



Procedimiento Nº PS/00230/2008

RESOLUCIÓN: R/01270/2008

En el procedimiento sancionador PS/00230/2008, instruido por la Agencia Española de Protección de Datos a la entidad **WAJAL CANARIAS, S.L.**, vista la denuncia presentada por **D. R.R.R., D. L.L.L., D^a G.G.G.** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 30 de mayo de 2007 tiene entrada en esta Agencia un escrito de D. L.L.L., D. R.R.R. y Dña. G.G.G. en el que declaran que la entidad Wajal Canarias S.L. (en adelante WAJAL) ha instalado dos cámaras de videovigilancia en la fachada de un edificio de su propiedad. La entidad no ha registrado el fichero correspondiente y consideran que por la orientación y la instalación vulnera su derecho a la intimidad y la instrucción 1/2006 de la Agencia Española de Protección de Datos.

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:

1. RESPECTO DE WAJAL CANARIAS S.L.

1.1. Con motivo de la edificación del inmueble donde se sitúa la sede social de WAJAL se produjeron varios altercados que aconsejaron a la entidad, la instalación de un sistema de videovigilancia con objeto de proteger la integridad del edificio.

Para ello se encomendó a la entidad COMERALSE S.L., empresa que comercializa sistemas y equipos de seguridad homologada en el R.E.S. con el número **+, el suministro y colocación de un sistema de videovigilancia que capturase imágenes de las dos fachadas que posee el inmueble, una hacia la (C/.....) y la otra hacia la (C/.....). Este hecho se ve acreditado por la copia de la factura emitida por COMERALSE S.L. Dicha instalación quedó finalizada en marzo de 2007, si



bien no entró en funcionamiento hasta no haber sido dado de alta el fichero y colocado los preceptivos carteles indicadores, encontrándose activa a fecha de hoy.

1.2. Durante la inspección se comprobó la existencia de dos cámaras de videovigilancia en las fachadas del inmueble. La videocámara ubicada en la fachada que da a la (C/.....) enfoca hacia las puertas principales y ventanas del edificio. La situada en la fachada de la (C/.....) enfoca hacia la puerta del garaje.

1.3. Asimismo se verificó la existencia de varios carteles informativos en las puertas y escaparates de las entradas en ambas calles. Estos carteles se corresponden a los modelos propuestos en la Instrucción 1/2006 de la Agencia Española de Protección de Datos.

1.4. El recinto donde se encuentra instalado el sistema de grabación se encuentra en un cuarto del edificio cuya puerta de seguridad se encuentra cerrada con llave. WAJAL manifiesta que las llaves de dicha puerta son controladas por el administrador de la entidad en todo momento, no permitiendo la entrada de nadie más en el cuarto. El sistema se encuentra encendido, y consta de un monitor en color y un aparato controlador-grabador modelo NLDVR3014X. Sobre el monitor del que está dotado el sistema de videovigilancia se realizaron las siguientes comprobaciones:

Es posible visualizar las imágenes captadas por cada una de las dos cámaras instaladas. Estas imágenes se visualizan en color, y las personas que transitan podrían ser identificables.

No es posible modificar de forma automática la direccionalidad de los objetivos, ni hacer acercamientos con el objetivo.

Aunque es posible conectar el sistema a una red de área local, esta funcionalidad se encuentra deshabilitada.

Ambas cámaras captan imágenes de la vía pública y de la acera situada inmediatamente frente al edificio.

El dispositivo grabador tiene una capacidad máxima de 160 Gb y está configurado para realizar una grabación a la máxima calidad y con un ratio de 9 imágenes por segundo (Frames per Second). El sistema está configurado para que en el momento en el que se alcance el tamaño máximo del sistema de almacenamiento, se procede a la regrabación sobre el mismo fichero. El sonido se encuentra deshabilitado.

Se comprueba que las imágenes más antiguas almacenadas en el sistema corresponden al 26 de enero de 2008.

2. RESPECTO DEL REGISTRO GENERAL DE PROTECCIÓN DE DATOS

El Registro General de Protección de Datos incluyó en fecha 23 de mayo de 2007 el fichero de nombre "Video cámaras de vigilancia" con el número de registro ##### cuyo responsable se identifica con la entidad WAJAL CANARIAS S.L.

TERCERO: En fecha 25 de abril de 2008 el Director de la Agencia Española de Protección de Datos, acordó iniciar procedimiento sancionador a Wajal Canarias, S.L.,



por la posible infracción del artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, 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 sancionada con multa de 60.101,21 € a 300.506,05 €, de acuerdo con el artículo 45.2 de la citada Ley Orgánica.

CUARTO: En fecha 6 de junio de 2008, D. D.D.D., en representación de Wajal Canarias, S.L., formuló, en síntesis, las siguientes alegaciones al acuerdo de inicio:

- Que las personas que han formulado denuncia contra Wajal, han mantenido durante los últimos tres años disputas con ésta, existiendo varios juicios en materia inmobiliaria, habiéndole causado daños significativos a su propiedad. Debido a dichas disputas el denunciado tuvo que contratar un servicio de seguridad privada del 8 al 31 de mayo de 2006, con la empresa Aconcagua Seguridad S.L.U. para proteger la integridad física de los trabajadores que llevaban acabo la construcción del edificio, propiedad del denunciado. Aporta copias de las sentencias y de la factura del servicio de seguridad privada.
- Aconsejada por la empresa de seguridad Comeralse, S.L., y con el fin de proteger el inmueble y controlar las entradas y salidas de dicha construcción, procedió en fecha 12 de febrero de 2007 a la formalización de contrato de servicio de seguridad con la empresa de seguridad citada, en el que se incluía la instalación de dos cámaras de videovigilancia que capturasen imágenes de las dos fachadas del inmueble. Aporta contrato con la empresa de seguridad.
- En fecha 14 de febrero de 2007, contrata nuevamente los servicios de vigilancia de Aconcagua Seguridad S.L., debido a hechos vandálicos sufridos días anteriores en el inmueble de su propiedad. Aporta copia de dichos servicios contratados.
- Que en fecha 16 de marzo de 2007, la empresa de seguridad Comeralse instala en el inmueble propiedad de Wajal un sistema de seguridad de circuito cerrado debidamente registrado en la Comisaría de Policía, sin que dichas cámaras invadiesen la intimidad del transeúnte al enfocar únicamente a la puerta y fachada del local comercial. Adjunta copia al respecto.
- Que antes de la activación de las cámaras de videovigilancia, la entidad denunciada procedió en fecha 23 de mayo de 2007, a la inscripción del fichero de nombre "Videocámaras de Videovigilancia" en el Registro de la Agencia Española de Protección de datos. Asimismo instaló varios carteles informativos de zona videovigilada en las puertas y escaparates de las entradas al inmueble de la entidad denunciada. En fecha 25 de mayo de 2007, se activaron las cámaras.



- Que el sistema se encontraba continuamente encendido hasta que la situación de inseguridad cesara y se procedería entonces a la retirada de las cámaras.
- El sistema no cuenta con sistema de sonido, ni se pueden realizar acercamientos con el objetivo, ni es posible modificar de forma automática la direccionalidad del objetivo. Las imágenes nunca permanecen más de 5 días en el sistema y la ubicación de las cámaras en las fachadas es de 6 ó 7 metros desde el suelo y a 1 metro del linde del edificio en construcción.
- Que las imágenes son mostradas en un monitor en una habitación con puerta de seguridad cerrada con llave las 24 horas del día, no contratando la entidad denunciada a personal alguno de seguridad para que visualizara las imágenes.
- Que en fecha 14 de noviembre de 2006 fue retirada de la Gerencia Municipal de Urbanismo del Ayuntamiento de (.....), licencia de demolición del edificio contiguo al de propiedad de la entidad denunciada. Que la demolición produjo vibraciones en el inmueble de Wajal, provocando daños estructurales en uno de sus pilares. Adjunta informe técnico de reparación del pilar afectado con firma de la empresa reparadora de 20 de junio de 2007.
- Que la demolición pudo ocasionar la desubicación del objetivo de las cámaras, no pudiéndose acreditarse dicho punto. En fecha 25 de mayo de 2007, la empresa de seguridad Comeralse procede a reubicar las cámaras por haberse éstas desplazado del ángulo permitido posiblemente por vibraciones ocasionadas por la obra cercana.
- Que el representante de la entidad denunciada colaboró con los inspectores de esta Agencia, en la absoluta convicción de estar cumpliendo con toda la normativa de protección de datos.
- Que tras la inspección de esta Agencia, en fecha 11 de febrero de 2008 la entidad denunciada al observar que el enfoque de las cámaras no era el originario requirieron a la empresa de seguridad contratada para que procediese a la recolocación de las mismas declarando ésta que: *“el ángulo de enfoque de las cámaras vuelve a ser el correcto...”*. Que la empresa instaladora afirma en su informe que *“procedió a verificar la fecha desde la que las cámaras se encuentran desplazadas y corresponde según las grabaciones al día 26 de enero de 2008”*. Adjunta informes al respecto.
- Que en fecha 5 de marzo de 2008, fue necesario nuevamente recolocar la posición de las cámaras desplazadas. Adjunta informe de la empresa instaladora.



- Se adjunta peritaje realizado por ingeniero técnico industrial en el que certifica *“que la única forma posible para que las cámaras pierdan la orientación de instalación, es la manipulación directa o golpes...”*.
- Que ante la imposibilidad de mantener las cámaras en posición correcta más de 5 días seguidos, procedió a desactivar completamente el circuito de grabación, manteniendo las cámaras como medida disuasoria.
- Que la medida de instalación de las cámaras fue necesaria, idónea y proporcional para la protección y seguridad de la entidad denunciada.
- Que si bien en el momento de la inspección, una de las cámaras enfocaba una parte sustancial de la acera, éste hecho se debe a una manipulación intencionada por terceros o a un desplazamiento fortuito.
- Que ha cumplido lo dispuesto en el artículo 3 y 6 de la Instrucción 1/2006.
- Que se ha cumplido con el artículo 4 de la LOPD, relativo a que los datos de carácter personal recogidos han sido adecuados, pertinente y no excesivos, en relación al ámbito y la finalidad perseguida.
- Por último solicita en el caso de no proceder al archivo de las actuaciones que se le aplique el artículo 45.5 de la LOPD en base a la existencia de un riesgo cierto para la integridad física de las personas y la seguridad de los bienes jurídicos a proteger, a la insuficiencia de medidas alternativas a la utilización de las videocámaras, a la búsqueda de asesoramiento de profesionales en materia de sistemas de seguridad, a la inscripción de ficheros con carácter previo a la puesta en funcionamiento de las cámaras, al cumplimiento del artículo 5 de la LOPD y 3 de la Instrucción 1/2006, a la instalación de elementos adicionales de seguridad para custodiar las grabaciones y la disposición colaboradora y de buena fe de la entidad denunciada.

QUINTO: En fecha 6 de junio de 2008, se recibe escrito de ratificación de los denunciantes, adjuntando listado de firmas de vecinos y visitantes de la (C/.....) y (C/.....) que manifiestan su oposición a la cámaras de videovigilancia instaladas en la (C/.....) y (C/.....).

SEXTO: Transcurrido el plazo de alegaciones, por parte de la instructora del procedimiento se inició el período de práctica de pruebas, dando por reproducidas las actuaciones previas de investigación E/01063/2007, desarrolladas por los Servicios de Inspección de esta Agencia Española de Protección de Datos, así como las alegaciones y documentos presentados.



SÉPTIMO: En fecha 29 de julio de 2008, 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 Wajal Canarias S.L., con multa de 6.000 euros (seis mil 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.

OCTAVO: En fecha, 16 de septiembre de 2008, D. D.D.D., en representación de Wajal Canarias S.L., presentó escrito de alegaciones a la Propuesta de Resolución, argumentando, en síntesis, lo siguiente:

- Solicita una graduación inferior de la sanción aplicando el artículo 45.4 de la LOPD, en base a las limitaciones técnicas del sistema de videovigilancia instalado, a la eliminación de las imágenes en períodos no superiores a 5 días, a la ausencia de beneficios obtenidos, al grado de intencionalidad que fue el salvaguardar la integridad de las personas e inmuebles de la empresa, a la falta de reincidencia y a los daños y perjuicios causados a las personas interesadas y a terceras personas.

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

HECHOS PROBADOS

PRIMERO: En fecha 30 de mayo de 2007, tiene entrada en esta Agencia escrito de denuncia a la entidad Wajal Canarias S.L., relativa a la instalación de sistemas de videovigilancia en la vía pública, adjuntando fotos al respecto. (Folios 1 a 9).

SEGUNDO: Los inspectores de esta Agencia verificaron en fecha 31 de enero de 2008, la existencia de dos cámaras de videovigilancia en las fachadas del inmueble denunciado. La primera videocámara estaba ubicada en la fachada que da a la (C/.....) y la segunda en la fachada de la (C/.....). Las imágenes captadas por ambas cámaras son en color, no siendo posible modificar de forma automática la direccionalidad de los objetivos, ni hacer acercamientos con los mismos. (Folio 13)..

TERCERO: Según consta en Acta, ambas cámaras captan imágenes de la vía pública y de la acera situada inmediatamente frente al edificio. Estas imágenes se visualizan en color y las personas que transitan por la vía pública podrían ser identificables. (Folio 13,16).

CUARTO: El dispositivo grabador tiene capacidad máxima de 160 Gb, estando configurado para realizar una grabación a la máxima calidad y con un ratio de 9 imágenes por segundo. El sistema está configurado para que en el momento en el que alcance el tamaño máximo del sistema de almacenamiento, se procede a la regrabación sobre el mismo fichero. Se comprueba que la última grabación corresponde al 26 de enero de 2008.(Folio 13).



QUINTO: El sistema de grabación se encuentra instalado en un cuarto del edificio con puerta de seguridad y cerrado con llave.(Folio 13, 113).

SEXTO: Se verifica la existencia de varios carteles informativos en las puertas y escaparates de las entradas en ambas calles. Estos carteles se corresponden a los modelos propuestos en la Instrucción 1/2006 de la Agencia Española de Protección de Datos. (Folios 3, 4 y 13).

SÉPTIMO: Comeralse S.L., fue la entidad encargada del suministro e instalación del sistema de videovigilancia. Esta empresa está debidamente homologada en el R.E.S., con el número *+*+. Con dicha empresa suscribió la entidad denunciada el debido contrato de prestación de servicios, siendo éste debidamente registrado en la Comisaría de Policía, con número de contrato 566 (Folio 13, 106,111,112).

OCTAVO: El motivo de la instalación del sistema de videovigilancia fueron varios altercados con vecinos de la zona que aconsejaron, según manifestación del denunciado, la protección de la integridad del edificio. (Folio 12)

NOVENO: Consta inscrito en fecha 23 de mayo de 2007, en el Registro General de Protección de Datos de esta Agencia , el fichero denominado “ Videocámaras de vigilancia”, figurando como responsable del mismo Wajal Canarias S.L.(Folios 18 a 23).

FUNDAMENTOS DE DERECHO

I

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

II

Con carácter previo, debe señalarse que 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.

III

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;”.

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 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 31 de enero de 2008, se constató que las cámaras ubicadas en ambos lados de la fachada del edificio propiedad de la entidad denunciada grababan imágenes de la vía pública pudiendo identificarse a las personas que por ella transitaban, por



cuanto ésta era la finalidad de la instalación, el controlar los accesos y fachada del edificio de la entidad denunciada.

IV

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”.

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, las cámaras ubicadas en la fachada exterior del establecimiento Wajal Canarias S.L., grababan imágenes de los viandantes sin que tuvieran autorización administrativa al respecto, puesto que como ya se ha establecido “ut supra”, la instalación de cámaras en la vía pública es competencia exclusiva de los Fuerzas y Cuerpos de Seguridad del Estado.

V

En cuanto a la alegación del representante de la entidad demandada relativa al carácter proporcional, idóneo y necesario de la medida de instalación de cámaras de videovigilancia 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.

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

En este sentido, el citado Dictamen 4/2004, del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre 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, relativo al tratamiento de datos personales mediante vigilancia por videocámara, apartado D), 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”.

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

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

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

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



La aplicación de estos principios resulta especialmente relevante, dado que la instalación de dicho sistema de seguridad debe ser como consecuencia de que se hayan producido en repetidas y numerosas ocasiones determinadas conductas violentas.

Así para el efectivo cumplimiento de los principios indicados, en especial los relativos a la proporcionalidad, finalidad de los medios utilizados para el servicio de videovigilancia, se debe señalar que en aquellos casos en los que los dispositivos instalados tengan la capacidad de captar o registrar tanto imágenes como sonidos mediante técnicas desproporcionadas para la finalidad del tratamiento, como podrían ser dispositivos móviles, direccionables, de ampliación de imágenes o posibilidad de enfoque de imágenes ajenas a la finalidad concreta y específica de videovigilancia, sin que de ningún modo la videovigilancia afecte a la vía pública, puesto que en ese caso la competencia es exclusiva de los Cuerpos y Fuerzas de Seguridad del Estado de conformidad con lo dispuesto en la Ley Orgánica 4/1997, el responsable de tales tratamientos deberá responder de la responsabilidad que en su caso incurra.

Asimismo, en el preámbulo de la citada Instrucción 1/2006, señala lo siguiente: *“En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.*

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

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

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones <<si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

El principio de moderación en el uso de datos personales, debería aplicarse en todos los sectores, teniendo en cuenta, también el hecho de que muchos objetivos pueden alcanzarse realmente sin recurrir a datos personales.



En consecuencia cualquier medida que permita preservar la seguridad, sin necesidad de implementar sistemas de videovigilancia, deberá de aplicarse con preferencia. Asimismo de existir con anterioridad medidas que garanticen la seguridad sin necesidad de acudir a sistemas de videovigilancia y aquellas resulten eficaces, deberá prevalecer el mantenimiento de dichas medidas, en aras de proteger la intimidad de las personas.

Respecto a 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 cumplir con 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 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 caso que nos ocupa, la entidad denunciada alega que el motivo de la instalación del sistema de videovigilancia, fue consecuencia de varios altercados que se produjeron con motivo de la edificación del inmueble, que aconsejaron su instalación, para proteger la integridad del edificio, aportando sentencias relativas a diversos altercados en materia inmobiliaria con vecinos de la zona. Este hecho podría justificar la instalación del sistema de videovigilancia, ahora bien, de acuerdo a la normativa y jurisprudencia enunciada, existen otros métodos menos intrusivos para la intimidad de las personas antes de proceder a la instalación de cámaras de videovigilancia. Ciertamente es, como se ha podido acreditar con la aportación de documentos de la entidad demandada, que antes de proceder a la instalación del sistema de videovigilancia, procedió a la contratación de un servicio de seguridad privada del inmueble durante un periodo corto de tiempo, pero en ningún caso puede considerarse la instalación de dicho sistema de videovigilancia proporcional, desde el momento que se acredita por el Acta de Inspección de esta Agencia de fecha 31 de enero de 2008, que la visualización que se produce de la vía pública es excesiva en relación con la finalidad que ha justificado su instalación, por cuanto no sólo capta las puertas principales y ventanas del edificio sino que también graba imágenes de la vía pública, hasta la acera situada inmediatamente frente al edificio.

La entidad denunciada afirma que efectivamente en el momento de la inspección por parte de esta Agencia, una de las cámaras enfocaba una parte sustancial de la acera “*de manera tangencial y con mínima intervención sobre terceros*”. Esta “*mínima intervención*” como afirma la entidad denunciada, no puede ser tal desde el momento, en el que se constata de la información recogida tanto del Acta de Inspección de esta Agencia, como de los informes elaborados por la empresa instaladora de seguridad Comeralse S.L., de fecha 25 de mayo de 2007, 11 de febrero de 2008 y 6 de marzo de 2008, que ambas cámaras enfocaban y recogían imágenes fuera del ángulo permitido legalmente. Así los informes de la empresa de seguridad



afirman que han procedido a la reubicación de las cámaras al encontrarse éstas desplazadas un poco del ángulo permitido. En el informe de dicha empresa de seguridad de fecha 25 de mayo de 2007 y 25 de mayo de 2008 afirman que dicho desplazamiento podría haberse producido posiblemente por vibraciones provocadas por la obras cercanas al mismo, declinando toda responsabilidad de los desplazamientos de los enfoques de dichas cámaras.

En cuanto a las posibles causas de estos desplazamiento, el peritaje realizado en fecha 2 de junio de 2008, por un ingeniero técnico industrial, afirma que “la única forma posible para que las cámaras pierdan la orientación de instalación, es la manipulación directa o golpes” y *“que los soportes y fijaciones de las cámaras son los adecuados y no permiten el movimiento accidental de las cámaras, sin, como ya se menciona anteriormente, se manipulen directamente”*.

VI

Se imputa a Wajal Canarias S.L., la comisión de 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 comercial, 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”.

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, 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.

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 procedimiento, el denunciado capta datos personales. Dichas imágenes, capturadas constituyen datos personales, y por tanto sometidos al consentimiento de sus titulares, de conformidad con lo dispuesto en el artículo 6.1 de la LOPD.

El artículo 3 de la LOPD define en su apartado h), lo siguiente :

“h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”.

Por lo tanto, el consentimiento del interesado para el tratamiento de sus datos debe ser *“informado”, “específico”, “inequívoco” y “libre”*, o bien, que no sea necesario tal consentimiento al contar el sistema de videovigilancia de habilitación legal conforme dispone el segundo inciso del citado artículo 6.1 de la LOPD.

En relación con el segundo inciso del artículo 6.1 de la LOPD, tampoco ha quedado acreditado que el sistema de videovigilancia de Wajal Canarias S.L., estuviera acogido a las disposiciones de la Ley Orgánica 4/1997, de 4 de agosto, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, por lo que el tratamiento de los datos recogidos en la vía pública carecía de habilitación legal.

VII

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, la entidad Wajal Canarias S.L., 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 con su consentimiento, lo que supone una vulneración de este principio, conducta que encuentra su tipificación en este artículo 44.3.d).

VIII

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 entidad denunciada, solicita en su caso, la aplicación del artículo 45.5 de la LOPD, en base a que los hechos parten de una situación de riesgo para la integridad física de las personas y bienes; que procedieron antes de la instalación de las videocámaras a la contratación de empresa de seguridad, a la instalación de carteles informativos, a la inscripción de ficheros y colaboraron con los inspectores de esta Agencia, dando muestra de la buena fe en todas las actuaciones de la entidad denunciada.

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

En relación con la aplicación del artículo 45.5 de la LOPD, la Audiencia Nacional ha señalado, entre otras, en Sentencia de 27/10/2004, que “el citado precepto concreta el principio de proporcionalidad (reconocido para el Derecho administrativo sancionador, con carácter general, en el art. 131.3 de la Ley 30/1992), permitiéndose la disminución en un grado de la sanción aplicable en casos de cualificada disminución de la culpa o de la antijuridicidad. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en 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 de justicia (art. 1.1 CE), por excepción, en casos muy extremos (de aquí la expresión “especialmente cualificada”) y concretos. Pues bien, en el caso de autos, la Sala entiende que dicho precepto no es de aplicación porque a la antijuridicidad no obsta la falta de intención de infringir las normas jurídicas (Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 4 de junio de 1999), y ya hemos razonado la falta de diligencia de la entidad recurrente”.

En el presente caso, ha quedado acreditado que la entidad Wajal Canarias S.L., tenía instaladas dos cámaras de videovigilancia en la fachada del inmueble, que recogía imágenes de la vía pública, superando el principio de proporcionalidad, establecido en materia de protección de datos. Si bien, dicha entidad antes de proceder a la instalación del sistema de videovigilancia, formalizó mediante contrato con una empresa de seguridad debidamente homologada, la instalación y mantenimiento de las videocámaras, instaló los carteles informativos conformes a la Instrucción 1/2006 y procedió a la inscripción del fichero de videovigilancia., lo que denota una diligencia en su actuación, que permite apreciar una cualificada disminución de la culpabilidad existente en la concreta actuación infractora. Asimismo la empresa denunciada, al ser informada, por la empresa de seguridad en sus diferentes intervenciones para reubicar las cámaras a la posición correcta, que dichos desplazamientos podrían deberse a la vibraciones ocasionadas por las obras cercanas, no haciéndose responsable de estos hechos, procedió a la desactivación



del circuito de grabación. Por todo ello, procede la aplicación del artículo 45.5 de la LOPD.

Por otro lado, la entidad denunciada solicita una atenuación de la sanción basada en los criterios establecidos en el artículo 45.4 de la LOPD. A este respecto hay que apreciar que el sistema de videovigilancia instalado no dispone de la posibilidad de acercar la imagen, siendo el circuito cerrado y directo, las imágenes se conservan por un mínimo de tiempo. Así mismo dichas imágenes eran enviadas a un monitor que se encontraba en una habitación con puerta de seguridad cerrada. Todo ello unido a la ausencia de beneficios obtenidos y a la ausencia de intencionalidad apreciadas en el presente procedimiento procede imponer la sanción en la cuantía de 601,01 euros.

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 **WAJAL CANARIAS, S.L.**, por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3. d) de dicha norma, una multa de 601,01 € (seiscientos un euro con un céntimo de euro de conformidad con lo establecido en el artículo 45.2. 4 y 5 de la citada Ley Orgánica.

SEGUNDO: NOTIFICAR la presente resolución a **WAJAL CANARIAS, S.L.** con domicilio en (C/.....) y a **D. R.R.R.** con domicilio en (C/.....), **D. L.L.L.** con domicilio en (C/.....), **D^a G.G.G.** con domicilio en (C/.....)

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 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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



a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

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

Madrid, 24 de septiembre de 2008

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte