Procedimiento Nº PS/00108/2010

RESOLUCIÓN: R/00992/2010

En el procedimiento sancionador PS/00108/2010, instruido por la Agencia Española de Protección de Datos a la ***COMUNIDAD DE PROPIETARIOS IRACHE, 1ª FASE***, vista la denuncia presentada por D. ***A.A.A.*** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 14 de abril de 2009 tiene entrada en esta Agencia, escrito remitido por D. A.A.A. en el que manifiesta que ha sido instalada una cámara de videovigilancia en la Urbanización Irache de la localidad de (.....), sin consentimiento de los propietarios ni realización de asamblea general de vecinos para la adopción del acuerdo de la instalación. Asimismo manifiesta que no ha sido señalizada la zona que cubre la cámara ni los accesos al lugar, y que la cámara está conectada a Internet, teniendo cualquier persona acceso a la misma en todo momento y desde cualquier lugar del mundo mediante la dirección http://##########.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se solicita información, con fecha 14 de abril de 2009, a la Comunidad de Propietarios Irache, teniendo entrada en esta Agencia, en fecha 24 de julio de 2009, escrito de contestación de D. B.B.B., en calidad de administrador de la citada Comunidad, quien manifiesta lo siguiente:

1. Respecto de los lugares donde se encuentra ubicada la cámara de videovigilancia, manifiesta que la cámara se encuentra instalada “debajo del alero de un tejado que cubre tanto la oficina como la caseta de los empleados de servicios múltiples de la Comunidad”.

Aporta fotografías del lugar donde se ubica la cámara citada.

Respecto de la finalidad por la cual se han instalado la misma manifiesta que única y exclusivamente es tener posibilidad de visión del exterior de la oficina desde el interior de la misma, dado que ésta se encuentra en un plano inferior al exterior (las ventanas de la oficina se encuentran a la altura del suelo).

Respecto de la información facilitada a terceros sobre la existencia de monitores que permitan visualizar las imágenes captadas por las videocámaras, aporta fotografías del cartel donde se informa de la existencia de cámaras de videovigilancia, dentro del panel de informaciones destinadas a la Comunidad, ubicado en el acceso principal a la oficina de la Comunidad y a la caseta de los empleados, vía principal de acceso a la urbanización, el cual es acorde al recogido en la Instrucción 1/2006, de 8 de noviembre de la Agencia Española de Protección de Datos. Asimismo manifiesta que existe un único monitor en el interior de la oficina, el cual es visualizado por el administrador de la Comunidad, el cual tiene su puesto de trabajo en la citada oficina.

Respecto del formulario informativo que debe estar a disposición de los ciudadanos según se recoge en el artículo 3.b de la Instrucción 1/2006, adjunta copia del modelo a disposición de los interesados.

Respecto de la empresa de seguridad que ha realizado la instalación de las videocámaras manifiesta que, la instalación ha sido realizada por los servicios de la propia Comunidad sin intervención de empresa externa de seguridad.

Las imágenes son únicamente visualizadas, no siendo las mismas, por lo tanto, grabadas.

Tienen inscrito el fichero denominado "VIDEOVIGILANCIA" en el Registro General de Protección de Datos, con fecha 30 de junio de 2008, figurando como responsable la Comunidad de Propietarios Irache, 1ª fase.

No se aporta documentación relativa a que la instalación del sistema de videovigilancia haya sido aprobado en Junta, por la Comunidad de Propietarios del Complejo Irache.

2. En fecha 7 de septiembre de 2009 y 6 de marzo de 2010 se realiza una consulta por el inspector actuante a la página de Internet designada por el denunciante http://##########, a través de la cual se accede a la cámara de video instalada en la Comunidad de Propietarios Irache.

El visionado de la cámara es de libre acceso para cualquier usuario de Internet, ya que se ha realizado sin que haya existido ningún tipo de control de acceso previo y con la simple selección de la citada dirección de Internet.

Para los parámetros de "audio", "Video Size" y "Administrador Menú" es necesario privilegio de acceso con el usuario "Admin."

La cámara transmite imágenes en tiempo real desde el interior de un recinto con denominación "COMPLEJO IRACHE" hacia la vía pública. Se adjuntan fotografías al respecto. (Documento 1).

TERCERO: En fecha 9 de marzo de 2010, el Director de la Agencia Española de Protección de Datos, acordó iniciar procedimiento sancionador a la COMUNIDAD DE PROPIETARIOS IRACHE, 1ª FASE , por la posible infracción de los artículos 6 y 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en los sucesivo LOPD), tipificados como grave y leve respectivamente en los artículos 44.3.d) y 44.2.e) de dicha norma, pudiendo ser sancionado con multa de 60.101,21 € a 300.506,05 € por la comisión de la infracción grave y de 601,01 € a 60.101,21 € por la comisión de la infracción leve, de acuerdo con los artículos 45.2 y 45.1 , de la citada Ley Orgánica.

CUARTO: Notificado el acuerdo de inicio, en fecha 26 de marzo de 2010, el representante de la Comunidad de Propietarios Irache, 1ª fase, solicita obtener copia de los documentos obrantes en el expediente. En fecha 29 de marzo de 2010, se hace entrega al representante de la Comunidad denunciada, copia de todos los documentos obrantes en el citado expediente.

QUINTO: En fecha 31 de marzo de 2010, el denunciante solicita su personación en el presente expediente y aporta copia del documento de la Junta Rectora de fecha 8 de marzo de 2008.

En fecha 5 de abril de 2010, se le comunica al denunciante, que de conformidad con lo dispuesto en el artículo 31.1.c) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se le tiene por interesado en el procedimiento de referencia, pudiendo ejercer todos los derechos inherentes a esta condición.

SEXTO: En fecha 31 de marzo de 2010, el representante de la Comunidad de Propietarios Irache,

1ª fase, formuló en síntesis, las siguientes alegaciones al acuerdo de inicio:

- Que la videcámara se instaló con la intención de proteger a los vecinos de la comunidad, lo que habilita dicha instalación, no siendo necesaria intervención de empresa de seguridad alguna, según reconoce la propia Agencia en su Informe Jurídico 0650/2009; la instalación se realizó mediando acuerdo del oportuno órgano de la Comunidad de Propietarios(siendo, éste diferente de la Junta de Propietarios) y la cámara sólo enfoca a una vía que forma parte del conjunto residencial, abarcando sólo de forma marginal e inevitable una pequeña parte de la vía pública.
- Que según confirma el tenor del citado Informe Jurídico, la realización de funciones de videovigilancia proporcionadas al peligro y/o daño que se pretende evitar justifican el tratamiento implicado en la instalación y/u operación de dicha videocámara, sin que sea necesario, desde la entrada en vigor de la Ley 25/2009, que dicha instalación sea llevada a cabo por una empresa de seguridad debidamente habilitada a tal efecto.
- Que la instalación de la videocámara se realizó sólo tras el oportuno acuerdo del órgano legalmente habilitado a acordar tal instalación. Así, *la Comunidad de Propietarios Irache*, en su Junta Rectora de fecha 8 de marzo de 2008(copia de cuya Acta se adjunta), aprobó en su punto 6º, la instalación de un sistema de videocámaras. La citada Acta fue aprobada en la Junta Posterior del mismo órgano de fecha 17 de mayo de 2008, sin existir alegaciones en contra de la instalación del sistema de videocámara (adjunta copia del citado Acta). La citada Acta, fue expuesta en el tablón de anuncios de la comunidad, por un período no inferior a 20 días, sin que durante dicho período de exposición ni posteriormente, se recibieron negativas a dicha instalación por parte de ningún propietario. (adjunta copia de certificación emitida por el Administrador de la Comunidad, al respecto).
- Que la Junta Rectora es plenamente competente para la gestión y administración de la comunidad por delegación de la Junta General y por lo tanto, para tomar la decisión de la instalación del sistema de videocámaras, conforme al artículo 26 de los Estatutos de la Comunidad (estatutos cuya copia se adjunta).
- Que la finalidad del sistema de videovigilancia instalado afecta únicamente al control de acceso a la urbanización desde el interior de la misma, función que realiza el administrador desde el interior de la oficina. La vista que se obtiene viene referida a las vías interiores de la citada urbanización, y sólo a distancia y de forma difícilmente inidentificable se aprecia una vista exterior de la misma (vía pública) cuando las puertas se abren. Se adjunta copia de Plano de la urbanización y el Plan Municipal de Ayegui.
- Respecto a la infracción del deber de secreto sobre el fichero, la comunidad reconoce la misma, si bien alega que tal incumplimiento se ha debido únicamente al desconocimiento de la debida técnica informática en la instalación de las videocámaras. Que si se hubiese pretendido un acceso libre no se vería la cámara a través de un nombre de usuario y contraseña ya rellenados por defecto, sino que los mismos no aparecerían en absoluto. No obstante, han subsanado tal deficiencia impidiendo el acceso no autorizado a las mencionadas imágenes (adjunta certificación del administrador de fecha 30 de marzo de 2010).
- Solicita que se tengan por reproducidos los documentos que acompañan el presente escrito y se proceda al archivo del presente procedimiento y/o subsidiariamente, dada la naturaleza de los hechos, y su no intencionalidad, así como la diligencia mostrada en la subsanación de las deficiencias en el mantenimiento del debido secreto, se acuerde la imposición de una sanción leve aplicando la cuantía más rebajada de la escala aplicable.

SÉPTIMO: Transcurrido el plazo de alegaciones, por parte de la instructora del procedimiento se inició el período de práctica de pruebas, se dan por reproducidos a efectos probatorios la denuncia interpuesta por D. A.A.A. y su documentación, los documentos obtenidos y generados por los

Servicios de Inspección ante la Comunidad de propietarios Irache, 1ª fase, y el Informe de actuaciones previas de Inspección que forman parte del expediente E/02146/2009. Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00108/2010 presentadas por D. C.C.C., en nombre y representación de la Comunidad de Propietarios Irache, 1ª fase, y la documentación que a ellas acompaña.

OCTAVO: En fecha 26 de abril de 2010, el Instructor del Procedimiento emitió Propuesta de Resolución, en la que se propone que por el Director de la Agencia Española de Protección de Datos, se sancione a la Comunidad de Propietarios Irache, 1ª fase, con multa de 2.500 euros (dos mil quinientos euros) por la infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, dándose traslado a ésta para que en el plazo máximo de quince días hábiles presentara alegaciones.

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

HECHOS PROBADOS

PRIMERO: Consta que con fecha de 14 de abril de 2009 tiene entrada en esta Agencia escrito remitido por D. A.A.A. en el que manifiesta que ha sido instalada una cámara de videovigilancia en la Urbanización Irache de la localidad de (.....), sin consentimiento de los propietarios ni realización de asamblea general de vecinos para la adopción del acuerdo de la instalación. Asimismo manifiesta que no ha sido señalizada la zona que cubre la cámara ni los accesos al lugar, y que la cámara está conectada a Internet, teniendo cualquier persona acceso a la misma en todo momento y desde cualquier lugar del mundo mediante la dirección http://##########. (Folio 1 a 2).

SEGUNDO: En fecha 24 de julio de 2009, se recibe escrito de D. B.B.B., en calidad de administrador de la citada Comunidad, en contestación a la solicitud de información realizado por esta Agencia, quien manifiesta que la cámara se encuentra instalada debajo del alero de un tejado que cubre tanto la oficina como la caseta de los empleados de servicio múltiples de la Comunidad y que la finalidad de la misma es única y exclusivamente tener posibilidad de visión del exterior de la oficina desde el interior de la misma, dado que ésta se encuentra en un plano inferior al exterior (las ventanas de la oficina se encuentran a la altura del suelo) (Folio 7 y 11)

Aporta fotografías del cartel donde se informa de la existencia de cámaras de videovigilancia, dentro del panel de informaciones destinadas a la Comunidad, ubicado en el acceso principal a la oficina de la Comunidad y a la caseta de los empleados, vía principal de acceso a la urbanización, el cual es acorde al recogido en la Instrucción 1/2006, de 8 de noviembre de la Agencia Española de Protección de Datos. Asimismo manifiesta que existe un único monitor en el interior de la oficina, el cual es visualizado por el administrador de la Comunidad, el cual tiene su puesto de trabajo en la citada oficina.(Folio 7, 12, 13)

Aporta copia de la cláusula informativa que debe estar a disposición de los ciudadanos según se recoge en el artículo 3.b de la Instrucción 1/2006.(Folio 10).

Respecto de la empresa de seguridad que ha realizado la instalación de las videocámaras manifiesta que, la instalación ha sido realizada por los servicios de la propia Comunidad sin intervención de empresa externa de seguridad.(Folio 8).

Asimismo manifiesta que las imágenes son únicamente visualizadas, no siendo las mismas, por lo tanto, grabadas.(Folio 8).

Tienen inscrito el fichero denominado “VIDEOVIGILANCIA” en el Registro General de Protección de Datos, con fecha 30 de junio de 2008, figurando como responsable la Comunidad de Propietarios Irache, 1ª fase.(Folio 9).

TERCERO: No se aporta por la Comunidad denunciada, documentación relativa a que la instalación del sistema de videovigilancia haya sido aprobado en Junta, por la Comunidad de Propietarios del Complejo Irache. Si bien se aporta, tanto por el denunciante como por la Comunidad denunciada, Acta de la Junta Rectora de fecha 8 de marzo de 2008 donde figurando como únicamente presente en la misma, su Presidente, se recoge *“Se presenta un presupuesto de 845 € correspondientes a la instalación de una video cámara de seguridad, la cual grabará imágenes las 24 horas del día. Teniendo la posibilidad incluso de colgar dichas imágenes en Internet. El Presidente aprueba dicho gasto*”.(Folio 40 y 51)

Asimismo se aporta Acta de la Junta Rectora de fecha 17 de mayo de 2008, donde figura el Vicepresidente y otra persona como presentes, en la que se manifiesta *“1. Aprobación Actas anteriores. Se aprueban las actas de las Juntas Rectoras celebradas los días 12 de enero y 8 de marzo”.* (Folio 53).

CUARTO: En fecha 7 de septiembre de 2009 y 6 de marzo de 2010 se realiza una consulta por el inspector actuante a la página de Internet designada por el denunciante http://########, a través de la cual se accede a la cámara de video instalada en la Comunidad de Propietarios Irache.

El visionado de la cámara es de libre acceso para cualquier usuario de Internet, ya que se ha realizado sin que haya existido ningún tipo de control de acceso previo y con la simple selección de la citada dirección de Internet.

Para los parámetros de “audio”, “Video Size” y “Administrador Menú” es necesario privilegio de acceso con el usuario “Admin.”

La cámara transmite imágenes en tiempo real desde el interior de un recinto con denominación “COMPLEJO IRACHE” hacia la vía pública. Se adjuntan fotografías al respecto. (Folio 14, 15 y 20 a 25).

QUINTO: Consta certificación emitida, en fecha 30 de marzo de 2010, por el Secretario Administrador de la Comunidad de Propietarios Irache, 1ª Fase, en la que se manifiesta que desde el día 24 de marzo de 2010, se ha cancelado en su totalidad la visión de las imágenes de la entrada del Complejo Irache desde Internet en la forma de libre acceso y por medio de la cámara instalada en la oficina de la Comunidad.(Folio 67).

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, la Comunidad de Propietarios Irache, 1ª fase, es responsable del tratamiento 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 Comunidad de Propietarios Irache, 1ª fase, 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".

El artículo 2.1 de la LOPD 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".*

De acuerdo con esta definición de tratamiento de datos personales, la captación de imágenes de las personas, constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.

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.

Atendiendo a la definición contenida en las normas citadas, que considera dato de carácter personal *"cualquier información concerniente a personas físicas identificadas o identificables"*, las captaciones de imágenes indicadas se ajustarán a este concepto siempre que permitan la identificación de las personas que aparecen en dichas imágenes. La Directiva 95/46/CE en su Considerando 14 lo afirma expresamente al señalar:

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

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

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

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

Por su parte, la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (en lo sucesivo Instrucción 1/2006), en sus artículos 1.1 y 2 señala lo siguiente:

"Artículo 1.1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.
El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.
Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.

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

"Artículo 2.

1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia."

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

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

Para determinar si el supuesto que se analiza 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.

En el caso que nos ocupa, la Comunidad de Propietarios Irache, 1ª fase, tiene instalada una cámara de videovigilancia ubicada encima de la oficina de la Comunidad, y a cuyas imágenes se puede acceder, en tiempo real, vía Internet a través del sitio web http://########, sin existir ningún control de acceso previo. A través de la citada cámara se visualiza la entrada a la Comunidad, tanto por personas como vehículos. 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 contiene, entre otra información, datos concernientes a personas identificadas o identificables dado el entorno en el que se recogen, y sobre las que suministran información relativa a la imagen personal de éstas, el lugar de su captación y la actividad o conducta desarrollada por los individuos a las que las imágenes se refieren. Así, de conformidad con la normativa y jurisprudencia expuesta, la captación de imágenes a través de videocámaras, como es el caso que nos ocupa, constituye un tratamiento de datos personales, cuyo responsable se identifica, en el presente caso, con la Comunidad denunciada, toda vez que es aquélla la que decide sobre la finalidad, contenido y uso del citado tratamiento. Dicha Comunidad, como se desarrollará más adelante, carecía de legitimación para el tratamiento de las imágenes captadas, realizando un tratamiento de datos personales sin cumplir la normativa reguladora de protección de datos.

IV

Así se le imputa, a la Comunidad de Propietarios Irache, 1ª fase, en primer lugar, la comisión de una infracción del artículo 6, apartados 1 y 2 de la LOPD, que estipula 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."

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.

A este respecto, procede realizar varias aclaraciones relativas a la instalación de sistemas de videocámaras en Comunidades de Propietarios. Así, la Instrucción 1/2006 hace especial referencia

a la necesidad de ponderar los bienes jurídicos protegidos. Así viene a señalar expresamente que la instalación de este tipo de dispositivos se deberá respetar el principio de proporcionalidad, valorando así la posibilidad de adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, la instalación de cámaras de videovigilancia en el caso de una comunidad de propietarios con el fin de evitar determinadas situaciones de inseguridad para los residentes o sus visitantes, ha de ser una medida proporcional en relación con la infracción que se pretenda evitar y en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia, por lo que desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, tal y como señala la propia Instrucción, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de "una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad".

Así, el artículo 4 de la Instrucción 1/2006 recoge los principios de calidad, proporcionalidad y finalidad del tratamiento estableciendo lo siguiente:

"1.- De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.
2.- Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.
3.- Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida."

En este sentido, si la finalidad de la instalación de cámaras de videovigilancia tiene como objetivo controlar por ejemplo, determinados actos de vandalismo, robos o acciones violentas que vienen siendo habituales en la finca, en principio, la medida podría considerarse idónea, necesaria y proporcional, siempre y cuando se limitase estrictamente a esa finalidad. No obstante lo anterior, sería necesario atender las circunstancias particulares de la Comunidad de propietarios de que se trate.

Además, es necesario indicar, que el tratamiento de las imágenes por parte del responsable del tratamiento, le obliga a cumplir con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD.

Finalmente, hay que señalar que la decisión de la instalación de las cámaras en el recinto de una Comunidad de Vecinos debe ser aprobado por la Junta de Propietarios, según establece la Ley 49/1960, de 21 de julio de Propiedad Horizontal.

Así, el artículo 2 de la citada Ley 49/1960, dispone en lo que se refiere a su ámbito de aplicación:

"Esta Ley será de aplicación:

a) A las comunidades de propietarios constituidas con arreglo a lo dispuesto en el artículo 5.

b) A las comunidades que reúnan los requisitos establecidos en el artículo 396 del Código Civil y no hubiesen otorgado el título constitutivo de la propiedad horizontal.

Estas comunidades se regirán, en todo caso, por las disposiciones de esta Ley en lo relativo al régimen jurídico de la propiedad, de sus partes privativas y elementos comunes, así como en cuanto a los derechos y obligaciones recíprocas de los comuneros.

c) A los complejos inmobiliarios privados, en los términos establecidos en esta Ley."

Mientras que el artículo 14 de la misma Ley 49/1960, establece que: *"Corresponde a la Junta de propietarios: (…)*

d) Aprobar o reformar los estatutos y determinar las normas de régimen interior.

e) Conocer y decidir en los demás asuntos de interés general para la comunidad, acordando las medidas necesarios o convenientes para el mejor servicio común."

El artículo 17 de la citada Ley, regula el quorum y régimen de la aprobación de acuerdos por la Junta de Propietarios señalando que: "Los acuerdos de la Junta de propietarios se sujetarán a las siguientes normas:

1. *La unanimidad sólo será exigible para la validez de los acuerdos que impliquen la aprobación o modificación de las reglas contenidas en el título constitutivo de la propiedad horizontal o en los estatutos de la comunidad.*

El establecimiento o supresión de los servicios de ascensor, portería, conserjería, vigilancia u otros servicios comunes de interés general, incluso cuando supongan la modificación del título constitutivo o de los estatutos, requerirá el voto favorable de las tres quintas partes del total de los propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación. El arrendamiento de elementos comunes que no tenga asignado un uso específico en el inmueble requerirá igualmente el voto favorable de las tres quintas partes del total de los propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación, así como el consentimiento del propietario directamente afectado, si lo hubiere.

(…)

A los efectos establecidos en los párrafos anteriores de esta norma, se computarán como votos favorables los de aquellos propietarios ausentes de la Junta, debidamente citados, quienes una vez informados del acuerdo adoptado por los presentes, conforme al procedimiento establecido en el artículo 9, no manifiesten su discrepancia por comunicación a quien ejerza las funciones de secretario de la comunidad en el plazo de 30 días naturales, por cualquier medio que permita tener constancia de la recepción.

Los acuerdos válidamente adoptados con arreglo a lo dispuesto en esta norma obligan a todos los propietarios".

Por lo tanto, a la vista de lo expuesto la instalación del sistema de videovigilancia en una

Comunidad de propietarios, al afectar a zonas comunes de todos los vecinos, resulta necesario para su instalación contar con la pertinente aprobación, con el quórum establecido en la LPH, de los vecinos de la Comunidad de Propietarios.

En el caso que nos ocupa, la Comunidad denunciada alega que la instalación de la videocámara se realizó sólo tras el oportuno acuerdo del órgano legalmente habilitado a acordar tal instalación. A este respecto se alega que la Junta Rectora, de la citada comunidad, aprobó en fecha 8 de marzo de 2008, la instalación de un sistema de videocámaras, siendo la citada Junta Rectora plenamente competente para la gestión y administración de la comunidad por delegación de la Junta General, según el artículo 26 de los Estatutos de la Comunidad. Pues bien, hay que decir que el citado artículo 26 de los Estatutos de la Comunidad de Propietarios Irache, 1ª Fase, establece: *"La Junta General acordará, para dar mayor agilidad a la gestión y administración de esta Zona, el nombramiento de una Junta Rectora, integrada por los Propietarios que se presenten voluntarios y aceptados por la Junta General, además del Presidente, Vicepresidente y del Secretario-Administrador. Por operatividad se marca como máximo número de junteros la cantidad de 16 personas. Dicha Junta Rectora tendrá las facultades que dicha Junta General delegue en ella. Tendrá como misión principal la gestión de la Zona entre Juntas Generales. La duración de éste cargo será bianual, pudiendo repetir otros mandatos con el visto bueno de la Junta General."*

Cabe precisar que el citado artículo recoge que dicha Junta Rectora tendrá las facultades que le delegue la Junta General de Propietarios, sin que se recoga en los Estatutos, las materias que han sido objeto de delegación, como sería en el caso que nos ocupa el establecimiento de los servicios de vigilancia. A este respecto el propio artículo 20.4 de los Estatutos, en una redacción muy similar al citado artículo 17 de la LPH, establece que*:"El establecimiento o supresión de los servicios de portería, vigilancia u otros servicios comunes de interés general, (…) requerirá el voto favorable de las tres quintas partes del total de los propietarios que, a su vez, representen las tres quintas partes de las cuotas de participación".*

Por otro lado en la citada Acta de 8 de marzo de 2008, lo que se recoge es: *"Se presenta un presupuesto de 845 € correspondientes a la instalación de una videocámara de seguridad, la cual grabará imágenes las 24 horas del día. Teniendo la posibilidad incluso de colgar dichas imágenes en Internet. El Presidente aprueba dicho gasto."* Por lo tanto lo que se aprueba, en la citada Acta, de manera unilateral por parte del Presidente de la Junta Rectora, al ser el único asistente, es un presupuesto de gastos, del que no consta una previa aprobación del sistema de videovigilancia en Junta de Propietarios.

No obstante y sin perjuicio de lo trascrito "ut supra", lo cierto es que con independencia de que el sistema de videovigilancia fuera aprobado o no legalmente según establece la normativa al efecto, hay que diferenciar claramente el consentimiento que se prestase para la instalación de un sistema de cámaras con funciones de videovigilancia de la urbanización, del consentimiento necesario para la difusión de las imágenes captadas por la citada cámara vía Internet, consentimiento inequívoco que en el presente caso no existía.

La LOPD proporciona, como ya ha sido recogido "ut supra", un amplísimo concepto de tratamiento de datos personales. Serán tratamiento de datos personales las 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 Directiva 95/46/CE es aún más minuciosa en la enumeración de las operaciones o procedimientos que constituyen tratamiento: recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el

acceso a los mismos, cotejo o interconexión, así como bloqueo, supresión o destrucción.

Ahora bien, 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".*

Del concepto de consentimiento se desprende la necesaria concurrencia para que el mismo pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto. Un adecuado análisis del concepto exigirá poner de manifiesto cuál es la interpretación que ha de darse a estas cuatro notas características del consentimiento, tal y como la misma ha indicado en numerosas Resoluciones de la AEPD, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa. A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

b) Específico, es decir referido a un determinado tratamiento o serie de tratamientos concretos y en el ámbito de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado.

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.

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)...».

Así, en el caso que nos ocupa, en fecha 7 de septiembre de 2009 y 6 de marzo de 2010, se constató por el inspector actuante que, a través de Internet, en la dirección http://##########, se accedía a las imágenes, en tiempo real, captadas por la cámara de video instalada en la Comunidad. El acceso al visionado de la cámara se realizaba sin que existiera ningún tipo de control de acceso previo. Respecto a las imágenes captadas, deben ser consideradas datos de carácter personal, conforme al artículo 3.a) de la LOPD, y tales imágenes constituyen, en sí mismas consideradas, un tratamiento de datos en los términos de la LOPD.

La captación de imágenes de las personas y vehículos que pasan por la zona de captación de la cámara, y su difusión a través de la web, accesible para cualquier usuario de Internet, se encuentra sometida al consentimiento de sus titulares, de conformidad con lo dispuesto en el artículo 6.1 de la LOPD. No consta que la Comunidad denunciada tuviese consentimiento de las personas captadas por la cámara instalada para que sus imágenes fuesen difundidas en redes de comunicación telemática. Tampoco se ha producido ninguna excepción del consentimiento exigido, según las excepciones previstas en el trascrito artículo 6.2 de la LOPD. En conclusión, la actuación de la Comunidad, consistente en la captación de imágenes y su transmisión a la web, requiere el consentimiento de los afectados, que no consta que la misma recabe, por lo que ha incumplido el principio de consentimiento regulado en el artículo 6 de la LOPD.

En relación con la divulgación de datos personales a través de Internet, como ocurre en el caso que nos ocupa, existe un pronunciamiento del Tribunal de Justicia de la Comunidades Europeas (Sentencia de 6 de noviembre de 2003, relativa al caso de la señora Lindqvist) en el que, interpretando el concepto de tratamiento en la Directiva, se indicó lo siguiente:

"25. En cuanto al concepto de <<tratamiento>> de dichos datos que utiliza el artículo 3, apartado 1 de la Directiva 95/46, éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, <<cualquier operación o conjunto de operaciones ,efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales>>. Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole.

26. Queda por determinar si dicho tratamiento está <<parcial o totalmente automatizado>>. A este respecto, es preciso observar que difundir información en una página web implica, de acuerdo con los procedimientos técnicos e informáticos que se aplican actualmente, publicar dicha página en un servidor, así como realizar las operaciones necesarias para que resulte accesible a las personas que están conectadas a Internet. Estas operaciones se efectúan, al menos en parte, de manera automatizada.

27. Por tanto, procede responder a la primera cuestión que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un <<tratamiento total o parcialmente automatizado de datos personales>> en el sentido del artículo 3, apartado 1, de la Directiva 95/46."

La doctrina expuesta en el caso transcrito, es perfectamente trasladable a la difusión a través de una página web de la imagen de una persona (Sentencia de la Audiencia Nacional de 1 de octubre del 2008, Recurso Nº: 0000001/2007).

Por lo tanto, la difusión de imágenes a través de Internet, es indudable que, con arreglo a las anteriores definiciones, constituye tratamiento de ese dato de carácter personal, en el sentido expresado en la LOPD y en la Directiva comunitaria.

V

Respecto a las alegaciones formuladas por la Comunidad denunciada, relativas a que en la instalación del sistema de videovigilancia no es necesario la intervención de empresa de seguridad

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

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

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

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

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

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

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

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

En todo caso, el tratamiento de las imágenes deberá cumplir los restantes requisitos

exigibles en materia de protección de datos de Carácter Personal, recogidos en la Ley Orgánica y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, como son, entre otros, los relativos a que las imágenes que se capten sean las necesarias y no excesivas para la finalidad perseguida; el deber de informar a los interesados, tanto a través de la colocación de carteles informativos como mediante la puesta a disposición de aquéllos de impresos en que se detalle la información; la notificación de la existencia de los ficheros a la Agencia Española de Protección de Datos; o la implantación de medidas de seguridad.

Por lo tanto tras la aplicación de la Ley Ómnibus no se requeriría que los dispositivos de videovigilancia hayan sido instalados por una empresa de seguridad autorizada, si bien y centrándonos en el caso que nos ocupa, en todo caso se requeriría el consentimiento inequívoco de los afectados para la difusión y divulgación de sus imágenes, vía Internet, a través de las cámara instalada en el complejo residencial, consentimiento que no existía.

A la vista de lo expuesto, cabe decir que el tratamiento de imágenes, 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 la LOPD.

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)".

La Audiencia Nacional ha manifestado en su Sentencia de 22 de octubre de 2003 que <<la descripción de conductas que establece el artículo 44.3d) de la Ley Orgánica15/1999 cumple las exigencias derivadas del principio de tipicidad, a juicio de esta Sala, toda vez que del expresado precepto se desprende con claridad cual es la conducta prohibida. En efecto, el tipo aplicable considera infracción grave *"tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la 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 Ley Orgánica. Ahora bien, estos principios no son de aquellos que deben inferirse de dicha regulación legal, sino que aparecen claramente determinados y relacionados en el título II de la Ley, concretamente, por lo que ahora interesa, en el artículo 6 se recoge un principio que resulta elemental en la materia, que es la necesidad de consentimiento del afectado para que puedan tratarse automatizadamente datos de carácter personal. Por tanto, la conducta ilícita por la que se sanciona a la parte recurrente como responsable del tratamiento consiste en usar datos sin consentimiento de los titulares de los mismos, realizando envíos publicitarios.>>_

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 el presente caso, ha quedado acreditado que la captación y difusión en Internet de imágenes de la Comunidad, sin que haya constancia del consentimiento de éstos para dicha captación y difusión, supone 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 sin contar con su consentimiento, lo que supone una vulneración de este principio, conducta que encuentra su tipificación en este artículo 44.3.d).

VII

En segundo lugar, se imputa a la Comunidad de Propietarios Irache 1ª fase, la comisión de una infracción del artículo 10 de la LOPD que establece:

"*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*."

Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su sentencia n. 361, de 19/07/01: "*El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...*)".

En este sentido, la sentencia de la Audiencia Nacional de fecha 18/01/02, recoge en su Fundamento de Derecho Segundo, segundo y tercer párrafo: *"El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable* –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a

conocer su contenido teniendo el "*deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo*" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto."

"*Este deber de sigilo resulta esencial en las sociedades actuales cada vez mas complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un* "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "*es decir, el poder de resguardar su vida privada de una publicidad no querida*"

Así, el deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento.

El deber de secreto profesional que incumbe a los responsables de los ficheros, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable o quienes intervengan en cualquier fase del tratamiento de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el "*deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*". Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente o no, no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

En el caso que nos ocupa, ha quedado acreditado que, a través de Internet, en la dirección http://##########, se accedía a las imágenes, en tiempo real, captadas por la cámara de video instalada en la Comunidad. El acceso al visionado de la cámara se realizaba sin que existiera ningún tipo de control de acceso previo. Respecto a estas imágenes, deben ser consideradas datos de carácter personal, conforme al artículo 3.a) de la LOPD, y tales imágenes constituyen, en sí mismas consideradas, un tratamiento de datos en los términos de la LOPD.

Por tanto queda acreditado que por parte de la Comunidad de Propietarios Irache 1ª fase, responsable de la custodia de las imágenes en cuestión, se vulneró el deber de secreto garantizado en el artículo 10 de la LOPD, al haber posibilitado el acceso no restringido a datos personales sin consentimiento de sus titulares.

A este respecto, la Comunidad denunciada reconoce el incumplimiento del citado artículo 10 de la LOPD, si bien alega que tal incumplimiento se ha debido únicamente al desconocimiento de la debida técnica informática en la instalación de las videocámaras. Hay que señalar que el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal regula la Seguridad de los datos, concretando lo siguiente:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar

las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

El citado artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquella.

Así, la Comunidad denunciada, estaba obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas en la normativa y, entre ellas, las dirigidas a impedir que la imagen de los afectados fueran difundidas a través de la red, sin el consentimiento de éstos. Así la citada Comunidad manifiesta que la impericia del responsable de la instalación del sistema de videovigilancia provocó la infracción objeto de sanción. Sin embargo este hecho no exonera de responsabilidad a la Comunidad denunciada.

Así, el principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

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*".

También la Sentencia de la Audiencia Nacional de 25 de marzo de 2003 indica que *"Por lo que afecta a la culpabilidad, ha de decirse que generalmente este tipo de conductas no tienen un componente doloso, y la mayoría de ellas se producen sin malicia o intencionalidad. Basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia para evitar, como en el caso que nos ocupa, un tratamiento de datos personales sin consentimiento de la persona afectada, lo que denota una falta evidente en la observancia de esos deberes que conculcan claramente os principios y garantías establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de* Datos de carácter Personal, concretamente el del consentimiento del afectado".

El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."* El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa"* sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia." (STS 23 de enero de 1998).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."*(SAN 29 de junio de 2001).

VIII

El artículo 44.2.e) de la LOPD establece: "*2. Son infracciones leves: e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.*"

En relación con la infracción del artículo 10 de la LOPD por parte de la Comunidad de Propietarios Irache 1ª fase, para su tipificación como falta leve o grave, ha de tenerse en cuenta que:

a) La Sentencia de la Audiencia Nacional de fecha 7/01/02, que en su Fundamento de Derecho Cuarto, segundo párrafo señala lo siguiente: "...*Lo que no permite la norma es la transmisión de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo y al efecto cita ficheros en los que de transmitirse sus datos se obtendría una evaluación de dicha personalidad (...) Pues bien, en el caso de autos nos consta y nadie discute que el único dato transmitido fue el número de teléfono y dicho dato no permite realizar una evaluación o juicio sobre la personalidad del titular del dato. Lo que nos lleva a entender que el tipo que debe aplicarse es el correspondiente a la falta leve no a la grave..."*

b) Asimismo, la Sentencia de la Audiencia Nacional de fecha 17/01/02, cuyo Fundamento de Derecho Cuarto, segundo y tercer párrafo afirma que: "*La resolución sancionadora señala que la entidad recurrente ha quebrado el deber de confidencialidad establecido en el artículo 10 de la Ley Orgánica 5/1992, y que su conducta está tipificada como infracción grave en el artículo 43.3.g) de dicha Ley Orgánica. Sin embargo debe notarse que en la Ley Orgánica15/1999 (...) el incumplimiento del deber de secreto del artículo 10 constituye por regla general una infracción leve tipificada en el artículo 44.2.e), de modo que tal incumplimiento sólo constituye una infracción grave en los casos específicamente enunciados en el artículo 44.3.g), es decir, cuando la vulneración del secreto afecta a (...).*

Aunque la redacción dada a este último precepto ofrece alguna dificultad para su interpretación, esta Sala considera que la razón de ser del tipo agravado queda explicada en el último inciso del citado artículo 44.3.g) (...). Pues bien, teniendo en cuenta que en el caso presente los datos a los que indebidamente tuvo acceso un tercero fueron el número de cuenta y el saldo existente pero no el nombre del titular de dicha cuenta, esta Sala considera que la conducta no es subsumible en el tipo agravado ya que la información proporcionada no aparece vinculada a una persona determinada ni permite, por tanto, hacer valoración alguna sobre el perfil o personalidad del titular de tales datos." (el subrayado es de la Agencia Española de Protección de Datos).

c) Por último, la Sentencia de la Audiencia Nacional de fecha 18/01/02, que recoge en su

Fundamento de Derecho Tercero, segundo párrafo lo siguiente: "*Pues bien, de estos dos tipos sancionadores resulta aplicable a este caso, a juicio de esta Sala, el previsto en el artículo 44.2.e) de la Ley Orgánica 15/1999. En efecto, en la vigente Ley, a diferencia de la de 1992, la respuesta sancionadora al deber de guardar secreto se gradúa pudiendo ser una infracción grave o leve. La diferencia en la descripción de uno y otro tipo sancionador radica en que mientras que el legislador describe de modo completo la infracción grave, sin embargo la infracción leve la concibe como una categoría residual prevista para todos los casos que no revistan el carácter grave que describe el artículo 44.3.g) de la Ley Orgánica de tanta cita. Así las cosas, cuando la entidad bancaria facilita el teléfono de una cliente a otro es indudable que se está facilitando un dato personal que consta en los archivos de la recurrente sin consentimiento del afectado. Ahora bien, este dato personal incorporado a un fichero que contiene datos relativos a la prestación de servicios financieros, pero no constituye un dato suficiente para obtener una evaluación de la personalidad del individuo...*" (el subrayado es de la Agencia Española de Protección de Datos).

Por tanto Los hechos que se imputan en el presente procedimiento constituyen la infracción leve descrita en el artículo 44.2.e), pues el incumplimiento del deber de secreto sólo constituye el tipo agravado en los casos específicamente enunciados en el artículo 44.3.g) de la LOPD, es decir, cuando la vulneración del secreto afecte a "...*los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo".*

De acuerdo con la citada doctrina legal, en el presente caso, de los datos comunicados no se deriva la posibilidad de efectuar una evaluación de la personalidad de los afectados, por lo que la vulneración del artículo 10 de la LOPD ha de ser tipificada como infracción leve a tenor del artículo 44.2. e) de la citada Ley Orgánica.

IX

En el presente caso, de acuerdo con lo señalado en los anteriores Fundamentos de Derecho de esta Propuesta, ha quedado probado que la difusión de las imágenes, a través de la red, constituye una base fáctica para fundamentar la imputación de las infracciones de los artículos 6 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto de concurso medial, en el que un mismo hecho deriva en dos infracciones dándose la circunstancia que la comisión de una, implica necesariamente la comisión de la otra. Así, la difusión, a través de la red de las imágenes de la Comunidad, y por tanto la infracción del art. 10 de la LOPD (deber de secreto) deriva de la infracción del art. 6 de la LOPD, esto es, no estaba acreditado el consentimiento de los titulares de dichas imágenes para su difusión en Internet.

Así, como señala el Tribunal Supremo en Sentencia de 17 de noviembre de 1998, "… una necesaria derivación de unas infracciones respecto de las demás y viceversa, por lo que es indispensable que las unas no puedan cometerse sin ejecutar las otras…".

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora que establece: "En defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida", procede subsumir ambas infracciones

en una.

En tales casos, el legislador apuesta por aplicar la teoría de la absorción de la penalidad y, en consecuencia imponer la sanción más grave en lugar de imponer tantas sanciones como infracciones cometidas.

Dado que, en este caso, una infracción está tipificada como leve y otra como grave, se considera que procede imputar únicamente la infracción del artículo 6 de la LOPD, como infracción originaria que ha implicado la comisión de la otra.

X

Los artículos 45.2, 4 y 5 de la LOPD indican:

"2. Las infracciones graves serán sancionadas con multa de 60.101,21 € a300.506,05 €.."

"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 antijuricidad 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 antijuricidad 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 citado artículo 45.5 de la LOPD, 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. Dicho artículo, que no es sino la manifestación del llamado principio de proporcionalidad (art. 131 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común), incluido en el más general de prohibición de exceso reconocido por la Jurisprudencia como Principio General del Derecho (Sentencia del Tribunal Constitucional 62/1982), y es consecuencia del valor justicia que informa nuestro Ordenamiento Jurídico (Art. 1 de la Constitución Española), sin embargo debe aplicarse con exquisita ponderación, y sólo en los casos en los que la culpabilidad resulte sustancialmente atenuada atendidas las circunstancias del caso concreto.

En este caso, ha quedado acreditado que la captación y difusión, a través de la red de las imágenes de las personas y vehículos que transitan por el ángulo de captación de la cámara instalada en la Comunidad de Propietarios Irache, sin el consentimiento de éstos, supone una infracción al principio de consentimiento regulados en el artículo 6 de la LOPD y calificado como infracción grave.

Ahora bien aunque la conducta se encuadre en la infracción grave tipificada en el artículo 44.3.d) de la LOPD, resulta necesario hacer una valoración conjunta de las circunstancias concurrentes.

La Comunidad denunciada solicita en su caso, la aplicación del artículo 45.5. de la LOPD, en base a la naturaleza de los hechos y su no intencionalidad, así como la diligencia mostrada en la subsanación de las deficiencias en el mantenimiento del debido secreto, impidiendo el acceso no autorizado a las imágenes.

En concreto, hay que considerar que la Comunidad de Propietarios Irache 1ª fase, no tenía ánimo de producir ningún daño a las personas que fueron captadas por la cámara y difundidas su imagen vía internet. No consta acreditada intencionalidad en la conducta imputada. Asimismo, ha procedido a la eliminación inmediata de la emisión por Internet, lo que denota una diligencia en su actuación , que permiten entender que existe una disminución de la culpabilidad del imputado, considerándose procedente aplicar la graduación prevista en el artículo 45.5 de la LOPD.

Por otro lado a efectos de graduar la sanción, de conformidad con lo dispuesto en el artículo 45.4 de la LOPD, ha de tenerse en cuenta que las imágenes captadas por la cámara se difundieron a través de Internet y que este tratamiento va más allá del mero tratamiento de imágenes mediante un sistema de cámaras o videocámaras, por lo que se considera procedente la imposición de la sanción en la cuantía de 2.500 €.

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 ***COMUNIDAD DE PROPIETARIOS IRACHE, 1ª FASE***, por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 2.500 € (dos mil quinientos euros) de conformidad con lo establecido en el artículo 45.2.4 y 5 de la citada Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución a ***COMUNIDAD DE PROPIETARIOS IRACHE, 1ª FASE*** y a D. ***A.A.A.***.

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de

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

Madrid, 24 de mayo de 2010

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte