Don ***A.A.A.*** en las que solicita actuar como interesado en el presente procedimiento

Asimismo, se dio por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00538/2010 presentadas por HIPERCOR, S.A.., y la documentación que a ellas acompaña.

SÉPTIMO: Con fecha 12 de enero de 2011, se formuló propuesta de resolución, proponiendo la imposición de una sanción de 60.101, 21€ a la entidad HIPERCOR, S.A.., por la comisión de una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 45.2 y 4 de dicha Ley.

OCTAVO: Con fecha 10 de febrero de 2011, HIPERCOR, S.A.. realizó alegaciones

frente a la citada propuesta de resolución en las que, básicamente, manifestó lo siguiente:

1. Que da por reproducidas las alegaciones que formuladas hasta la fecha en el procedimiento sancionador.

2. Que los datos recogidos por las cámaras del establecimiento no se incluyen en ningún fichero estructurado. Se graban unas a continuación de las otras, sin establecer un criterio de búsqueda fácil y sencillo que permita localizar e identificar a las personas. Las imágenes se guardan en el disco duro del sistema de videovigilancia, a medida que se van obteniendo, sin ningún criterio y si hay que localizar o buscar a alguien, por ejemplo a petición de las fuerzas y cuerpos de seguridad, el único criterio de búsqueda existente es el de lugar (hay que señalar un lugar del interior o exterior del establecimiento), el día y la hora. A continuación se busca esa fecha y hora en el servidor para, a partir de ese momento y en el tramo horario solicitado, visualizar las imágenes (de todas las cámaras) una a una para ver si lo que se ha solicitado se encuentra grabado ya que no hay ninguna estructura en el fichero que permita acotar la búsqueda en función de nombre, características de la persona o similar que localice la imagen de la persona buscada inmediatamente.

3. Que los datos de imágenes captadas en la vía pública en el perímetro del edificio de mí representada, no se consideran, por esta parte, excesivos porque sólo es la imagen de un transeúnte al que no se identifica de ninguna forma y todas las imágenes se retienen, como dice la Agencia, durante 7 días, no unas durante un plazo y oras durante otro distinto; todas se tratan por igual y, además, el plazo establecido por mí representada, 7 días, es claramente inferior al que la Instrucción que regula la materia permite, 30 días, lo que demuestra que no tiene ningún interés en guardar o tratar imágenes per se, sino que si alguna de las imágenes permite que la Policía identifique al autor de un hecho delictivo, se le entregan dichas imágenes y no se retienen por la entidad denunciada ni se realiza labor alguna encaminada a la identificación de las personas que aparecen en las mismas, esa labor es una función propia de las fuerzas y cuerpos de seguridad del Estado que son las que tienen la competencia para la identificación de las personas, por lo que mí representada, no sólo no tiene medios para identificar a nadie, sino que tampoco entra dentro de sus funciones realizar dicha identificación.

4. Sólo cuando concurre la existencia de un fichero de datos personales y posibilidad de tratamiento, es de aplicación la ley de protección de datos. De todo lo visto hasta la fecha, podemos llegar a la conclusión de que la entidad denunciada, cuando recoge las imágenes a través de su sistema de videovigilancia, no las introduce en un fichero estructurado que permita localizar las imágenes que se deseen de forma fácil y sencillo realizar posteriores tratamientos de las mismas, es decir, no nos encontramos ante un fichero en el sentido estricto de la Directiva Comunitaria ni de la ley española, por lo que faltando el elemento esencial del fichero, la actuación de mí representada no puede ser incardinada en el régimen de protección de la Ley 15/1999 de Protección de Datos y, en consecuencia, no debe ser sancionada.

5. Por otra parte, cabe destacar la incongruencia de la argumentación mantenida por la Agencia en este procedimiento respecto del consentimiento. Por una parte se acepta que no sería sancionable la captación de imágenes en la vía pública si dicha

captación se limitara única y exclusivamente al espacio inmediatamente aledaño al perímetro del establecimiento porque el sistema de videovigilancia está para eso; es decir, si los datos que se obtienen, en este caso imágenes, son adecuados, pertinentes y no excesivos y se retienen durante un plazo en consonancia con las características específicas de cada caso. Por otra parte, se pretende que la captación de las imágenes cuente con el consentimiento del afectado. Pero como se obtiene el consentimiento del afectado cuando el mismo va andando por la calle. ¿El empleado que está en el cuarto de control avisa a cada vigilante de cada una de las puertas, le pide que pare al ciudadano que aparece en el campo de visión de la cámara y que le firme un documento en el que dice que consiente que se capte su imagen?

6. La entidad denunciada cumple con el deber de informar mediante la instalación de los correspondientes carteles en las entradas a los establecimientos, lo cual es una forma indirecta el consentimiento de los peatones ya que todos ven el cartel y si no quisieran prestar su consentimiento, podrían manifestarlo en ese momento; sino que además, ha limitado a 7 días, no 30 como permite la norma, el plazo por el cual se conservan las imágenes, lo cual demuestra que no tiene ningún interés en tratar las imágenes, utilizarlas para ninguna finalidad oscura, sino que para el único y exclusivo caso de que se produjera un acto delictivo, utilizaría las imágenes que lo recogieran y solo esas imágenes, no el resto para entregárselas a la Policía que es la única que podría identificar a la/s persona/s que en las mismos figurase/n.

7. Lo que la denunciada pretende con la instalación de las cámaras de videovigilancia no es captar las imágenes de los que por allí pasen y si cometen un delito identificarlos] lo que se pretende es que si se comete un delito, comprobar si el autor sale en las imágenes y facilitárselas a la Policía para que identifique al autor.

8. La realidad es que Hipercor lo que hace es vigilar su establecimiento, vigilar una propiedad privada que en no pocas ocasiones ha sido atacada causando daños de distinta naturaleza y, si cuando se comete uno de esos hechos delictivos aparece la imagen del autor, se le entrega a la Policía que, reiteramos una vez más, se encarga de identificar, si puede, al autor.

9. Respecto de la proporcionalidad de la captura de imágenes para el fin perseguido, el argumento de la Agencia no es congruente. Por una parte dice que si se permite la grabación de un reducido espacio de la vía pública porque sin la misma "*resultaría en todo punto imposible el control de la segundad en el acceso a las instalaciones*". Es decir, si se capta una parte de la vía pública, justo delante de las puertas de acceso al centro comercial, no hay ningún problema y dicha actuación no es sancionable porque se trata de una medida de seguridad; ahora bien, si se capta una espacio de la vía pública, en el perímetro del centro comercial, eso no es una cuestión de seguridad y es sancionable. Parece desconocer la Agencia que la seguridad del centro comercial no se reduce a las entradas y salidas del mismo, sino que incluye el edificio en su totalidad. Si se puede captar imágenes, por seguridad, en la vía pública como son los accesos al centro comercial, por el mismo motivo, seguridad, se podrá captar imágenes en la vía pública que no sea acceso al centro comercial y, en ambos, casos, reduciendo el espacio público al mínimo imprescindible que es lo que intenta, siempre, la entidad denunciada.

Por todo ello solicitó el archivo del expediente.

HECHOS PROBADOS

PRIMERO: Con fecha de 3 de noviembre de 2009, tuvo entrada en esta Agencia un escrito de Don ***A.A.A.*** en el que denuncia el presunto incumplimiento de la Instrucción 1/2006, del establecimiento Hipercor Bahía, ubicado en la Carretera de Cártama, Km. 2 de Málaga (folios 1-36)

SEGUNDO: La sociedad propietaria del centro comercial HIPERCOR BAHÍA DE MÁLAGA es HIPERCOR, S.A.., la cual también es responsable del sistema del videovigilancia instalado (folio 45).

TERCERO: Consta copia del contrato suscrito con la empresa PLETTAC INSTALACIONES DE SEGURIDAD, S.L., con fecha 4 de marzo de 2003, con objeto de la instalación de sistemas electrónicos de seguridad que sean necesarios en los establecimientos de EL CORTE INGLES e HIPERCOR. Consta que la citada empresa de seguridad dispone de autorización administrativa para el ejercicio de la actividad de seguridad privada de la citada sociedad. (Folios 71-74).

CUARTO: Los representantes de la entidad han manifestado que el sistema de videovigilancia instalado en el Centro Comercial tiene como finalidad exclusiva la seguridad del personal, los clientes y de las instalaciones (folio 45)

QUINTO: Consta que el sistema de videovigilancia lo constituye un total de 109 cámaras distribuidas por los departamentos del centro comercial y 9 de ellas se encuentran ubicadas en la parte exterior del inmueble de forma que permitan la visualización del perímetro exterior del mismo. Éstas últimas son de tipo DOMO con movilidad que permite la visualización de 360º. Las imágenes son visualizadas en un centro de control que se ubica en el mismo Centro Comercial y tienen acceso a las mismas, además del responsable de seguridad y directivos del Centro Comercial, los vigilantes de la empresa de seguridad que HIPERCOR, S.A.. tiene contratada (folios 45-46).

SEXTO: Las imágenes son conservadas por un periodo máximo de 7 días, disponiendo para ello de 11 grabadores digitales. Así mismo, HIPERCOR, S.A.. ha creado un fichero denominado VIDEOVIGILANCIA, inscrito en el Registro General de Protección de Datos con el código ###COD1 (folio 46).

SÉPTIMO: Con respecto a la instalación de cámaras en el exterior del edificio, las empresas del grupo EL CORTE INGLÉS enviaron una comunicación dirigida por el Director de Seguridad de la compañía a la Secretaría de Estado de Interior con fecha 12 de mayo de 2009, por la que se solicita concesión de la correspondiente autorización administrativa para la grabación de imágenes en la vía pública, en todos y cada uno de los centros comerciales que la compañía tiene en el territorio español, con la finalidad de prevenir la comisión de delitos y, si éstos se produjeran, poder utilizar dichas imágenes para la identificación del autor o autores de los mismos, así como ayudar en la organización de los planes de evacuación y desalojo de los edificios. A este respecto se recibió respuesta de la Secretaria de Estado, en el que se comunican que no tienen capacidad legal para autorizar a empresas la instalación de cámaras de video que recojan imágenes de la vía pública (folios 46 y 75-84).

OCTAVO: En cada uno de los accesos al edificio hay un cartel informativo de zona videovigilada, en el que se identifica al responsable del fichero ante quién pueden ejercitarse los derechos recogidos en el artículo 5 de la L.O. 15/1999 (folios 46 y 49)

NOVENO: En el exterior del Centro Comercial existen un total de nueve cámaras de tipo DOMO y en las fachadas exteriores del edificio se encuentran pegados carteles informativos de la existencia de un sistema de videovigilancia (folios 46 y 50).

DÉCIMO: Las cámaras números 42-49 y 108 ubicadas en la parte exterior del edificio, disponen de funcionalidad de ZOOM y un ángulo de giro de 360º y recogen imágenes de parte de la vía pública apreciándose en las mismas personas identificables que transitan (folios 46-47 y 51-64)

UNDÉCIMO: El Centro Comercial dispone de un Servicio de Seguridad Privado que presta la empresa SECURITAS SEGURIDAD ESPAÑA, S.A. cuyo personal utiliza el sistema de videovigilancia en las labores de seguridad. El contrato de prestación de dicho servicio ha sido contratado por EL CORTE INGLES, S.A., con fecha 15/1/2005 cuya copia ha aportado el representante de la entidad a la inspección de datos. En dicho contrato consta que el pago del servicio lo realiza un 59% EL CORTE INGLES, S.A. y un 41% HIPERCOR, S.A.. aunque el contrato sólo lo suscribe el primero (folios 93-99 y 102).

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

La vigente LOPD atribuye la condición de responsables de las infracciones a los responsables de los ficheros (art. 43), concepto que debe integrarse con la definición que de los mismos recoge el artículo 3.d). Este precepto, 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. Conforme al artículo 3.d) de la LOPD, el responsable del fichero o del tratamiento es *"la persona física o jurídica (…) que decida sobre la finalidad, contenido y uso del tratamiento".*

En el presente caso, HIPERCOR, S.A.., es responsable del fichero de conformidad con las definiciones legales, por tanto está sujeto al régimen de responsabilidad recogido en el Título VII de la LOPD.

III

Con carácter previo al análisis del artículo 6.1 de LOPD, cuya vulneración se imputa a la entidad HIPERCOR, S.A.., procede entrar a situar el contexto normativo en el que se ubica la materia de videovigilancia.

Así, el artículo 1 de la LOPD dispone: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

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";* definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *"Cualquier información concerniente a personas físicas identificadas o identificables".*

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones*, *consultas, interconexiones y transferencias*". 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 artículo 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define datos de carácter personal como: *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables".*

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

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.
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.

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.

Por otra parte, para determinar si el supuesto que se analiza implican 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 cuanto a las obligaciones y precauciones que deberán respetarse por los responsables del tratamiento de los datos se mencionan, 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.

Por tanto, 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.

De acuerdo con los preceptos transcritos, la videocámara 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.

En el caso que nos ocupa, del Acta levantada por Inspectores de esta Agencia en fecha 6 de septiembre de 2010, se constató que las cámaras ubicadas en la fachada del edificio propiedad de la entidad denunciada grababan imágenes de espacios públicos, pudiendo identificarse a las personas que por ella transitaban, por cuanto ésta es su finalidad, la de prevenir la comisión de delitos, y si éstos se produjeran, poder utilizar dichas imágenes para la identificación del autor de los mismos, ya que de otro modo escaparía de toda lógica llegando a un absurdo la finalidad de vigilancia, que con el sistema de videocámaras se pretende.

A este respecto, cabe decir que el artículo 5.1.o. del Real Decreto 1720/2007 define 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 desproporcionados*". En este mismo sentido se pronuncia el ya citado artículo 2.a) de la Directiva 95/46/CE, al establecer como 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 aquella.

Así, de acuerdo a la normativa expuesta, las imágenes captadas y grabadas por las cámaras de videovigilancia de la entidad denunciada tienen carácter automatizado, almacenando imágenes que proporcionan información física, fisiológica, económica,… de las personas captadas durante el período establecido, permitiendo búsquedas de

imágenes en base a criterios de estructura u organización previa, como sería el lugar, día y hora. Así dicha información facilitada por las cámaras permitirían hacer identificables a las personas que aparecen en las mismas, dado que las imágenes que aparecen reproducidas en el expediente administrativo tanto por la aproximación del foco como por el grado de nitidez, sí permiten identificar al menos a algunas de las personas que en las mismas aparecen, sin requerir plazos o actividades desproporcionadas, bien por el responsable del tratamiento o por cualquier otra persona para identificar a aquéllas, como serían los Cuerpos y Fuerzas de Seguridad del Estado. Asimismo hay que tener en cuenta, que las imágenes aportadas al expediente, son las imágenes visionadas y grabadas que aparecían en los monitores de visualización.

IV

Se imputa a la entidad HIPERCOR, S.L., una infracción del artículo 6 de la LOPD, que dispone lo siguiente:

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

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*.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

En el caso que nos ocupa, consta acreditado que en el establecimiento Hipercor Bahía, ubicado en la Carretera de Cártama, Km. 2 de Málaga, tiene instalado un sistema de videovigilancia compuesto por 109 cámaras distribuidas por los departamentos del centro comercial y 9 de ellas se encuentran ubicadas en la parte exterior del inmueble de forma que permitan la visualización del perímetro exterior del mismo. Éstas últimas son de tipo DOMO con movilidad que permite la visualización de 360º. Las imágenes son visualizadas en monitores que se encuentran en el Centro de Control que se ubica en el mismo Centro Comercial y tienen acceso a las mismas, además del responsable de seguridad y directivos del Centro Comercial, los vigilantes de la empresa de seguridad que HIPERCOR, S.A.. tiene contratada. Las imágenes captadas por las

videocámaras se almacenan organizadamente en distintos discos duros, por un plazo no superior a siete días. Según el Acta de Inspección realizada en los establecimientos denunciados, algunas de las cámaras exteriores, ubicadas en ambos establecimientos, grababan imágenes de espacios públicos, pudiendo identificarse a las personas que por ella transitaban, por cuanto ésta es su finalidad, la de prevenir la comisión de delitos, y si éstos se produjeran, poder utilizar dichas imágenes para la identificación del autor de los mismos, ya que de otro modo escaparía de toda lógica llegando a un absurdo la finalidad de vigilancia, que con el sistema de videocámaras se pretende. 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 que captan las mencionadas videocámaras y después se graba 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. Dicha entidad, como se desarrollará más adelante, carecía de legitimación para el tratamiento de las imágenes captadas de la vía pública, realizando un tratamiento de datos personales no proporcional al fin perseguido.

En el presente caso consta la existencia de un contrato de arrendamiento de los servicios de seguridad entre Hipercor y la empresa de seguridad autorizada Plettac Instalaciones de Seguridad S.L., fechado el 4 de marzo de 2003. Sin embargo, aún cuando dicho sistema de videovigilancia esté habilitado por la LSP, esto no le autoriza a captar y grabar imágenes en la vía pública, espacio en el que únicamente están legitimadas para la captación de imágenes las Fuerzas y Cuerpos de Seguridad del Estado, a tenor de lo dispuesto en 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 pues, debe rechazarse lo alegado por Hipercor en el sentido de que, el tratamiento de datos que supone la captación por videocámaras de la imagen de las personas que transiten por las vías públicas, en su campo de visión, está excepcionado del consentimiento de las mismas por la normativa de seguridad privada citada anteriormente, ya que dicha legitimación únicamente alcanza a las imágenes captadas en recintos privados, y no en espacios públicos, como es el presente caso.

En el presente supuesto ha quedado acreditado que Hipercor capta imágenes de las personas que transitan por las vías públicas circundantes al edificio, sin contar con su consentimiento ni con habilitación legal para efectuar tal tratamiento de datos personales, habida cuenta que la grabación de imágenes en lugares públicos, como es el caso que nos ocupa, únicamente puede efectuarse por las Fuerzas y Cuerpos de Seguridad del Estado al amparo de lo dispuesto en la *Ley Orgánica 4/1997* (y su Reglamento de desarrollo y ejecución aprobado por el *Real Decreto 596/1996*). Esta captación de imágenes en la vía pública excede el principio de proporcionalidad exigido por la normativa de protección de datos habida cuenta de que se captan imágenes de personas y vehículos en todas las vías públicas circundantes al citado edificio sin que se circunscriba la captación de imágenes al espacio de la vía pública imprescindible (como serían las inmediaciones de los accesos al edificio) que aseguraría la finalidad de vigilancia del edificio que se persigue.

Por lo tanto, las imágenes captadas por las cámaras son datos de carácter personal conforme al artículo 3.a) de la LOPD y al artículo 5.1. f) del citado Real Decreto

1720/2007, toda vez que las cámaras captan imágenes de las personas que circulan por la vía pública. Asimismo, tales imágenes constituyen, en sí mismas consideradas, un tratamiento de datos en los términos de la LOPD.

Dicho tratamiento, por tanto, ha de contar con el consentimiento del afectado, circunstancia que no se ha acreditado por lo que cabe estimar cometida la infracción por la que se ha instruido el presente procedimiento, y por tanto sancionable, de conformidad con lo que dispone el artículo 44.3. d) de dicha norma, que establece como tal: *"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas 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".*

El tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo), "...*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"*.

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.

En el presente expediente, cabe apreciar que la entidad denunciada grabó imágenes de personas, de conformidad con lo anteriormente expuesto. Dichas imágenes, capturadas en un soporte magnético incorporarían datos personales de los viandantes que se introdujeran dentro de su campo de visión y, por lo tanto, los datos personales captados deberían estar sometidos al consentimiento de sus titulares, conformidad con lo dispuesto en el artículo 6.1 de la LOPD.

V

Procede, por tanto, entrar en el análisis de cada una de las alegaciones formuladas por la entidad denunciada tanto al Acuerdo de Inicio como a la Propuesta de Resolución.

1. Respecto a las alegaciones de Hipercor relativas a que el único medio de llevar a cabo una correcta vigilancia de sus establecimientos es mediante la instalación de sistemas de videovigilancia, que sólo permiten ver la vía pública en el espacio inmediatamente aledaño a las fachadas del establecimiento, con la finalidad de evitar actos delictivos y que por la propia naturaleza del lugar y finalidad de la instalación del sistema de videovigilancia, se obtengan imágenes de las personas que pasan por el perímetro de dichos centro comercial no implica el uso de las mismas con ninguna finalidad, si no ocurre ningún hecho delictivo contra los bienes o intereses de

Hipercor.

Por lo tanto, el presente expediente sancionador se apertura por el tratamiento de datos de carácter personal originado en la captación, transmisión, visualización y grabación de las imágenes recogidas por las cámaras de videovigilancia exteriores que enfocaban espacios públicos de las calles adyacentes al edificio de HIPERCOR, las cuales incorporaban información de las personas que transitaban por las vías públicas circundantes al edificio, sin contar con su consentimiento ni con habilitación legal para efectuar tal tratamiento de datos personales, habida cuenta que la grabación de imágenes en lugares públicos, como es el caso que nos ocupa, como será desarrollado seguidamente, únicamente puede efectuarse por las Fuerzas y Cuerpos de Seguridad del Estado al amparo de lo dispuesto en la *Ley Orgánica 4/1997* (y su Reglamento de desarrollo y ejecución aprobado por el *Real Decreto 596/1996*).

HIPERCOR justifica, tanto en las alegaciones al Acuerdo de Inicio como a la Propuesta de Resolución, la grabación de imágenes exteriores por razones de seguridad y vigilancia de sus instalaciones, frente a cualquier actuación violenta por parte de terceros, así como la prevención de actos terroristas. En relación con dicho alegato, debe tenerse en cuenta que los motivos de seguridad alegados por HIPERCOR para justificar el tratamiento de imágenes procedentes de la vía pública, que contenían datos personales, se encuadran dentro de las funciones de seguridad pública que la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, atribuye como competencia exclusiva del Estado. Así el artículo 1 de dicha Ley Orgánica establece que:

"1. La seguridad pública es competencia exclusiva del Estado. Su mantenimiento corresponde al Gobierno de la Nación.
2. Las Comunidades Autónomas participarán en el mantenimiento de la seguridad pública en los términos que establezcan los respectivos Estatutos y en el marco de esta Ley.
3. Las Corporaciones Locales participarán en el mantenimiento de la seguridad pública en los términos establecidos en la Ley reguladora de las Bases de Régimen Local y en el marco de esta Ley.
4. El mantenimiento de la seguridad pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad."

Por su parte el artículo 2 de la reseñada Ley Orgánica 2/1986, de 13 de marzo, dispone que "*Son Fuerzas y Cuerpos de Seguridad:*

a) Las Fuerzas y Cuerpos de Seguridad del Estado dependientes del Gobierno de la Nación.
b) Los Cuerpos de Policía dependientes de las Comunidades Autónomas.
c) Los Cuerpos de Policía dependientes de las Corporaciones Locales."

Así para entender las especialidades derivadas del tratamiento de las imágenes en vía pública es preciso conocer la regulación que sobre esta materia se contempla 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, cuyo artículo 1 establece respecto de su objeto que: *"La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares*

públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública".

Este precepto es preciso ponerlo, a su vez, en relación con lo dispuesto en el artículo 3.e) de la referida Ley Orgánica 15/1999, donde se prevé que: *"Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:*

e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia".

El artículo 3.1 y 2 de la citada Ley Orgánica 4/1997, establece:

"1. La instalación de videocámaras o de cualquier medio técnico análogo en los términos del artículo 1.2 de la presente Ley está sujeta al régimen de autorización, que se otorgará, en su caso, previo informe de un órgano colegiado presidido por un Magistrado y en cuya composición no serán mayoría los miembros dependientes de la Administración autorizante.
Las instalaciones fijas de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y de las Corporaciones Locales serán autorizadas por el Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión cuya presidencia corresponderá la Presidente del Tribunal Superior de Justicia de la misma Comunidad. La composición y funcionamiento de la Comisión, así como la participación de los municipios en ellas, se determinarán reglamentariamente."

Para la autorización de la instalación de estas cámaras fijas la citada Ley establece en su artículo 4*: "Para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes".*

El principio de proporcionalidad que se exige para la autorización previa ya citada, es también una exigencia en su utilización, teniendo en cuenta dos aspectos esenciales de la misma, como son la idoneidad e intervención mínima.

La idoneidad supone que sólo podrá emplearse cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en la citada Ley.

La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación al derecho al honor, a la propia imagen y a la intimidad.

En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, señalándose en su artículo 2.2, en lo que hace mención a su ámbito

de aplicación que *"2.2. Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizados de los Datos de Carácter Personal."*

Respecto también de la legislación relativa a la seguridad ciudadana hay que valorar que la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de La Seguridad Ciudadana, establece en su artículo 13 como medidas de seguridad en establecimientos e instalaciones lo siguiente:

"1. El Ministerio del Interior podrá ordenar, conforme a lo que se disponga reglamentariamente, la adopción de las medidas de seguridad necesarias en establecimientos e instalaciones industriales, comerciales y de servicios, para prevenir la comisión de los actos delictivos que se puedan cometer contra ellos, cuando generen riesgos directos para terceros o sean especialmente vulnerables.

2. No obstante, las autoridades competentes podrán eximir de la implantación o el mantenimiento de medidas de seguridad obligatorias a los establecimientos, cuando las circunstancias que concurran en el caso concreto las hicieren innecesarias o improcedentes.

3. La apertura de los establecimientos que estén obligados a la adopción de medidas de seguridad, estará condicionada a la comprobación, por las autoridades competentes, de la idoneidad y suficiencia de las mismas.

4. Los titulares de los establecimientos e instalaciones serán responsables de la adopción o instalación de las medidas de seguridad obligatorias, de acuerdo con las normas que respectivamente las regulen, así como de su efectivo funcionamiento y de la consecución de la finalidad protectora y preventiva propia de cada medida, sin perjuicio de la responsabilidad en que al respecto puedan incurrir sus empleados."

Por su parte, el Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada, en cuanto a medidas de seguridad en general, establece en sus artículos 111.1, y 112.1.c) lo siguiente:

"111.1. De acuerdo con lo dispuesto en el artículo 13 y en la disposición adicional de la Ley Orgánica 1/1992, sobre protección de la seguridad ciudadana, y con la finalidad de prevenir la comisión de actos delictivos, la Secretaría de Estado de Interior, para supuestos supraprovinciales, o los Gobernadores Civiles podrán ordenar que las empresas industriales, comerciales o de servicios adopten las medidas de seguridad que, con carácter general o para supuestos específicos, se establecen en el presente Reglamento".
"112.1. Cuando la naturaleza o importancia de la actividad económica que desarrollan las empresas y entidades privadas, la localización de sus instalaciones, la concentración de sus clientes, el volumen de los fondos o valores que manejen, el valor de los bienes muebles u objetos valiosos que posean, o cualquier otra causa lo hicieran necesario, el Secretario de Estado de Interior para supuestos supraprovinciales, o los Gobernadores Civiles, podrán exigir a la empresa o entidad que adopte, conjunta o separadamente, los servicios o sistemas de seguridad siguientes:
"c) Instalación de dispositivos y sistemas de seguridad y protección."

Por lo tanto, el Ministerio del Interior puede exigir medidas preventivas en los establecimientos e instalaciones industriales, comerciales y de servicios para prevenir la comisión de delitos que generen riesgos para terceros o sean especialmente vulnerables.

A este respecto, las empresas del grupo El Corte Inglés solicitaron a la Secretaría de Estado, en fecha 12 de mayo de 2009, autorización administrativa para la grabación de imágenes en la vía pública, en todos y cada uno de los centros comerciales que la misma tiene en territorio español, siendo contestada dicha solicitud por el citado órgano, en fecha 24 de agosto de 2009, manifestando que no tienen capacidad legal para autorizar a empresas la instalación de cámaras de vídeo que recojan imágenes de la vía pública, en concreto: *"En contestación a los escritos dirigidos a esta Secretaría de Estado, solicitando autorización para la grabación de imágenes en la vía pública en distintos centros a los que representa, a la vista del informe cuya fotocopia se acompaña, le comunico lo siguiente:*

La normativa vigente en esta materia está contenida fundamentalmente en la Ley 23/1992, de 30 de julio, de seguridad privada(LSP) y el Reglamento que la desarrolla, aprobado por Real Decreto 2364/1994, de 9 de diciembre, en Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de video cámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, en Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento aprobado por Real Decreto 1720/2007, de 21 de diciembre y 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 cámaras o videocámaras . Hasta la fecha no se han cumplimentado las previsiones de la Disposición Adicional Novena de la citada Ley Orgánica 4/1997, sobre elaboración de la normativa correspondiente para adaptar los principios inspiradores de dicha Ley al ámbito de la seguridad Privada.

De acuerdo con dicha normativa esta Secretaría de Estado carece de competencia para autorizar lasa grabaciones objeto de las solicitudes.

Se significa igualmente que no existe amparo jurídico sobre las instalación y uso de sistemas de video vigilancia en los términos expresados en las solicitudes: "grabación de imágenes en la vía pública, en todos y cada uno de los centros comerciales que dichas empresas tienen en territorio español"·

"…La citada Ley Orgánica 4/1997, en su disposición adicional novena, señala que el Gobierno elaborará en el plazo de un año a partir de su publicación, la normativa correspondiente, para adaptar sus principios inspiradores al ámbito de la seguridad privada. Aunque no se ha llevado a cabo el citado desarrollo normativo, el legislador a través de esta disposición adicional novena, contempla la posibilidad de la instalación de este tipo de medios en el ámbito privado. Por lo tanto, en el momento actual y hasta que no se cumpla dicho mandato legal, dicha utilización estará sujeta a las diferentes normas que inciden en esta materia, como son, la Ley 23/1992, de 30 de julio, de seguridad privada (LSP) y normas que la desarrollan, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y 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 cámaras o videocámaras.

A este respecto, se considera importante destacar lo recogido en el punto 2 del artículo 2 de la citada Ley Orgánica 4/1997, donde se hace referencia a que, sin perjuicio de las disposiciones específicas contenidas en la misma, el tratamiento automatizado de las imágenes y sonidos obtenidos por medio de sistemas de video vigilancia en espacios públicos, deberán regirse por lo dispuesto en la Ley Orgánica de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal, que fue derogada por la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

Continua el citado informe en sus conclusiones*: "En el ordenamiento jurídico vigente, la video vigilancia en lugares públicos, se regula mediante la Ley Orgánica 4/1997, de 4 de agosto, siendo su ámbito de aplicación el relativo a la utilización de video cámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Este régimen no resulta aplicable a las videocámaras objeto de las solicitudes formuladas por el grupo empresarial "El Corte Inglés", en cuanto se trata de videocámaras para la vigilancia en el ámbito privado, cuyo régimen legal a falta del desarrollo previsto en la Disposición Adicional novena, deberán atenerse a lo dispuesto en la Ley 23/1992, de 30 de julio, de seguridad privada (LSP) y normas que la desarrollan, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Instrucción 1/2006, de 8 de noviembre, de la Agencia de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras".*

Por lo tanto, la legitimación para el uso de instalaciones de videovigilancia se ciñe a la protección de entornos privados. La prevención del delito y la garantía de la seguridad en las vías públicas corresponden en exclusiva a las Fuerzas y Cuerpos de Seguridad del Estado. Por tanto la regla general es la prohibición de captar imágenes de la calle desde instalaciones privadas, al ser competencia de los Cuerpos y Fuerzas de Seguridad del Estado.

Procede, por lo tanto, desestimar las alegaciones formuladas por Hipercor a este respecto.

2. En segundo lugar, respecto a la alegación de la mercantil denunciada relativa a que la instalación de las cámaras de Hipercor, sólo permiten ver la vía pública en el espacio inmediatamente aledaño a la fachada del establecimiento, cumpliendo la instalación el principio de proporcionalidad, y que no resulta congruente que la captación de un porcentaje reducido de la vía pública no sea sancionable al estar instaladas las cámaras en la entrada del edificio, pero si sea sancionable si se captan imágenes del perímetro del edificio, hay que señalar que el artículo 4.1 y 2 de la LOPD, garantiza el cumplimiento del principio de proporcionalidad en todo tratamiento de datos personales, cuando señala que:

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

3. 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".

La legislación específica sobre videovigilancia procede, fundamentalmente de lo previsto en la Instrucción 1/2006 que ya en su exposición de motivos habla de la necesidad de que el uso y empleo de estos mecanismos de grabación sea proporcionado a la finalidad que se persigue dejando al margen dos clases de grabaciones: por un lado las de contenido estrictamente doméstico y las que tienen relación con las grabaciones realizadas por las Fuerzas y Cuerpos de seguridad del Estado.

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".

Precisamente la redacción del artículo no viene sino a recoger el principio de proporcionalidad del artículo 4 de la LOPD. Quiere ello decir que la grabación de imágenes en un lugar público, como es el caso que nos ocupa, no está permitida en ningún supuesto. Ahora bien, si las cámaras están instaladas en la entrada de un edificio u orientadas a las fachadas del edificio, por el campo de visión de éstas podría captar un porcentaje reducido de la vía pública, no siendo necesario en éste caso obtener el consentimiento de los transeúntes.
Por lo tanto, esta Instrucción no se refiere a la vigilancia de espacios públicos y sólo la permite cuando sea imprescindible para la vigilancia previamente autorizada, como es la impuesta para los bancos y entidades de crédito.

En este sentido, la posibilidad de captar un pequeño ángulo de la vía pública a través de una cámara instalada por una empresa de seguridad privada, ésta deberá de cumplir el principio de proporcionalidad, sin que sea posible extender la grabación de imágenes a un alcance mayor al que resulte necesario para garantizar la seguridad de las instalaciones. Por ello, la referencia a los alrededores de las instalaciones, únicamente resultaría ajustada a la normativa de protección de datos en caso de que la misma se refiera exclusivamente a aquellos espacios públicos sin cuya grabación resultaría en todo punto imposible el control de la seguridad en el acceso a las instalaciones, sin que en modo alguno esta referencia pueda entenderse efectuada, con carácter general a la vía pública.

En el acta de Inspección levantada con fecha 6 de septiembre de 2010, consta acreditado que se recogen imágenes captadas por las cámaras exteriores de la fachada de Hipercor, donde se aprecian los vehículos y las personas que circulan por las vías públicas de las calles que demarcan el edificio. Esta visualización de vehículos y transeúntes no encuentra justificación alguna en la normativa específica y obliga a entender que se trata de un uso excesivo que infringe el principio de proporcionalidad de los datos previsto en el articulo 4.1 de la Ley Orgánica de Protección de Datos cuando se habla de que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

De lo expuesto resulta que la instalación de las cámaras en el edificio de Hipercor, si bien se encuentra amparada por lo que señala la normativa de seguridad privada, se ha realizado de modo excesivo infringiendo los limites que señala la Instrucción 1/2006 a la que nos hemos también referido y ello puesto que permite la captación de imágenes de los transeúntes de las calle, sin que la misma sea obligada para conseguir la finalidad de vigilancia pretendida.

Por lo tanto, no se puede estimar la alegación de la entidad denunciada referente a que las cámaras instaladas en el inmueble propiedad de Hipercor, *"sólo permiten ver la vía pública en el espacio inmediatamente aledaño a la fachada del establecimiento",* porque no resulta imprescindible para la función de vigilancia del establecimiento la grabación de imágenes de la vía pública. Lo adecuado y no excesivo hubiera sido que dichas cámaras sólo tomaran imágenes de las entradas a dicho edificio y fachadas y en su caso un espacio mínimo de la vía pública. Sin embargo, a través de las fotografías aportadas en las labores de inspección de esta Agencia, donde se muestran algunas de las imágenes visualizadas a través de los monitores, se puede constatar que dichas cámaras ubicadas en el exterior del inmueble grababan imágenes de la vía pública, de la acera anexa al inmueble, incluyendo las zona de tránsito de los viandantes y todo ello con una perfecta claridad de imágenes. Así, la ocho cámaras exteriores son tipo "domo", cuyo ángulo de visión puede desplazarse 360 grados y disponen todas ellas de *"zoom*". Por lo tanto la entidad denunciada realizaba un tratamiento de datos no proporcional al fin perseguido.
A este respecto, señalar que aun cuando en todas la cámaras se había instalado un dispositivo que ciega parte de los 360º de visión, lo cierto es, a juzgar por las imágenes obtenidas por las mismas, que dicha pantalla de privacidad debería haberse ampliado para evitar las captaciones de imágenes de la vía pública, que no son idóneas ni necesarias para la finalidad perseguida.

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, ha quedado acreditado que el sistema de videovigilancia instalado en Hipercor, permite seleccionar cualquiera de las cámaras y desplazar su enfoque 360º, alcanzando su ángulo de visión la vía pública y a las personas que circulan por la misma, realizando por tanto 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 demandada podría igualmente obtenerse por medios menos intrusivos para la intimidad de las personas afectadas, como sería la instalación de pantallas de privacidad que impidiesen la captación de imágenes en la vía pública más allá de lo necesario y proporcional. Por lo tanto procede desestimar la alegación de la entidad demandada a este respecto.

3. Respecto a las alegaciones de Hipercor relativas a que el sistema de videovigilancia del establecimiento denunciado ha sido instalado por una empresa de seguridad autorizada, por lo que el tratamiento de los datos se encuentra habilitado por la Ley de Seguridad Privada, no siendo necesario el consentimiento del afectado.

A este respecto hay que señalar que la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), define en sus apartados a) y c) del artículo 3: *"a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables"* y *"c) Tratamiento de datos: 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.".*

Por tanto, entendido el tratamiento de imágenes como tratamiento de datos personales y por tanto sujeto a las prescripciones de la LOPD, para poder realizar dicho tratamiento, se debe contar con la legitimación establecida en el artículo 6 de la LOPD, que en su apartado 1 establece, en cuanto al *"Consentimiento del interesado", "1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".*

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"*.

Es por tanto necesario encontrar una ley que legitime el tratamiento, de lo contrario

resultaría prácticamente imposible obtener el consentimiento de cada una de las personas que resulten captados o grabados por las cámaras.

El mencionado artículo debe de conectarse con lo dispuesto en la Ley 23/1992, de 30 de julio, de Seguridad Privada (en adelante LSP), que establece en su artículo 1.1:

"Esta Ley tiene por objeto la prestación por personas, físicas o jurídicas privadas, de servicios de vigilancia y seguridad de personas o de bienes, que tendrán la consideración de actividades complementarias y subordinadas respecto a las de seguridad pública".

Asimismo, añade el artículo 1.2 que: *" A los efectos de esta Ley, únicamente pueden realizar actividades de seguridad privada y prestar servicios de esta naturaleza las empresas de seguridad y el personal de seguridad privada, que estará integrado por los vigilantes de seguridad, los vigilantes de explosivos, los jefes de seguridad, los directores de seguridad, los escoltas privados, los guardas particulares del campo, los guardas de caza, los guardapescas marítimos y los detectives privados".*

El artículo 5.1 e) de la LSP dispone que: *"Con sujeción a lo dispuesto en la presente Ley y en las normas reglamentarias que la desarrollan, las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades (…) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad*". Esta previsión se reitera en el artículo 1 del Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre.

De este modo, la Ley habilitaría que los sujetos previstos en su ámbito de aplicación puedan instalar dispositivos de seguridad, entre los que podrían encontrarse las cámaras, siempre con la finalidad descrita en el citado artículo 1.1.
Para la efectiva puesta en funcionamiento de la medida, el artículo 6.1 de la LSP dispone que: *"Los contratos de prestación de los distintos servicios de seguridad deberán en todo caso consignarse por escrito, con arreglo a modelo oficial, y comunicarse al Ministerio del Interior, con una antelación mínima de tres días a la iniciación de tales servicios".*
El artículo 20 del RSP regula el procedimiento de notificación del contrato, la autoridad competente y el régimen aplicable a la contratación del servicio por las Administraciones Públicas y a supuestos excepcionales que exijan la inmediata puesta en funcionamiento del servicio.

Por último, el artículo 7 de la LSP, establece que para la prestación privada de servicios o actividades de seguridad, las empresas de seguridad habrán de obtener la oportuna autorización administrativa mediante su inscripción en un Registro que se lleva en el Ministerio del Interior.

En consecuencia, siempre que se haya dado cumplimiento a los requisitos formales establecidos en los artículos precedentes (inscripción en el Registro de Empresas de Seguridad de y comunicación del contrato al Ministerio del Interior), las empresas de seguridad autorizadas podrán instalar dispositivos de seguridad en ámbitos y recintos privados, entre los que se encontrarían los que tratasen imágenes con fines de videovigilancia, existiendo así, en principio, y en lo que se refiere a la normativa de protección de datos una habilitación legal que permitiría al responsable del tratamiento

y/o del fichero tratar los datos de carácter personal (imágenes) captados en espacios privados por las cámaras de videovigilancia y almacenados en ficheros una vez grabados, cuando esta última circunstancia se produzca, sin precisar del consentimiento inequívoco de los afectos cuya imagen resulta captada y, en su caso grabada, por los sistemas de seguridad privada instalados por tales empresas.

En este caso, como bien señala la entidad denunciada, consta la existencia de un contrato de arrendamiento del servicio de seguridad respecto a las videocámaras, entre Hipercor, S.A. y Plettac Instalaciones de Seguridad S.L., fechado el 4 de marzo de 2003. Dicha empresa figura como empresa autorizada e inscrita en el Registro de Empresas de Seguridad con el número 1319, de fecha 7 de julio de 1988. Por lo tanto, el sistema de videovigilancia de la sociedad denunciada ha sido instalado por una empresa de seguridad autorizada, por lo que el tratamiento de los datos de las personas que acceden al establecimiento comercial se encuentra habilitado por la LSP. Sin embargo esta legitimación no puede hacerse extensible a la captación y grabación de imágenes de las personas que circulan por la vía pública.

Por lo tanto aun cuando dicho sistema de videovigilancia haya sido instalado conforme a la normativa de seguridad, este hecho no le autoriza, a realizar grabaciones de imágenes en la vía pública, como es el caso que nos ocupa, mucho más allá de lo que resulta idóneo, adecuado y proporcional.

Por otro lado queda acreditado que la Secretaría de Estado de Seguridad, ha manifestado que el régimen de la citada norma es de aplicación únicamente al uso de las videocámaras por los Cuerpos y Fuerzas de Seguridad en lugares públicos, hay que señalar que para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 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 que establece: *"La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública".*

Este precepto es preciso ponerlo en relación con lo dispuesto en el artículo 3 e) de la Ley Orgánica 15/1999, donde se prevé que: *"Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:*

e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia".

El artículo 3.1 y 2 de la citada Ley Orgánica 4/1997, establece:
"1. La instalación de videocámaras o de cualquier medio técnico análogo en los términos del artículo 1.2 de la presente Ley está sujeta al régimen de autorización, que se otorgará, en su caso, previo informe de un órgano colegiado presidido por un Magistrado y en cuya composición no serán mayoría los miembros dependientes de la

Administración autorizante.
2. Las instalaciones fijas de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y de las Corporaciones Locales serán autorizadas por el Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión cuya presidencia corresponderá la Presidente del Tribunal Superior de Justicia de la misma Comunidad. La composición y funcionamiento de la Comisión, así como la participación de los municipios en ellas, se determinarán reglamentariamente."

En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, y además en el mismo texto legal se regulan los criterios para instalar las cámaras y los derechos de los interesados.
En el presente caso, se trata de imágenes captadas en la vía pública, espacio en el que únicamente están legitimadas para la captación de imágenes las Fuerzas y Cuerpos de Seguridad del Estado, a tenor de los dispuesto en la Ley Orgánica 4/1997.

Así pues, debe rechazarse lo alegado por Hipercor, en el sentido de que el tratamiento de datos que supone la captación por videocámaras de la imagen de las personas que transiten por las vías públicas, está excepcionado del consentimiento de las mismas por la normativa de seguridad privada citada ut supra, dado que dicha legitimación únicamente alcanza a las imágenes captadas en recintos privados, y no en espacios públicos como en el presente caso.

Por lo tanto y al margen de lo establecido acertadamente por el informe de la Secretaría de Estado de Seguridad, 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 su Reglamento de desarrollo ,y el criterio establecido respecto a esta materia en la citada ley, se complementa con lo dispuesto en la Instrucción 1/2006.

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.

4. Respecto a las alegaciones formuladas por la entidad recurrente, a la Propuesta de Resolución, relativas a que los datos recogidos por sus cámaras, no se incluyen en ningún fichero estructurado que permita localizar las imágenes de forma fácil y sencilla hay que señalar que, la Directiva 95/46/CE del Parlamento Europeo 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, definió en su artículo 2 el fichero como *"todo conjunto estructurado de datos personales accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica"*, permitiendo a los Estados que regulen los criterios que permitan determinar los elementos de un conjunto estructurado de datos y los distintos criterios que regulan el acceso a dicho conjunto de datos.

La LOPD al establecer el concepto de fichero en su artículo 3.b) configura a éste como *"todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso"*, sin recoger distinción alguna entre ficheros manuales y ficheros automatizados.

Respecto a la alusión que realiza la entidad recurrente al considerando 27 de la citada Directiva, hay que señalar que en lo relativo a ficheros manuales dicho considerando reza lo siguiente: *"Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de alusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva."*

Consecuentemente con lo previsto en la Directiva el criterio seguido por esta Agencia para dilucidar si nos encontramos ante un fichero y, por ello, sujeto a las previsiones de la normativa de protección de datos, parte de la necesidad de que los datos sean objeto de una organización sistemática, con arreglo a criterios que permitan la búsqueda de los mismos.

Este criterio ha sido corroborado por la Audiencia Nacional que declara en sentencia de 16 de febrero de 2006 lo siguiente: "Así, todo fichero de datos exige para tener esta consideración una estructura u organización con arreglo a criterios determinados. El mero acúmulo de datos sin criterio alguno no podrá tener la consideración de fichero a los efectos de la ley."

El Reglamento de protección de datos de carácter personal, ha aportado, a efectos de clarificación del ámbito objetivo de la LOPD una definición de fichero no automatizado. Nos encontramos así ante los siguientes conceptos en su artículo 5.1 letras k) y n)

"Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso."

"Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica."

Por otro lado, la LOPD se refiere al tratamiento de datos en su artículo 3.c) como *"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."* De la misma manera el Reglamento de desarrollo de la LOPD define el tratamiento de datos *"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."*

A este respecto, la Sentencia de la Audiencia Nacional de 24/01/2003, al tratar la cuestión de lo que se entiende por tratamiento de datos, recoge*: "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, de acuerdo a la normativa expuesta, las imágenes captadas y grabadas por las cámaras de videovigilancia de la entidad recurrente, en contra de lo alegado por la misma, constituyen un tratamiento de datos personales, dado que el sistema de videovigilancia instalado es automatizado y va almacenado imágenes durante el período establecido, permitiendo búsquedas de imágenes en base a criterios de lugar, día y hora. Por lo tanto dichas imágenes constituyen un fichero a los efectos de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Para mayor abundamiento, respecto a esta cuestión, ya se pronunciado la sentencia nº 05539/2009, anteriormente citada, dictada por la Sala de lo Contencioso-Administrativo de Audiencia Nacional de fecha 17 de junio de 2010, en la que desestima el recurso número 684/2009, interpuesto por EL CORTE INGLÉS, S.A., contra la resolución dictada por el Director de la Agencia Española de Protección de Datos de fecha 24 de julio de 2009, dictada en el Procedimiento Sancionador PS/00640/2008, al recoger en su Fundamento de Derecho Quinto lo siguiente*:" En cuanto al fondo se cuestiona la existencia de tratamiento por considerar que los datos recogidos por las cámaras no se incluyen en ningún fichero estructurado, como exige el artículo 3 de la Directiva 95/46/CE. Señala la recurrente que dichas imágenes se graban unas a continuación de*

otras, a medida que se van obteniendo, sin ningún orden establecido y se van eliminando automáticamente por el propio sistema, al cabo de 7 días, por lo que no se incluyen en un fichero organizado o estructurado que permita su localización de forma fácil o sencilla, sin grandes esfuerzos, no hallándonos ante un fichero en el sentido de la Directiva citada ni de la LOPD.

Por esa razón al faltar el elemento esencial del fichero, concluye que la actuación de la entidad recurrente no puede ser incardinada en la LOPD.

Se trata de una cuestión que fue suscitada en el recurso de reposición interpuesto contra la resolución sancionadora y analizada por la resolución impugnada, que argumenta para desestimarla que las imágenes captadas y grabadas por las cámaras de videovigilancia de dicha entidad no pueden tener la consideración de carpetas no estructuradas, dado que el sistema de vigilancia instalado es automatizado y va almacenando imágenes identificables durante el periodo establecido, permitiendo búsquedas de imágenes en base a criterios de lugar, día y hora y constituyen un fichero a los efectos de lo dispuesto la LOPD.

Para abordar dicha cuestión hay que partir del concepto de tratamiento de datos, que se define en la LOPD, artículo 3.c) como "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 transferencia".

En la línea de la Directiva 95/46/CE que transpone, nuestra LOPD incluye en dicha definición tanto el tratamiento automatizado de datos como el manual.

Ahora bien, como señala la SAN, Sec. 1ª, de 16 de febrero de 2006 (Rec. 511/2004) *citada por la resolución impugnada, no basta con la realización de una de estas actuaciones en relación con datos personales para que la ley despliegue sus efectos protectores y garantías y derechos del afectado. "Es preciso algo más, que esas actuaciones de recogida, grabación, conservación etc, se realicen de forma automatizada o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a estar contenidos en un fichero".*

Se basa para ello la citada sentencia en el artículo 3 de la Directiva que delimita su ámbito de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de dichos datos contenidos o destinados a ser contenidos en un fichero.

En el caso de autos, atendidos los amplios términos del concepto de tratamiento de datos contenido en la LOPD, cabe sostener que la captación de la imagen de una persona y su grabación por el sistema de videovigilancia instalado y conservación durante un periodo de 7 días, como se ha constatado por los Inspectores de la AEPD en la inspección realizada documentada en el acta del acta de fecha 16 de febrero de 2009 - folio 95 y siguientes del expediente- constituye una operación o procedimiento técnico de recogida de datos, que al realizarse de forma automatizada (no manual), dado que el sistema de videovigilancia instalado es automatizado, tiene la consideración de tratamiento de datos de carácter personal en el sentido de la LOPD y esta sometido a la misma.

Pero es que además, las imágenes recogidas por dicho sistema se almacenan o incluyen en el fichero "Videovigilancia" por un periodo de 7 días, del que es responsable HIPERCOR S.A., que lo ha inscrito en el Registro General de Protección de Datos – folios 157 y siguientes del expediente-. Es de destacar que como finalidad del citado fichero figura la "captura de imágenes de personas y vehículos por motivos de seguridad ... se conservan por un periodo de 7 días", reconociendo la propia parte que se pueden realizar búsquedas de imágenes de personas en base a criterios de lugar, día y hora.

Con estos presupuestos hablar de inexistencia de fichero en el sentido del artículo 3.c) LOPD resulta gratuito, hallándonos ante un supuesto al que es plenamente aplicable la citada LOPD.

Por todo lo cual, al haberse realizado un tratamiento de datos de carácter personal excesivo y no proporcional al fin perseguido (a la vista de las circunstancias concurrentes reseñadas en los hechos probados), sometido al consentimiento de sus titulares, según dispone el artículo 6.1 LOPD, del que se carece, se ha incurrido en la infracción apreciada."

5. Respecto a la invocación relativa a que existen procedimientos resueltos en esta Agencia PS/353/2008, 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 que éste fue resuelto con el archivo del mismo, al constatarse que la entidad denunciada no era responsable del fichero, hecho que no es aplicable al caso que nos ocupa.
6. Por último en cuanto a las alegaciones realizadas por la entidad denunciada, a la Propuesta de Resolución relativas a que cumple con el deber de información mediante la instalación de los correspondientes carteles a las entradas a los establecimientos, lo cual es una forma indirecta de obtener el consentimiento de los peatones, hay que señalar que para que exista consentimiento, elemento base en el tratamiento de los datos, deben concurrir los requisitos legalmente previstos para considerar que se ha obtenido libremente el consentimiento. El artículo 3 h) de la LOPD lo define como *"Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que el conciernen".*

La Jurisprudencia de la Audiencia Nacional ha entendido que los requisitos del consentimiento, se agotan en la necesidad de que este sea "inequívoco", es decir, que no exista duda alguna sobre la prestación de dicho consentimiento, de manera que en esta materia el legislador, mediante el articulo 6.1 de la LO de tanta cita, acude a un criterio sustantivo, esto es, nos indica que cualquiera que sea la forma que revista el consentimiento, éste ha de aparecer como evidente, inequívoco – que no admite duda o equivocación- , pues éste y no otro es el significado del adjetivo utilizado para calificar al consentimiento.

Por tanto, el establecimiento de presunciones de consentimiento establecidas por la entidad denunciada, en base a que los afectados han sido informados, resulta irrelevante, pues dar carta de naturaleza a este tipo de interpretaciones pulverizaría esta exigencia esencial del consentimiento, porque dejaría de ser inequívoco para ser

“equivoco”, es decir, su interpretación admitiría varios sentidos y, por esta vía, se desvirtuaría la naturaleza y significado que desempeña como garantía en la proteccion de los datos, e incumpliría la finalidad que está llamado a verificar, esto es, que el poder de disposición de los datos corresponde únicamente a su titular. Es este el sentido recogido en la Sentencia de la Audiencia Nacional de 21 de noviembre de 2007 (Rec 356/2006) en su Fundamento de Derecho Quinto.

Ello es así en la medida que la jurisprudencia ha reiterado (Sentencias de 20 de julio de 2006 [RJ 2006, 4738] y 10 de junio de 2005 [RJ 2005, 4364], entre muchas otras), que *«los hechos determinantes de la apreciación del consentimiento han de ser inequívocos -"falta concludentia"-*, es decir, que con toda evidencia los signifiquen -S. 7 junio 1986 (RJ 1986, 3296)-, sin posibilidad de dudosas interpretaciones -SS. 5 julio 1960, 14 junio 1963, 13 febrero 1978-», lo cual implica a su vez, que también sea un criterio consolidado en la doctrina a la hora de valorar el silencio como consentimiento tácito que *«generalmente el mero conocimiento no implica conformidad, ni basta el mero silencio para entender que se produjo la aquiescencia* (pese a la máxima *"tacite consensu convenire intelligitur"*, Paulo, Libro II, Tit. XIV, 2 Digesto; S. 13 febrero 1978)...».

Por lo tanto, a la vista de lo expuesto, del hecho que los afectados por el tratamiento de las imágenes en el establecimiento denunciado no se hayan opuesto de forma expresa a dicho tratamiento, no se puede inferir un consentimiento al mismo como alega la entidad denunciada, procediendo desestimar las alegaciones efectuadas a este respecto.

En este sentido, se ha pronunciado esta Agencia Española de Protección de Datos, en su informe nº 0041/2008 al recoger: *“ La consulta plantea cómo habrá de obtenerse el consentimiento respecto de las grabaciones obtenidas a través de cámaras de videovigilancia de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y la Instrucción 1/2006 de 8 de noviembre de 2006, 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 primer lugar, se plantea la posibilidad de obtener el consentimiento tácito, en esta materia, lo que exige tener en cuenta lo dispuesto en el artículo 6.1 de la Ley Orgánica 15/1999 que señala lo siguiente “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”.

Por otro lado, respecto a la forma de obtener el consentimiento, es necesario acudir a lo dispuesto en del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la Ley Orgánica 15/1999, donde en el artículo 14, se regulan las formas de obtener el consentimiento señalando que “1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al

tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud."

El procedimiento descrito en el artículo 14 del Real Decreto 1720/2007, es el único que puede entenderse válido a la hora de obtener el consentimiento tácito y resulta de aplicación imposible cuando se trata de grabaciones o reproducciones en tiempo real de imágenes. En consecuencia, podemos concluir que en materia de videovigilancia resulta prácticamente imposible obtener el consentimiento, de las personas cuyas imágenes capten las cámaras por lo que es preciso acudir a una ley que habilite el tratamiento."

Por lo tanto, el tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo), "*...consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"*.

En el caso analizado, de lo expuesto resulta que la instalación de las cámaras, si bien se encuentra justificada, en principio, por lo que señala la normativa de seguridad privada en lo que se refiere al control de accesos; el uso de las mismas se ha realizado de modo excesivo y no proporcional, infringiendo con ello los límites que señala la citada

Instrucción 1/2006, y ello puesto que permite la captación de imágenes de los transeúntes de las calles que se encuentran en la confluencia de los establecimientos comerciales, en los que están instaladas las cámaras exteriores, sin que HIPERCOR haya acreditado que dicha captación es obligada para conseguir la finalidad de vigilancia que originó su instalación de conformidad con la normativa de seguridad privada.

VI

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 automatizado de datos personales o su uso posterior – que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la LOPD.

En este caso, Hipercor, ha incurrido en la infracción grave descrita ya que el consentimiento para el tratamiento de los datos personales es un principio básico del derecho fundamental a la protección de datos, recogido en el artículo 6 de la LOPD , habiendo tratado datos de las personas que pudieran haber sido captadas por la cámara de videovigilancia sin contar habilitación legal para ello, lo que supone una vulneración de este principio, conducta que encuentra su tipificación en este artículo 44.3.d).

VII

El artículo 45.2, 4 y 5 de la LOPD establece lo siguiente:

"2. Las infracciones graves podrán ser sancionadas con multas de 60.101,21 € a 300.506,05 €".
"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."

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 antijuricidad del hecho.
Respecto a la aplicación del art. 45.5 de la LOPD, conviene señalar que la Audiencia Nacional, en su Sentencia de 24/05/2002, ha señalado en cuanto a la aplicación del apartado 5 del citado precepto que *"... 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, de forma que repugne a la sensibilidad jurídica, siempre guiada por el valor justicia, la imposición de la sanción correspondiente al grado. Lo cual insistimos puede darse, por excepción, en casos muy extremos y concretos"*.

Conviene recordar que desde el punto de vista material, la culpabilidad consiste en al capacidad que tiene el sujeto obligado para obrar de modo distinto y, por tanto, de acuerdo con el ordenamiento jurídico. Por tanto, lo relevante es la diligencia desplegada en la acción por el sujeto, lo que excluye la imposición de una sanción, únicamente en base al mero resultado, es decir al principio de responsabilidad objetiva.

No obstante lo anterior, la Sentencia de la Audiencia Nacional dictada el 21 de septiembre de 2005, Recurso 937/2003, establece que *"Además, en cuanto a la aplicación del principio de culpabilidad resulta que (siguiendo el criterio de esta Sala en otras Sentencias como la de fecha 21 de enero de 2004 dictada en el recurso 113/2001) que la comisión de la infracción prevista en el art. 77.3 d) puede ser tanto dolosa como culposa. Y en este sentido, si el error es muestra de una falta de diligencia, el tipo es aplicable, pues aunque en materia sancionadora rige el principio de culpabilidad, como se infiere de la simple lectura del art. 130 de la Ley 30)1992, lo cierto es que la expresión "simple inobservancia" permite la imposición de la sanción, sin duda en supuestos doloso, y asimismo en supuestos culposos, bastando la inobservancia del deber de cuidado*".

Los hechos fundamentales acaecidos en el presente supuesto se centran en la captación y grabación de imágenes de personas identificables en la vía pública, lo que

denota una falta de diligencia inexcusable. A este respecto señalar que la diligencia exigible nos la da la profesionalidad del infractor, es decir, la actividad a la que se dedica, por lo que ésta debe ser mayor cuando, precisamente, se maneja un gran número de datos personales. Así lo han recogido la Sentencia de la Audiencia Nacional de Recurso 104/2006 señala que *"la entidad demandante por la actividad que realiza debe tratar un gran volumen de datos personales en sus ficheros, lo que hace que deba extremar el cuidado en el manejo de dichos datos para lograr una proteccion eficaz, pues está en juego un derecho fundamental autónomo, el derecho a la proteccion de datos personales según la STS 292/2000".*

En el mismo sentido la Sentencia de la Audiencia Nacional, Recurso 143/2006 señala que" *así es, no se aprecia la disminución de la culpabilidad del sancionado o de la antijuridicidad del hecho, pues la naturaleza de la actividad desarrollada por la entidad recurrente, y su permanente relación con los datos personales, determina que el comportamiento exigible a quien habitualmente está en contacto con este tipo de datos sea de distinguido y exquisito cuidado sobre el cumplimiento de las exigencias impuestas por la LOPD, porque está en juego la proteccion de derechos fundamentales-art. 18.4 CE-.* "

Por su parte, el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible, y en la valoración del grado de dicha diligencia, ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda que, en el caso ahora examinado, cuando la actividad de El Corte Inglés, S.A. de constante y abundante manejo de de datos, ha de insistirse en el rigor y el exquisito cuidado para ajustarse a las prevenciones legales al respecto (STS de 5 de junio de 1998).

En lo que respecta a la falta de perjuicios causados, la Audiencia Nacional, en Sentencia de 19/10/2005, declara que "*Los perjuicios directamente causados o beneficios obtenidos por la entidad recurrente son circunstancias que no admiten ser incluidas dentro de los que deben ser objeto de valoración al amparo de lo previsto por el artículo 45 de la LO 15/1999"*.

Por tanto, no se considera que concurran las circunstancias necesarias para que pueda aplicarse, en el presente supuesto, lo dispuesto en el artículo 45.5. de la LOPD.

Respecto a los criterios de graduación de las sanciones recogidas en el artículo 45.4 de la LOPD, y en especial, la falta de intencionalidad, procede proponer la imposición de la sanción en su cuantía mínima.

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 **HIPERCOR, S.A..,** por una infracción del artículo 6 de la LOPD, tipificada como 6 en el artículo 44.3.d) de dicha norma, una multa de 60.101,21 € (sesenta mil ciento un euros con veintiún céntimos de euro) de conformidad con lo establecido en el artículo 45.2.4 de la citada Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución a **HIPERCOR, S.A..** y a Don ***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 0182 2370 43 0200000785 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, 21 de febrero de 2011

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte