GUÍA DE VIDEOVIGILANCIA

Agencia de Protección de Datos de la Comunidad de Madrid

Agencia de Protección de Datos
de la Comunidad de Madrid

C/ Cardenal Marcelo Spínola, 14
28016 Madrid
Teléfonos: +34-91-580.28.74 / 28.75
Fax: +34-91-580.28.76

apdcm@madrid.org
www.apdcm.es

Comunidad de Madrid

ÍNDICE DE CONTENIDOS

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

4.- SUPUESTOS ESPECÍFICOS

5.- VIDEOVIGILANCIA EMPRESARIAL

6.- INFORMES JURÍDICOS DE LA APDCM

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

6.5.- Instalación de cámaras de videovigilancia en el servicio de transportes de viajeros por carretera.

6.6.- Existencia de regulación normativa o jurisprudencia en base a la cual el Alcalde o Pleno del Ayuntamiento pueden resolver o acordar la prohibición de grabación con cámara de los Plenos municipales.

6.7.- La grabación de las sesiones del Pleno de un Ayuntamiento con el fin de crear un archivo histórico que complemente el resto de la documentación referida a las sesiones constituye un fichero de datos de carácter personal.

6.8.- Implantación de un sistema de control de videocámaras en los calabozos de las dependencias de la policía local de un Ayuntamiento.

6.9.- Implantación de un sistema de control de tráfico por medio de cámaras en el término municipal de un Ayuntamiento.

7.- JURISPRUDENCIA

7.1.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 12 de noviembre de 2010 sobre el cumplimiento de la normativa de protección de datos en materia de videovigilancia.

7.2.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de febrero de 2011 sobre instalación de cámaras en la vía pública.

7.3.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 27 de mayo de 2010 sobre tratamiento de imágenes sin cumplir la LOPD.

7.4.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 17 de junio de 2011 sobre la aplicación de la nueva figura del apercibimiento en una sanción impuesta por la AEPD por instalar una cámara en su plaza de garaje de una comunidad de vecinos.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

7.5.- Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Galicia sobre la instalación de cámaras en la vía pública. Analiza la falta de justificación y proporcionalidad para instalarlas.

7.6.- Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid de 10 de diciembre de 2010 sobre cumplimiento de los trámites normativos en la creación de ficheros de videovigilancia de varios Institutos de Educación Secundaria.

7.7.- Sentencia de la Sala Contencioso-Administrativo de la Audiencia Nacional de 3 de febrero de 2011 sobre instalación de una cámara en la terraza de un bar.

8.- BUENAS PRÁCTICAS

8.1.- "Documento de política de privacidad".

8.2.- Documentos de otras autoridades de control.

8.2.1.- Guía de videovigilancia del Supervisor Europeo de Protección de Datos.

8.2.2- Informes del Grupo del Artículo 29.

8.2.3.- Guía sobre videovigilancia en el sector privado. Autoridad de Protección de Datos de Canadá.

8.2.4.- Guía sobre videovigilancia en el sector público: utilización por la policía y otros organismos de control. Autoridad de Protección de Datos de Canadá.

8.2.5.- Código de videovigilancia de la Autoridad de Protección de Datos del Reino Unido.

8.2.6.- Decisión sobre videovigilancia de la Autoridad de Protección de Datos de Italia, adoptada el 8 de abril de 2010.

8.2.7.- 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.

8.2.8.- Guía de Videovigilancia de la Agencia Española de Protección de Datos.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

8.2.9.- Plan Sectorial de Oficio de Videocámaras en Internet. Agencia Española de Protección de Datos.

8.2.10.- Instrucción 1/2009, de 10 de febrero, de la Autoridad Catalana de Protección de Datos sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

9.- LECCIONES RÁPIDAS SOBRE VIDEOVIGILANCIA

10.- SERVICIOS DE LA APDCM

11.- BIBLIOGRAFÍA RECOMENDADA SOBRE VIDEOVIGILANCIA

12.- ANEXO:

Instrucción 1/2007, de 16 de mayo, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

1.- PRESENTACIÓN

En los últimos años estamos asistiendo a la proliferación de la instalación de cámaras de videovigilancia cuya finalidad principal es garantizar la seguridad, si bien en ocasiones pueden utilizarse para otros fines, entre los que se encuentran el control del tráfico, el acceso a zonas restringidas, la vigilancia empresarial y la asistencia sanitaria. La instalación de estos sistemas supone realizar un balance de intereses entre el derecho a la protección de datos personales y el derecho a la seguridad, puesto que el tratamiento de la imagen de una persona supone la aplicación de la normativa de protección de datos personales, ya que la imagen es un dato de carácter personal relativo a una persona identificada o identificable.

En ocasiones es aplicable, además, diversa legislación sectorial, en función de los actores que intervengan, como puede ser el uso por parte de las Fuerzas o Cuerpos de Seguridad del Estado o por las empresas de seguridad privada, o de los sectores afectados, como sería la regulación en el ámbito de los bancos y las competiciones deportivas.

Dado que los tratamientos de datos personales de imágenes captadas a través de estos dispositivos se han hecho cada vez más comunes y debido a su especial naturaleza, que no encaja en el concepto tradicional de fichero, se hizo necesaria la publicación por parte de la APDCM de una instrucción que clarificara la situación y precisara las obligaciones de las instituciones que recurran a estos sistemas de vigilancia.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Con este motivo, en el año 2007 la APDCM elaboró y aprobó la Instrucción 1/2007, de 16 de mayo, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, con la finalidad de disciplinar y acomodar estos sistemas a las exigencias derivadas del derecho a la protección de datos de carácter personal, haciendo más racional y ordenada la captación, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesión de las imágenes de las personas físicas realizados por los Órganos y Administraciones Públicas de la Comunidad de Madrid.

Tras la entrada en vigor de la citada Instrucción 1/2007, habiendo elaborado diversos informes jurídicos sobre el uso de la videovigilancia y fruto de la experiencia acumulada durante estos años, la APDCM considera conveniente y adecuado la publicación de la presente Guía, que sirva de soporte a los responsables de ficheros así como los encargados de tratamiento del ámbito competencial de esta Agencia para cumplir con la normativa de protección de datos cuando se decida la utilización de estos sistemas.

Además de exponer cuáles son estos requisitos de obligado cumplimiento, la Guía de la APDCM también recoge diversa información que puede ser muy útil para los responsables, como es la utilización de un "check-list" para saber si se están cumpliendo todos los requisitos que impone la normativa de protección de datos con carácter previo al funcionamiento de las cámaras.

También hemos incluido un apartado analizando la normativa aplicable en diferentes ámbitos, por ejemplo el uso en los espacios y áreas públicas o en los centros educativos, extractos de informes jurídicos emitidos por la APDCM sobre videovigilancia y sentencias de los tribunales.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Por último, siguiendo la línea del resto de Guías que ha publicado esta Agencia, se alude a las "Buenas prácticas", con la inclusión del llamado "Documento de política de privacidad" así como menciones a documentos elaborados por otras Autoridades de Control, un apartado novedoso de curiosidades titulado "Lecciones rápidas sobre videovigilancia" y bibliografía recomendada en esta materia.

Para finalizar, sólo espero que esta Guía sea de gran utilidad para sus destinatarios y que utilicen la misma con el fin de adecuar los tratamientos mediante estos sistemas y que de esta forma se garantice el derecho fundamental a la protección de los datos personales de los ciudadanos de esta Comunidad Autónoma.

Santiago Abascal Conde
Director de la Agencia de Protección de Datos de la Comunidad de Madrid

2.- APROXIMACIÓN A LA VIDEOVIGILANCIA DESDE LA ÓPTICA DE PROTECCIÓN DE DATOS PERSONALES

El Grupo del Artículo 29 de Protección de Datos, creado al amparo de la Directiva 95/46, estableció los principios aplicables al tratamiento de datos personales mediante cámaras de videovigilancia en el Informe 67/2002[1]. Posteriormente, publicó una nueva versión mediante el Informe 89/2004[2]. A través de los citados documentos el Grupo fija la postura, que sería posteriormente implementada en el resto de países de la Unión Europea, de aplicar los principios de la Directiva 95/46 en la grabación de las imágenes de personas físicas identificadas o identificables mediante el uso de los sistemas de videovigilancia.

Los citados documentos del Grupo del Artículo 29 analizan diversas cuestiones como son los fines de la videovigilancia, las obligaciones del responsable del fichero, el período de cancelación de imágenes, el principio de proporcionalidad, los derechos de los ciudadanos –sobre todo el derecho de acceso y el derecho de información-, y las medidas de salvaguarda, como es la prohibición de utilizar las cámaras con el único fin de grabar datos –o imágenes- referentes al origen racial, hábitos sexuales, opiniones políticas o religiosas.

En cuanto a la regulación existente en nuestro ordenamiento jurídico, debemos partir en primer lugar del concepto de dato de carácter personal que recoge el artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD). Así, su apartado a) define "Datos de carácter personal" como "Cualquier

[1] Ver resumen de este documento en el apartado 8.2.2 Informes del Grupo del Artículo 29 de esta Guía.

[2] Ver resumen de este documento en el apartado 8.2.2 Informes del Grupo del Artículo 29 de esta Guía.

información concerniente a personas físicas identificadas o identificables". Más preciso se muestra el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD, cuyo artículo 5 f) dice que "Dato de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".

En este sentido, se considerará identificable una persona cuando su identidad pueda determinarse mediante la captación, grabación, transmisión, conservación o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o a través del tratamiento que resulte de los datos personales relacionados con dichas imágenes. Es decir, mediante estas operaciones se produce un tratamiento de datos personales, independientemente de que se realice a través de soportes físicos de carácter digital o mediante soportes analógicos.

Por lo tanto, partiendo de que la imagen es un dato de carácter personal, se aplicará la LOPD a la recogida y tratamiento de la citada imagen mediante el uso de la videovigilancia. Al objeto de asegurar un cumplimiento adecuado de la LOPD y con la intención de resolver las dudas al respecto, las Autoridades de Control han aprobado instrumentos normativos. Así, nos encontramos con los siguientes:

- 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[3].
- Instrucción 1/2007, de 16 de mayo, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de

[3] Ver resumen de este documento en el apartado 8.2.7 de esta Guía.

sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid[4].

- Instrucción 1/2009, de 10 de febrero, de la Autoridad Catalana de Protección de Datos, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia[5].

Además del respeto de los principios de protección de datos regulados por la LOPD y por los instrumentos normativos citados anteriormente, debemos tener en consideración la aplicación de la normativa sectorial, que establecerá diferentes obligaciones en función del ámbito y los agentes implicados. Entre esta normativa podemos destacar:

- Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana.
- Ley 23/1992, de 30 de julio, de Seguridad Privada.
- 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.
- Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte.
- Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.
- Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte.
- Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores.

[4] Puede consultar el contenido íntegro de esta norma en el Anexo de esta Guía.
[5] Ver resumen de este documento en el apartado 8.2.10 esta Guía.

- Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio.

Especial consideración merece esta última, la Ley 25/2009, de 22 de diciembre, conocida con el nombre de "Ley Omnibus", que ha liberalizado el servicio que prestan las compañías de seguridad privada, de manera que la contratación de éstas ya no será necesaria para instalar y utilizar los sistemas de videovigilancia, salvo que dicho sistema esté conectado a una central de alarmas.

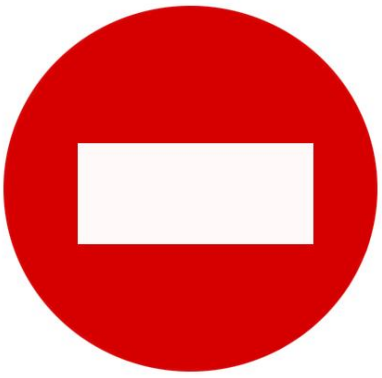
Otro de los elementos importantes sobre la videovigilancia son los fines para los cuales puede ser utilizada la misma. Estos fines se pueden clasificar en dos grupos, por una parte, la seguridad y por otra los llamados otros fines. A su vez, encontramos varios supuestos de cada uno de ellos. A modo de ejemplo podemos citar los siguientes:

- 1.- Seguridad.
    - Protección de personas físicas.
    - Protección de edificios.
        - Edificios públicos.
        - Edificios privados.
        - Escuelas, Institutos y Universidades.
        - Hospitales.
        - Hoteles.
        - Joyerías.
        - Casinos.
        - Aeropuertos.
        - Bancos
    - Detención, prevención y control de delitos y faltas.

- Vigilancia de plazas y calles.
- Control de eventos deportivos.

- 2.- Otros fines.
  - Control de la prestación laboral.
  - Disciplina de tráfico y seguridad vial.
  - Control de acceso de vehículos a zonas delimitadas o de estacionamiento regulado.
  - Monitorización de pacientes.
  - Telemedicina.
  - Investigación.
  - Turísticos.

No obstante lo anterior y relacionado con estos fines, tanto las Autoridades de Control como la jurisprudencia han delimitado una serie de supuestos en los que no se puede utilizar la videovigilancia, ya que su uso sería desproporcional en relación con su finalidad. Entre estas prohibiciones destacan las siguientes:



-En baños y aseos.

-Salas para cambiarse la ropa en el trabajo.

-Captación de imágenes para finalidad de marketing (por ejemplo, en un centro comercial usar las cámaras para conocer los hábitos de consumo y poder influir en las posibles ventas de productos).

Por otra parte, y como hemos mencionado anteriormente, sin perjuicio de la normativa específica, cuando un responsable de fichero decide instalar un sistema de videovigilancia debe cumplir con los principios de protección de datos de carácter personal. En el siguiente apartado, analizaremos qué principios deben ser cumplidos y cómo realizar su efectivo cumplimiento. Además, en el caso de que exista un encargado de tratamiento, es decir, un tercero contratado para vigilar y custodiar las imágenes, la relación entre responsable y encargado conllevará también otra serie de obligaciones.

A modo de resumen, estos son los principios de protección de datos que deben ser cumplidos:

- Creación e inscripción del fichero de videovigilancia.
- Principio de calidad de los datos personales.
- Principio del consentimiento.
- Derecho de información.
- Derechos ARCO.
- Cesiones de datos de carácter personal.
- Contrato del artículo 12 de la LOPD si existe un encargado.
- Medidas de seguridad.

La imagen es un dato de carácter personal.

La videovigilancia supone la aplicación de los principios de la LOPD.

Los sistemas de videovigilancia pueden ser utilizados para diversos fines.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

3.- OBLIGACIONES DEL RESPONSABLE DEL FICHERO

3.1.- El responsable del fichero

En primer lugar, tenemos que definir quién podría ser el responsable del fichero. La APDCM tiene fijado su ámbito de control y actuación en la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid. Según el apartado 2 de esta Ley, la APDCM ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por:

- Administración de la Comunidad de Madrid.
- Administración Institucional de la Comunidad de Madrid (excepto las Sociedades Anónimas).
- Entes que forman parte de la Administración Local.
- Universidades públicas.
- Corporaciones de derecho público en el ejercicio de funciones públicas:
    - Colegios profesionales.
    - Cámara de Comercio e Industria.
    - Cámara Agraria.

Este precepto de la Ley 8/2001 de 13 de julio hay que ponerlo en relación con la Norma Primera de la Instrucción 1/2007, de la APDCM sobre videovigilancia, en virtud de la cual, se entenderá que el tratamiento mediante el uso de un sistema de videovigilancia está bajo el control de la APDCM cuando la instalación se lleve a cabo en edificios, instalaciones o bienes inmuebles afectados a un uso o servicio público cuya vigilancia y protección se encuentren atribuidas legalmente a los responsables citados anteriormente, de acuerdo a lo establecido por el artículo 148.1.22 de la Constitución española y por el

artículo 26.1.27 de la Ley Orgánica 3/1983, de 25 de febrero, de Estatuto de Autonomía de la Comunidad de Madrid.

Además, también se considera sometido al control de esta Agencia el uso de estos sistemas por parte de la Policía local de los Ayuntamientos de la Comunidad de Madrid.

Ejemplos de responsables de ficheros de videovigilancia:

Los hospitales de la Comunidad de Madrid

Las secretarías generales técnicas de cada una de las Consejerías

El servicio regional de bienestar social respecto a los sistemas instalados en las residencias de mayores

Los ayuntamientos de la Comunidad de Madrid

Asimismo, puede darse el caso de que un sistema de videovigilancia tenga varios responsables del fichero. Este supuesto tiene lugar, por ejemplo, cuando existe un sistema instalado en un edificio que es utilizado por órganos administrativos diferentes.

3.2.- Legitimación

Dos son las cuestiones que tiene que analizar un responsable previamente a la instalación de un sistema de videovigilancia: si está legitimado para ello y si el sistema es proporcional (a esto último nos referiremos en el siguiente punto).

Entre las diferentes formas de legitimación, destaca la posibilidad de que las imágenes se recojan para el ejercicio de las funciones propias de las Instituciones, Órganos, Organismos y demás Entes y Entidades de la Comunidad de Madrid en el ámbito de sus competencias, no sólo con fines de vigilancia para la seguridad, sino también con la

finalidad de control y disciplina del tráfico -circulación de vehículos a motor y seguridad vial al objeto de controlar el acceso de vehículos a zonas especialmente delimitadas o de estacionamiento regulado, establecimiento de sistemas de aforo del tráfico- y con la finalidad de prestación de un determinado servicio público o del cumplimiento de funciones públicas de soberanía.

Además, se establecen supuestos concretos de legitimación para el tratamiento de imágenes con fines sanitarios y asistenciales para el diagnóstico y tratamiento a distancia de enfermedades a través de técnicas de telemedicina o con fines de monitorización de pacientes en Unidades Médicas de Cuidados Intensivos.

Asimismo, entre otros supuestos concretos, se recogen los tratamientos de imágenes con fines históricos, estadísticos y científicos, así como la realización de tratamientos de imágenes con fines de investigación y/o docencia.

También se reputará legítima la utilización de sistemas de cámaras o videocámaras:

a) Cuando el tratamiento de la imagen tenga por objeto el seguimiento, control y garantía del cumplimiento de la relación laboral, funcionarial o estatutaria.
b) Cuando el tratamiento de la imagen se realice en el marco de una relación jurídica derivada del sometimiento del afectado a una relación administrativa de sujeción especial.
c) Cuando el tratamiento de la imagen se dirija a la mejora en la calidad de la gestión de los servicios públicos.
d) Cuando se realice cualquier otro tratamiento que resulte necesario para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa, vinculada al ámbito competencial del responsable del tratamiento en el ejercicio de sus funciones.

El uso de cámaras para controlar la prestación laboral de un trabajador debe ser utilizado de manera muy excepcional.

La APDCM recomienda en este supuesto utilizar cualquier otro medio que sea menos intrusivo para el trabajador.

Otro supuesto que regula de manera específica la Instrucción 1/2007 de la APDCM es cuando el tratamiento de la imagen del afectado o, en su caso, el tratamiento de cualquier otro dato de carácter personal realizado mediante sistemas de cámaras o videocámaras por las Instituciones, Órganos, Organismos y demás Entes y Entidades a las que se refiere esta Instrucción, se realice por profesionales sanitarios sujetos al secreto profesional o por otras personas sujetas a una obligación equivalente de secreto, y:

a) Tenga por objeto proteger el propio interés vital del afectado o el de otra persona.
b) Resulte necesario para la prevención o para el diagnóstico médico, incluida la evaluación y diagnóstico médicos a distancia mediante la Telemedicina.
c) Tenga por objeto la prestación de asistencia sanitaria o tratamientos médicos, incluido el tratamiento a distancia a través de la Telemedicina.
d) Se realice mediante la monitorización de pacientes en Unidades Médicosanitarias y especialmente en Unidades de Cuidados Intensivos.
e) Tenga por objeto la gestión de los servicios sanitarios.
f) Resulte necesario para solucionar una urgencia médica o para realizar estudios epidemiológicos en los términos establecidos en la legislación estatal o autonómica sobre sanidad.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

En el caso de las Fuerzas y Cuerpos de Seguridad, cuando tenga por objeto el mantenimiento de la seguridad pública que legalmente les corresponda en relación con las siguientes competencias:

a) La protección y custodia de autoridades, edificios, instalaciones, dependencias, infraestructuras y equipamientos cuando lo tengan legalmente atribuido, así como la colaboración con las Administraciones competentes en materia de seguridad.
b) En colaboración con las Administraciones competentes, cuando lo tengan legalmente atribuido, la prevención, mantenimiento y restablecimiento de la seguridad ciudadana y tratar de garantizarla en lo referente a aquellos actos que ocasionen molestia social o daños sobre bienes y personas en la vía pública.
c) El ejercicio de las competencias que en materia de policía administrativa y policía de seguridad les atribuya la normativa estatal, así como, en su caso, la denuncia en las materias de policía administrativa especial de competencia estatal.
d) El ejercicio de las competencias que en materia de policía judicial les atribuya la normativa estatal.

La videovigilancia puede utilizarse para diferentes finalidades: Seguridad, control del tráfico, vigilancia de la vía pública, asistencia sanitaria, control de zonas reguladas de accesos de vehículos, vigilancia y excepcionalmente control del cumplimiento de la prestación laboral.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

3.3.- Informe de proporcionalidad

Con carácter previo a la instalación de un sistema de videovigilancia el responsable del fichero debe ponderar los bienes jurídicos protegidos, es decir, analizar si no es posible alcanzar el fin perseguido con la citada instalación mediante la adopción de otros medios que sean menos intrusivos para la protección de datos de carácter personal. Esto supone aplicar consecuentemente el principio de proporcionalidad.

De esta forma, la proporcionalidad se constituye como un elemento fundamental en la instalación de los sistemas de videovigilancia, ya que en ocasiones se vulnera este principio originando situaciones abusivas. No sólo nos estamos refiriendo a aquellos supuestos en que se han colocado cámaras en sitios que no está permitido su uso, como cuartos de baño o habitaciones para que los empleados puedan cambiarse de ropa, sino también se vulnera este principio cuando se colocan más cámaras de las necesarias o se han colocado en la vía pública sin la autorización correspondiente, e incluso cuando se utilizan para otro fin que no sea el de seguridad o cualquiera de los otros fines posibles.

Para valorar este principio de proporcionalidad, la APDCM exige con carácter previo no sólo a la instalación sino a la creación del correspondiente fichero, que el responsable elabore un Informe de proporcionalidad.

Este informe, contendrá como mínimo, de conformidad a lo establecido en la Instrucción 1/2007, un análisis jurídico en el cual se evalúe:

- **Juicio de idoneidad**: si el tratamiento de datos personales a través de la videovigilancia constituye una medida susceptible de conseguir el objetivo que se pretende.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

- **Juicio de necesidad**: si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva, teniendo en cuenta la protección de los datos de carácter personal, debiendo argumentar el responsable del fichero que dicha medida es necesaria por no existir otra más moderada para la consecución de tal propósito con la misma eficacia.

- **Juicio de proporcionalidad**: si la medida adoptada es proporcional resultando equilibrada en atención a la ponderación entre la finalidad perseguida y el grado de restricción del derecho fundamental a la protección de datos de carácter personal, con expresa mención a si de la referida medida derivan más beneficios o ventajas para el interés general que perjuicios sobre la protección de datos.

Antes de instalar un sistema de videovigilancia valore si se puede conseguir el fin con otra medida menos intrusiva para los ciudadanos.
Si decide realizar la instalación deberá elaborar el "Informe de proporcionalidad" y enviarlo a la APDCM para su análisis previo.

Para facilitar la elaboración de este Informe de proporcionalidad, la APDCM además de su servicio de asesoramiento y consultoría al responsable del fichero, recomienda el uso del siguiente formulario:

INFORME DE PROPORCIONALIDAD
CON CARÁCTER PREVIO A LA
INSTALACIÓN DE UN SISTEMA DE VIDEOVIGILANCIA

Agencia de Protección de Datos de la Comunidad de Madrid

Datos del responsable del fichero
Órgano administrativo:
CIF/NIF:
Dirección:
Representante:
Nombre y apellidos:
DNI:
Finalidad de la instalación de la videovigilancia: ○ Seguridad ○ Control del tráfico ○ Control de zonas de acceso restringido
Sistema de videovigilancia: ○ Descripción del sistema: ○ Número de cámaras: ○ Zoom: ○ Cámaras fijas o móviles:
Juicio de idoneidad: *(describa que el sistema es adecuado para el fin perseguido)*
Juicio de necesidad: *(justifique que la finalidad no se puede conseguir con otra medida menos intrusiva)*
Juicio de proporcionalidad: *(describa los beneficios que conlleva la instalación de cámaras)*
Supuestos especiales: ○ Autorización de la comisión de videovigilancia ○ Tráfico
Los datos personales contenidos en este documento serán incorporados y tratados en el fichero "Registro de ficheros de carácter personal" cuya finalidad es velar por la publicidad de la existencia de los ficheros que contengan datos de carácter personal. Puede ejercitar los derechos de acceso, cancelación, rectificación y oposición ante la APDCM, Subdirección General de Consultoría y Registro de Ficheros, C/ Cardenal Marcelo Spínola 14, 14 Madrid".

Además, el principio de proporcionalidad también se aplicará en el número de cámaras que se vayan a instalar, si son fijas o móviles, y el zoom que tenga las mismas, de manera que por regla general no habrá que instalar cámaras en todos los espacios de, por ejemplo, un edificio. Es decir, las cámaras se deben instalar en aquellos espacios en los que su fin sea estrictamente necesario.

3.4.- Creación del fichero de datos de carácter personal

Con carácter previo a la puesta en funcionamiento de las cámaras de videovigilancia, y una vez que se haya justificado debidamente en el Informe de proporcionalidad la legitimación de su instalación, se debe tramitar y aprobar una disposición de carácter general mediante la cual se cree el fichero de datos de carácter personal correspondiente y proceder a su inscripción en el Registro de Ficheros de Datos Personales de la APDCM. El procedimiento para elaborar la disposición de carácter general en el ámbito competencial de la APDCM está regulado por el Decreto 99/2002, de 22 de mayo, por el que se Regula el procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales, en el cual se especifica quién es el órgano que tiene la competencia para aprobar la disposición correspondiente así como todos los trámites a seguir.

Durante esta tramitación debemos destacar lo siguiente:

- Elaborado el proyecto de disposición se abrirá una fase de alegaciones durante un plazo no inferior a quince días hábiles.
- El proyecto de disposición y las alegaciones presentadas, en su caso, se enviarán a la APDCM.

- La APDCM con toda la información elabora un informe preceptivo, pudiendo recabar toda la información que considere necesaria del responsable.

Además, el proyecto de disposición deberá incluir el siguiente contenido mínimo:

1. Nombre del fichero.
2. El órgano, ente o autoridad administrativa responsable del fichero.
3. El órgano, servicio o unidad ante el que se deberán ejercitar los derechos de acceso, rectificación, cancelación y oposición (este apartado se cumplimentará sólo en el caso de que sea diferente al responsable del fichero).
4. El nombre y la descripción del fichero que se crea.
5. El carácter informatizado, mixto o manual estructurado del fichero.
6. Las medidas de seguridad que se apliquen.
7. Los tipos de datos de carácter personal que se incluirán en el mismo.
8. La descripción detallada de la finalidad del fichero y los usos previstos del mismo.
9. Las personas o colectivos sobre los que se pretenda obtener datos o que resulten obligados a suministrarlos.
10. La procedencia o el procedimiento de recogida de los datos.
11. Los órganos y entidades destinatarios de las cesiones previstas, indicando de forma expresa las que constituyan transferencias internacionales.

A continuación un par de ejemplos ilustrativos del contenido mínimo de la disposición de carácter general por la que se cree un fichero de videovigilancia:

Contenido mínimo	Ejemplo 1	Ejemplo 2
Nombre	Videovigilancia sede Consejería de Educación	Videovigilancia
Responsable	Secretaría General Técnica	Hospital Santa Cristina
Órgano ante el cual ejercitar derechos ARCO	Subdirección General de Régimen Interior	Hospital Santa Cristina
Descripción del fichero	Seguridad y control de acceso a edificios	Videovigilancia
Carácter informatizado, mixto o manual	Informatizado	Informatizado
Medidas de seguridad	Básicas	Básico
Tipo de datos	Identificativos (imagen)	Identificativos (imagen)
Finalidad y usos	Grabación de imágenes del entorno e interior de la sede de la Consejería para garantizar la seguridad	Videovigilancia y grabación de imágenes
Personas o colectivos afectados	Empleados y ciudadanos	Empleados, ciudadanos y pacientes
Procedencia de la recogida de datos	El propio interesado	El propio interesado
Cesiones	Las previstas en la Ley	Las previstas en la ley

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Una vez que se haya emitido el informe por parte de la APDCM, se remitirá toda la documentación a la Secretaría General Técnica de la Consejería correspondiente o al órgano competente en virtud de lo dispuesto por el artículo 11 del Decreto 99/2002 para que emitan informe preceptivo. Posteriormente, la disposición de carácter general por la que se cree el fichero, una vez que haya sido aprobada, tiene que publicarse en el Boletín Oficial de la Comunidad de Madrid o Diario oficial correspondiente, debiendo comunicar esta publicación el responsable del fichero a la APDCM para proceder a la inscripción del fichero en el Registro de Ficheros de la APDCM.

La LOPD califica como una infracción grave proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos sin autorización de disposición general publicada en el Boletín Oficial o diario correspondiente.

No ponga en funcionamiento el sistema de videovigilancia si no ha aprobado la disposición de carácter general de creación del fichero y se ha publicado la misma en el Boletín Oficial que corresponda.

3.5.- El derecho de información

El responsable del fichero debe cumplir con el deber de información regulado en el artículo 5 de la LOPD, puesto que mediante los sistemas de videovigilancia se recaba y trata el dato de la imagen, que es un dato de carácter personal.

Para dar efectivo cumplimiento al deber de información y correlativo al derecho de información de los afectados, los responsables deben colocar en emplazamientos claramente visibles de las zonas videovigiladas, tantos distintivos como resulten necesarios

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

para garantizar que en todo momento los afectados conozcan la presencia de la cámara o videocámara y por consiguiente, del tratamiento de datos realizados.

No obstante, la ubicación concreta de dichos distintivos dependerá en cada caso de la naturaleza y estructura de las zonas y espacios videovigilados. Para cumplir con el derecho de información resultará admisible la utilización de un único distintivo ubicado en un espacio de acceso principal, preferentemente antes de entrar en la zona videovigilada.

Asimismo, en el supuesto de edificios divididos en plantas, será suficiente con la utilización de un único distintivo ubicado en un espacio de acceso principal, siempre y cuando dicho distintivo cumpla con la información mínima que a continuación se especifica.

Este distintivo debe cumplir con los siguientes requisitos:

- Identidad del responsable
- Mención al ejercicio de los derechos ARCO
- Finalidad de la recogida de las imágenes ("Zona videovigilada")
- Referencia a la LOPD

La Instrucción 1/2007 contiene dos tipos de carteles para cumplir con el derecho de información, ya que el contenido de los mismos es diferente en función de si las cámaras son usadas para fines de seguridad, o se utilizan para otro fin.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Además de los carteles informativos, el responsable deberá tener a disposición de los ciudadanos documentación comprensible ofrecida en cualquier soporte inteligible, en la que se proporcione la información prevista en el artículo 5.1 de la LOPD. En concreto, a través de dicha documentación, deberá informarse a los afectados de modo expreso, preciso e inequívoco:

a) De la existencia de un tratamiento de datos de carácter personal realizado por medio de cámaras o videocámaras.
b) De la finalidad de la recogida de las imágenes y de los destinatarios de dichas imágenes.
c) Del carácter obligatorio o facultativo de la captación y tratamiento de las imágenes a través de cámaras o videocámaras.
d) De las consecuencias de la obtención de las imágenes a través de las cámaras o videocámaras y de las consecuencias de la negativa a su obtención.
e) De la posibilidad de ejercitar los derechos de acceso, cancelación y oposición.
f) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Las Fuerzas y Cuerpos de Seguridad deberán cumplir con el deber de información de acuerdo a lo dispuesto en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

En ningún caso resultará exigible que los carteles informativos especifiquen el emplazamiento de las cámaras o videocámaras ni que coincidan con el lugar físico destinado a la colocación de éstas.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

3.6.- Existencia de un encargado del tratamiento

De conformidad con el artículo 12 de la LOPD, el responsable podrá contratar los servicios de otra persona física o jurídica, pública o privada, que trate los datos personales por cuenta de dicho responsable, en calidad de Encargado del tratamiento. En estos casos, no se considerará comunicación o cesión de datos el acceso del Encargado del tratamiento a las imágenes cuando dicho acceso sea necesario para la prestación de su servicio al responsable del tratamiento.

La realización de tratamientos de datos mediante cámaras o videocámaras por cuenta de terceros, deberá estar regulada en un contrato que constará por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará las imágenes conforme a las instrucciones del responsable del tratamiento, y que no las aplicará o utilizará con fin distinto al que figure en dicho contrato, ni las comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, que el Encargado del tratamiento está obligado a implementar.

Además, la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, obliga a comunicar a la APDCM este tipo de contratos con carácter previo a su perfeccionamiento. La APDCM, una vez recibido el contrato, elabora un informe en el cual analiza si se han recogido las estipulaciones a las que se refiere el artículo 12 de la LOPD.

Para facilitar el cumplimiento de lo dispuesto en el artículo 9 la APDCM propone que se usen los siguientes tipos de cláusulas, adecuándolas al tipo de tratamiento que se vaya a realizar. En el caso que nos ocupa, a la implantación de la videovigilancia y sus diferentes fines:

El contratista, como encargado del tratamiento, tal y como se define en la letra g) del artículo 3 de ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, declara expresamente que conoce quedar obligado al cumplimiento de lo dispuesto en la citada LOPD y especialmente en lo indicado en sus artículos 9, 10, 12 y adoptará las medidas de seguridad que le correspondan según el Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD.

El/los adjudicatario/s se compromete/n a cumplir lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (y, muy especialmente, lo indicado en su artículo 12). El/los adjudicatario/s se comprometen explícitamente a formar e informar a su personal en las obligaciones que de tales normas dimanan.

Igualmente, serán de aplicación las disposiciones de desarrollo de las normas anteriores que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia, y aquellas normas del Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD.

La empresa adjudicataria declara expresamente que conoce quedar obligada al cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, expresamente, en lo indicado en su artículo 10, en cuanto al deber de secreto, así como lo dispuesto en la Ley 8/2001 de la Comunidad de Madrid y, especialmente, lo indicado en su artículo 11. La empresa adjudicataria se compromete explícitamente a formar e informar a su personal en las obligaciones que de tales normas dimanan.

La empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual.

El/los licitador/es aportarán una memoria descriptiva de las medidas que adoptarán para asegurar la confidencialidad e integridad de los datos manejados y de la documentación facilitada. Asimismo, el/los adjudicatario/s deberán comunicar a "el organismo contratante", antes de transcurridos siete días de la fecha de comunicación de la adjudicación, la persona o personas que serán directamente responsables de la puesta en práctica y de la inspección de dichas medidas de seguridad, adjuntando su perfil profesional.

Si la empresa adjudicataria aporta equipos informáticos, una vez finalizadas las tareas el adjudicatario, previamente a retirar los equipos informáticos, deberá borrar toda la información utilizada o que se derive de la ejecución del contrato, mediante el procedimiento técnico adecuado. La destrucción de la documentación de apoyo, si no se considerara indispensable, se efectuará mediante máquina destructora de papel o cualquier otro medio que garantice la ilegibilidad, efectuándose esta operación en el lugar donde se realicen los trabajos.

La documentación se entregará al adjudicatario para el exclusivo fin de la realización de las tareas objeto de este contrato, quedando prohibido para el adjudicatario y para el personal encargado de su realización, su reproducción por cualquier medio y la cesión total o parcial a cualquier persona física o jurídica. Lo anterior se extiende asimismo al producto de dichas tareas.

El resultado de las tareas realizadas, así como el soporte utilizado (papel, fichas, disquetes, etc.) serán propiedad del "organismo contratante".

Recuerde que antes de perfeccionar el contrato con el encargado del tratamiento debe comunicarlo a la APDCM para que ésta elabore un informe sobre su adecuación a la LOPD.

La LOPD tipifica como infracción leve aquellos casos en que el contrato con el encargado del tratamiento no recoge el contenido del artículo 12 de la LOPD.

La Ley 8/2001 de 13 de julio de Protección de Datos en la Comunidad de Madrid establece que será causa de resolución del contrato el incumplimiento del artículo 12 de la LOPD.

3.7.- Cancelación de imágenes

Los datos de carácter personal recogidos mediante sistemas de cámaras o videocámaras serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados y, en todo caso, en el plazo máximo de un mes desde su captación, sin perjuicio de las excepciones existentes.

Con carácter general, el responsable procederá a la supresión y borrado de las imágenes cuando dejen de ser necesarias o pertinentes en relación con dicha finalidad, sin que la existencia del plazo máximo al que se refiere el apartado anterior en relación con la cancelación de dichas imágenes pueda servir de base para la conservación de las mismas por un período de tiempo mayor del estrictamente necesario.

Las imágenes captadas para finalidades distintas a la seguridad podrán conservarse hasta que hayan dejado de ser necesarias, dentro de los plazos máximos establecidos por la normativa sectorial específicamente aplicable.

En particular, se estará a lo dispuesto en la legislación estatal y autonómica sobre sanidad, reguladora de la autonomía del paciente y de sus derechos y obligaciones en materia de información y documentación clínica, en relación con la conservación de las imágenes cuyo tratamiento se encuentre asociado, de manera accesoria y/o complementaria, a los datos de salud y/o a la documentación clínica de los afectados por los tratamientos.

Cuando el tratamiento no se ajuste a lo dispuesto en la LOPD la imagen deberá ser cancelada en el plazo de diez días desde que se tuviese conocimiento de dichas circunstancias.

Si la imagen hubiera sido comunicada previamente, el responsable del tratamiento deberá notificar al cesionario, en el plazo de diez días, la cancelación efectuada.

No obstante, las imágenes podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica, de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado, siempre que la concurrencia de dichas circunstancias quede suficientemente probada a

través del correspondiente soporte documental. En estos supuestos, la conservación se referirá únicamente a las imágenes afectadas por dichas responsabilidades, debiendo extraerlas el responsable del tratamiento de su soporte originario.

Una vez concluido el período al que se refieren los párrafos anteriores, la imagen no podrá conservarse, sin perjuicio de la obligación de bloqueo prevista por el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, a disposición de las Administraciones Públicas y los Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de las correspondientes responsabilidades y/o acciones.

Asimismo, la conservación de la imagen podrá traer causa de la atención por el responsable del ejercicio de sus derechos por el afectado por el tratamiento.

En el supuesto de conservación de las imágenes -en cumplimiento de la obligación de bloqueo prevista por LOPD- a disposición de las Administraciones Públicas y los Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción correspondiente, el responsable del tratamiento retendrá y bloqueará únicamente las imágenes afectadas a dichas responsabilidades, extrayéndolas de su soporte originario, sin perjuicio de la cancelación del resto de las imágenes contenidas en dicho soporte o, en su caso, de la destrucción física del mismo.

También podrán conservarse las imágenes, previa disociación de las mismas, siguiéndose para ello el procedimiento definido en el artículo 3.f) de la LOPD.

En relación con la cancelación de las imágenes cuyo tratamiento se realice mediante sistemas de cámaras o videocámaras instaladas en áreas de acceso restringido, ubicadas en centros neurálgicos de vital importancia para la población en general, se estará

especialmente a lo dispuesto en la Disposición Adicional de la Instrucción 1/2007 de la APDCM[6].

Las imágenes deberán ser canceladas cuando dejen de ser útiles para la finalidad que motivó su grabación y, en todo caso, en un plazo máximo de 30 días. Se exceptúa si las imágenes se han puesto a disposición de las Administraciones públicas o Tribunales para las correspondientes responsabilidades. También si existe normativa específica como en materia de asistencia sanitaria.

3.8.- Cesiones de datos de carácter personal

Las imágenes obtenidas mediante los sistemas de videovigilancia sólo podrán ser cedidas en los casos regulados en el artículo 11 y 21 de la LOPD, es decir, se aplica el régimen general que regula dicha comunicación de datos de carácter personal.

En este sentido, el artículo 11 de la LOPD establece lo siguiente:

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado

2. El consentimiento exigido en el apartado anterior no será preciso:

a. Cuando la cesión está autorizada en una ley.
b. Cuando se trate de datos recogidos de fuentes accesibles al público.

[6] Ver Anexo de esta Guía.

c. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d. Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e. Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Y por su parte, el artículo 21 dispone lo siguiente:

1. *Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

No obstante, cuando exista una petición para una cesión de datos de carácter personal, dicha cesión debe ajustarse al principio de calidad de los datos cumpliendo dos requisitos:

- La petición debe ser motivada, es decir, se tiene que justificar por el órgano peticionario la razón de la cesión.

- Los datos personales comunicados deben ser los adecuados a la finalidad que motiva dicha petición para evitar una cesión indiscriminada.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Las cesiones de imágenes tendrán lugar en los supuestos del artículo 11 y 21 LOPD. También será de aplicación el artículo 4 de la LOPD que regula el principio de calidad.

Para su seguridad, documente la cesión realizada y los motivos por los cuales le han solicitado las imágenes.

Por esta razón y aún más teniendo en cuenta que en videovigilancia la petición de imágenes en la mayoría de los casos será solicitada por las Fuerzas y Cuerpos de Seguridad del Estado o por los órganos jurisdiccionales, la APDCM recomienda dejar constancia de la citada cesión utilizando para ello el siguiente modelo:

DOCUMENTO ACREDITATIVO DE CESIÓN DE DATOS DE CARÁCTER PERSONAL
Responsable del tratamiento:
Nombre del fichero:
Finalidad del fichero:
Nº en el Registro de Ficheros de la APDCM:
Peticionario:
Motivo de la petición:
Normativa que legitima la cesión:
Imágenes que se facilitan:
Fecha en que se realiza la petición:
Fecha en que se realiza la cesión:

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

3.9.- Medidas de seguridad

Con carácter general, la instalación de las medidas de seguridad en los sistemas de videovigilancia serán las de carácter básico que regula el Reglamento de desarrollo de la LOPD. Obviamente, si estuviésemos en algunos de los supuestos en que son de aplicación las de nivel medio o alto, serán éstas las que deban ser implantadas.

Ejemplo: las cámaras instaladas en la sede de una Consejería de la Comunidad de Madrid con fin de videovigilancia deben cumplir las medidas de seguridad de nivel básico.

Las cámaras instaladas por un Hospital de la Comunidad de Madrid con la finalidad de asistencia médica deben cumplir las medidas de seguridad de nivel alto.

La Instrucción 1/2007 de la APDCM dedica su Norma Octava a la seguridad[7]. Para más información sobre medidas de seguridad puede consultar la Guía que sobre esta materia tiene publicada la APDCM. El documento de seguridad puede descargase de forma gratuita en la página web de la Agencia.

3.10.- Deber de secreto

Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las imágenes objeto de tratamiento deberá observar la debida reserva en relación con las mismas. Esta obligación subsistirá aun después de que finalice la vinculación de las personas que intervengan en el tratamiento con el responsable del mismo.

[7] Ver Anexo de esta Guía.

El responsable deberá informar a las personas con acceso a las imágenes tratadas del deber de secreto al que se refiere el apartado anterior.

El deber de secreto será exigible en todo caso, con independencia de que el acceso a las imágenes captadas mediante sistemas de cámaras o videocámaras, se produzca mediante la simple visualización realizada en tiempo real, o sobre el contenido de las imágenes una vez grabadas y almacenadas.

La vulneración del deber de guardar secreto sobre las imágenes tratadas dará lugar, en su caso, a la exigencia de las responsabilidades administrativas o penales legalmente previstas.

Cualquier persona que acceda a las imágenes debe cumplir con el deber de secreto.

Corresponde al responsable informar sobre el cumplimiento de este deber a quien acceda.

La APDCM recomienda firmar documentos de confidencialidad con los trabajadores que vayan a controlar y acceder a las grabaciones de las cámaras.

3.11.- Ejercicio de los derechos ARCO

La LOPD reconoce como derechos personalísimos de los afectados respecto al tratamiento de sus datos personales los derechos de acceso, rectificación, cancelación y oposición. Puesto que la grabación de la imagen es un tratamiento de datos personales, como ya hemos indicado anteriormente, se podrán ejercitar estos derechos ante el responsable del tratamiento, salvo el derecho de rectificación, que lógicamente no cabe su ejercicio en este ámbito.

El responsable del tratamiento deberá atender la solicitud de acceso, cancelación u oposición ejercida por el interesado adoptando las medidas oportunas para garantizar, en todo caso, la debida disociación de la imagen o, en su caso, de cualquier otro dato de carácter personal de las terceras personas afectadas por los tratamientos.

A dichos efectos, el responsable del tratamiento se servirá de los programas y/o herramientas informáticas adecuadas que, aplicadas sobre los datos de carácter personal de las terceras personas afectadas, impidan su identificación y la cesión de su imagen a la persona que realice la solicitud.

No obstante lo anterior, nos encontramos con una serie de excepciones al ejercicio de estos derechos:

- Cuando se trate de la mera captación de imágenes que se reproduzcan en tiempo real sin que se incorporen a un fichero de datos de carácter personal.
- Cuando el tratamiento de la imagen se encuentre vinculado a los fines policiales recogidos en el art. 22 de la LOPD.

Asimismo, cuando el responsable del tratamiento tuviera fundadas dudas en relación con la coincidencia existente entre las imágenes tratadas y la correspondiente a la persona que ejercite sus derechos, deberá denegar la solicitud del interesado, fundamentando su resolución en la carencia de la certidumbre necesaria.

La denegación también tendrá lugar cuando el sistema de cámaras o videocámaras disponga de herramientas u otros productos de «software» adecuados para el reconocimiento de imágenes, el responsable del tratamiento podrá denegar la solicitud del interesado si el porcentaje de coincidencia entre la imagen aportada en su solicitud y la imagen objeto de tratamiento no permite asegurar que esta última corresponda al

interesado. En este supuesto deberá ofrecerse al afectado la información relativa al porcentaje de coincidencia que el sistema de reconocimiento haya facilitado en el procedimiento de búsqueda.

La APDCM recomienda que el responsable del tratamiento de sistemas de videovigilancia tenga a disposición de los interesados modelos para poder ejercitar los derechos de acceso, cancelación y oposición.

Modelos de impresos - Agencia de Protección de Datos de la Comunidad de Madrid.

3.12.- "Check-list" para verificar el cumplimiento de la LOPD en la instalación de cámaras

La APDCM recomienda a los responsables de tratamiento que están bajo su ámbito de control que previamente a poner en funcionamiento las cámaras de videovigilancia, comprueben si cumplen todos los requisitos relacionados con la LOPD. Para ello, se puede utilizar el siguiente "CHECK-LIST":

VERIFICACIÓN DEL CUMPLIMIENTO DE LA LOPD EN LA INSTALACIÓN DE CÁMARAS DE VIDEOVIGILANCIA	SI	NO
¿Está definido quién es el responsable del fichero?		
¿Ha elaborado el informe de proporcionalidad justificando la necesidad de instalar las cámaras de videovigilancia?		
¿Ha enviado toda lo documentación a la APDCM?		
¿Ha obtenido el informe favorable de la APDCM de creación del fichero?		
¿Se ha creado el fichero mediante la aprobación de una disposición de carácter general?		
¿La disposición general de creación del fichero ha sido publicada en el Boletín correspondiente?		
¿Se ha inscrito el fichero en el Registro de Ficheros de la APDCM?		
¿Ha instalado el cartel informativo del artículo 5 de la LOPD?		
Si existe un encargado del tratamiento ¿El contrato cumple con lo dispuesto en el artículo 12 de la LOPD?		
¿Están las cámaras debidamente instaladas sin que se encuentren ubicadas en espacios invasivos como podrían ser los aseos?		
¿Las imágenes grabadas se cancelan como máximo a los 30 días de su grabación?		
¿Ha adoptado las correspondientes medidas de seguridad?		
¿Ha elaborado el documento de seguridad?		
¿Existen formularios para el ejercicio por parte de los afectados de los derechos de acceso, cancelación y oposición?		
¿El personal que va a controlar las imágenes ha sido informado sobre su correcto funcionamiento y sus implicaciones respecto a la LOPD?		
¿Y sobre el cumplimiento del deber de secreto?		
¿Tiene un documento en el cual se pueda dejar constancia de las cesiones de imágenes en el caso de que le sean solicitadas?		

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

4.- SUPUESTOS ESPECÍFICOS

En el punto anterior hemos analizado las obligaciones del responsable del tratamiento cuando los sistemas de videovigilancia son utilizados con la finalidad de garantizar la seguridad. A continuación pasamos a desglosar supuestos específicos con las particularidades de cada uno de ellos.

4.1.- Grabaciones en lugares y espacios públicos

La Ley Orgánica 4/1997, de 4 de agosto, regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, desarrollada por el Real Decreto 596/1999, de 16 de abril, de manera que únicamente los citadas Fuerzas y Cuerpos pueden proceder a la grabación de imágenes en espacios públicos tanto abiertos como cerrados, pudiendo incluir también la grabación de sonidos.

Si bien esa Ley Orgánica establece que también es de aplicación la LOPD, existen algunas diferencias y matices.

En primer lugar, se necesitará una autorización previa para la instalación de las cámaras por parte del Delegado del Gobierno de la Comunidad Autónoma que se trate, previo informe de una Comisión cuya presidencia corresponderá al Presidente del Tribunal de Justicia de la misma Comunidad, no pudiendo realizar la instalación cuando dicha Comisión considere que la misma supondría una vulneración de los criterios establecidos en el artículo 4 de esa Ley Orgánica (asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana y prevenir la causación de daños a las personas y bienes).

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Si se acordarse la autorización, la resolución debe ser motivada y referida al lugar público concreto en el que se instalarán las cámaras. Dicha resolución contendrá también todas las limitaciones o condiciones de uso necesarias, en particular la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes. Asimismo deberá precisar genéricamente el ámbito físico susceptible de ser grabado, el tipo de cámara, sus especificaciones técnicas y la duración de la autorización, que tendrá una vigencia máxima de un año, a cuyo término habrá de solicitarse su renovación.

En numerosas ocasiones esta Comisión ha denegado la instalación de cámaras. Incluso, en algún caso ya se habían puesto en funcionamiento o se habían comprado las cámaras.

No adquiera ni instale videocámaras en la vía pública si no tiene la correspondiente autorización.

A modo de ejemplo, podemos citar que la Comisión de Videovigilancia de la Comunidad de Madrid ha autorizado el uso de la videovigilancia en la Plaza Mayor, en la calle Montera o en el barrio Lavapiés (Madrid).

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Sólo las Fuerzas y Cuerpos de Seguridad pueden grabar en lugares de la vía pública como calles o plazas.

Antes de instalar las cámaras, debe existir autorización previa de la Comisión de Videovigilancia de la respectiva Comunidad Autónoma.

En segundo lugar, las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación en curso o con un procedimiento judicial o administrativo abierto.

Asimismo, cuando las grabaciones capten hechos que pudieran ser constitutivos de ilícitos penales, se pondrán a disposición de la autoridad judicial en el plazo máximo de setenta y dos horas desde su captación. Si en ese tiempo no fuese posible redactar el correspondiente atestado, se relatarán verbalmente los hechos a la autoridad judicial o al Ministerio Fiscal y se les entregará la grabación, en todo caso en el plazo ineludible de setenta y dos horas desde su realización. Si las grabaciones captasen hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad ciudadana,

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

se remitirán de inmediato al órgano competente para el inicio del oportuno procedimiento sancionador.

En tercer lugar, y respecto a la información a los ciudadanos sobre las grabaciones, relacionado con el derecho de información, la Ley Orgánica 4/1997, ha recogido este derecho, de manera que existirá una placa informativa que no especificará el emplazamiento concreto de las instalaciones fijas de videocámaras, deberá contener en todo caso una descripción genérica de la zona de vigilancia y de las autoridades responsables de la autorización y custodia de las grabaciones.

En este sentido, el cartel informativo difiere del que antes hemos mostrado:

En la práctica se utiliza el cartel que antes hemos expuesto o el que contiene la Instrucción 1/2006 de la AEPD.

Por último, en relación con el ejercicio de los derechos de acceso y cancelación, ambos podrán ser denegados por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Este límite al ejercicio de esos derechos que recoge el artículo 9.2 de la Ley Orgánica 4/1997, está en consonancia con el artículo 23.1 de la LOPD, que también lo contempla respecto a los ficheros de las Fuerzas y Cuerpos de Seguridad para fines policiales.

Por otra parte, la Norma Sexta apartado 3 de la Instrucción 1/2007 de la APDCM se refiere a la instalación de cámaras por las Fuerzas y Cuerpos de Seguridad de la siguiente forma:

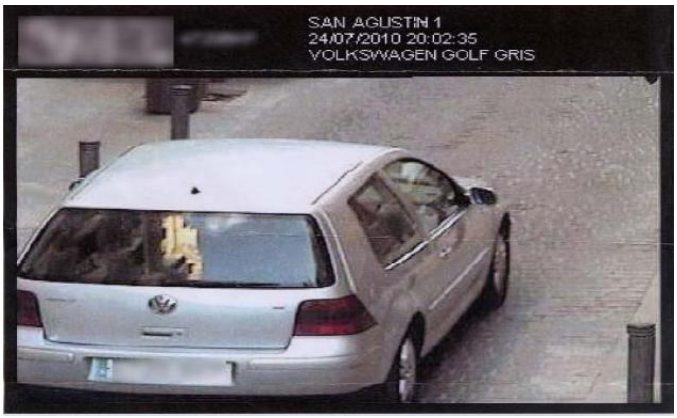
"Las Fuerzas y Cuerpos de Seguridad a las que se refiere la Norma Primera de esta Instrucción que realicen tratamientos de imágenes mediante cámaras o videocámaras en lugares públicos, abiertos o cerrados, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública, deberán cumplir con el deber de información de acuerdo con lo dispuesto por 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.

A tal fin, el público será informado de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable."

4.2.- Control y disciplina de tráfico

Otra de las posibles finalidades de las cámaras de videovigilancia es utilizarlas para el control y disciplina de tráfico, y garantizar de esta forma la seguridad vial. La Disposición Adicional Octava de la Ley Orgánica 4/1997 se refiere a este supuesto:

"La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico se efectuará por la autoridad encargada de la regulación del tráfico a los fines previstos en el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial, aprobado por Real Decreto legislativo 339/1990, de 2 de marzo, y demás normativa específica en la materia, y con sujeción a lo dispuesto en las Leyes Orgánicas 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y 1/1982, de 5 de mayo, de Protección Civil del derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, en el marco de los principios de utilización de las mismas previstos en esta Ley."



En este sentido, el Real Decreto 596/1999, de 16 de abril, mediante su Disposición Adicional Única ha regulado de manera más pormenorizada el uso de las videocámaras para esté fin:

"1. La instalación y uso de videocámaras y de cualquier otro medio de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico en las vías públicas, se realizará con sujeción a lo dispuesto en la disposición adicional octava de la Ley Orgánica 4/1997 y en la presente disposición.

2. Corresponderá a las Administraciones públicas con competencia para la regulación del tráfico, autorizar la instalación y el uso de los dispositivos aludidos en el apartado anterior.

3. La resolución que ordene la instalación y uso de los dispositivos fijos de captación y reproducción, identificará genéricamente las vías públicas o los tramos de aquéllas cuya imagen sea susceptible de ser captada, las medidas tendentes a garantizar la preservación de la disponibilidad, confidencialidad e integridad de las grabaciones o registros obtenidos, así como el órgano encargado de su custodia y de la resolución de las solicitudes de acceso y cancelación.

La vigencia de la resolución será indefinida en tanto no varíen las circunstancias que la motivaron.

En el ámbito de la Administración General del Estado la facultad resolutoria recaerá en el Director general de Tráfico.

4. La utilización de medios móviles de captación y reproducción de imágenes, que no requerirá la resolución a la que se refiere el apartado anterior, se adecuará a los principios de utilización y conservación enunciados en el mismo.

5. La custodia y conservación de las grabaciones y la resolución de las solicitudes de acceso y cancelación a las mismas corresponderá a los órganos que determinen las Administraciones públicas competentes. En el caso de la Administración General del Estado, corresponderá al responsable de los servicios provinciales del Organismo Autónomo Jefatura Central de Tráfico.

6. Cuando los medios de captación de imágenes y sonidos a los que se refiere esta disposición resulten complementarios de otros instrumentos destinados a medir con precisión, a los efectos de la disciplina del tráfico, magnitudes tales como la velocidad de circulación de los vehículos a motor, dichos aparatos deberán cumplir los requisitos que, en su caso, prevean las normas metrológicas correspondientes.

7. La utilización de las videocámaras contempladas en esta disposición por las Fuerzas y Cuerpos de Seguridad para fines distintos de los previstos en la misma se regirá por lo dispuesto en la Ley Orgánica 4/1997 y en el presente Reglamento.

En el caso de que dicha utilización se realice por las Unidades de Policía Judicial en sentido estricto, se estará a lo dispuesto en la Ley de Enjuiciamiento Criminal y en su normativa específica."

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

La instalación de videocámaras para control del tráfico en vías urbanas será competencia del respectivo Ayuntamiento donde discurran las mismas. Deberán aprobar una resolución en la que se incluyan las calles afectadas –de manera genérica– y el órgano ante el cual ejercer los derechos de acceso y cancelación.

Ligado al control del tráfico está el uso de las cámaras para regular **espacios de acceso restringido**, es decir, barrios o calles en los que sólo los residentes pueden acceder, y dicho acceso se controla mediante las cámaras. Existirán algunos supuestos excepcionales, en los cuales se permitirá el acceso, como pueden ser transporte público o los servicios de emergencia. Dos ejemplos de este uso nos los encontramos en la ciudad de Madrid, en el barrio de "Las letras" y en Embajadores.

Ejemplo de fichero de uso de videovigilancia para el control de tráfico.

Fichero "Videovigilancia de tráfico"	
Responsable del fichero.	ÁREA DE GOBIERNO DE SEGURIDAD Y MOVILIDAD. DIRECCIÓN GENERAL DE MOVILIDAD.
Órgano, servicio o unidad ante el que se deberán ejercitar los derechos de acceso, rectificación, cancelación y oposición.	DIRECCIÓN GENERAL DE MOVILIDAD. CALLE ALBARRACÍN, 33. 28037 MADRID.
Nombre y descripción del fichero.	VIDEOVIGILANCIA DE TRÁFICO. VIDEOVIGILANCIA PARA EL CONTROL DEL TRÁFICO.
Carácter informatizado o manual estructurado del fichero.	AUTOMATIZADO.
Sistema de información al que pertenezca el fichero.	SISTEMA DE VIDEOVIGILANCIA DEL TRÁFICO.
Nivel de medidas de seguridad aplicadas.	BÁSICO
tipos de Datos de carácter personal que se incluirán en el mismo.	-Datos de carácter identificativo: IMAGEN
Descripción detallada de la finalidad del fichero y los usos previstos del mismo.	MEJORAR LA SEGURIDAD Y EL CONTROL DEL TRÁFICO MEDIANTE LA VIDEOVIGILANCIA DE LA VÍA PÚBLICA.
Personas o colectivos sobre los que se pretenda obtener datos o que resulten obligados a suministrarlos.	VEHÍCULOS QUE CIRCULEN POR LA VÍA PÚBLICA.
Procedencia o procedimiento de recogida de los datos:	— Origen: EL PROPIO INTERESADO U OTROS. — Procedimiento de recogida: VIDEOVIGILANCIA. — Soporte utilizado para la obtención: VIDEOVIGILANCIA.
Cesiones.	DIRECCIÓN GENERAL DE TRÁFICO.

Ejemplo de fichero de uso de videovigilancia para el control acceso a áreas restringidas.

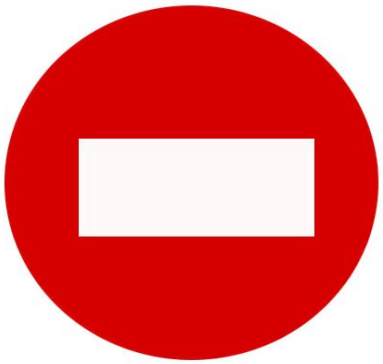
Fichero "Acceso Áreas Prioridad Residencial"	
Responsable del fichero.	ÁREA DE GOBIERNO DE SEGURIDAD Y MOVILIDAD. DIRECCIÓN GENERAL DE MOVILIDAD.
Órgano, servicio o unidad ante el que se deberán ejercitar los derechos de acceso, rectificación, cancelación y oposición.	DIRECCIÓN GENERAL DE MOVILIDAD. CALLE ALBARRACÍN, 33. 28037 MADRID.
Nombre y descripción del fichero.	ACCESO ÁREAS PRIORIDAD RESIDENCIAL. VEHÍCULOS AUTORIZADOS AL ACCESO A LAS ÁREAS DE PRIORIDAD RESIDENCIAL DE LA CIUDAD DE MADRID.
Carácter informatizado o manual estructurado del fichero.	AUTOMATIZADO.
Sistema de información al que pertenezca el fichero.	SISTEMA DE ACCESO A LAS ÁREAS DE PRIORIDAD RESIDENCIAL
Nivel de medidas de seguridad aplicadas.	BÁSICO
tipos de Datos de carácter personal que se incluirán en el mismo.	-Datos de carácter identificativo: DNI/NIF-NOMBRE Y APELLIDOS-DIRECCIÓN (POSTAL, ELECTRÓNICA)-VEHÍCULO, MATRÍCULA
Descripción detallada de la finalidad del fichero y los usos previstos del mismo.	PROTEGER LAS ÁREAS DE PRIORIDAD RESIDENCIAL DE LA CIUDAD DE MADRID, MEDIANTE EL CONTROL DE ACCESO A LAS MISMAS.
Personas o colectivos sobre los que se pretenda obtener datos o que resulten obligados a suministrarlos.	TITULARES DE VEHÍCULOS AUTORIZADOS QUE ACCEDAN A LAS ÁREAS DE PRIORIDAD RESIDENCIAL DE LA CIUDAD DE MADRID.
Procedencia o procedimiento de recogida de los datos:	— Origen: EL PROPIO INTERESADO O SU REPRESENTANTE LEGAL-ENTIDAD PRIVADA-ADMINISTRACIONES PÚBLICAS. — Procedimiento de recogida: FORMULARIOS O CUPONES-TRANSMISIÓN ELECTRÓNICA DE DATOS/INTERNET. — Soporte utilizado para la obtención: SOPORTE PAPEL-SOPORTE INFORMÁTICO/MAGNÉTICO-VÍA TELEMÁTICA.
Cesiones.	NO SE PREVÉN CESIONES.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

4.3.- Centros educativos

Si bien en la instalación de cámaras con fines de seguridad en los centros educativos tiene que cumplir con los requisitos que hemos descrito en el apartado 3 de esta Guía (crear el fichero, instalación del cartel…etcétera), el principio de proporcionalidad debe ser aplicado con mayor rigor, puesto que se van a captar imágenes de menores y dependiendo de donde se instalen las cámaras, además de afectar a su vida privada, se podría estar también limitando su derecho fundamental al desarrollo de su personalidad.

En consecuencia, la APDCM considera que no se pueden instalar cámaras en vestuarios, baños, patios de recreo, gimnasios, ni tampoco en relación con la posible comisión de infracción como tirar papeles, colillas o fumar. Con carácter general, tampoco en salas de juego y aulas.



Vestuarios

Baños

Patios de Recreo

Gimnasios

Para control de asistencia escolar

Para control de infracciones (tirar colillas o papeles)

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Mención aparte merece el uso de las cámaras para el control de asistencia escolar, finalidad que la APDCM considera excesiva y no proporcionada. Sobre esta cuestión, la APDCM también se ha pronunciado sobre el uso de la huella de los menores para el control de presencia en un polideportivo. Dada su especial relevancia y puesto que nos podemos encontrar con sistemas que utilicen la videovigilancia y la huella dactilar para los fines descritos, procedemos a publicar un extracto del citado informe:

Utilización de un control de acceso basado en el reconocimiento de la huella digital en un Centro Deportivo Municipal en relación con una menor de tres años, que acude al mismo para realizar una actividad de "expresión corporal".

En el presente caso, el juicio de idoneidad ha de ser necesariamente positivo, ya que la medida propuesta, aun con las deficiencias (falsos positivos y falsos negativos) inherentes a todo sistema biométrico –que, por otra parte, harían necesaria la previsión de medidas alternativas cuando dichos problemas se produzcan- sirve al propósito perseguido, esto es, el control del uso y/o acceso de las instalaciones deportivas por parte de los participantes en las actividades realizadas en el Polideportivo Municipal.

Pero es en la valoración del juicio de necesidad cuando comienzan a percibirse dificultades. No corresponde a esta Agencia de Protección de Datos de la Comunidad de Madrid el proponer o decidir unas u otras medidas para llevar a cabo para el control de la utilización, acceso y/o control de asistencia de las personas a las instalaciones del Polideportivo, pero sí resulta necesario que por parte de dicho Polideportivo se valoren con cautela las implicaciones de la adopción de un sistema basado en el reconocimiento de la "huella digital" y la posibilidad de adoptar otros que, siendo igualmente idóneos, resulten menos intrusivos en la intimidad y privacidad de las personas que deben someterse a los mismos.

Igualmente, también han de apuntarse ciertas reservas en el ámbito del estricto juicio de proporcionalidad. Si en el ámbito del juicio de necesidad parece que podrían existir otras medidas que satisfarían los fines propuestos, el Centro Deportivo Municipal también debería plantearse si la existencia de dichas medidas alternativas hace que el juicio de proporcionalidad en relación con la medida que se pretende implantar plantee también importantes dudas.

En efecto, será necesario reflexionar sobre si existe un claro beneficio para el interés general en la aplicación de un sistema que suscita dudas en cuanto al juicio de necesidad en su confrontación con el derecho fundamental a la protección de datos en la utilización del propio cuerpo de los usuarios y/o alumnos que asisten a las actividades del Polideportivo como elemento de identificación en el acceso a las instalaciones, máxime teniendo en cuenta que la relación que se establece entre los usuarios y el Centro Deportivo no es en modo alguno permanente, sino limitada a un determinado curso, plazo, o jornadas.

Asimismo, tal y como se ha venido indicando por el Grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE, en el "Documento de Trabajo sobre Biometría", de fecha 1 agosto de 2003, la obtención de la huella dactilar como medio para identificar a los alumnos en el centro resulta excesivo y desproporcionado, para dicha finalidad, a saber:

"El Grupo opina que la mayor parte de los datos biométricos implican el tratamiento de datos personales. Por consiguiente, es necesario respetar plenamente los principios de la protección de datos que aparecen en la Directiva 95/46/CE teniendo en consideración, al desarrollar los sistemas biométricos, la especial naturaleza de la biometría, y entre otras cosas su capacidad de recopilar datos biométricos sin el conocimiento del interesado y la casi seguridad del vínculo con la persona".
(...)

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

"El tratamiento de los datos biométricos debe basarse en uno de los motivos de legitimidad contemplados en el artículo 7 de la Directiva 95/46/CE. Si el responsable del tratamiento del registro utiliza el consentimiento como motivo de legitimidad, el Grupo subraya que deberá cumplir las condiciones fijadas en el artículo 2 de la Directiva 95/46/CE (toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen)".

(...)

"Con arreglo al artículo 6 de la Directiva 95/46/CE, los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Además, los datos personales serán adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de fines). El cumplimiento de este principio implica en primer lugar una determinación clara de los fines para los que se recogen y tratan los datos biométricos.

Por otra parte, hace falta evaluar el cumplimiento de la proporcionalidad y de la legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas y especialmente si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva. La proporcionalidad ha sido el criterio principal en casi todas las decisiones adoptadas hasta ahora por las autoridades encargadas de la protección de datos sobre el tratamiento de datos biométrico (...).

El uso de la biometría plantea también el tema de la proporcionalidad de cada categoría de datos a la luz de los fines para los que se tratan dichos datos. Los datos biométricos sólo pueden usarse de manera adecuada, pertinente y no excesiva, lo cual supone una estricta valoración de la necesidad y proporcionalidad de los datos tratados. Por ejemplo, la CNIL francesa ha rechazado el uso de huellas digitales en el caso del acceso de los niños a un comedor escolar, pero ha aceptado con el mismo fin el uso de los resultados de muestras de

las manos. La autoridad portuguesa de protección de datos ha tomado recientemente una decisión desfavorable sobre la utilización de un sistema biométrico (huellas digitales) por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente."

Sin perjuicio de las anteriores consideraciones jurídicas, conviene ahora insistir en que, a juicio de esta Agencia de Protección de Datos de la Comunidad de Madrid, el establecimiento de un sistema de control de usuarios y/o alumnos de un Centro Deportivo Municipal, basado en la obtención de la huella dactilar de éstos, resulta claramente desproporcionado y contrario al principio de calidad de los datos recogido por el artículo 4.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

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

El problema consiste en que el tratamiento de la información biométrica de la huella dactilar puede ser considerado claramente excesivo para el fin que motiva dicho tratamiento, teniendo en cuenta el marco en el que se efectúa, cual es el relativo a la utilización y acceso a unas instalaciones deportivas municipales por parte de alumnos (incluso menores de edad), y para las finalidades de control de horario, acceso y/o asistencia a las que la utilización de dicho sistema podría subvenir. Esto es, mediante dicha huella dactilar podría pretenderse controlar la entrada y salida, así como la utilización de las instalaciones deportivas.

De igual modo, deberá reputarse también ilegítimo por desproporcionado el control de utilización y/o acceso a unas instalaciones deportivas realizado a través de la captación y tratamiento de dicha huella dactilar.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

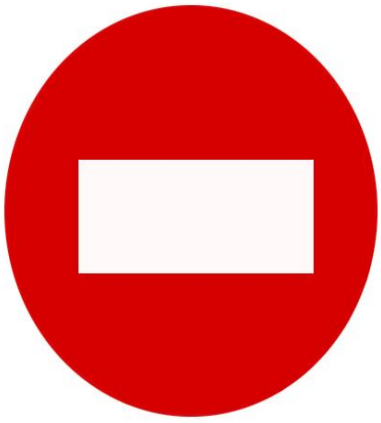
4.4.- Polideportivos

Al igual que en el supuesto anterior, se pueden instalar cámaras para garantizar la seguridad de las instalaciones. No obstante, existen una serie de limitaciones, ya que es excesivo y desproporcional la instalación y grabación mediante cámaras en los lugares donde se realiza la actividad deportiva (gimnasio, pistas deportivas, spas, zona de balneario).

La Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte, regula la instalación de circuitos cerrados de televisión para grabar el acceso y el aforo completo al recinto deportivo, incluyendo los aledaños en que puedan producirse aglomeraciones de público. Además, estos circuitos cerrados deberán adoptar las medidas necesarias para garantizar su buen estado de conservación y adecuado funcionamiento.
El circuito cerrado de televisión tendrá las siguientes características:

- Contará con cámaras fijas y móviles.
- Las fijas:
    - Controlarán el exterior e interior del recinto, incluyendo las zonas de acceso y gradas y una visión total de aquél.
    - En competiciones oficiales de carácter profesional de fútbol grabarán el aforo completo del recinto desde el comienzo hasta el abandono del público.
- Las móviles:
    - Se situarán en aquellos espacios que el Coordinador de Seguridad estime necesario controlar en cada acontecimiento deportivo, disponiendo de medios para grabar las actitudes de los asistentes y su comportamiento.

- Las grabaciones se conservarán durante un mes a contar desde la conclusión del espectáculo, y pasado ese plazo se destruirán si no fueran requeridas por las autoridades competentes.
- En los accesos a los recintos que cuenten con este sistema se colocarán carteles informativos y se tendrá a disposición de los interesados, en los términos previstos en las Instrucciones de la AEPD, impresos en los que se detalle la información prevista en el artículo 5 de la LOPD.



Gimnasio
Pistas deportivas
Áreas deportivas
Vestuarios
Spas
Piscinas
Zona de balneario

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

4.5. Centros neurálgicos

Se trata de espacios y áreas de acceso restringido[8] por motivos de seguridad neurálgica, ya que son centros de vital importancia para la comunidad. La Disposición Adicional Primera de la Instrucción 1/2007 de la APDCM contiene una serie de normas específicas respecto a los mismos:

- Cancelación de imágenes: según los plazos que, en su caso, establezca la normativa sectorial aplicable.
- Acceso a las instalaciones: el personal autorizado para acceder a las dependencias donde se realicen los tratamientos de imágenes quedará taxativa y específicamente definido en el documento de seguridad.
- Derecho de información: además de los carteles informativos, el responsable del tratamiento establecerá protocolos de información sobre el tratamiento de imágenes y sobre las condiciones específicas que concurran en las zonas de acceso restringido. En todo caso, esta información se ofrecerá a los empleados del centro en el momento de incorporarse a su destino y periódicamente con carácter trimestral. También se ofrecerá a todas aquellas personas vinculadas al mismo y que, en cumplimiento de cualquier tipo de relación negocial, laboral o administrativa pueda acceder a las citadas zonas. En todo caso, la información adicional incluirá una referencia sobre la imposibilidad de ejercitar el derecho de oposición en relación con el tratamiento de imágenes.

[8] Ver Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

- Uso de las cámaras como apoyo a los sistemas de control de acceso físico: el responsable del tratamiento podrá supervisar adicionalmente, a través de la captación de imágenes, la identidad de las personas que accedan a los espacios o áreas restringidas utilizando cualquier otro tipo de sistema o dispositivo de control de acceso físico.

4.6. Aparcamientos públicos

El uso de cámaras en los aparcamientos públicos (también en los privados) supone un tratamiento de datos de carácter personal, ya que en este caso se va a grabar la matrícula del coche que de conformidad con la definición de datos de carácter personal que recoge la LOPD y su reglamento de desarrollo tiene tal condición, ya que con la misma se podría identificar al propietario del vehículo (en la Dirección General de Tráfico existe un fichero con los datos personales de todos los titulares de vehículos).

Por lo tanto, deben cumplirse las obligaciones que ya hemos analizado en el apartado 3 de esta Guía.

4.7.- Prestación de asistencia sanitaria

La Instrucción 1/2007 de la APDCM también regula la utilización de las cámaras para otros fines que no sean la seguridad, como es el caso de la finalidad de asistencia sanitaria (por ejemplo, cámaras para monitorizar al paciente que está en la unidad de cuidados intensivos, uso de la telemedicina o para diagnosticar a los pacientes). En relación con las obligaciones que se deben cumplir por el responsable para adecuar este tipo de tratamientos, nos encontraremos con una serie de especialidades respecto a las obligaciones descritas anteriormente sobre el uso de cámaras para la seguridad:

- Creación y registro del fichero: si las imágenes se incorporan a un fichero principal (por ejemplo, la historia clínica), formarán parte del mismo sin necesidad de crear uno nuevo.
- El cartel del derecho de información del artículo 5 de la LOPD es diferente, ya que la finalidad no es la de videovigilanica, debiendo constar una mención del tipo "Captura de imágenes con fines de…".

- Para determinar el plazo de cancelación de las imágenes se estará a lo dispuesto en la legislación estatal y autonómica sobre sanidad, así como a la ley de autonomía del paciente.
- El derecho de acceso también se ejercitará de acuerdo a su legislación específica.
- Las medidas de seguridad, al grabar datos de salud, serán las de nivel alto.

4.8. Prestación de asistencia social

Se trata de un supuesto muy similar al anterior y que podría tener cabida, por ejemplo, para la atención de los residentes de un centro de servicios sociales que están afectados

por la enfermedad de Alzheimer, si bien puede afectar a derechos de terceros cuando los citados residentes reciban las visitas de familiares y amigos.

En este sentido, y sin perjuicio de las obligaciones generales como sería la creación e inscripción del fichero, existirán especialidades en el cartel del derecho de información del art.5 o en la cancelación de imágenes (normativa específica).

Otro ejemplo de actualidad es la utilización de cámaras en guarderías, pudiendo los padres conectarse por internet para ver a sus hijos. En este caso, al ser menores, los padres tienen que prestar el consentimiento. Asimismo son especialmente relevantes las medidas de seguridad, ya que sólo podrán acceder a las imágenes por internet los padres y no cualquiera, de manera que se les deberá facilitar un nombre de usuario y contraseña.

4.9. Fines turísticos

Únicamente se puede utilizar las cámaras para esta finalidad cuando no se pueda identificar a las personas. Si la persona es identificable, no se podrán instalar, ya que su instalación se realiza en lugares y espacios públicos, y la competencia al respecto la tienen las Fuerzas y Cuerpos de Seguridad, y aún menos difundir dichas imágenes a través de Internet.

4.10.- Instalación de videovigilancia por las empresas de seguridad privada

La Ley "Omnibus" ha liberalizado la prestación de este servicio, ya que con anterioridad sólo las empresas de seguridad privada, debidamente acreditadas y cumpliendo con los requisitos exigidos por la normativa[9], podían instalar cámaras de videovigilancia. Con la aprobación de la Ley "Omnibus" se ha modificado la Ley 23/1992, de 30 de julio, de Seguridad Privada, de manera que los prestadores de servicios o filiales de empresas de seguridad privada 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 excluidos de la legislación de seguridad privada siempre y cuando no se dediquen a ninguno de los fines definidos en el artículo 5 de la citada Ley, sin perjuicio de otras legislaciones específicas que pudieran resultarles de aplicación.

Por lo tanto, la instalación, venta o mantenimiento de sistemas de videovigilancia puede realizarse por particulares y empresas cuyo objeto no sea la seguridad privada, a condición de que la instalación no se conecte con centrales de alarma.

No obstante lo anterior, se deberá cumplir con lo dispuesto en la normativa de protección de datos y en la Instrucción 1/2007 de la APDCM.

[9] Ver Ley 23/1992, de 30 de julio, de Seguridad Privada; Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada; Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada. Orden INT/315/2011, de 1 de febrero, por la que se regulan las Comisiones Mixtas de Coordinación de la Seguridad Privada; Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada; Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada; y Orden INT/318/2011, de 1 de febrero, sobre personal de seguridad privada.

¡Recuerde!

Si contrata con una empresa, ya sea de seguridad o de otro carácter, la gestión del sistema de videovigilancia, ésta actuará como encargado del tratamiento del fichero de imágenes y deberá firmar un contrato con el contenido previsto en el artículo 12 de la LOPD.

El contrato, con carácter previo a su perfeccionamiento, deberá ser enviado a la APDCM para su informe preceptivo.

4.11.- Acceso a edificios

Cuando se instalen cámaras dentro de los edificios con la finalidad de garantizar la seguridad dentro de los mismos, habrá que cumplir las obligaciones generales descritas la Instrucción 1/2007 de la APDCM (ver apartado 3 de esta Guía)

4.12.- No aplicación de la Instrucción 1/2007

Dos son los supuestos en los que la Instrucción 1/2007 de la APDCM no se aplica:

- Tratamiento de datos personales captados o grabados para uso o finalidad doméstica, quedando excluidos de la misma la instalación y uso de sistemas de video portero.

- Tratamiento de imágenes realizado mediante cámaras o videocámaras con fines periodísticos sin perjuicio, en su caso, de la tutela judicial prevista por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

5.- VIDEOVIGILANCIA EMPRESARIAL

Por su especial relevancia hemos querido dedicar un apartado individual a la videovigilancia empresarial. Aunque en un primer momento puede pensarse que esta actividad abarca únicamente la colocación de cámaras por parte de la empresa –ya sea pública o privada- para controlar la actividad del trabajador, en la práctica este control empresarial puede realizarse mediante el control de otros instrumentos que la empresa pone a disposición del trabajador como son el correo electrónico e Internet.

En cuanto al primero de los supuestos, la Instrucción 1/2007 de la APDCM en la Norma Cuarta, que analiza la legitimación y finalidad en el tratamiento de imágenes, contempla la posibilidad de utilizar la videovigilancia cuando 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, resulten necesarios para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa vinculada al ámbito competencial propio de las instituciones, órganos, organismos y demás entes y entidades a los que se refiere esa Instrucción.

Concretamente:

- Cuando el tratamiento de la imagen tenga por objeto el seguimiento, control y garantía del cumplimiento de la relación laboral, funcionarial o estatutaria.

- Cuando el tratamiento de la imagen se realice en el marco de una relación jurídica derivada del sometimiento del afectado a una relación administrativa de sujeción especial.

- Cuando el tratamiento de la imagen se dirija a la mejora en la calidad de la gestión de los servicios públicos.

- Cuando se realice cualquier otro tratamiento que resulte necesario para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa vinculada al ámbito competencia del responsable del tratamiento en el ejercicio de sus funciones.

En consecuencia, si se instalan las cámaras con las finalidades anteriormente descritas, hay que cumplir con lo dispuesto en la Instrucción 1/2007.

No obstante lo anterior, esta facultad de usar la videovigilancia con el objetivo de controlar la prestación laboral del trabajador debe ser interpretado de forma restrictiva, de manera que:

Con carácter general, se utilizarán otros medios menos intrusivos para el trabajador.

Habrá que analizar las peculiaridades de cada caso.

Asimismo, podemos mencionar dos supuestos en los cuales sería factible la instalación:

- Control del centro de emergencias 112.
- Cámaras enfocando a una caja registradora de dinero.

En cuanto a la instalación para el control horario de los empleados públicos, al igual que hemos mencionado antes, se deben usar otros medios menos intrusivos.

En ningún caso, se podrá utilizar las cámaras cuyo fichero ha sido registrado únicamente con la finalidad de seguridad para otro fin, sin perjuicio del acceso a las imágenes por parte de la inspección de servicios en el marco del correspondiente procedimiento disciplinario.

Por lo que se refiere al control del correo electrónico y uso de Internet, inicialmente la jurisprudencia justificaba dicho control en base al artículo 18 del Estatuto de los Trabajadores –registro sobre la persona del trabajador, en sus taquillas y efectos particulares-, pero ha sido la Sala de lo Social del Tribunal Supremo en la Sentencia de 26 de septiembre de 2007 para la unificación de la doctrina quien ha fijado el mencionado control, basándose en el artículo 20.3 del citado Estatuto –*"el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso"-,* sin perjuicio de adoptar una serie de cautelas al respecto.

En este sentido, y con ocasión de la consulta planteada al respecto por un Ayuntamiento, se reproduce un extracto del informe jurídico elaborado por la APDCM en el cual se fija nuestra postura:

Se alude a la posibilidad de acceder a la información contenida en los correos electrónicos que el Ayuntamiento pone a disposición del empleado público para el desarrollo de su actividad laboral, con expresión de los diferentes supuestos (situación de baja, vacaciones o cese en el puesto de trabajo) en que dicho acceso pudiera producirse.

"En conclusión, podemos señalar lo siguiente:

1.- El artículo 20.3 del Estatuto de los Trabajadores habilita al Ayuntamiento (en su calidad de empleador) a controlar el correo electrónico que facilita a los trabajadores para el desarrollo de sus funciones. Asimismo, esta legitimación para el acceso puede encontrarse en todos aquellos supuestos excepcionales –tales como el quebrantamiento de la confianza por parte del empleado, la existencia de mala fe por parte del mismo, su baja definitiva, o su ausencia prolongada-, en la letra f) del artículo 7 de la Directiva 95/46/CE, que prevé que el tratamiento sólo pueda efectuarse si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos.

En los supuestos en que un determinado Órgano administrativo o Centro directivo -a través de las correspondientes "Instrucciones de uso"-, haya prohibido taxativamente la utilización privada del correo electrónico por parte de sus empleados públicos, habrá de estarse al debido cumplimiento de dicha prohibición en los términos en que la misma se encuentre establecida.

Por el contrario, en el resto de supuestos, que constituyen la regla general en el ámbito de las Administraciones públicas y Órganos administrativos de la Comunidad de Madrid, cuando –tal y como se plantea el Ayuntamiento que solicita este Informe- se ha procedido al dictado de las correspondientes "Instrucciones de uso del Servicio de Correo Electrónico por los Empleados Públicos, en las que el Órgano administrativo competente no prohíbe el uso

privado del correo electrónico, estableciendo determinados límites, tales como la prohibición de la remisión de correos masivos, con fines comerciales o de negocio, relativos a actividades políticas, de carácter ofensivo, etcétera, o bien, cuando dichas "Instrucciones de Uso" no han sido reguladas a través de este tipo de documentos, deberá estarse a las conclusiones que se exponen a continuación.

2.- En consecuencia, en el caso del Ayuntamiento consultante, que acompaña a la solicitud de informe las correspondientes "Instrucciones de uso del Servicio de Correo Electrónico por los Empleados Públicos", resultarán aplicables las previsiones comprendidas en dicho documento, interpretadas conforme a los siguientes criterios:

A).- Que concurra una causa legítima que justifique el acceso a la información obrante en los buzones de correo de los empleados, para lo cual habrá que estar al supuesto concreto en relación con el cual se pretenda el correspondiente acceso, habiéndose informado previamente sobre este extremo a los trabajadores, y cumpliendo de ese modo el deber de informar previsto en el artículo 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

B).- El Responsable del fichero queda sujeto –muy especialmente- al cumplimiento del principio de "calidad de datos", regulado en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, debiendo velarse específicamente por el cumplimiento del principio de finalidad, teniendo en cuenta el carácter taxativo de los límites establecidos por la habilitación normativa a la que se ha hecho mención, incorporada en el artículo 20.3 del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 1/1995, de 24 marzo.

De este modo, deberá asegurarse que los referidos accesos, tengan su única causa en la necesidad del empleador de acceder a la información obrante en las cuentas de correo electrónico de sus empleados, cuando no exista ningún otro medio para garantizar su

necesario acceso a determinada información obrante en dichas cuentas de correo, y dicha información resulte absolutamente necesaria –dentro del ámbito de su poder de dirección y control establecido por la normativa laboral- para garantizar el correcto desenvolvimiento la actividad administrativa (o empresarial) que tiene legalmente encomendada.

A su vez, en beneficio del "principio de finalidad", y para conseguir el necesario equilibrio entre el derecho a la vida privada de los trabajadores y el poder de dirección del empresario, será necesario tener en cuenta, muy especialmente, el principio de proporcionalidad, debiendo el empleador ponderar debidamente la adopción de cualquier medida de acceso al correo electrónico de los empleados, en consideración a que la finalidad pretendida con dicho acceso no se pueda alcanzar con otra medida menos intrusiva para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

El principio de legitimidad se vincula al de proporcionalidad. Así, el control deberá ser una respuesta proporcionada del empleador ante riesgos potenciales, teniendo en cuenta el derecho a la vida privada y otros intereses de los trabajadores.

En orden a garantizar que tal uso será legítimo, necesario, adecuado, pertinente, y proporcionado a la finalidad que lo justifica, pueden establecerse controles, siendo aconsejable que se implique muy especialmente a los "representantes de los trabajadores".

C).- Que el empleador haya informando correctamente a los trabajadores ("principio de transparencia") de las condiciones en que se autoriza la utilización de Internet y el correo electrónico con fines privados. El derecho de información en la recogida de datos (artículo 5 de la LOPD) constituye un requisito indispensable para utilizar, en su caso, la información recabada en el lugar de trabajo contra el propio trabajador.

En este sentido, resulta fundamental que –por parte del Organismo administrativo o Administración pública actuante- se aprueben las correspondientes "Instrucciones de Uso del Servicio de Correo Electrónico", ofreciendo a dichas Instrucciones la necesaria publicidad dentro del ámbito administrativo propio. De este modo, se garantizará que todos los empleados públicos conozcan, con carácter previo a su implantación, las características y condiciones del uso del correo electrónico, así como la existencia de posibles sistemas de control y/o filtrado establecidos por el empleador (y sus límites) implementados a través del posible acceso a la información de carácter personal obrante en sus cuentas de correo electrónico.

Así, tanto los trabajadores como sus representantes, deberán ser informados del tipo de tecnología utilizada por el empresario en relación con la vigilancia y seguimiento de su actividad laboral, debiendo abstenerse el empleador de recoger datos personales que resulten excesivos en razón de la propia naturaleza de la relación laboral.

D).- Finalmente, sin perjuicio de que –en los supuestos excepcionales a los que se refiere la consulta- el acceso del Ayuntamiento a las cuentas de correo electrónico de sus empleados públicos se encuentre amparado en el artículo 20.3 del Estatuto de los Trabajadores (tanto en las situaciones de baja, vacaciones o cese en el puesto de trabajo), deberán sopesarse -caso por caso- los principios generales sobre protección de datos, con especial respeto a la vida privada y al derecho al secreto de las comunicaciones en relación con las personas ajenas a la organización afectadas por dicho acceso.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

6.- INFORMES JURÍDICOS DE LA APDCM.

Los responsables de ficheros que están bajo el ámbito de control de la APDCM pueden dirigirse a la misma para plantear cuestiones relacionadas con la interpretación y aplicación de la legislación vigente en materia de protección de datos de carácter personal.

La APDCM, en virtud del principio de transparencia administrativa, publica las respuestas de estas consultas a través de diversos medios (www.apdcm.es, www.datospersonales.org).

A continuación, incluimos un extracto de los más significativos que versan sobre la videovigilancia:

6.1.- Determinación de la figura del responsable del fichero de captación de imágenes mediante un sistema de videovigilancia instalado en un Hospital de nueva creación.

El artículo 3.d) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), se define al Responsable del fichero o tratamiento, como persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Por su parte, el nuevo Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, completa la definición anterior, indicando que se considerará Responsable del fichero o del tratamiento, la Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Esta nueva definición introduce dos novedades importantes a efectos de delimitar la figura del Responsable de un fichero que trate datos de carácter personal, admitiendo la posibilidad de que más de una persona, física o jurídica, pueda tener atribuciones para decidir sobre la finalidad, contenido y uso del tratamiento, así como que quién efectivamente sea el responsable del tratamiento de los datos no tenga porqué realizarlo materialmente.

También se definen en el artículo 5 del Reglamento de desarrollo de la LOPD, los conceptos de ficheros de titularidad privada y pública, con el siguiente tenor literal:

Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

La Ley 4/2006, de 22 de diciembre, de Medidas Fiscales y Administrativas, procedió en su artículo 12, a la creación de las Empresas Públicas de la Comunidad de Madrid que tendrán como objeto la gestión y administración de los nuevos hospitales con forma de Entidad de

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Derecho público adscritas a la Consejería de Sanidad y Consumo (hoy Consejería de Sanidad) de la Comunidad de Madrid.

El artículo 26.1.27 de la Ley Orgánica 3/1983, de 25 de febrero, del Estatuto de Autonomía de la Comunidad de Madrid, de acuerdo con lo establecido en el artículo 148.1.22 de la Constitución Española, atribuye a la Comunidad de Madrid la competencia exclusiva en materia de vigilancia y protección de sus edificios e instalaciones.

Conforme a la regulación analizada, la vigilancia y protección de los edificios e instalaciones de ese Hospital está atribuida como competencia exclusiva, a la Empresa Pública que tiene como objeto su gestión y administración, constituyendo una potestad de derecho público.

De acuerdo a la definición de fichero de responsable de fichero, como aquel que decide sobre la finalidad, contenido y uso del tratamiento, y atendiendo a que la captación de imágenes con fines de seguridad se ha considerado una potestad de derecho público, en los edificios e instalaciones de la Comunidad de Madrid, en el supuesto planteado, debe considerarse como tal a la Empresa Pública de ese Hospital, correspondiendo al mismo cumplir con todas las obligaciones descritas en la Instrucción 1/2007 de la APDCM.

Los hospitales de la Comunidad de Madrid en forma de entidad de derecho público son competencia de la APDCM.

La instalación de sus cámaras de videovigilancia tienen que cumplir con la LOPD, su Reglamento de desarrollo y la Instrucción 1/2007 de la APDCM.

6.2.- Instalación de un sistema de control de la actividad de los empleados públicos por medio de cámaras en el centro de recepción de llamadas Madrid-112.

En cuanto a los tratamientos de imágenes de personas identificadas o identificables realizados en el ámbito de la relación laboral, mediante la instalación de sistemas de cámaras o videocámaras en el "lugar de trabajo", en primer lugar, debe traerse a colación lo dispuesto por el artículo 20.3 del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores. De acuerdo con dicho precepto, *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".*

Pues bien, sobre la base de lo dispuesto por dicho artículo, con pleno respeto a los principios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y, especialmente, con plena observancia del principio de calidad de los datos, entre las diferentes formas de legitimación de imágenes derivadas de la aplicación de lo dispuesto por el artículo 6 de dicha Ley Orgánica, se encuentra la posibilidad de que las mismas se recojan en el marco de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

En el supuesto sometido a consulta, deberá considerarse Responsable del tratamiento de datos personales realizado a través de sistemas de cámaras o videocámaras, a la Administración pública u Órgano administrativo que ostente la competencia administrativa a cuyo fin sirve la instalación del sistema de cámaras o videocámaras en el ámbito laboral. En este sentido, deberá estarse a la definición de Responsable contenida en el artículo 3 d) de

la Ley Orgánica 15/1999, de acuerdo con la cual concurre dicha condición en la *"Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*

En consecuencia, de acuerdo con el contenido de la consulta, el tratamiento de las imágenes se realiza en el ámbito de actuación y bajo la dirección del Organismo Autónomo Madrid 112, toda vez que las finalidades, el contenido y el uso del tratamiento responden a la decisión del mismo, que se encuentra sometido a lo dispuesto por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, adoptándose dicha decisión en el ejercicio de una competencia propia atribuida por el ordenamiento jurídico.

La Instrucción 1/2007, de 16 de mayo, de esta Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, señala en su NORMA CUARTA (Legitimación y Finalidad en el tratamiento de imágenes):

"No será preciso el consentimiento de los afectados para el tratamiento de las imágenes objeto de la presente Instrucción cuando, de acuerdo con lo dispuesto por los artículos 6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con pleno respeto a los principios establecidos en dicha Ley Orgánica y, especialmente, con plena observancia del principio de calidad de los datos, concurra alguno de los siguientes supuestos:
(...)

1. *Cuando la imagen se recoja para el ejercicio de las funciones propias de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere el*

Apartado 1 de la NORMA Primera de la presente Instrucción, en el ámbito de sus competencias.

En concreto se reputará legítima la utilización de sistemas de cámaras o videocámaras:

a) Con fines de vigilancia para la seguridad.

(...).”

Pues bien, a nuestro juicio, de acuerdo con dicha previsión, la instalación y mantenimiento por parte del Centro de Recepción de llamadas Madrid-112 de sistemas de cámaras o videocámaras, podría encajar en el supuesto al que se refiere el precepto transcrito, por cuanto que, en el desarrollo de las actividades propias del servicio de emergencias Madrid 112, se ponen de manifiesto necesidades específicas relativas al mantenimiento de la seguridad de personas y bienes.

A mayor abundamiento, podría considerarse la necesidad de realizar las correspondientes grabaciones en atención a la obtención de pruebas suficientes en orden al posible ejercicio de acciones administrativas y/o judiciales, dirigidas a la defensa del Centro de emergencias frente a eventuales denuncias y acciones de exigencia de responsabilidad.

De otra parte, y en lo que respecta específicamente a las grabaciones realizadas en relación con la actividad de los trabajadores, resultaría –asimismo- de aplicación lo dispuesto en el Apartado 3 de la NORMA CUARTA de la Instrucción a saber:

3. *“Cuando 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, resulten necesarios para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa,*

vinculada al ámbito competencial propio de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere la presente Instrucción.

En concreto se reputará legítima la utilización de sistemas de cámaras o videocámaras:

a) *Cuando el tratamiento de la imagen tenga por objeto el seguimiento, control y garantía del cumplimiento de la relación laboral, funcionarial o estatutaria.*
b) *Cuando el tratamiento de la imagen se realice en el marco de una relación jurídica derivada del sometimiento del afectado a una relación administrativa de sujeción especial.*
c) *Cuando el tratamiento de la imagen se dirija a la mejora en la calidad de la gestión de los servicios públicos.*
d) *Cuando se realice cualquier otro tratamiento que resulte necesario para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa, vinculada al ámbito competencial del Responsable del tratamiento en el ejercicio de sus funciones".*

Debido a las peculiaridades y características del Centro de Emergencias 112 es proporcional el uso de cámaras para controlar la actividad laboral.

6.3.- Acceso de un instructor de un expediente disciplinario que se tramita por la Inspección de Servicios de una Universidad a determinadas imágenes sobre un trabajador afectado por ese procedimiento.

Según se expone en la consulta, el Órgano instructor del expediente disciplinario (Inspección de Servicios de la Universidad) ha requerido formalmente dicha grabación para documentar las actuaciones que está llevando a cabo.

Con carácter general, debe indicarse que la comunicación, mediante la puesta a disposición de los Servicios de Inspección de las imágenes del trabajador (personal laboral) obrantes en poder de la Gerencia de la Universidad, que es la responsable del fichero de "VIGILANCIA" constituye, conforme a lo dispuesto en el artículo 3 i) de la citada Ley Orgánica, una cesión de datos de carácter personal, definida como *"Toda revelación de datos efectuada a persona distinta del interesado".*

Tal y como determina el artículo 11.1 de la Ley Orgánica 15/1999, *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"*.

No obstante, la propia Ley Orgánica atendiendo a circunstancias especiales, regula en su apartado 2, una serie de excepciones a la norma general del consentimiento, y así, entre dichas excepciones, prevé la posibilidad de que una Ley autorice la cesión.

Así, el artículo 73 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, *(el personal de administración y servicios)* establece lo siguiente:

"1. El personal de administración y servicios de las Universidades estará formado por personal funcionario de las escalas de las propias Universidades y personal laboral contratado por la propia Universidad, así como por personal funcionario perteneciente a los cuerpos y escalas de otras Administraciones públicas.
2. Corresponde al personal de administración y servicios la gestión técnica, económica y administrativa, así como el apoyo, asesoramiento y asistencia en el desarrollo de las funciones de la universidad.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Corresponde al personal de administración y servicios de las universidades públicas el apoyo, asistencia y asesoramiento a las autoridades académicas, el ejercicio de la gestión y administración, particularmente en las áreas de recursos humanos, organización administrativa, asuntos económicos, informática, archivos, bibliotecas, información, servicios generales, servicios científico-técnicos, así como el soporte a la investigación y la transferencia de tecnología y a cualesquiera otros procesos de gestión administrativa y de soporte que se determine necesario para la universidad en el cumplimiento de sus objetivos.

3. El personal funcionario de administración y servicios se regirá por la presente Ley y sus disposiciones de desarrollo, por la legislación general de funcionarios, y por las disposiciones de desarrollo de ésta que elaboren las Comunidades Autónomas, y por los Estatutos de su Universidad.

El personal laboral de administración y servicios, además de las previsiones de esta Ley y sus normas de desarrollo y de los Estatutos de su Universidad, se regirá por la legislación laboral y los convenios colectivos aplicables."

Complementariamente, en razón de las remisiones legales contenidas en la vigente Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, es menester –en lo relativo al personal laboral de administración y servicios- acudir a lo dispuesto en su vigente Convenio Colectivo, aprobado por Resolución de 25 noviembre 2005, y publicado en el BOCM de 4 de mayo de 2006. Así, en su TÍTULO XVII, artículos 103 a 106, se contiene el régimen disciplinario al que queda sometido dicho personal, estableciéndose que (artículo 103) *"Los trabajadores podrán ser sancionados por resolución del Rectorado de su Universidad, con ocasión de incumplimiento laboral y de acuerdo con la tipificación y graduación de faltas y sanciones que se establecen en el presente título"*. A su vez, en el artículo 104 de dicho Convenio Colectivo se establecen las "Faltas" disciplinarias en las que pueden incurrir los trabajadores, en el artículo 105, las "Sanciones" que podrán imponerse en función de las faltas cometidas, y, en el artículo 106, el "Procedimiento" a seguir en relación con este tipo de expedientes.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

A su vez, a efectos de determinar el régimen jurídico aplicable –en materia disciplinaria- al personal laboral al servicio de las Administraciones Públicas, debe acudirse a la regulación contenida en la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, en cuyo artículo 7 ("Normativa aplicable al personal laboral"), se dispone que *"El personal laboral al servicio de las Administraciones Públicas se rige, además de por la legislación laboral y por las demás normas convencionalmente aplicables, por los preceptos de este Estatuto que así lo dispongan".*

Por su parte, el artículo 153 del Decreto 58/2003, de 8 mayo, por el que se aprueban los Estatutos de la Universidad *("Servicio de Inspección"),* establece que:

"1. En la UCM existirá un Servicio de Inspección, dependiente del Rector en el ejercicio de su potestad disciplinaria y de gobierno, que tendrá como finalidad inspeccionar el funcionamiento de los servicios y colaborar en las tareas de instrucción de todos los expedientes disciplinarios y el seguimiento y control general de la disciplina académica.

2. Los cargos académicos que dirijan el Servicio de Inspección, serán nombrados por el Rector.

3. Las actuaciones de la Inspección son reservadas, sin perjuicio del derecho de los interesados a acceder a la información que legalmente corresponda.

4. El Servicio de Inspección elaborará una memoria de sus actividades, de la que dará cuenta al Consejo de Gobierno.

5. La instrucción de los procedimientos disciplinarios se encomendará a personas que no formen parte del Servicio de Inspección, aunque se adscriban temporalmente al mismo, de acuerdo con lo establecido en el Reglamento de Disciplina Académica".

A su vez, de acuerdo con el artículo 150.1 de los referidos Estatutos, se prevé –en relación con los funcionarios docentes y personal de administración y servicios- la siguiente norma de régimen disciplinario:

"En materia disciplinaria, los funcionarios se regirán por las normas generales de la función pública que les resulte de aplicación, sin perjuicio del desarrollo que de estas normas se realice en el Reglamento de Disciplina Académica, incluido en el de la Comunidad Universitaria que apruebe el Claustro".

En conclusión, el Servicio de Inspección de la Universidad, a los efectos del impulso y efectividad de su actuación inspectora, podrá acceder a las imágenes –también a las grabadas por los sistemas de cámaras o videocámaras de la Gerencia de la Universidad-, de todos los trabajadores que se hallen incursos en un determinado expediente disciplinario al objeto de documentar las correspondientes actuaciones, accediendo a dicha información a través de la información videográfica que obre en poder de la Gerencia de la Universidad ("responsables del fichero"), y procediendo –en consecuencia- a las oportunas comprobaciones necesarias para la verificación de la identidad de las personas a las que se refieren las correspondientes actuaciones instructoras, sin necesidad del previo consentimiento de los afectados.

Ello no obstante, es imprescindible que en la petición efectuada y las comprobaciones realizadas se limiten a la finalidad del acceso a los datos, así como que se entregue el mínimo de datos necesario de las personas que permitan alcanzar la finalidad pretendida con el acceso. De igual forma, por el Servicio de Inspección no se podrán utilizar los datos a

los que acceda para funciones distintas de las previstas en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y en los Estatutos de la Universidad, aprobado por Decreto 58/2003, de 8 mayo.

En este sentido, la petición realizada –debidamente fundamentada- deberá referirse a las investigaciones e indagaciones derivadas de un expediente o expedientes concretos, debiendo los datos recabados resultar "adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que fueron obtenidos", y no pudiendo usarse dichos datos "para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos" (artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre).

Si por parte de los Servicios de Inspección, o por cualquier otro Órgano de la Universidad, se pretendiere el acceso a imágenes tratadas a través de cámaras o videocámaras con cualquier otra finalidad incompatible con la expresamente declarada para el mencionado fichero, debería procederse –en su caso- a la modificación del mismo, o bien a la creación e inscripción de otro nuevo y distinto del actualmente registrado en el Registro de Ficheros de esta Agencia, que respondiera –en dicho caso- a tal finalidad (incompatible con la actualmente declarada).

Asimismo, conviene señalar que, una vez obtenida la información por parte del Servicio de Inspección, el acceso a la información contenida en las grabaciones debe regirse en todo caso por el deber de secreto, de acuerdo con lo previsto en el artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el artículo 11 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

El incumplimiento de lo previsto en dichos preceptos y/o el uso de los datos de carácter personal obtenidos por parte del Servicio de Inspección que realiza la petición para finalidades distintas de las propiamente inspectoras, podría dar lugar, en su caso, a la incoación del correspondiente expediente sancionador por parte de la autoridad de control competente por infracción de lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El servicio de inspección de una Universidad puede acceder a las imágenes en el ejercicio de su labor inspectora.

La cesión debe cumplir con el principio de calidad de datos de manera que no haya una cesión indiscriminada.

El acceso a las imágenes debe regirse también por el cumplimiento del deber de secreto.

6.4.- Uso de las cámaras instaladas en un edificio de un Ayuntamiento para controlar el horario de los trabajadores.

El artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal regula el principio de la calidad de los datos estableciendo su apartado 1 que "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

El apartado 2 del mismo artículo preceptúa que "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidad incompatibles con aquellas para las que los datos hubieran sido recogidos".

En este sentido, la finalidad del tratamiento de los datos personales debe ser puesta en relación con lo que se haya declarado en la disposición de carácter general de creación del fichero correspondiente.

Así, tanto el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, apartado 2 a), como el artículo 4.2.a) de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, establecen que en las *"disposiciones de creación o de modificación de los ficheros se deberá indicar: la finalidad del fichero y los usos previstos para el mismo"*.

Según la información obrante en el Registro de Ficheros de Datos Personales, la finalidad declarada de este fichero es "garantizar la seguridad de las sedes del Ayuntamiento mediante videovigilancia perimetral y de los accesos tanto exteriores como interiores".

En consecuencia, y puesto que la finalidad del fichero citado es el "control de seguridad" no se pueden utilizar las imágenes captadas por el sistema de videovigilancia para otros fines que no sea el control de la seguridad, ya que si se utilizase para otro fin se estaría vulnerando el artículo 4.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
Además, se procedería a un uso del fichero con una finalidad diferente a la declarada en la propia disposición general de creación del fichero, pudiendo el responsable incurrir en la comisión de alguna de las infracciones tipificadas por la Ley Orgánica 15/1999, de 13 de diciembre.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

En este sentido, según el artículo 44.3.d) de la citada Ley se considera 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 constituyan una infracción muy grave".*

No obstante lo anterior, cabría la posibilidad de que las imágenes grabadas con la finalidad de garantizar la seguridad del edificio pudiesen ser utilizadas en el marco de un procedimiento disciplinario cuando en el mismo hubiera elementos relativos a la violación o incumplimiento de las normas de seguridad y control de accesos, si bien la incorporación de las citadas imágenes debe ajustarse a lo que las normas reguladoras de los procedimientos disciplinarios establezcan al respecto (por ejemplo, en lo referente a la práctica e incorporación de pruebas) y el acceso a las mismas debe realizase por parte de los Servicios de Inspección en el ejercicio de sus competencias.

Si la finalidad declarada de las cámaras es la seguridad, éstas no pueden utilizarse para vigilar el control horario de los trabajadores, exceptuándose que el acceso se realice en el marco de un procedimiento disciplinario.

6.5.- Instalación de cámaras de videovigilancia en el servicio de transportes de viajeros por carretera.[10]

Conviene referir que, de acuerdo con el contenido del escrito de consulta, la entidad consultante justifica debidamente la adopción de la medida a la que se refiere este Informe, en atención a los incidentes que se producen en los autobuses que prestan el servicio público regular de transportes de viajeros por carretera que, en algunas ocasiones, han

[10] Este informe es anterior a la aprobación de la Instrucción 1/2007 de la APDCM.

desembocado en agresiones a los conductores. Asimismo, según se expone, la frecuencia y reiteración de los incidentes mencionados impide su consideración como hechos aislados, aconsejando la adopción de medidas que eviten que este tipo de incidentes vuelvan a repetirse.

A su vez, según se indica en el dicho escrito, se ha puesto de manifiesto la existencia de una serie de riesgos laborales que afectan a los empleados de las empresas que prestan el servicio público de transporte, dando lugar a que la Inspección de Trabajo prescriba la necesidad de adoptar ciertas medidas de protección tendentes a garantizar la seguridad de los trabajadores.

Igualmente, se refiere a la adecuación e idoneidad de la medida de cuya adopción se trata, considerando que, con base en el estudio de los medios y sistemas de autoprotección aplicables para el riesgo que se trata de evitar, "la medida planteada es la más adecuada y acertada de las que se pueden adoptar, en consideración a las circunstancias en que se producen los hechos". Así, según se expone, el sistema de videovigilancia por medio de cámaras posee un importante carácter disuasorio, sirviendo de ayuda para la investigación de los hechos y la identificación de los responsables, lo que le convierte en un sistema necesario.

A su vez, la entidad consultante, se refiere a "la proporcionalidad de la medida, por medio de la cual se pretende garantizar la integridad física, resultando equilibrada en atención al resultado de la ponderación entre el bien jurídico protegido y el grado de restricción del derecho fundamental a la intimidad y a la propia imagen".

Asimismo, según se indica, "siguiendo los criterios marcados por la Jurisprudencia del Tribunal Constitucional, la entidad consultante pretende no conservar las imágenes obtenidas más allá del plazo establecido, procediéndose a su destrucción, salvo en aquellos

casos en que se deban facilitar a la autoridad judicial, a requerimiento de ésta, para el esclarecimiento de hechos susceptibles de tipificarse como ilícitos penales".

De acuerdo con el contenido de la Instrucción 1/2006, de 8 de noviembre, de la AEPD, en la instalación de sistemas de videocámaras será necesario ponderar los bienes jurídicos protegidos, con especial atención al respeto del principio de proporcionalidad. De acuerdo con la doctrina del Tribunal Constitucional, la *"superación del juicio de proporcionalidad"* en la instalación de este tipo de dispositivos exige la concurrencia de tres requisitos básicos, a saber: que la medida adoptada sea susceptible de cumplir el objetivo propuesto (juicio de idoneidad), que no exista otra medida más moderada para la consecución del fin pretendido (juicio de necesidad), y que dicha medida resulte ponderada o equilibrada (juicio de proporcionalidad en sentido estricto).

Estos criterios de legitimación y proporcionalidad a la hora de valorar la captación de imágenes con fines de vigilancia a través de cámaras o videocámaras, son los que han sido considerados por la Jurisprudencia del Tribunal Constitucional (ver en sus Sentencias SSTC 66/1995, de 8 de mayo F. 5; SSTC 55/1996, de 28 de marzo FF. 6, 7, 8 y 9; SSTC 207/1996, de 16 de diciembre F. 4.e; y SSTC 37/1998, de 17 de febrero F. 8).

A juicio de esta Agencia de Protección de Datos de la Comunidad de Madrid, el cumplimiento de lo previsto por los artículos 2 (Legitimación) y 4 (Principios de calidad, proporcionalidad y finalidad del tratamiento) de la citada Instrucción 1/2006, de 8 de noviembre, implica una determinación clara de los fines para los que se recogen y tratan los datos de carácter personal relativos a la imagen de los afectados.

Además, se hace necesario evaluar el cumplimiento de la proporcionalidad y legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

fundamentales de las personas y, especialmente, si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva.

En el presente caso, el juicio de idoneidad ha de ser necesariamente positivo, ya que la medida propuesta, aun con las deficiencias técnicas que, en su caso, pudiera presentar, sirve al propósito perseguido, esto es, establecer un sistema disuasorio que sirva para evitar o disminuir las agresiones que se producen en el transporte público y, en su caso, sirva de ayuda para la investigación de los hechos y la identificación de los responsables.

Pero es en la valoración del juicio de necesidad cuando comienzan a percibirse dificultades. De este modo, para llevar a cabo la vigilancia y seguimiento de las incidencias que se producen en los sistemas de transporte, resulta necesario que por parte del Consorcio Regional de Transportes se valoren con cautela las implicaciones de la adopción de un sistema como el propuesto y la posibilidad de adoptar otros que, siendo igualmente idóneos, resulten menos intrusivos en la intimidad y privacidad de las personas que deben someterse a los mismos.

Igualmente, también han de apuntarse ciertas reservas en el ámbito del estricto juicio de proporcionalidad. De tal suerte, el Órgano consultante debería también plantearse si la existencia de dichas medidas alternativas hace que del juicio de proporcionalidad en relación con la medida que se pretende implantar se obtengan los resultados óptimos, sin menoscabo de los derechos fundamentales a la intimidad y a la propia imagen, y a la protección de datos de carácter personal.

En consecuencia, corresponderá a la entidad consultante la decisión en orden a la implementación del sistema propuesto, en atención tanto a las diversas circunstancias concurrentes, como a los diferentes supuestos de hecho que se plantean en la realidad del transporte urbano, decidiendo –en consideración a dichos hechos y circunstancias- sobre la

instalación de sistemas de cámaras y videocámaras de acuerdo con el referido principio de *"Proporcionalidad"*.

En razón de la argumentación anterior (juicio de proporcionalidad), el Órgano consultante debería considerar la instalación de dichos sistemas en aquéllas líneas y/o servicios de transporte en los que la concurrencia de motivos de seguridad aconsejaran indubitadamente dicha instalación, en atención a la existencia una experiencia, previamente contrastada y consolidada, referida a los problemas de seguridad de los usuarios y de los profesionales del transporte urbano.

Se cumple el principio de proporcionalidad al instalar cámaras en los autobuses de transportes de viajeros en los que los conductores han sufrido agresiones.

6.6.- Existencia de regulación normativa o jurisprudencia en base a la cual el Alcalde o Pleno del Ayuntamiento pueden resolver o acordar la prohibición de grabación con cámara de los Plenos municipales.

La grabación de las sesiones del Pleno del Ayuntamiento mediante sistemas de cámaras o videocámaras, a la que se refiere la consulta constituye, desde el punto de vista de la Ley Orgánica 15/1999, una forma de tratamiento de datos de carácter personal, definido por su artículo 3 c) como *"Operaciones y Procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

En idéntico sentido, el Apartado 2 (*"Ámbito objetivo y tipos de tratamiento sometidos a la norma"*) de la NORMA PRIMERA, de la Instrucción 1/2007, de 16 de mayo (BOCM de 18 de julio), de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, establece que:

> *"2.1 Esta Instrucción se aplica al tratamiento de la imagen de las personas físicas identificadas o identificables, así como al tratamiento de cualquier otro dato de carácter personal realizado a través de sistemas de cámaras o videocámaras, por parte de las Instituciones, Órganos, Organismos, y demás Entes y Entidades mencionados en esta NORMA Primera.*
>
> *2.2 Se considerará identificable una persona cuando su identidad pueda determinarse mediante la captación, grabación, transmisión, conservación o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, o a través del tratamiento que resulte de los datos personales relacionados con dichas imágenes, sin que ello requiera plazos, actividades o esfuerzos desproporcionados.*
>
> *2.3 Las referencias a la imagen de las personas físicas identificadas o identificables contenidas en esta Instrucción se entenderán hechas también a cualquier otro dato de carácter personal sobre el que se realicen tratamientos a través de sistemas de cámaras o videocámaras. A dichos efectos, se estará a la definición de dato de carácter personal contenida en el artículo 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre.*
>
> *2.4 El tratamiento de datos personales objeto de esta Instrucción comprende la captación, grabación, transmisión, conservación y almacenamiento de imágenes, realizados tanto a través de soportes físicos de carácter digital,*

como mediante soportes analógicos estructurados con arreglo a criterios personales.

2.5 La presente Instrucción resultará aplicable aún cuando las imágenes captadas no se incorporen y/o registren en un soporte físico, limitándose la captación a los fines de su reproducción o emisión en tiempo real, incluido el visionado de dichas imágenes a distancia, sin perjuicio de lo dispuesto en el Apartado 1.7 de la NORMA Séptima".

Por su parte, de acuerdo con su *"Ámbito subjetivo"* de aplicación, contenido en el Apartado 1 de la propia NORMA PRIMERA de la citada Instrucción, *"1.1 La presente Instrucción se aplica a los tratamientos de datos personales a los que se refiere el apartado 2 de esta NORMA Primera, realizados por las Instituciones de la Comunidad de Madrid, por sus Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de su Administración Pública, así como por los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, y por las Universidades Públicas de la Comunidad de Madrid".*

Lo anterior apunta a la necesidad de analizar, con carácter previo, si en el presente supuesto concurre el mencionado ejercicio de funciones propias por parte del Ayuntamiento consultante, ejercidas dentro del ámbito de las competencias que le son atribuidas legalmente.

En razón del análisis propuesto, conviene traer a colación lo dispuesto por el artículo en los artículos 69 y siguientes de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, a saber:

"Artículo 69:

1. Las Corporaciones locales facilitarán la más amplia información sobre su actividad y la participación de todos los ciudadanos en la vida local.

2. Las formas, medios y procedimientos de participación que las Corporaciones establezcan en ejercicio de su potestad de autoorganización no podrán en ningún caso menoscabar las facultades de decisión que corresponden a los órganos representativos regulados por la ley.

Artículo 70.

1. Las sesiones del Pleno de las Corporaciones locales son públicas. No obstante, podrán ser secretos el debate y votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta.

No son públicas las sesiones de las Comisiones de Gobierno.

2. Los acuerdos que adopten las Corporaciones locales se publican o notifican en la forma prevista por la Ley. Las Ordenanzas, incluidas las normas de los Planes urbanísticos, se publican en el «Boletín Oficial» de la Provincia y no entran en vigor hasta que se haya publicado completamente su texto y haya transcurrido el plazo previsto en el artículo 65.2. Idéntica regla es de aplicación a los Presupuestos, en los términos del artículo 112.3, de esta Ley.

3. Todos los ciudadanos tienen derecho a obtener copias y certificaciones acreditativas de los acuerdos de las Corporaciones locales y sus antecedentes, así como a consultar los archivos y registros en los términos que disponga la legislación de desarrollo del artículo 105, letra b) de la Constitución. La denegación o limitación de este derecho, en todo cuanto afecte a la seguridad y defensa del Estado, la averiguación de los delitos o la intimidad de las personas, deberá verificarse mediante resolución motivada.

(...)

Artículo 72.

Las Corporaciones locales favorecen el desarrollo de las asociaciones para la defensa de los intereses generales o sectoriales de los vecinos, les facilitan la más amplia información sobre sus actividades y, dentro de sus posibilidades, el uso de los medios públicos y el acceso a las ayudas económicas para la realización de sus actividades e impulsan su participación en la gestión de la Corporación en los términos del número 2 del artículo 69. A tales efectos pueden ser declaradas de utilidad pública".

Por su parte, el artículo 207 del Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Corporaciones Locales, aprobado por Real Decreto 2568/1986, de 28 de noviembre, establece que, *"todos los ciudadanos tienen derecho a obtener copias y certificaciones acreditativas de los acuerdos de los órganos de gobierno y administración de las entidades locales y de sus antecedentes, así como a consultar los archivos y registros en los términos que disponga la legislación de desarrollo del artículo 105 b), de la Constitución Española. La denegación o limitación de este derecho, en todo cuanto afecte a la seguridad y defensa del Estado, la averiguación de los delitos o la intimidad de las personas, deberá verificarse mediante resolución motivada".*

A su vez, de acuerdo con lo dispuesto por el artículo 229 del propio Real Decreto 2568/1986, de 28 de noviembre:

"229.2 Sin perjuicio de lo dispuesto en el artículo 70.2 de la Ley 7/1985, de 2 de abril, la Corporación dará publicidad resumida del contenido de las sesiones plenarias y de todos los acuerdos del Pleno y de la Comisión de Gobierno, así como de las resoluciones del Alcalde y las que por su delegación dicten los Delegados".

"229.3 A tal efecto, además de la exposición en el tablón de anuncios de la Entidad, podrán utilizarse los siguientes medios:

a) Edición, con una periodicidad mínima trimestral, de un Boletín Informativo de la Entidad.

b) Publicación en los medios de comunicación social del ámbito de la Entidad."

De la normativa transcrita, se infiere claramente que las sesiones del Pleno de dicho Ayuntamiento, son de carácter público, y se transcriben, en cuanto a las intervenciones y debates que en las mismas se producen en un diario de sesiones que, a semejanza de lo que ocurre en otros órganos de similar naturaleza, constituirán la memoria histórica de la institución municipal.

A su vez, del conjunto de preceptos a los que se ha hecho cumplida mención, se extrae, con carácter general, la existencia de una habilitación legal suficiente en orden al tratamiento de los referidos datos por parte del Ayuntamiento consultante, que no exigirá del consentimiento de las personas afectadas, y que encaja plenamente con lo previsto por el artículo 6, apartados 1 y 2, de la Ley Orgánica 15/1999, de 13 de diciembre, cuando –por vía de excepción- establecen que:

"Artículo 6. Consentimiento del afectado

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 (…)"

No obstante lo anterior, y si ese Excmo. Ayuntamiento decidiese proceder a las grabaciones del Pleno, de acuerdo a lo establecido en la Ley 8/2001, de 13 de julio de Protección de Datos de Carácter Personal en la Comunidad de Madrid, y en el Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones

de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro, con carácter previo a la realización de las grabaciones se debe crear, mediante la aprobación de una ordenanza municipal, el correspondiente fichero de datos de carácter personal.

Asimismo, de acuerdo con los datos obrantes en el Registro de Ficheros de esta Agencia de Protección de Datos de la Comunidad de Madrid, se observa que no aparece inscrito fichero alguno relativo al tratamiento de los datos personales recabados con motivo del desarrollo de las sesiones del Pleno del Ayuntamiento consultante, referido a la grabación del desarrollo de las sesiones plenarias.

Por otra parte, desde la perspectiva de lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, el tratamiento por parte del Ayuntamiento de las imágenes del Pleno por medio de sistemas de cámaras o videocámaras, realizado en el ejercicio de sus competencias legalmente atribuidas, deberá respetar el principio de calidad de datos, al que se refiere el artículo 4 de la LOPD, cuando dispone 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 consecuencia, si esa Corporación decidiese realizar la grabación del Pleno, la misma deberá ajustarse a su necesaria compatibilidad con las finalidades derivadas de la atribución normativa de funciones que le son propias, ajustando el tratamiento de los

datos a su debida proporcionalidad, con plena garantía de dichos principios (compatibilidad y proporcionalidad) en las grabaciones que lleve a cabo.

En este sentido, en relación con el *"principio de calidad de los datos"*, en la CONSIDERACIÓN JURÍDICA PRIMERA de su Informe de 26 de noviembre de 2007, el Servicio Jurídico de la Comunidad de Madrid en esta Agencia de Protección de Datos de la Comunidad de Madrid, señalaba lo siguiente:

"En relación con la consulta planteada, esto es, si el Ayuntamiento puede conservar las imágenes para propio uso del pleno durante el tiempo necesario, es necesario acudir a la norma quinta, apartado 3, de la Instrucción 1/2007, de 16 de mayo, de la Agencia de protección de datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid, que dispone lo siguiente:

.-Los datos de carácter personal recogidos mediante sistemas de cámaras o videocámaras serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, y en todo caso en el plazo máximo de un mes desde su captación, sin perjuicio de las excepciones contenidas en esta norma.-

Con arreglo a esto, el plazo máximo de conservación de las imágenes es de un mes, pero el apartado 3.2 se encarga de establecer una excepción:

.-Las imágenes captadas para finalidades distintas a la seguridad podrán conservarse hasta que hayan dejado de ser necesarias, dentro de los plazos máximos establecidos por la normativa sectorial específicamente aplicable.-

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Puesto que la legislación de régimen local no establece nada al respecto, debe entenderse que no hay un límite máximo temporal y que las imágenes pueden conservarse el tiempo que sea necesario".

Dicho lo anterior, si ese Excmo. Ayuntamiento decidiese además de realizar la grabación publicar la misma en su página Web Institucional, nos encontraríamos ante una cesión de datos de carácter personal, puesto que habría una cesión de imágenes mediante retransmisión y mantenimiento de las mismas en un sitio Web institucional.

Esta cesión quedará sometida a lo dispuesto por el artículo 11.1 de la citada Ley Orgánica, en cuya virtud *"los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".* Esta disposición se ve excepcionada en el supuesto que ahora nos ocupa por lo dispuesto en el apartado 2.a) del propio artículo 11 de la meritada Ley Orgánica, que posibilita la cesión inconsentida de los datos en caso de que la misma se encuentre fundamentada en lo establecido por una norma con rango de Ley.

En este sentido, debe traerse de nuevo a colación lo dispuesto por los artículos 69 y siguientes de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local. De este modo, de acuerdo con el tenor literal de dichos preceptos, que establecen la *"publicidad de las sesiones del Pleno",* la cesión de los datos personales correspondientes resultaría plenamente habilitada por lo dispuesto en las referidas normas.

Mas, de otra parte, es menester volver a reiterar el necesario respeto de las garantías derivadas del denominado *"principio de calidad de los datos",* reconocido por el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En relación dicho principio, en la CONSIDERACIÓN JURÍDICA SEGUNDA de su Informe de 26 de noviembre de 2007, el Servicio Jurídico de la Comunidad de Madrid en esta Agencia de Protección de Datos de la Comunidad de Madrid, señalaba lo siguiente:

"La cuestión planteada implica que los datos personales objeto del tratamiento ya no son sólo las imágenes de los miembros del pleno, sino también datos personales de otras personas. En este supuesto, se realizaría una cesión de datos personales de personas que no son miembros del pleno a través de Internet.

El principio de calidad de los datos del artículo 4.1 de la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal exige que los datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. La finalidad de la grabación y difusión de las sesiones del pleno es, como se ha señalado en la consideración jurídica anterior, permitir el conocimiento por los ciudadanos de la actividad política que desarrolla. Para dicha finalidad, lo más habitual es que no sea necesario incluir datos personales de los ciudadanos, sobre todo si la difusión de tales datos ya está regulada y tiene asignada otros canales para ello. Por ejemplo, los actos administrativos se notifican a los interesados o se publican en los boletines oficiales, según lo dispuesto en los artículos 58 a 60 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Sin embargo, debe tenerse en cuenta que en algunos casos puede ocurrir que en la discusión de un tema esencial en la actividad política del Ayuntamiento se incluyan datos personales y que estos datos sean imprescindibles para la comprensión del asunto de que se trate. En este caso, deberá considerarse que la cesión de dichos personales no es excesiva para la finalidad perseguida.

Por tanto, sólo en el supuesto de que la grabación y difusión de los datos personales que surjan en los debates puedan contribuir al conocimiento por los ciudadanos de la actividad política que desarrolla el pleno podrán realizarse dichos tratamientos sin infringir el principio de calidad de los datos".

Para concluir en su CONSIDERACIÓN JURÍDICA TERCERA, manteniendo que:

"Por lo que respecta a la última cuestión planteada, también el principio de calidad de los datos es decisivo para su resolución. La grabación del público que asiste a las sesiones y su posterior publicación en Internet no es necesaria para el cumplimiento de la finalidad de dar conocimiento de la actividad política del Ayuntamiento y, por ello, resulta excesiva. Por tanto, el Ayuntamiento no deberá grabar imágenes del público que asiste al pleno".

En conclusión, de la normativa reseñada se extrae la existencia de habilitaciones legales concretas, contenidas en normas con rango de Ley formal, en orden a la comunicación de los datos de carácter personal (imágenes) a los que se refiere el presente informe. Ello no obstante, por parte del Responsable del tratamiento se deberá garantizar plenamente lo dispuesto en relación con el "principio de calidad" en el tratamiento de los datos de carácter personal, por lo que sólo en el supuesto de que la grabación y difusión de los datos personales que surjan en los debates puedan contribuir al conocimiento por los ciudadanos de la actividad política que desarrolla el pleno podrán realizarse dichos tratamientos sin infringir el principio de calidad de los datos.

Así, en relación con la eventual grabación y difusión de los datos personales de los ciudadanos en general, surgidos en el marco de los debates del Pleno municipal y que contribuyan al conocimiento por los ciudadanos de la actividad política que desarrolla dicho Pleno, deberá estarse a lo previsto en la Instrucción 1/2007, de 16 de Mayo, de la APDCM,

sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, y, en consecuencia, a los criterios de proporcionalidad a la hora de valorar la captación de imágenes a través de cámaras o videocámaras, que han sido considerados determinantes por la Jurisprudencia del Tribunal Constitucional, entre otras, en sus Sentencias STC 186/2000, de 10 de julio, FFJJ. 6 y 7, y STC 98/2000, de 10 de abril, FJ. 8.

De este modo, de acuerdo con dicha Jurisprudencia, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: 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).

La proporcionalidad es un elemento fundamental en la instalación de sistemas de cámaras o videocámaras en el ámbito público, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas. En consecuencia, el Ayuntamiento consultante deberá valorar con cautela las implicaciones de la adopción de estos sistemas y la posibilidad de adoptar otros que, siendo igualmente idóneos, resulten menos intrusivos para la protección de los datos de las personas que deben someterse a los mismos.

En consecuencia, la eventual grabación y difusión de los datos personales de los ciudadanos en general, surgidos en el marco de los debates del Pleno municipal y que contribuyan al conocimiento por los ciudadanos de la actividad política que desarrolla dicho

Pleno, quedará también sometida a la Instrucción 1/2007, de 16 de Mayo, de la APDCM, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, en relación con el derecho de *"Información"* (NORMA SEXTA de la Instrucción), y en relación con lo dispuesto en su NORMA SÉPTIMA, en la que bajo el título *"Derechos de las personas",* se acomete el desarrollo de los derechos de los afectados por el tratamiento de las imágenes, cuya regulación general se contiene en los artículos 15 y siguientes de la Ley Orgánica de Protección de Datos, detallándose las especialidades del procedimiento para el ejercicio de los derechos de acceso, cancelación y oposición.

De este modo, el Ayuntamiento consultante deberá atender las posibles solicitudes de acceso, cancelación u oposición ejercidas por los ciudadanos afectados por los tratamientos, debiendo adoptar las medidas oportunas para garantizar, en todo caso, la debida disociación de la imagen o, en su caso, de cualquier otro dato de carácter personal de las terceras personas afectadas por los tratamientos cuando dichas solicitudes se produjeren. A dichos efectos, el Responsable del tratamiento deberá servirse de los programas y/o herramientas informáticas adecuadas que, aplicadas sobre los datos de carácter personal de las terceras personas afectadas, impidan su identificación y la cesión de su imagen a la persona que realice la solicitud.

Finalmente, es menester referir que, en el artículo 27, *"Publicación de sesiones y acuerdos del Pleno de las Corporaciones Locales y de otros Órganos de la Administración Local"*, de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre Publicación de Datos en Boletines y Diarios Oficiales en Internet, en sitios Webs Institucionales y en otros medios electrónicos y telemáticos, se establece la siguiente regulación al respecto:

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

"27.1 La publicidad de la actividad administrativa de los gobiernos locales favorece la objetividad de la actuación administrativa local y el control social de su actividad, facilitando la participación de los ciudadanos en los asuntos públicos.

27.2 El artículo 70 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, establece que las sesiones del Pleno de las Corporaciones Locales son públicas, salvo en aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta. Sin embargo las sesiones de las Comisiones de Gobierno no son públicas.

El apartado 2 del referido artículo 70 establece que los acuerdos que adopten las Corporaciones Locales se publicarán o notificarán en la forma prevista por la ley.

27.3 En el ámbito de la Comunidad de Madrid, la Ley 2/2003, de 11 de marzo, de Administración Local de la Comunidad de Madrid, regula en su artículo 23 la forma de efectuar la información a los vecinos de manera que:

a. Los Municipios adoptaran las medidas organizativas oportunas para facilitar a los vecinos el derecho de información sobre los asuntos de interés local.

b. En todo caso los municipios establecerán a través de su Reglamento Orgánico el régimen de publicidad en lo que concierne a acuerdos, decretos y resúmenes de las sesiones del pleno, sin perjuicio de que para aquellos cuya población sea inferior a 20.000 habitantes, dicha publicidad se encuentre garantizada mediante el tablón de anuncios.

27.4 El artículo 207 del Real Decreto 2568/1986, de 28 de noviembre, que aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Corporaciones Locales, establece que todos los ciudadanos tienen derecho a obtener copias y certificaciones acreditativas de los acuerdos de los órganos de gobierno y administración de las entidades locales y de sus antecedentes, así como a consultar los archivos y registros en los términos que disponga la legislación de desarrollo del artículo 105 b), de la Constitución Española. La denegación o limitación de este derecho, en todo cuanto afecte a la seguridad y defensa del Estado, la averiguación de los delitos o la intimidad de las personas, deberá verificarse mediante resolución motivada.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Además, de acuerdo con lo dispuesto por el artículo 229 del propio Real Decreto 2568/1986, de 28 de noviembre, sin perjuicio de lo dispuesto en el artículo 70.2 de la Ley 7/1985, de 2 de abril, la Corporación dará publicidad resumida del contenido de las sesiones plenarias y de todos los acuerdos del Pleno y de la Comisión de Gobierno, así como de las resoluciones del Alcalde y las que por su delegación dicten los Delegados. A tal efecto, además de la exposición en el tablón de anuncios de la Entidad, podrán utilizarse los siguientes medios:

a) Edición, con una periodicidad mínima trimestral, de un Boletín Informativo de la Entidad.

b) Publicación en los medios de comunicación social del ámbito de la Entidad.

27.5 En relación con el Ayuntamiento de Madrid, de acuerdo con el artículo 9.2 de la Ley 22/2006, de 4 de julio, de Capitalidad y Régimen Especial de Madrid, las sesiones del Pleno son públicas. No obstante, podrán ser secretos el debate y votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta.

El Pleno puede funcionar en Comisiones que estarán formadas por los Concejales que designen los grupos políticos en proporción a su representación en el Pleno. En todo lo no previsto en dicha Ley en lo que se refiere a su convocatoria, constitución, funcionamiento y adopción de acuerdos, el Pleno se rige, en el marco de lo dispuesto por la legislación estatal básica en materia de gobierno y administración local, por su Reglamento Orgánico y las Resoluciones dictadas por su Presidente en interpretación de este.

Esta regulación se complementa con lo previsto en el Reglamento Orgánico del Pleno del Ayuntamiento de Madrid, aprobado el 31 de mayo de 2004, que en relación con la publicidad de las sesiones del Pleno establece, en su artículo 55, que las sesiones del Pleno de las Corporaciones Locales son públicas. No obstante, podrán ser secretos el debate y votación de aquellos asuntos que puedan afectar al derecho fundamental de los ciudadanos a que se refiere el artículo 18.1 de la Constitución, cuando así se acuerde por mayoría absoluta. Para ampliar la difusión del desarrollo de las sesiones podrán utilizarse sistemas de megafonía, circuitos de televisión o redes de comunicación tales como Internet.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

27.6 De acuerdo con lo anterior, el Reglamento Orgánico de cada Ayuntamiento es la norma prevista en la ley a través de la cual se establecerá el régimen de publicidad de los acuerdos, decretos y resúmenes del pleno. Habrá que acudir por tanto al Reglamento Orgánico de cada Ayuntamiento para comprobar si contiene un régimen específico a través del cual se pueda publicar en el sitio Web municipal el contenido de estos acuerdos plenarios.

En consecuencia, si así se encuentra previsto reglamentariamente y siempre que dichos acuerdos en los que se contiene información con datos de carácter personal no afecten al honor, a la intimidad personal o familiar y a la propia imagen de los afectados, los mismos podrán ser objeto de publicación en el sitio Web institucional del Ayuntamiento sin contravenir por ello la Ley Orgánica 15/1999, de 13 de diciembre.

27.7 De conformidad con el principio de finalidad previsto en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, los datos personales serán cancelados cuado hayan dejado de ser necesarios o pertinentes para la finalidad para la cual se registraron, por lo que la Administración u Órgano competente deberá analizar caso por caso la finalidad por la que los datos personales fueron incorporados al acuerdo municipal para determinar cuándo deberán ser cancelados.

27.8 A su vez, debe tenerse en cuenta que, en ocasiones, los datos personales objeto de publicación no son los de los miembros del Pleno, sino de terceras personas. En consecuencia, con la publicación de los datos a través del sitio Web del Ayuntamiento se realizaría una cesión de datos personales de personas que no son miembros del Pleno a través de Internet.

En estos casos, para la consecución de la finalidad perseguida, lo más habitual es que no sea necesario incluir datos personales de los ciudadanos y, por ello, dicha publicación resultaría excesiva. Por tanto, el Ayuntamiento no debería publicar en Internet dichos datos.

Sin embargo, debe tenerse en cuenta que en algunos casos puede ocurrir que en la discusión de un tema esencial en la actividad política del Ayuntamiento se incluyan datos personales y que estos datos sean imprescindibles para la comprensión del asunto de que se trate. En este caso, deberá considerarse que la publicación de dichos datos personales no es excesiva para la finalidad perseguida. Por tanto, sólo en el supuesto de que la publicación de los datos personales de terceras

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

personas que surjan en los debates pueda contribuir al conocimiento por los ciudadanos de la actividad política que desarrolla el Pleno podrá realizarse dicha publicación sin infringir el principio de calidad de los datos.

En consecuencia, se recomienda que en la publicación y la eventual difusión de los datos personales de los ciudadanos en general surgidos en el marco de los debates del Pleno municipal a través de Internet, el Ayuntamiento correspondiente atienda las posibles solicitudes de acceso, cancelación u oposición ejercidas por los ciudadanos afectados por dicha publicación, debiendo adoptar las medidas oportunas para garantizar el ejercicio de estos derechos cuando dichas solicitudes se produjeren.

27.9 Para la publicación de actas y acuerdos del resto de Órganos de la Administración Local en sitios Web institucionales regirán las reglas descritas en este artículo, de manera que no podrán publicarse datos personales de los ciudadanos que afecten a su derecho al honor, a la intimidad personal o familiar y a la propia imagen".

La grabación de las sesiones del Pleno de los Ayuntamientos constituye un tratamiento de datos de carácter personal, debiendo aplicar la Instrucción 1/2007 de la APDCM.

Si se difunde por Internet, habrá que tener en cuenta la Recomendación 2/2008 de la APDCM sobre publicación de Datos en Boletines y Diarios Oficiales en Internet, en sitios Webs Institucionales y en otros medios electrónicos y telemáticos.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

6.7.- La grabación de las sesiones del Pleno de un Ayuntamiento con el fin de crear un archivo histórico que complemente el resto de la documentación referida a las sesiones constituye un fichero de datos de carácter personal.

En su escrito, el Ayuntamiento consultante solicita que se emita Informe acerca de la necesidad de declarar un fichero, distinto a los ya declarados por dicho Ayuntamiento, en relación con la captación de imágenes de personas identificadas o identificables en los Plenos del Ayuntamiento por medio de sistemas de cámaras o videocámaras.

En este sentido, según se expone en la propia consulta y literalmente se transcribe a continuación, *"la organización de las imágenes captadas obedecerá a las fechas en que han tenido lugar las reuniones del pleno"; "la grabación de las sesiones del pleno a través de cámaras, en cualquier caso, va a constituir un soporte documental complementario del propio diario de sesiones y de las actas del pleno,(…)";* y *"la grabación de las imágenes del pleno se va a incorporar como soporte documental al contenido del diario de sesiones y de las actas del Pleno del Ayuntamiento".* Ello no obstante, por la Corporación consultante se plantean dudas acerca de la necesaria creación, declaración e inscripción del correspondiente fichero de datos personales.

Así, según cabe inferir del escrito de consulta, la grabación de imágenes se realizaría de manera complementaria o coadyuvante en relación con otra finalidad principal, cual es la propia descrita por las normas a las que se ha hecho cumplida mención, relativas a la publicidad de las sesiones y de las actas del Pleno del Ayuntamiento, por lo que coincidiría con la de otros ficheros declarados por dicha Corporación municipal ante el Registro de Ficheros de esta Agencia de Protección de Datos de la Comunidad de Madrid, coincidiendo en su contenido, uso y finalidad con la de dichos ficheros previamente declarados e inscritos.

Sin embargo, de acuerdo con los datos obrantes en el Registro de Ficheros de esta Agencia de Protección de Datos de la Comunidad de Madrid, se observa que no aparece inscrito fichero alguno

relativo al tratamiento de los datos personales recabados con motivo del desarrollo de las sesiones del Pleno del Ayuntamiento de Madrid, referido al contenido de las actas y del Diario de sesiones que, en virtud de la normativa con rango de Ley formal a la que se ha hecho cumplida mención, sean objeto de tratamiento por parte de la Corporación municipal consultante.

Ello apunta, en primer lugar, a la posibilidad de que –hasta el momento actual- por parte del Ayuntamiento consultante no se hayan realizado tratamientos de datos de carácter personal en relación con el diario de sesiones y de actas del Pleno del Ayuntamiento por no encontrarse dicha documentación informatizada, ni incorporada a *"ficheros manuales"* estructurados de acuerdo a criterios personales.

En este caso, para el supuesto sometido a consulta (grabación de las sesiones por un sistema de cámara o videocámaras) por parte del Órgano consultante se deberá proceder a la creación, declaración e inscripción de dicho fichero, donde se almacenen los datos de carácter personal objeto de tratamiento a través de cámaras o videocámaras, debiendo realizarse dicha inscripción siguiendo el procedimiento previsto en el artículo 4 de la Ley 8/2001, de 13 de julio de Protección de Datos de Carácter Personal en la Comunidad de Madrid y desarrollado posteriormente por el Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro.

En relación con la necesidad de declarar un determinado fichero con datos de carácter personal, resulta obligada la referencia a la regulación legal contenida en el artículo 6 del Decreto 99/2002, de 13 de junio, que desarrolla la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, en virtud del cual, los proyectos de disposición de carácter general deberán indicar para cada uno de los ficheros los siguientes apartados:

1. El órgano, ente o autoridad administrativa responsables de un fichero
2. El órgano, servicio o unidad ante el que se deberán ejercitar los derechos de acceso, rectificación cancelación y oposición

3. El nombre y descripción del fichero que se crea

4. El carácter informatizado ó manual estructurado del fichero

5. El sistema de información al que pertenezca

6. Las medidas de seguridad que se apliquen

7. Los tipos de datos de carácter personal que se incluirán en el mismo.

8. La descripción detallada de la finalidad del fichero y los usos previstos del mismo

9. Las personas o colectivos sobre los que se pretenda obtener datos o que resulten obligados a suministrarlos.

10. La procedencia o el procedimiento de recogida de datos

11. Los órganos y entidades destinatarios de las cesiones previstas, indicando de forma expresa las que constituyan transferencias internacionales de datos.

(...)

Por el contrario, como segunda hipótesis, en el supuesto de que, por parte de la Corporación Municipal se procediera –con carácter previo- a la creación, declaración e inscripción del correspondiente fichero relativo al diario de sesiones y actas del Pleno del Ayuntamiento (al encontrarse la información personal informatizada, o bien incorporada a ficheros manuales estructurados conforme a criterios personales), y se pretendiera la mera modificación del mismo, debería estarse a lo previsto en el artículo 7 del citado Decreto 99/2002, de 13 de junio, en el que se regula la modificación de ficheros, del siguiente modo:

"Para cada uno de los ficheros que se modifiquen, el proyecto de disposición de carácter general deberá contener principalmente:

1. El nombre del fichero que se modifica y el número de registro con el que figura inscrito en el Registro de ficheros de datos personales de la Agencia de Protección de Datos de la Comunidad de Madrid.

2. El apartado de la inscripción que se modifica sea uno o varios de los once que se recogen en la disposición de carácter general."

En resumen, la modificación de cada uno de los once apartados que figuran en la declaración inicial de creación de un fichero, implicaría la declaración de modificación de ese fichero especificando el apartado o apartados modificados.

La anterior distinción debe ponerse en relación con lo previsto por el Apartado 4 ("*Excepciones: Tratamientos accesorios de datos mediante cámaras o videocámaras"*), de la NORMA TERCERA *("Procedimiento de elaboración de la disposición de carácter general e inscripción del fichero"*), de la Instrucción 1/2007, de 16 de mayo, de la APDCM, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, en cuya virtud:

"4.1 No será exigible la declaración e inscripción de un fichero independiente con datos de carácter personal en el Registro de Ficheros, cuando el tratamiento de datos realizado por el Responsable a través de cámaras o videocámaras se incorpore, de manera inseparable, a otro fichero con datos de carácter personal debidamente notificado e inscrito en dicho Registro, a cuyo fin general sirva de forma accesoria.

4.2 En todo caso, corresponde al Responsable del tratamiento realizado por medio de cámaras o videocámaras, cuya utilización se asocie de manera inseparable y accesoria a otro fichero con datos de carácter personal, el estricto cumplimiento de lo dispuesto por el artículo 6 del Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales.

4.3 A dichos efectos, sin perjuicio de lo dispuesto por el Decreto 99/2002, de 13 de junio, en la disposición de creación o modificación del fichero principal, a cuyo fin general sirva de forma accesoria la utilización de cámaras o videocámaras, el Responsable del tratamiento deberá señalar especialmente:

a) La descripción detallada de la finalidad y los usos previstos para el fichero principal, indicando expresamente que en relación con dicha finalidad y usos se prevé la utilización de cámaras o videocámaras.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

b) Las personas o colectivos sobre los que se pretenda obtener las imágenes o que resulten obligados a suministrarlas.

c) El procedimiento de recogida de la imagen de las personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal, realizado mediante sistemas de cámaras o videocámaras.

4.4 En relación con los tratamientos de datos previamente inscritos por el Responsable, para el cumplimiento de las obligaciones previstas en esta NORMA será exigible la realización de las modificaciones necesarias, siguiendo para ello el procedimiento previsto por el artículo 7 del Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales".

En conclusión, no constando en el Registro de Ficheros de esta Agencia la inscripción de fichero alguno relativo al diario de sesiones y actas del Pleno del Ayuntamiento, deberá procederse en el sentido expuesto, deviniendo necesaria la creación, notificación e inscripción de un nuevo fichero a los efectos de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, sin perjuicio del carácter coadyuvante o accesorio que, en relación con la creación e inscripción de dicho fichero deba atribuirse al tratamiento de imágenes realizado a través de sistemas de cámaras o videocámaras, y con el debido cumplimiento de lo dispuesto en el Apartado 4 de la NORMA TERCERA de la Instrucción 1/2007, de 16 de mayo, de la APDCM.

Para dicho supuesto, esto es, cuando el tratamiento de la imagen de las personas identificadas o identificables coincida en su contenido, uso y finalidad con la propia del tratamiento documental del diario de sesiones y de las actas del Pleno del Ayuntamiento, devendrá innecesaria la creación, notificación e inscripción de un nuevo fichero a los efectos de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, resultando suficiente la declaración de un único fichero en los términos a los que se ha hecho mención. De este modo, el "fichero único", notificado e inscrito, por sus propias características, incorporaría los usos y finalidades a los que se refiere el escrito de consulta.

La grabación de las sesiones del Pleno puede considerarse un fichero de datos de carácter personal o bien ser accesorio del fichero de "Actas del Pleno" si éste ya está creado.

6.8.- Implantación de un sistema de control de videocámaras en los calabozos de las dependencias de la policía local de un Ayuntamiento.

Según se expone en el escrito de consulta, a través de dicho sistema, se pretende –dentro del ámbito de las competencias comprendidas en el artículo 53 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, que –por la propia seguridad personal de los encausados y de los propios agentes actuantes- durante la detención se garantice de manera eficiente su integridad física y sus derechos fundamentales.

Asimismo, se aduce que, además de un control o vigilancia personal, la instalación de cámaras dentro del recinto cerrado (calabozo) proporcionaría un haz de garantía, seguridad y bienestar superior, afectando las grabaciones que se realizaren solamente al recinto de la estancia, y nunca a aquellos lugares donde el interesado hiciere sus necesidades más íntimas, realizándose la grabación únicamente de imágenes y no de voz.

La normativa reguladora del tratamiento de datos personales a través de sistemas de cámaras o videocámaras actualmente vigente, se encuentra contenida en la Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y su Reglamento de desarrollo y ejecución, aprobado por Real Decreto 596/1999, de 16 de abril, en la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, en la Ley 23/1992, de 30 de julio, de Seguridad

Privada, y en el Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre.

La Instrucción 1/2007, de 16 de mayo, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, de esta Agencia de Protección de Datos de la Comunidad de Madrid, resulta aplicable a los tratamientos de datos personales realizados por medio de sistemas de cámaras o videocámaras, cuando dichos tratamientos se realicen por las Instituciones de la Comunidad de Madrid, por sus Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de su Administración Pública, así como por los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, y por las Universidades Públicas de la Comunidad de Madrid.

A su vez, de acuerdo con su NORMA PRIMERA, dicha Instrucción 1/2007, de 16 de mayo resulta aplicable a los siguientes tratamientos de datos personales:

"1.2. Los tratamientos de datos personales a los que se refiere el apartado 2 de esta Norma Primera, realizados por las Policías Locales de los municipios que integran la Comunidad de Madrid, quedarán sometidos a esta Instrucción en lo que no se oponga a la regulación específica contenida en la Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y en su Reglamento de desarrollo y ejecución, aprobado por Real Decreto 596/1999, de 16 de abril.

La recogida y tratamiento para fines policiales de los datos de carácter personal a los que se refiere el apartado 2 de esta Norma Primera, realizados por las Policías Locales de los municipios que integran la Comunidad de Madrid y que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones

penales, quedarán sometidos a esta Instrucción, sin perjuicio de lo dispuesto en el artículo 22 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.3. Esta Instrucción también se aplicará a la realización de tratamientos de imágenes mediante cámaras o videocámaras llevados a cabo por parte de otras Fuerzas y Cuerpos de Seguridad distintas de las Policías Locales, cuando actúen dentro del ámbito de dirección y para el desarrollo."

En relación con el supuesto objeto de consulta, la Instrucción 1/2007, de 16 de mayo, de esta Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la Comunidad de Madrid, dispone en su NORMA PRIMERA, apartados 2.2 y 2.5 que:

"2.2. Se considerará identificable una persona cuando su identidad pueda determinarse mediante la captación, grabación, transmisión, conservación o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o a través del tratamiento que resulte de los datos personales relacionados con dichas imágenes, sin que ello requiera plazos, actividades o esfuerzos desproporcionados".

"2.5. La presente Instrucción resultará aplicable aun cuando las imágenes captadas no se incorporen y/o registren en un soporte físico, limitándose la captación a los fines de su reproducción o emisión en tiempo real, incluido el visionado de dichas imágenes a distancia, sin perjuicio de lo dispuesto en el apartado 1.7 de la Norma Séptima."

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

A su vez, en relación con la necesaria "Legitimación y Finalidad" en el tratamiento de imágenes, debe señalarse que en la NORMA CUARTA de la citada Instrucción, se dispone que:

"No será preciso el consentimiento de los afectados para el tratamiento de las imágenes objeto de la presente Instrucción cuando, de acuerdo con lo dispuesto por los artículos 6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con pleno respeto a los principios establecidos en dicha Ley Orgánica y, especialmente, con plena observancia del principio de calidad de los datos, concurra alguno de los siguientes supuestos:

(...)

2. *Cuando la imagen se recoja para el ejercicio de las funciones propias de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere el Apartado 1 de la NORMA Primera de la presente Instrucción, en el ámbito de sus competencias.*

En concreto se reputará legítima la utilización de sistemas de cámaras o videocámaras:

b) Con fines de vigilancia para la seguridad.

(...)."

b) Con la finalidad de control y disciplina del tráfico, circulación de vehículos a motor y seguridad vial.

(...)

d) Con la finalidad de prestación de un determinado servicio público o del cumplimiento de funciones públicas de soberanía.

(...)

3. Cuando 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, resulten necesarios para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa, vinculada al ámbito competencial propio de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere la presente Instrucción.

En concreto, se reputará legítima la utilización de sistemas de cámaras o videocámaras:

(...)

b) Cuando el tratamiento de la imagen se realice en el marco de una relación jurídica derivada del sometimiento del afectado a una relación administrativa de sujeción especial.

c) Cuando el tratamiento de la imagen se dirija a la mejora en la calidad de la gestión de los servicios públicos.

(...)

7. Cuando el tratamiento de imágenes realizado a través de sistemas de cámaras o videocámaras por las Fuerzas y Cuerpos de Seguridad a los que se refiere la Norma Primera de esta Instrucción, tenga por objeto el mantenimiento de la seguridad pública que legalmente les corresponda en relación con las siguientes competencias:

a) La protección y custodia de autoridades, edificios, instalaciones, dependencias, infraestructuras y equipamientos cuando lo tengan legalmente atribuido, así como la colaboración con las Administraciones competentes en materia de seguridad.

b) En colaboración con las Administraciones competentes, cuando lo tengan legalmente atribuido, la prevención, mantenimiento y restablecimiento de la seguridad ciudadana y tratar de garantizarla en lo referente a aquellos actos que ocasionen molestia social o daños sobre bienes y personas en la vía pública.

c) El ejercicio de las competencias que en materia de policía administrativa y policía de seguridad les atribuya la normativa estatal, así como, en su caso, la denuncia en las materias de policía administrativa especial de competencia estatal.

d) El ejercicio de las competencias que en materia de policía judicial les atribuya la normativa estatal.

(...)".

Pues bien, a nuestro juicio, de acuerdo con dicha previsión, la instalación y mantenimiento por parte del Ayuntamiento consultante en las instalaciones de la Policía Local (calabozos) de sistemas de cámaras o videocámaras, podría encajar en alguno de los supuestos a los que se refiere el precepto transcrito, por cuanto que -en el desarrollo de sus servicios propios de la Policía Local-, de una parte, se ponen de manifiesto necesidades específicas relativas al mantenimiento de la seguridad de personas y bienes dentro las instalaciones policiales, dependencias, infraestructuras y equipamientos cuya custodia tiene legalmente atribuida la propia Policía Local, en aras de la mejora de la calidad del servicio prestado y en el marco de la relación administrativa de sujeción especial derivada de la detención de las personas afectadas por los sistemas de captación de imágenes, y, de otra parte, la medida podría ser adecuada para la protección de las propias personas recluidas y de los agentes de la autoridad encargados de su custodia.

Ello no obstante, el Responsable del tratamiento de las imágenes deberá estar a lo dispuesto en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre (Calidad de los datos), de acuerdo con el cual:

"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.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. (…)"

En atención a dichas previsiones, en la Instrucción 1/2007, de 16 de mayo, de la Agencia de Protección de Datos de la Comunidad de Madrid, se establecen referencias específicas a los principios de calidad y proporcionalidad en el tratamiento de las imágenes de las personas físicas identificadas o identificables.

En este sentido, dicha norma establece la obligación específica, a cargo del Responsable del tratamiento, de realizar el correspondiente juicio de proporcionalidad en relación con la instalación de sistemas de cámaras o videocámaras, debiendo incluirse entre la documentación que se remita a la Agencia de Protección de Datos de la Comunidad de Madrid para la declaración e inscripción del fichero correspondiente, un informe específico sobre la necesidad y proporcionalidad del tratamiento de las imágenes.

En concreto, en la NORMA TERCERA de dicha Instrucción (Procedimiento de elaboración de la disposición de carácter general e inscripción del fichero), se establece que:

"2.14 En su remisión a la Agencia de Protección de Datos de la Comunidad de Madrid, el proyecto de disposición de carácter general deberá ir acompañado de un informe sobre la necesidad y oportunidad del tratamiento de las imágenes realizado mediante sistemas de cámaras o videocámaras. De dicho informe quedará constancia en el expediente administrativo instruido al efecto por el Responsable del tratamiento con ocasión de la elaboración de su proyecto de disposición de carácter general de creación, modificación o supresión del fichero.

En su informe el Responsable fundamentará el tratamiento de las imágenes de personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal realizado mediante sistemas de cámaras o videocámaras, en la concurrencia de alguno de los supuestos que legitiman el tratamiento de las imágenes previstos en la NORMA Cuarta de esta Instrucción.

El Responsable razonará especialmente en su informe el cumplimiento de lo dispuesto en el Apartado 2 de la NORMA Quinta de esta Instrucción en relación con la proporcionalidad del tratamiento de las imágenes, indicando expresamente que la instalación del sistema de cámaras o videocámaras supera el juicio de idoneidad, el juicio de necesidad y el juicio de proporcionalidad en sentido estricto a los que se refiere dicha NORMA Quinta".

Enlazando con lo anterior, el Apartado 2 de la NORMA Quinta (Proporcionalidad del tratamiento de imágenes), de la Instrucción 1/2007, de esta Agencia de Protección de Datos de la Comunidad de Madrid, dispone que:

"2.1 Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad perseguida 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.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

2.2 En el informe que acompañe al proyecto de disposición de carácter general de creación, modificación o supresión de ficheros al que se refiere la NORMA Tercera de esta Instrucción, el Responsable del tratamiento justificará suficientemente que la instalación del sistema de cámaras o videocámaras resulta necesaria en consideración a los hechos y a las circunstancias concurrentes, motivando que la elección de este tipo de tratamiento de datos personales resulta la medida más adecuada, pertinente y proporcional de las que pueda adoptar.

En dicho informe, el Responsable del tratamiento deberá hacer expresa referencia a:

a) Si el tratamiento de datos personales a través de sistemas de cámaras o videocámaras constituye una medida susceptible de conseguir el objetivo que se pretende (juicio de idoneidad).

b) Si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva, teniendo en cuenta la protección de los datos de carácter personal. A dichos efectos, el Responsable del tratamiento argumentará que dicha medida es necesaria, por no existir otra más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad). En la fundamentación para la adopción de dicha medida, el Responsable del tratamiento podrá valorar la existencia una experiencia, previamente contrastada y consolidada, que aconseje la utilización de sistemas de cámaras o videocámaras para el tratamiento de los datos de carácter personal.

c) Si la medida adoptada es proporcional, resultando equilibrada en atención a la ponderación entre la finalidad perseguida y el grado de restricción del derecho fundamental a la protección de datos de carácter personal, con expresa mención a si de dicha medida derivan más beneficios o ventajas para el interés general que perjuicios

sobre la protección de los datos de carácter personal (juicio de proporcionalidad en sentido estricto).”

A su vez, de acuerdo con lo previsto por la NORMA SEXTA.- Información (Normas generales), de dicha Instrucción:

“1.1 El deber de información en relación con el tratamiento de la imagen del afectado o, en su caso, en relación con el tratamiento de cualquier otro dato de carácter personal del mismo realizado mediante sistemas de cámaras o videocámaras, se exigirá en todo caso al Responsable del tratamiento.

1.2 De acuerdo con lo dispuesto por el artículo 4.7 de la Ley Orgánica 15/1999, de 13 de diciembre, el Responsable del tratamiento velará por la recogida leal y lícita de las imágenes. Se prohíbe la recogida de imágenes por medios fraudulentos, desleales o ilícitos”.

En dicha NORMA SEXTA, de la Instrucción 1/2007, que se cita sobre el deber de *“Información”*, se recogen las especialidades derivadas del deber de informar en función de los distintos fines a los que puede responder la instalación de los sistemas de cámaras o videocámaras. La citada norma no contempla la necesidad o la obligación de identificar el lugar de ubicación de las cámaras.

A estos efectos sólo se contempla la necesidad de cumplir con el deber de informar previsto por el artículo 5 de la Ley Orgánica 15/1999, mediante la colocación, en emplazamientos claramente visibles de las zonas, áreas o espacios en los que se instalen los sistemas de cámaras o videocámaras distintivos informativos que deberán incorporar una información descriptiva de los espacios comprendidos dentro de la zona en la que se instalen los sistemas de cámaras o videocámaras, una referencia a la “LEY ORGÁNICA

15/1999, DE PROTECCIÓN DE DATOS", la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y la indicación de la posibilidad de obtener una información más detallada solicitando la misma en un lugar expresamente señalado al efecto.

La instalación de cámaras en los calabozos de la policía local de un Ayuntamiento es proporcional ya que su finalidad es mantener la seguridad de las personas y bienes dentro de esas instalaciones.

6.9.- Implantación de un sistema de control de tráfico por medio de cámaras en el término municipal de un Ayuntamiento.

En su escrito de consulta, el Ayuntamiento se refiere a si es conforme con lo dispuesto por la normativa sobre protección de datos que el control de dicho sistema se lleve a cabo por *"personal laboral",* ya sea del propio Ayuntamiento o de una concesión administrativa, siendo dicho personal el encargado de notificar a la Policía Local las incidencias que pudieran surgir al efecto.

Con pleno respeto a los principios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y, especialmente, con plena observancia del principio de calidad de los datos, entre las diferentes formas de legitimación de imágenes derivadas de la aplicación de lo dispuesto por los artículos 6 y 11 de dicha Ley Orgánica, se encuentra la posibilidad de que las mismas se recojan para el ejercicio de las funciones propias de los Ayuntamientos en el ámbito de sus competencias, con la finalidad de control y disciplina del tráfico, circulación de vehículos a motor y seguridad vial, al objeto de controlar el acceso de

vehículos a zonas especialmente delimitadas o de estacionamiento regulado, o para el establecimiento de sistemas de aforo del tráfico.

En consecuencia, deberá considerarse Responsable del tratamiento de datos personales realizado a través de sistemas de cámaras o videocámaras, al Ayuntamiento consultante, al ostentar el mismo la competencia administrativa a cuyo fin sirve la instalación del sistema de cámaras o videocámaras de tráfico.

Según dispone el artículo 2.3 e) de la Ley Orgánica de Protección de Datos, los tratamientos de datos procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, se rigen por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999, de 13 de diciembre.

En consecuencia, los tratamientos de imágenes realizados por las Policías Locales de los municipios que integran la Comunidad de Madrid quedarán sometidos a la Instrucción a la que se ha hecho mención (pendiente de publicación) en lo que no se oponga a la regulación específica contenida en la Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y en su Reglamento de desarrollo y ejecución, aprobado por Real Decreto 596/1999, de 16 de abril.

Entrando en las cuestiones planteadas, en el supuesto objeto de consulta el tratamiento de las imágenes se realiza en el ámbito de actuación y bajo la dirección del Ayuntamiento consultante, toda vez que las finalidades, el contenido y el uso del tratamiento responden a la decisión del mismo, que se encuentra sometido a lo dispuesto por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid,

adoptándose dicha decisión en el ejercicio de una competencia propia atribuida por el ordenamiento jurídico.

Asimismo, a juicio de esta Agencia, la actividad de tratamiento de datos realizada por empresas concesionarias que realicen dichos tratamientos de imágenes sobre el control de tráfico, a través de sistemas de cámaras o videocámaras, no afectará a la naturaleza pública de los tratamientos realizados por cuenta del propio Ayuntamiento consultante, pudiendo tener lugar, en su caso, a la realización de tratamientos de imágenes por cualquier tipo de empresas, entidades o personas jurídico-privadas que presten servicios de tratamiento de imágenes, siempre que dichos tratamientos se lleven a cabo por cuenta del Ayuntamiento consultante, y siempre que la finalidad, contenido y uso del tratamiento, correspondan al ejercicio de una competencia propia atribuida por el ordenamiento jurídico a dicho Ayuntamiento.

Para la implantación del sistema de control de tráfico por medio de cámaras, el Ayuntamiento consultante (Responsable del tratamiento), podrá servirse del personal laboral, funcionarial o estatutario de la propia Corporación, o bien contratar los servicios de otra persona física o jurídica, pública o privada, que trate los datos personales por cuenta de dicho Responsable, en calidad de Encargado del tratamiento.

En estos casos, no se considerará comunicación o cesión de datos el acceso del Encargado del tratamiento a las imágenes cuando dicho acceso sea necesario para la prestación de su servicio al Responsable del tratamiento.

De acuerdo con lo previsto por el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, la realización de tratamientos de datos mediante cámaras o videocámaras por cuenta de terceros, deberá estar regulada en un contrato que constará por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

expresamente que el encargado del tratamiento únicamente tratará las imágenes conforme a las instrucciones del responsable del tratamiento, y que no las aplicará o utilizará con fin distinto al que figure en dicho contrato, ni las comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, que el Encargado del tratamiento está obligado a implementar.

Para dicho supuesto, una vez cumplida la prestación contractual, las imágenes deberán ser destruidas o devueltas al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

En el caso de que el Encargado del tratamiento destine las imágenes a otra finalidad, las comunique o las utilice incumpliendo las estipulaciones del contrato, será considerado, también, Responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

La existencia de un encargado del tratamiento en la gestión del sistema de videovigilancia supone tener que cumplir de manera obligatoria con el artículo 12 LOPD.

7.- JURISPRUDENCIA.

A continuación publicamos un extracto de las sentencias más relevantes sobre videovigilancia de los últimos años.

7.1.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 12 de noviembre de 2010 sobre el cumplimiento de la normativa de protección de datos en materia de videovigilancia.

Se habían instalado cámaras en un bar sin los correspondientes carteles informativos del artículo 5 de la LOPD.

Primero. El presente recurso tiene por objeto la resolución de 17 de septiembre de 2009 del Director de la Agencia Española de Protección de Datos por el que se impuso a la entidad recurrente la sanción de 2000 € de multa como responsable de una infracción del art. 5 de la LOPD tipificada como leve en el art. 44.2 .d) de dicha norma.

De los datos obrantes en el expediente consta acreditado que la entidad mercantil "XXX" es titular del bar- restaurante denominado "...." en cuyo interior tenía instalados dos cámaras de vídeo-vigilancia sin que en la inspección realizada en el local conste que existiese un anuncio que advirtiese a los clientes de esta circunstancia.

Segundo. La entidad recurrente aduce en apoyo de su pretensión que la instalación de las dos cámaras de vídeo vigilancia en el local estuvo motivada por la grave enfermedad del administrador de la sociedad; su ausencia obligaba a vigilar las cajas durante su enfermedad por lo que se contrató la instalación de las cámaras de seguridad con la

empresa "...." presumiendo que esta empresa obtendría las autorizaciones necesarias para ello. Alega que no es cierto que no existiesen carteles indicadores de la presencia de las cámaras de vídeo vigilancia.
Considera que la sanción impuesta toma en consideración hechos que no se ajustan a la realidad (la falta de carteles anunciadores).

Tercero. De los datos obrantes en el expediente, especialmente del acta de inspección realizada en el citado local y los informes posteriores, se desprende que el bar-restaurante denominado "..." tenía instaladas en el interior dos cámaras de vídeo-vigilancia sin autorización para ello y tampoco tenía instalados los carteles que anunciasen a los clientes la presencia de dichas cámaras. Es más, en el informe elaborado por el área de gobierno y seguridad y movilidad de 20 de junio de 2008 (folio 5 del expediente) consta que el encargado del local manifestó que las cámaras solo visionan y no graban y que "desconocía que tenía que anunciar esta situación a los clientes, así como de tener autorización para la misma".

Cuarto. Hay que partir del concepto de tratamiento de datos, que se define en la LOPD, artículo 3 .c) como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencia". En la línea de la Directiva 95/46 /CE que transpone, nuestra LOPD incluye en dicha definición tanto el tratamiento automatizado de datos como el manual.

Ahora bien, como señala la SAN, Sec. 1ª, de 16 de febrero de 2006 no basta con la realización de una de estas actuaciones en relación con datos personales para que la ley despliegue sus efectos protectores y garantías y derechos del afectado. "Es preciso algo más, que esas actuaciones de recogida, grabación, conservación etc, se realicen de forma

automatizada o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a estar contenidos en un fichero".

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

En el caso de autos, atendidos los amplios términos del concepto de tratamiento de datos contenido en la LOPD, cabe sostener que la captación de la imagen de una persona y su grabación por el sistema de vídeo-vigilancia instalado constituye una operación o procedimiento técnico de recogida de datos, que al realizarse de forma automatizada (no manual), tiene la consideración de tratamiento de datos de carácter personal en el sentido de la LOPD y está sometido a la misma. Y así lo ha señalado este Tribunal en sentencia de 17 de Junio del 2010.

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 su artículo 1 señala que: "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. (...).

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".

En relación a esta cuestión no debe olvidarse que la Instrucción entiende que los responsables que cuenten con sistemas de vídeo vigilancia deberán cumplir con el deber de

información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán: a) Colocar, en las zonas vídeo vigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados; b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

Es por ello que las cámaras instaladas reproducen de forma automática la imagen de los clientes, constituyendo la imagen de una persona un dato de carácter personal, por lo que constituye el tratamiento de datos personales cuyo responsable es la entidad titular del establecimiento donde están instaladas. Sin que tampoco la citada entidad instalase distintivo alguno en los términos exigidos por el art. 5 de la Ley de Protección de Datos por lo que incurrió en la infracción tipificada en el art. 44.2.d) de la LOPD en cuya virtud se considera infracción leve "Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el art. 5 de la presente Ley".

Quinto. Finalmente la parte recurrente entiende que el importe de la sanción impuesta resulta desproporcionada al no estar justificada la elevación del importe desde la sanción mínima (601 €) hasta los 2000 € que se impuso a tenor de las circunstancias concurrentes.
Lo cierto es que las infracciones leves en materia de protección de datos, como la que ahora nos ocupa, tienen prevista, según dispone el art. 45.1. de la LOPD , la posibilidad de imponer una sanción de multa desde "601,01 a 60.101,21 euros".

De modo que la sanción de 2000 euros impuesta, lejos de ser desproporcionada ha sido aplicada casi en su grado mínimo y ello precisamente por no apreciar intencionalidad ni la obtención de beneficios con tal conducta, por lo que en ningún caso puede considerarse desproporcionado el importe de la multa impuesta, sin que la Administración este obligada

a imponer el mínimo de lo previsto legalmente para sancionar cada una de las infracciones apreciadas.

Fallamos que procede desestimar el recurso interpuesto por la entidad mercantil "XXX", contra la resolución de 17 de septiembre de 2009 del Director de la Agencia Española de Protección de Datos, sin hacer expresa condena en costas.

Se confirma la sanción de la AEPD por no haber puesto el cartel de videovigilancia.

No se había dado cumplimiento al derecho de información del artículo 5 de la LOPD.

7.2.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 10 de febrero de 2011 sobre instalación de cámaras en la vía pública.

Primero. La resolución recurrida parte de que la recogida y captación de imágenes se considera incluida y sometida a las indicaciones de la LOPD ya que puede constituir tratamiento de datos de carácter personal.

También entiende que son las empresas de seguridad privada (en aplicación a lo que señala sus artículos 1.2 y 5.1 .e) las que pueden instalar dispositivos de seguridad. No obstante, la grabación en lugares públicos debe realizarse por las Fuerzas y Cuerpos de Seguridad del Estado en aplicación a lo previsto en la Ley Orgánica 4/1997.

Entiende la resolución de la Agencia que está acreditada que la grabación se produce en zonas aledañas a la fachada exterior del centro comercial de la empresa recurrente sito en Málaga lo que solo se justificaría en razones de proporcionalidad (a las que se refieren tanto los artículos 4.1 y 2 de la LOPD como el artículo 4 de la Instrucción 1/2006).

Expresamente, la resolución impugnada utiliza los siguientes argumentos para justificar la imposición de la sanción: "Del acta de Inspección levantada con fecha 15 de julio de 2009, se recogen imágenes captadas por las cámaras exteriores de la fachada del Centro Comercial, donde se aprecian los vehículos y las personas que circulan por las vías públicas de las calles que demarcan el edificio. Esta visualización de vehículos y transeúntes no encuentra justificación alguna en la normativa específica y obliga a entender que se trata de un uso excesivo que infringe el principio de proporcionalidad de los datos previsto en el artículo 4.1 de la Ley Orgánica de Protección de Datos cuando se habla de que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. (...)

A este respecto, señalar que aun cuando en todas la cámaras se había instalado un dispositivo que ciega parte de los 360º de visión, lo cierto es, a juzgar por las imágenes obtenidas por las mismas, que dicha pantalla de privacidad debería haberse ampliado para evitar las captaciones de imágenes de la vía pública, que no son idóneas ni necesarias para la finalidad perseguida. (...)

En el caso analizado, ha quedado acreditado que el sistema de videovigilancia instalado en Centro Comercial permite seleccionar cualquiera de las cámaras y desplazar su enfoque 360º, alcanzando su ángulo de visión la vía pública y a las personas que circulan por la misma, realizando por tanto un tratamiento excesivo y no proporcional de las imágenes, en relación con el ámbito y las finalidades que podrían justificaban su recogida, toda vez que la seguridad demandada podría igualmente obtenerse por medios menos intrusivos para la intimidad de las personas afectadas, como sería la instalación de pantallas de privacidad que impidiesen la captación de imágenes en la vía pública más allá de lo necesario y proporcional. Por lo tanto procede desestimar la alegación de la entidad demandada a este respecto.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

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

Finalmente, se entiende que no concurren circunstancias que justifiquen la imposición de la sanción como infracción leve no siendo de aplicación lo previsto en el artículo 45.5 de la LOPD.

Segundo. Sobre la consideración de la imagen personal como dato y sobre el sometimiento de esta cuestión a las previsiones de la Ley Orgánica de Protección de Datos, poco hay que decir.

- El artículo 2.1 de la Ley orgánica 15/99 señala que "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"; definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como "Cualquier información concerniente a personas físicas identificadas o identificables".

- El artículo 3.a) de la LOPD define los datos de carácter personal como: "Cualquier información concerniente a personas físicas identificadas o identificables" y, el artículo 3. b) de la LOPD define el concepto de fichero como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". El artículo 3.c) de la LOPD define el tratamiento de datos como 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".

- El articulo 2.e) de la Directiva 95/46, 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".

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

En relación a los limites, resulta que es especialmente importante lo que señala el artículo 4.3 de la Instrucción cuando establece que: 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.

Por lo tanto, esta Instrucción no se refiere a la vigilancia de espacios públicos y solo la permite cuando sea imprescindible para la vigilancia previamente autorizada como es la impuesta para los bancos y entidades de crédito.

Tercero. La parte recurrente insinúa la posible prescripción de la infracción por no detallarse la fecha en que ocurrieron los hechos. Obviamente, no es posible acceder a dicha pretensión pues los hechos que se denuncian se venían produciendo, al menos, en la fecha de la Inspección (15 de Julio de 2009) por lo que a la fecha de la resolución sancionadora no habían transcurrido los plazos señalados en el artículo 47 de la LOPD.

Esta Sala en la sentencia correspondiente al recurso 684/2009 dictada con ocasión de una denuncia frente a la misma entidad ahora recurrente pero en relación a otro de sus centros comerciales, se dijo que: "Al respecto hay que señalar, que la resolución sancionadora argumenta en su Fundamento de Derecho III, que la imputación que se realiza a Centro Comercial no es exclusivamente por la captación de la imagen del denunciante sino por el tratamiento sin consentimiento de imágenes de todas las personas que se introdujeron dentro del campo de visión de las cámaras instaladas en la fachada del edificio y orientadas a la vía pública.

Es decir, la imputación realizada a la entidad recurrente no se circunscribe a la captación de la imagen del denunciante, sino que se extiende (como se constata también de la lectura de los hechos probados) al tratamiento de imágenes de las personas que transitan por la vía pública y que son captadas, sin su consentimiento, al introducirse dentro del campo visual de las cámaras instaladas en las fachadas del edificio de la recurrente y almacenadas en un fichero durante 7 días.

Las infracciones graves prescriben, según el artículo 47.1 LOPD, al año. Ese plazo comienza a computarse desde el día en que la infracción se hubiera cometido-artículo 47.2 de la citada Ley - y se interrumpirá desde la iniciación del procedimiento sancionador con conocimiento del interesado-apartado 3 del citado artículo 47 -."

También se alega que no existe tratamiento pues se produce recogida de datos sin orden ni criterio de búsqueda. Esta cuestión, que hace referencia al fondo de la pretensión anulatoria planteada por la parte recurrente también fue resuelta por esta Sala en el citado recurso 684/2009 (en relación a otro de los centros comerciales de la entidad ahora recurrente).

Aquí es importante reproducir lo dicho por la Sentencia citada en respuesta a esta misma alegación: "Para abordar dicha cuestión hay que partir del concepto de tratamiento de

datos, que se define en la LOPD, artículo 3 .c) como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencia".

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

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

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

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

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

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

Cuarto. Es importante señalar como el Director de Seguridad de la compañía recurrente dirigió una comunicación a la Secretaría de Estado de Interior con fecha 12 de mayo de 2009, por la que se solicita concesión de la correspondiente autorización administrativa para la grabación de imágenes en la vía pública, en todos y cada uno de los centros comerciales que la compañía tiene en el territorio español, con la finalidad de prevenir la comisión de delitos y, si éstos se produjeran, poder utilizar dichas imágenes para la identificación del autor o autores de los mismos, así como ayudar en la organización de los planes de evacuación y desalojo de los edificios. (folio 71 a 73).

La respuesta fue clara contestación de la Secretaría de Estado de Interior, de fecha 25 de 2009, en la que se recoge que no existe amparo jurídico sobre la instalación de videovigilancia en los términos expresado en la solicitud de "grabación de imágenes en la vía pública, en todos y cada uno de los centros comerciales que dichas empresas tienen en territorio español". Asimismo manifiesta que "La normativa vigente en esta materia está contenida fundamentalmente en la Ley 23/1992, de 30 de julio , de seguridad privada (LSP) y el Reglamento que la desarrolla, aprobado por Real Decreto 2364/1994, de 9 de diciembre , en la Ley Orgánica 4/1997, de 4 de agosto , sobre utilización de video cámaras

por las Fuerzas y Cuerpos de Seguridad en lugares públicos, en Ley orgánica 15/1999, de 13 de diciembre , de Protección de Datos de Carácter Personal y su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre y en la Instrucción 1/2006, de 8 de noviembre , de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras. Hasta la fecha no se han cumplimentado las previsiones de la Disposición Adicional Novena de la citada Ley Orgánica 4/1997, sobre elaboración de la normativa correspondiente para adaptar los principios inspiradores de dicha Ley al ámbito de la seguridad privada". (Folio 175).

Por lo tanto, resulta que la entidad recurrente conocía las limitaciones existentes para la grabación de imágenes en vías públicas y a pesar de ello no adoptó las precauciones precisas para evitar que dicha grabación se produjera y ello supone que debe hacerse responsable de dicho exceso en la grabación producida por las cámaras que estaban, eso sí, correctamente instaladas.

Quinto. Por lo que se refiere a la aplicación del principio de proporcionalidad, es necesario atender a que la resolución impugnada en atención a los criterios establecidos en el artículo 45.4 LOPD (ausencia de intencionalidad y reiteración etc) fija la sanción a imponer en el mínimo posible asignada a las infracciones graves, por lo que no es posible rebajarla más, salvo que se aprecie la atenuación cualificada del artículo 45.5 LOPD.

La aplicación del citado artículo 45.5 LOPD requiere como presupuestos la concurrencia de una cualificada disminución de la culpabilidad o de la antijuridicidad. Presupuestos que la Sala no aprecia, teniendo en cuenta por una parte que la captación y grabación de imágenes alcanza a las personas que circulan incluso alrededor del centro de la vía pública, siendo sumamente elocuentes al efecto las fotografías adjuntadas como documento nº 2 al acta de inspección -folios 96 y siguientes del expediente- y por otra, las características de la

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

entidad recurrente que realiza tratamientos de datos personales de gran alcance, a la que cabe exigir un especial cuidado.

El principio de proporcionalidad comporta, como señala la STS, Sala 3ª, de 3 de diciembre de 2008 que cualquier actuación de los poderes públicos limitativa o restrictiva de derechos responda a los criterios de necesidad y adecuación al fin perseguido, dicho en términos legales, debe de existir una "debida adecuación entre la gravedad del hecho constitutivo de la infracción y la sanción aplicada"(artículo 131.3 de la Ley 30/19992).

Principio que no puede entenderse vulnerado en el caso de autos, al haberse impuesto la sanción mínima asignada a la infracción grave apreciada y sin que sea posible aplicar ninguno de los argumentos que utiliza la parte recurrente relativos a la inexistencia de daño alguno (sí se ha producido daño a los transeúntes que se han visto indebidamente grabados) ó la situación de inseguridad por el alto número de hechos delictivos que se producen en las entradas y salidas del establecimiento (dicha circunstancia no puede servir para justificar una grabación indiscriminada producida en zonas en las que no está autorizada la grabación).

Todo ello obliga a la integra confirmación de la resolución impugnada.

El responsable no adoptó las medidas pertinentes para no grabar en la vía pública. La grabación de imágenes en la vía pública es competencia de las Fuerzas y Cuerpos de Seguridad.

7.3.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de 27 de mayo de 2010 sobre tratamiento de imágenes sin cumplir la LOPD.

Primero. Se interpone el presente recurso contencioso administrativo frente a resolución de fecha 3 de Junio de 2009 dictada por el Director de la AEPD por la que se impone a la empresa recurrente una multa por importe de 2.500 euros por infracción de lo previsto en el artículo 44.3.d) de la LOPD.

La resolución recurrida parte de los siguientes datos para imponer la sanción frente a la que se recurre:

- "La empresa" es responsable del fichero de conformidad con las definiciones legales, por tanto está sujeto al régimen de responsabilidad recogido en el Título VII de la LOPD.

- La captación de imágenes de las personas, constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.

- 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 el caso que nos ocupa, "la empresa" tiene el dominio de la página de Internet http://www....X...., que corresponde a una cámara de video, que transmite a tiempo real imágenes del interior de una sala, despacho u oficina. Dichas imágenes permiten identificar a las personas que se sitúan en su zona de cobertura. 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 empresa" toda

vez que es dicha entidad la que decide sobre la finalidad, contenido y uso del citado tratamiento.

- En relación a que la difusión de las imágenes se produjo por error, dice la resolución que: Así, "la empresa" estaba obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas en la normativa y, entre ellas, las dirigidas a impedir el acceso a los datos personales por parte de terceros no autorizados. Sin embargo, ha quedado acreditado que incumplió esta obligación, procediendo desestimar las alegaciones realizadas a este respecto.

- Por lo tanto, a la vista de lo expuesto, de la existencia de cartel informativo, aunque incompleto, de la presencia de la cámara en la entidad denunciada, no se puede inferir un consentimiento a la grabación de sus imágenes y aun menos a su difusión vía Internet, como alega la entidad denunciada, procediendo desestimar las alegaciones efectuadas a este respecto. Asimismo, hay que tener en cuenta que aun en el supuesto que los trabajadores tuvieran conocimiento de la existencia de la grabación de sus imágenes, esto no le autoriza a "la empresa" a realizar un tratamiento de sus datos y su difusión en Internet.

- Por último, conviene aclarar el hecho que aunque a "la empresa" se le sancione exclusivamente por la comisión de la infracción del artículo 6 y no se sancione también por la comisión de la infracción del artículo 10 de la LOPD , como constaba en el Acuerdo de Inicio del presente procedimiento sancionador, es debido no al archivo de la infracción del artículo 10 de la LOPD , cuya infracción ha sido acreditado que se ha cometido, sino por tratarse de 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. 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.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Finalmente, y en cuanto a la aplicación de lo previsto por el artículo 45.5 de la LOPD ; la resolución sancionadora ha establecido que: "En concreto, hay que considerar que "la empresa" como registrante del dominio http://www....X...., y desde la que se difundieron las imágenes captadas por la cámara ubicada en sus dependencias, no tenía ánimo de producir ningún daño a las personas que pudieran ser captadas por la citada cámara, sino que el hecho se produjo por un fallo del sistema. Asimismo, consta que la entidad denunciada ha procedido a desactivar la misma, lo que denota una diligencia en su actuación.

Asimismo, en el presente caso, ha de tenerse en cuanta que la complejidad de las normas que regulan el tratamiento de datos personales a través de sistemas de videovigilancia requieren una especial cualificación técnica, lo que lleva a apreciar la existencia de una cualificada disminución de la culpabilidad, al no poder obviarse que no puede exigirse a la entidad actora un elevado grado de diligencia pues por su naturaleza de pequeña o mediana empresa no realiza tratamientos de datos personales de gran alcance o volumen. Por todo ello, y tomando en consideración las citadas circunstancias, que permiten entender que existe una disminución de la culpabilidad del imputado, se considera procedente aplicar la graduación prevista en el artículo 45.5 de la LOPD .

Segundo. 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".

El artículo 44.2.e) de la LOPD considera infracción leve: e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave." Dicho precepto debe relacionarse con el artículo 10 de la LOPD cuando dice que: "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."

La adecuada resolución de la cuestión que se somete a la consideración de esta Sala exige partir de la base de que la parte recurrente nada ha dicho en su escrito de las cuestiones básicas planteadas por la resolución recurrida como son las referidas a la consideración de la imagen como dato personal, a la consideración de la grabación como tratamiento y a la falta de consentimiento de los empleados de la recurrente no tanto para ser grabados como para que dicha grabación tuviera acceso libre a Internet. Tampoco nada se dice sobre la suficiencia de la información ofrecida

La parte recurrente fundamenta su demanda, exclusivamente, en la falta de culpabilidad de su conducta y en solicitar la aplicación del artículo 45.5 de la LOPD.

Tercero. La exigencia de la culpabilidad procede de lo que señala el artículo 130 de la Ley 30/92 cuando dice que: "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". Hay que señalar (siguiendo el criterio de esta Sala en otras sentencias como la de fecha 21 de enero de 2004 dictada en el recurso 1139/2001) que la comisión de la infracción prevista en el artículo 44.3 .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" del Art. 130.1 de la Ley 30/1992, permite la imposición de la sanción, sin duda en supuestos dolosos, y asimismo en supuestos culposos, bastando la inobservancia del deber de cuidado.

Como ya se ha referido, la delicada materia a la que se refiere la LOPD, se traduce en la necesidad de exigir una especial diligencia a las entidades gestoras de los datos. Por lo tanto, la conducta que configura el ilícito administrativo-artículo 44.3.d) de la Ley Orgánica 15/1999 - requiere la existencia de culpa, que se concreta, según la resolución impugnada, en la falta de control de la entidad recurrente en comprobar las imágenes grabadas se iban a divulgar por Internet; la falta de diligencia en este aspecto configura la exigencia de culpa aplicable al caso presente. Esa falta diligencia configura el elemento culpabilístico de la infracción administrativa y resulta imputable a la recurrente, y, obviamente, no precisa de la concurrencia de dolo.

A estos razonamientos aun cabe añadir que en nuestras Sentencias de 23 de marzo y 16 de Junio de 2004 (recursos 435/2002 y 865/2002) también señalamos que "cuando se invoca la buena fe en el actuar, para justificar la ausencia de culpa -como se hace en el presente caso- basta con decir que esa alegación queda enervada cuando existe un deber específico de vigilancia derivado de la profesionalidad del infractor. En esta línea de tradicional reflexión, la STS de 12 de marzo de 1975 y 10 de marzo de 1978 , rechazan la alegación de buena fe, cuando sobre el infractor pesan deberes de vigilancia y diligencia derivados de su condición e profesional"-SAN (1ª) de 14 de septiembre de 2001-".

La sentencia del Tribunal Supremo (sala Tercera) de fecha 9 de Marzo de 2005 ha dicho he relación al principio de culpabilidad que: "este principio, que se garantiza en el artículo 25 de la Constitución como principio estructural básico del Derecho Penal y del Derecho Administrativo Sancionador, según refiere el Tribunal Constitucional en la sentencia 150/1991, de 4 de julio , que limita el ejercicio del ius puniendi del Estado, exige que la imposición de la sanción se sustente en la exigencia del elemento subjetivo de culpa para garantizar el principio de responsabilidad y el derecho a un procedimiento sancionador con todas las garantías(STC 129/2003, de 20 de junio)".

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Sobre esta base es necesario señalar que la parte recurrente se limita a aportar argumentos que para nada justifican su actuación y ello pues el hecho de que los trabajadores no hayan formulado denuncia alguna no puede justificar la contradicción entre la conducta y el ordenamiento jurídico; también se afirma que era necesario una password para el acceso a las imágenes, pero ha resultado acreditado que el acceso se produjo de modo libre y el propio recurrente reconoce que se produjo un fallo del sistema que, con mayor diligencia, debería haber sido evitado.

Que la empresa desconociera el hecho de la divulgación de las imágenes lo único que acredita es que era necesario un nivel mucho mayor de diligencia para controlar el destino de las imágenes que se grababan.

Por lo tanto, no puede entenderse que se haya producido ninguna violación del principio de culpabilidad y ello puesto que una mayor diligencia y cuidado en el tratamiento de las imágenes grabadas habría evitado que estas accedieran a Internet.

Cuarto. En cuanto a la aplicación del principio de proporcionalidad que deriva de lo previsto en el artículo 45.5 de la LOPD por entender que se ha producido una apreciable disminución de la culpabilidad y la antijuridicidad también debe ser rechazada y ello pues la parte recurrente insiste en que se lleve a efecto la reducción sobre la base de cuatro criterios:

- Falta de intencionalidad.

- Se trató de un fallo puntual.

- Se desactivó el sistema en cuanto se conoció el error.

- La empresa no realiza tratamientos de datos de gran volumen.

Parece olvidar la parte recurrente que ya la propia Agencia ha aplicado este criterio reductor y que, en su consecuencia, al poder imponer la multa entre 601,01 euros y 60.101 euros, ha optado por una cantidad muy prudente que está en el primer tercio de la primera décima parte del importe máximo que podía haberse aplicado.

Fallamos que desestimando el presente recurso contencioso administrativo.

La posibilidad de ver imágenes en Internet a tiempo real de un centro de trabajo puede conllevar responsabilidades por incumplimiento el de la LOPD.

7.4.- Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia de Nacional de 17 de junio de 2011 sobre la aplicación de la nueva figura del apercibimiento[11] en una sanción impuesta por la AEPD por instalar una cámara en su plaza de garaje de una comunidad de vecinos.

Primero. El presente recurso tiene por objeto la resolución de fecha 28 de mayo de 2010 dictada por el Director de la AEPD, por la que se impuso una sanción de 2000 € por una infracción del art. 6 de la LOPD tipificada como grave en el artículo 44.3.d) de dicha norma.

[11] La Ley 2/2011, de 4 de marzo, de Economía Sostenible, En su Disposición final quincuagésima sexta ha modificado varios artículos del régimen sancionador de la LOPD. En este sentido, se ha añadido un nuevo apartado al artículo 45 de la LOPD:
«6. Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:
a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.
Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.»

De los datos obrantes en el expediente, así como de las alegaciones formuladas por las partes y pruebas practicadas en el curso de las presentes actuaciones, resultan probados los siguientes hechos con relevancia para dictar la resolución que nos ocupa:

- La recurrente instaló en el techo de su plaza de garaje de la comunidad de propietarios una cámara que captaba imágenes de su plaza de garaje y de la zona contigua y las grababa en el disco duro de un ordenador.

- Para instalar esta cámara no contaba con la autorización de la comunidad de propietarios, y tampoco solicitó a la Agencia de Protección de datos para la creación de ficheros o para instalar la cámara. La cámara la instaló la empresa Esquema electrónica SA, inscrita en el Ministerio del Interior como empresa de seguridad privada.

Segundo. La recurrente alega que las razones que la llevaron a instalar una cámara en el garaje eran las continuas amenazas y agresiones que venía sufriendo por parte de los denunciantes, vecinos de la comunidad de propietarios, y que se plasmaron en una condena penal cuya sentencia aporta. No debe ser sancionada, a su juicio, por instalar una cámara que pretende preservar su integridad física al estar amparada por las circunstancias de estado de necesidad y miedo insuperable que la eximirían de toda responsabilidad por las infracciones que se le imputan a la LOPD (artículo 20 apartados 5 y 6 del Código Penal).

La resolución administrativa impugnada, con gran acierto en sus razonamientos, considera que la instalación de una cámara en una zona común del edificio, al margen de no contar con la autorización de la comunidad de propietarios, estaba captando imágenes de las personas que transitaban y las almacenaban en un ordenador por lo que realizaba un tratamiento de datos sin su consentimiento y creaba un fichero de datos con

esas imágenes al grabarlas en un ordenador, sin haberlo notificado a la Agencia de Protección de Datos la existencia de dicho fichero.

Este Tribunal ha señalado en numerosas sentencias que atendidos los amplios términos del concepto de tratamiento de datos contenido en la LOPD, la captación de la imagen de una persona y su grabación por el sistema de video-vigilancia instalado constituye una operación o procedimiento técnico de recogida de datos, que al realizarse de forma automatizada (no manual), tiene la consideración de tratamiento de datos de carácter personal en el sentido de la LOPD y está sometido a la misma. Y así lo ha señalado este Tribunal en sentencia de 17 de Junio del 2010.

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 videocamaras en su artículo 1 señala que: "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 videocamaras (...).

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".

En relación a esta cuestión no debe olvidarse que la Instrucción entiende que los responsables que cuenten con sistemas de vídeo vigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán: a) Colocar, en las zonas vídeo vigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como

cerrados; b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

Constituyendo la imagen de una persona un dato de carácter personal, la instalación de cámaras en el garaje que captan y graban de forma automática la imagen de los que transitan por esa zona común del edificio constituye un tratamiento de datos personales cuyo responsable es la persona que las ha instalado, sin que tampoco conste distintivo alguno en los términos exigidos por el art. 5 de la Ley de Protección de Datos por lo que incurrió en la infracción tipificada en el art. 44.2.d) de la LOPD en cuya virtud se considera infracción leve " *Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el* art. 5 de la presente Ley *".*

Al grabar esas imágenes en un disco duro está creando un fichero automatizado de datos que permite su localización sin haberlo comunicado a la Agencia de Protección de Datos en los términos exigidos en el art. 26.1 de la LOPD.

El hecho de que la recurrente mantuviese una mala relación con otros vecinos y que las razones que la impulsaron a la instalación de esa cámara fuesen el intento de preservar su integridad personal frente a las amenazas y posibles agresiones de ciertos vecinos no puede ser tomado como una circunstancia que la exima de la responsabilidad administrativa en la que incurrió por incumplir la normativa en materia de Protección de datos, pues ni concurren los requisitos que determinan la existencia de las eximentes de miedo insuperable o estado de necesidad que justifique la infracción cometida, ni aunque su conducta pudiese estar motivada por razones de seguridad personal puede justificarse el incumplimiento de la normativa en materia de protección de datos para la instalación de dicha cámara. La parte debería haber solicitado autorización para ello momento en el

que podría haber razonado sobre la concurrencia de circunstancias personales que justificasen su instalación.

Queda al margen de este proceso toda consideración sobre la existencia de responsabilidad penal de los agresores que ya ha sido valorada en el proceso penal cuya sentencia se aporta con la demanda y sobre la gravedad de la sanción penal impuesta, pues no nos corresponde enjuiciar la pena impuesta por otro tribunal en su sentencia ni existe base alguna que permita entender, en todo caso, que es más gravosa la sanción de multa impuesta a la recurrente por estos hechos que las sanciones penales impuestas a su agresor (condenado a 6 meses de prisión y a varias penas accesorias).

Tercero. Por lo que respecta a la graduación de la sanción, la Administración ya redujo considerablemente el importe de las sanciones tomando en consideración las circunstancias concretas concurrentes, entre ellas las razones que le impulsaron a tomar esta decisión y la complejidad técnica de las normas sobre tratamiento de datos de datos en relación con los sistemas de vídeo-vigilancia al tratarse de un particular, la ausencia de intencionalidad y la no obtención de beneficio alguno con su conducta, lo que llevó a apreciar una cualificada disminución de la culpabilidad que determinó una drástica rebaja en el importe de las multas impuestas.

Ahora bien, en el supuesto que nos ocupa debe también tomarse en consideración que mediante la Disposición Final Quincuagésima Sexta de la Ley 2/2011 por la que se han modificado diferentes preceptos de la Ley Orgánica 15/99 suponiendo, en algunos casos estableciendo unos criterios más favorables respecto de las sanciones que ahora nos ocupan.

Este Tribunal en diferentes sentencias, entre ellas SAN, Sección Primera, de 10 de marzo de 2011, de 17 de marzo de 2011, de 18 de marzo de 2011 y sentencia de 25 de marzo de 2011 y 11 de Abril del 2011 ha señalado que resulta aplicable esta norma pues es necesario atender al principio de la eficacia retroactiva de las normas sancionadoras más favorables que deriva de lo que señala el artículo 128.2 de la Ley 30/92: Las disposiciones sancionadoras producirán efectos retroactivos en cuanto favorezcan al presunto infractor.

Además, el propio Tribunal Supremo (sentencia dictada en fecha 21 de Septiembre de 1998 en el recurso 7071/1992) ha dicho que: "entiende la Sala que si bien ciertamente no pueden aplicarse de forma mimética al derecho administrativo sancionador los principios del derecho penal, y por otra parte en la fecha de autos el principio vigente era el de la irretroactividad de las disposiciones no favorables o restrictivas de derechos individuales consagrado por el artículo 9,3 de la Constitución y no el inverso de aplicación retroactiva de las normas favorables, este último principio venia afirmándose por la jurisprudencia del Tribunal Constitucional y de este Tribunal Supremo hasta que fue expresamente positivado por el artículo 128,2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Publicas y del Procedimiento Administrativo Común".

La nueva regulación añade el apartado sexto el artículo 45 de dicha LOPD en el que se dispone que " 6*. Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad".

La sanción de apercibimiento se trata, sin duda, de una sanción de menor gravedad que las multas impuestas y en el supuesto que nos ocupa, tal y como afirma en el escrito de alegaciones presentado por la Agencia de Protección de Datos en el trámite habilitado al efecto en este procedimiento, concurren los requisitos necesarios para aplicar esta previsión legal pues las infracciones aplicadas en este procedimiento son una leve y una grave, no consta la existencia de previa sanción alguna a la recurrente y al mismo tiempo concurren, de forma significativa, dos de las circunstancias previstas en el apartado 45.4 de dicha norma, cuales son la ausencia de beneficios obtenidos y la falta de intencionalidad en la conducta de la recurrente, circunstancias que ya fueron apreciadas, incluso, en la resolución administrativa impugnada.

La aplicación de esta nueva previsión legal establece también que el órgano sancionador ha de adoptar las medidas correctoras que en cada caso resultasen pertinentes y el plazo para ello. Se trata de una medida ligada a la sanción de apercibimiento y razonable en cuanto exige modificar la conducta infractora para evitar que esta se siga produciendo. La Sala considera que la adopción de tales medidas correctoras deben ser ponderadas y adoptadas por la Agencia de protección de datos en una nueva resolución que se pronuncie sobre estos extremos.

Cuarto. A los efectos previstos en el art. 139 de la Ley reguladora de esta jurisdicción en materia de costas procesales, no se aprecia temeridad o mala fe en ninguno de los litigantes.

Fallamos, que procede estimar en parte el recurso interpuesto por Doña XXX, contra la resolución de fecha 28 de mayo de 2010 dictada por el Director de la AEPD de 28 de mayo de 2010 por la que se impuso una sanción de 2000 € por una infracción del art. 6 de la LOPD tipificada como grave en el artículo 44.3.d) de dicha norma y una sanción de 601,01 € por infracción del art. 26.1 de la LOPD tipificada como leve en el artículo 44.2.c) de dicha norma. Este Tribunal acuerda anular las sanciones impuestas sustituyéndolas por la sanción de apercibimiento, debiendo la Agencia de Protección de datos acordar las medidas correctoras que estime necesarias y plazo para adoptarlas.

La instalación de cámaras de videovigilancia en las zonas comunes de una finca supone un tratamiento de datos de carácter personal, debiendo cumplir con la LOPD y la Instrucción 1/2006 de la AEPD.

7.5.- Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Galicia sobre la instalación de cámaras en la vía pública. Analiza la falta de justificación y proporcionalidad para instalarlas.

Primero. El Ayuntamiento demandante solicitó al Delegado del Gobierno en Galicia la instalación de videocámaras en el Fórum Metropolitano "con el fin de aumentar la seguridad" -folio 1 del expediente-. La Comisión de Garantías de Videovigilancia en Galicia acordó que "no se justifican los motivos de las cámaras que graban los exteriores" -folios 17 y 18-; notificado que le fue el acuerdo, el Ayuntamiento comunica a la Delegación del Gobierno en Galicia que "se solicita la autorización para la instalación de cámaras exteriores en el edificio del Fórum Metropolitano (...) con el fin de asegurar la protección del citado edificio y sus accesos" -folio 20-; a la vista de la comunicación la Comisión informa que "la justificación que se alega no parece de la suficiente entidad -principio de proporcionalidad- para autorizar las cámaras orientadas a grabar las vías

públicas próximas al edificio en base a lo previsto al efecto por el artículo 1 apartado 1 ,artículo 4 y artículo 6 apartados 1, 2, 3 y 4 de la Ley Orgánica 4/1997, de 4 de agosto " -folios 22 al 24 -. El Delegado del Gobierno en Galicia, vistos los antecedentes del expediente, resolvió "no autorizar la instalación de videocámaras que graban las vías públicas próximas al edificio" -folios 25 y 26-.

El Ayuntamiento interpuso recurso de reposición contra la resolución denegatoria de la autorización argumentando que "Ninguna de las dos cámaras restantes de nuestra solicitud, la D-2 y la D-3, graban las vías públicas próximas al edificio (...) Ambas cámaras ciñen el ámbito de su objetivo y visión a la vigilancia del acceso al edificio del Fórum Metropolitano en la medida necesaria para prevenir la causación de daños a sus bienes, no infrecuentes. De no autorizarse ambas cámaras es técnicamente imposible cumplir tal finalidad. / Existe un razonable riesgo para la seguridad ciudadana de un edificio público que frecuentemente sufre daños en sus instalaciones sin que existe otra posibilidad razonable para preservar su seguridad (...) nos ofrecemos para dar explicaciones completas (...)" -folios 29 al 31-. La Comisión "informa desfavorablemente el recurso de reposición interpuesto, al variar el contenido de la petición inicial (...)" -folios 44 y 45-. El Delgado del Gobierno en Galicia, visto el informe de la Comisión, resolvió desestimar el recurso de reposición -folios 46 y 47-.

El Ayuntamiento interpuso recurso contencioso-administrativo contra la resolución desestimatoria del recurso de reposición argumentando que "la razón de instalar cámaras en el exterior, enfocando las paredes exteriores del edificio y el espacio público inmediatamente pegado al edificio tiene su razón de ser ante la posible prevención en el caso de rotura de cristales, pintadas e incluso intentos de acceder al edificio. / No puede obviarse que en el interior del edificio se encuentran bases de datos de carácter personal, ordenadores, maquinaria, etc. (...) El perjuicio de tal instalación se encuentra perfectamente justificado por el perjuicio que se ocasionaría en el caso de desaparición, pérdida o deterioro de los documentos que se custodian en el edificio (...) de la

envergadura de proyectos de reparcelación, proyectos de obras de edificaciones, urbanizaciones o meras licencias urbanísticas (...) El hecho de que determinada cámara vigile el exterior del edificio atenuaría el riesgo o peligro potencial de cualquier persona, incluso la sola existencia de las cámaras intimidaría a las personas con intenciones perversas. / Las zonas públicas que se graban son de paso inmediatamente anteriores a las fachadas del edificio sin que se ocasiones intromisión alguna de ningún género" -fundamentos de derecho I y II del escrito de demanda-.

Segundo. En garantía de los derechos fundamentales y libertades públicas de los ciudadanos, para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los criterios de asegurar la protección de los edificios e instalaciones públicas y de sus accesos, salvaguardar las instalaciones útiles para la defensa nacional, constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes; y, también para que el ejercicio de los derechos y libertades reconocidos en la Constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública, la utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad, que determina que sólo podrá emplearse la videocámara cuando resulte adecuado en una situación concreta para el mantenimiento de la seguridad ciudadana de conformidad con lo dispuesto en esta Ley, y de intervención mínima, que exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas, y exige la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles -preámbulo y artículos 4 y 6 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-.

La finalidad primordial de la Ley Orgánica 4/1997, de 4 de agosto , consiste en establecer las garantías necesarias para que dicha utilización sea estrictamente

respetuosa con los derechos y libertades de los ciudadanos; la solicitud de instalación de deberá contener los motivos que la justifican -preámbulo y artículo 3.2.b del Real Decreto 596/1999, de 16 de abril , por el que se aprueba el Reglamento de desarrollo y ejecución 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-.

Tercero. Los motivos justificativos de la solicitud -"aumentar la seguridad (...) asegurar la protección del citado edificio y sus accesos"- y aun de los recursos contra la denegación de la solicitud -"prevenir la causación de daños a sus bienes, no infrecuentes (...) razonable riesgo para la seguridad ciudadana de un edificio público que frecuentemente sufre daños en sus instalaciones sin que existe otra posibilidad razonable para preservar su seguridad (...) posible prevención en el caso de rotura de cristales, pintadas e incluso intentos de acceder al edificio. / No puede obviarse que en el interior del edificio se encuentran bases de datos de carácter personal, ordenadores, maquinaria, etc. (...)"-, tales motivos, decimos, y así se resolvió y bien se contesta ahora, no son bastantes para entender que la utilización de las videocámaras en la situación concreta es adecuada para el mantenimiento de la seguridad ciudadana y para la ponderación en el caso concreto entre la finalidad pretendida y la posible afectación a los derechos.

Por su vaguedad o falta de precisión, reducida ésta en la solicitud inicial a la mera referencia a la finalidad legal de garantía de la seguridad ciudadana y en los sucesivos escritos completada con la referencia a unos daños que tampoco se circunstancian. El Ayuntamiento no explica la adecuación de la utilización de videocámaras en el edificio de la solicitud conectándola con la utilización de otros medios de garantía de la seguridad ciudadana ni con el mantenimiento de la seguridad ciudadana en otros edificios. Tampoco explica el Ayuntamiento la relación entre la existencia de videocámaras en el exterior del edificio para prevenir rotura de cristales y pintadas e intentos de entrada y la protección de documentos de relevancia custodiados en su interior.

Y porque, en todo caso, en ningún momento se aportó un principio de prueba sobre el hecho alegado de que el edificio "frecuentemente sufre daños en sus instalaciones".

Procede la desestimación.

Fallo: desestimamos el recurso contencioso-administrativo interpuesto por el Letrado en nombre y representación del Ayuntamiento de La Coruña, en relación con la resolución la resolución del Delegado del Gobierno en Galicia de fecha 27 de febrero de 2008 por la que se acordó "desestimar el requerimiento previo a la vía contencioso-administrativa del Ayuntamiento de La Coruña de fecha 13/12/2007, en el que se solicita que se anule o revoque la resolución de 20/11/2007 por la que no se autorizaba la instalación de las videocámaras solicitadas por el Ayuntamiento de La Coruña orientadas a grabar los alrededores del Forum Metropolitano de La Coruña".

La Comisión de Videovigilancia de la respectiva Comunidad Autónoma puede denegar la instalación de cámaras en la vía pública si considera que la instalación de las mismas no está debidamente justificada. En esta Sentencia, el Tribunal Superior de Justicia de Galicia confirma la denegación de dicha Comisión.

7.6.- Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Madrid de 10 de diciembre de 2010 sobre cumplimiento de los trámites normativos en la creación de ficheros de videovigilancia de varios Institutos de Educación Secundaria.

{...}

Tercero. Por lo que se refiere al fondo del recurso alega, en esencia, el Sindicato recurrente que la Orden impugnada ha incumplido las exigencias legales y reglamentarias

(Ley 8/2001, de Protección de Datos de la Comunidad de Madrid y Decreto 99/2002, de 13 de junio, por el que se aprueba su Reglamento) en la finalidad y usos de cada uno de los tres ficheros creados, no siendo válida la caracterización genérica que da, estando vacíos de contenido en lo esencial, los Informes Preceptivos de la Agencia de Protección de Datos de la CAM (folios 20 a 21 expediente) así como el de la Consejería de Educación de la CAM (folios 22 a 23 expediente), lo que supone vulneración de derechos fundamentales como el derecho a la intimidad personal y a la propia imagen (artº 18.1C.E) y el derecho a la educación con el objeto del pleno desarrollo de la personalidad humana (artº 27.2 C.E.).

De la transcripción literal del artº 4 de la Ley 8/2001 de 13 de julio y artº 6 del Decreto 99/2002, de 13 de junio, antes expresada, y que recoge la Administración demandada, disponen que "la creación de ficheros de datos de carácter personal deberán indicar, en todo caso, la finalidad del fichero y los usos previstos para el mismo." Del examen de esta normativa se desprende que la Orden impugnada cumple con todas las exigencias de contenido establecidas en la misma, y así, en lo relativo a la finalidad del fichero y los usos previstos del mismo, la Orden se refiere a "Imágenes del entorno e interior del inmueble por motivos de seguridad", entendiendo que tal delimitación es suficiente para concretar cuál es la finalidad, motivos de seguridad, y los usos de estos ficheros, la captación de imágenes del entorno e interior de los centros respectivos, siendo en los informes previos sobre necesidad y oportunidad del tratamiento de las imágenes por cámaras o videocámaras, donde se concretan específicamente los usos que en cada centro educativo se van a dar, sin que sea necesario ni exigible que la Orden alcance otro grado de detalles.

Por otro lado, la Orden impugnada también cumple con los requisitos legales de Informes previos preceptivos por parte de la Secretaría General Técnica de la Consejería de Educación y de la Agencia de Protección de Datos de la Comunidad de Madrid, pues tales informes constan en el expediente administrativo sin que la normativa ya invocada en esta materia exija un contenido concreto de los mismos, bastando para su emisión favorable que hayan tenido acceso previo a los informes justificativos emitidos por cada uno de los

responsables del fichero en cuestión, y hayan considerado que los mismos cumplen con todos los requisitos de idoneidad, necesidad y proporcionalidad exigidos por la normativa.

Cuarto. En relación con la vulneración de los derechos fundamentales expresados para la instalación de los sistemas de cámaras o videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por ello en la Instrucción 1/2007, de 16 de mayo, de la Agencia de Protección de Datos de la CAM, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los Órganos y Administraciones Públicas de la CAM (BOCAM 18 julio 2007) que se produce en su apartado 2.8 el contenido del artº 6 antes expresado del Reglamento, en la Norma Quinta se establece que toda instalación deberá respetar el principio de proporcionalidad, lo que, en definitiva, supone, siempre que resulte posible, adoptar otros medios menos intrusivos para la protección de los datos de carácter personal, 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 sus funciones por las Administraciones Públicas, debiéndose valorar la utilización de estos sistemas en atención a su proporcionalidad en relación con el fin perseguido.

Los criterios de legitimación y proporcionalidad a la hora de valorar la captación de imágenes a través de cámaras o videocámaras, han sido considerados determinantes por la jurisprudencia del Tribunal Constitucional, entre otras, en sus Sentencias STC 186/2000, de 10 de julio (fundamentos jurídicos 6 y 7), y STC 98/2000, de 10 de abril (fundamento jurídico 8). A su vez, con carácter general, dichos criterios han sido considerados como determinantes de cualquier medida restrictiva de derechos fundamentales en otras muchas Sentencias del Alto Tribunal STC 66/1995, de 8 de mayo, fundamento jurídico 5;SSTC 55/1996, de 28 de marzo , fundamentos jurídicos 6, 7, 8 y 9;SSTC 207/1996, de 16 de diciembre , fundamento jurídico 4.e), y SSTC 37/1998, de 17 de febrero , fundamento jurídico 8]. Así, de acuerdo con dicha jurisprudencia, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario

constatar si cumple los tres requisitos o condiciones siguientes: 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).

La proporcionalidad es un elemento fundamental en la instalación de sistemas de cámaras o videocámaras en el ámbito público, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llevar a generar situaciones abusivas. Este juicio de proporcionalidad tratándose de Centros Educativos Públicos de Enseñanza Secundaria Obligatoria, no ofrece duda que en los tiempos actuales concurren más ventajas y beneficios que inconvenientes en la instalación de videocámaras en pasillos (no en las aulas), ya que se utilizan: a) como medida preventiva y disuasoria, b) como instrumento de identificación de aquellas personas que privan de sus derechos a la gran mayoría de la Comunidad Educativa, c) no se pretende almacenar imágenes sino garantizar los derechos de la mayoría y d) disminuir los gastos por desperfectos.

En definitiva, la utilización de los tres ficheros creados por la Orden recurrida no se considera que afecta a derechos fundamentales de los trabajadores del Centro.

Quinto. Los razonamientos precedentes llevan a la desestimación del recurso, sin que se efectúe pronunciamiento en materia de costas (artículo 139.1 de la L.J.C.A.)

Fallamos que desestimamos el Recurso Contencioso-Administrativo nº 644/2009 interpuesto por la representación procesal del Sindicato de la Enseñanza de Madrid de la Confederación General del Trabajo contra la Orden 1944/2009 de 27 de abril (por la que se crean tres ficheros que contienen datos de carácter personal dependientes del Instituto

de Educación Secundaria "Avenida de los Toreros", del Instituto de Educación Secundaria "Carmen Martín Gaite" y del Instituto de Educación Secundaria "Salvador Dalí" (B.O.C.A.M. de 13 de mayo de 2009), y que se confirma por ajustarse a Derecho.

La creación del fichero de videovigilancia en el ámbito de las Administraciones públicas debe realizarse mediante la aprobación de una disposición de carácter general, siguiendo para ello los trámites correspondientes.

7.7.- Sentencia de la Sala Contencioso-Administrativo de la Audiencia Nacional de 3 de febrero de 2011 sobre instalación de una cámara en la terraza de un bar.

Primero. Se interpone el presente recurso contencioso administrativo frente a la resolución de fecha 2 de Diciembre de 2009 dictada por el Director de la Agencia Española de Protección de Datos por la que se desestima el recurso interpuesto frente a la resolución de fecha 5 de Octubre de ese año por la que se impone al recurrente una sanción por importe de 2.500 euros por infracción de lo previsto en el artículo 6 de la LOPD en relación con lo previsto en el articulo 44.3.d) de la misma Ley

En el caso analizado, las imágenes captadas por las cámaras son datos de carácter personal conforme al artículo 3.a) de la LOPD (y el articulo 2 .e) de la Directiva 95/46) y en aplicación, también, de lo que señala el artículo 5.1. f) del 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, datos en los términos de la LOPD.

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

procedimiento, el denunciado capta datos personales (imágenes de aquellos que se sitúan en la terraza del local ó que circulan por la vía pública). 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.

Ha quedado acreditado que el denunciado tenían instaladas una cámara de videovigilancia en el interior del local que recogía y captaba imágenes de la vía pública, superando el principio de proporcionalidad, establecido en materia de protección de datos, por lo que procede la imposición de sanción. Sin embargo, debido a que del informe de la Policía Municipal se desprende que el denunciado instaló el sistema en la creencia de que era legal y dado que no consta acreditado que en la actualidad las cámaras continúen grabando procede imponer la sanción en la cuantía de 2.500 euros. No obstante, deberá proceder a retirar las citadas cámaras.

Segundo. La parte recurrente emplea como primer motivo de nulidad el que hace referencia a que la resolución de inicio del expediente sancionador no le fue notificada personalmente sino que se notificó por edictos.

Examinando el expediente resulta que, efectivamente, la resolución de inicio del expediente se notificó mediante edictos publicados en el BOE (folio 35 del expediente) y edictos en el Ayuntamiento de Madrid (folio 44).

No obstante, posteriormente, al recurrente se le notificó la resolución de fecha 5 de Octubre de 2009 que imponía la sanción y este interpuso recurso de reposición que fue resuelto, en sentido desestimatorio, mediante la resolución que ahora es objeto del presente recurso contencioso.

Por lo tanto, la falta de notificación de la resolución de inicio del expediente no ocasionó ninguna indefensión al recurrente que pudo emplear el recurso ante la resolución

sancionadora para proponer prueba y, sin embargo, ni propuso prueba en el escrito de interposición del recurso ni lo hizo a lo largo de este recurso contencioso administrativo.

También hay que hacer notar que la Agencia, una vez acordado el inicio del expediente no acordó la práctica de diligencia alguna, y se limitó a sancionar con la base de la única prueba aportada que era la denuncia inicial formulada por la Policía Local (junto a su informa ampliatorio).

Por lo tanto, independientemente de la forma de notificación de la resolución de inicio del expediente sancionador, resulta que ninguna indefensión se ha causado al recurrente y no procede acceder a la nulidad interesada puesto que ha podido practicar cuantas pruebas ha considerado pertinentes.

Tercero. En cuanto al fondo, parece que la parte confunde el hecho de captar las imágenes con el hecho de que estas se conserven un determinado periodo de tiempo y ello pues parece ignorar que la captación de imágenes también supone un tratamiento que, en el caso presente, se ha realizado sin el consentimiento de los titulares del dato que son los viandantes que se han visto grabados por el sistema instalado por el ahora recurrente.

El recurrente afirma que la cámara recoge las imágenes y las transmite a un monitor donde solo pueden ser visionadas en tiempo real, pero que no se conservan en forma alguna por lo que concluye que no realiza tratamiento ni resulta posible su uso posterior; entiende que lo que hace la cámara sería algo similar a lo que haría un espejo que permitiese ver lo que ocurre en la terraza.

El Abogado del Estado se limita a insistir en que la simple recogida de datos es un tratamiento en el aspecto recogido por el apartado c) del artículo 3 de la LOPD.

Hay que partir de que el apartado c) del artículo 3 de la LOPD define el tratamiento de datos como: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y

cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Por lo tanto, la simple recogida de datos (aún independientemente de la grabación ó conservación) ya constituye un tratamiento de los datos, de las imágenes.

En el mismo sentido, la Instrucción 1/2006 del Director de la Agencia sobre la materia, comprende dentro de su ámbito de aplicación un amplio abanico de conductas "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". Por lo que resulta que no es necesario la grabación ni la conservación posterior de las imágenes grabadas para que sea aplicable lo previsto en dicha Instrucción y en la normativa general de protección de datos y basta la simple recogida del dato de la imagen de aquel que no ha sido informado ni ha consentido la grabación.

Esta conducta supone un tratamiento de datos sin consentimiento sancionado por el articulo 44.3.d) de la LOPD que considera 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. Dicho precepto debe relacionarse con lo previsto en el artículo 6 cuando habla de que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

La captación de imágenes de la vía pública de personas identificadas o identificables, como resulta que se hacía por la cámara del recurrente, y fuera de un ámbito estrictamente privado o domestico se encuentra reservada, con carácter exclusivo, a las Fuerzas y Cuerpos de Seguridad del Estado con fines de videovigilancia, en consonancia con lo establecido en la Ley Orgánica 4/1997. Resulta por lo tanto contrario a la normativa de

protección de datos, salvo la excepción citada, la captación y difusión de imágenes de la vía pública en las que pueda identificarse a las personas y ello independientemente de que las imágenes se conserven aunque en este caso, el visionado en la pantalla de un ordenador permite ampliamente la posibilidad de grabación de las imágenes que acceden procedentes de la videocámara.

La Instrucción 1/2006 del Director de la Agencia solo excluye la grabación en los casos de que esta se realice con finalidad familiar ó domestica, no siendo relevante que la grabación se realice de la terraza del establecimiento ó de la puerta de entrada y ello pues en ambos casos resulta que se incumplen las exigencia del artículo 3 de la Instrucción en cuanto a información de la grabación que se está produciendo.

Es fundamental en esta cuestión atender al principio de proporcionalidad que menciona el artículo 4.2 de la mencionada Instrucción 1/2006 según el cual la instalación de videocámaras solo es legitima cuando la finalidad de vigilancia no pueda obtenerse de otro modo ó exija esfuerzos desproporcionados. En el caso presente, resulta obvio que la vigilancia por parte del recurrente de la terraza de su establecimiento debe poderse realizar de modo diferente al realizado sin que sea precisa la captación de imágenes, no solo de clientes sino de personas que puedan transitar por la vía pública.

De la instrucción realizada por la Agencia y que obra en el expediente no resulta con claridad si se graban a viandantes que pasen por la calle ó a las personas que estaban en la terraza del establecimiento ó a las personas que entraban en el establecimiento del recurrente. En cualquier caso, la denuncia que obra al folio 3 y el informe ampliatorio que obra al folio 4 hablan de que la grabación se produce "del exterior visionando la entrada del local y la vía pública" lo cual debe tenerse por cierto al no haber acreditado el recurrente otra cosa.

En cualquier caso, por lo que se sanciona es por la captación sin consentimiento (tratamiento sin consentimiento) y la falta de información que debía ofrecer el ahora

recurrente hubiera podido dar lugar a otra infracción diferente derivada de la violación de las garantías que se recogen en el artículo 5 de la LOPD. Es decir, se sanciona el tratamiento sin consentimiento y no el hecho de no haber informado debidamente a los clientes ó viandantes cuyas imágenes fueron captadas.

Por todo ello, lo procedente es la integra desestimación de la demanda y la confirmación de la resolución objeto de recurso.

La instalación de una cámara en la terraza de un bar es considerada desproporcionada.

Deben buscarse otras alternativas que sean menos intrusivas para la privacidad.

8.- BUENAS PRÁCTICAS.

En los últimos años, tanto las Autoridades de Control como la Comisión Europea están impulsando la adopción de nuevas herramientas mediante las cuales se implementen las buenas prácticas en la protección de datos, de manera, que no sólo los responsables de ficheros cumplan con la normativa vigente, sino que se adopten una serie de medidas para ser más respetuoso con la privacidad de los ciudadanos. Entre ellas, podemos citar la "Privacidad por diseño" o los "Informes de Impacto de Privacidad".

En este sentido, la APDCM recomienda a los responsables de ficheros, con la finalidad de implementar las buenas prácticas, la puesta en marcha del llamado "Documento de política de privacidad sobre videovigilancia".

Asimismo, en este apartado de la Guía también queremos reflejar un resumen de los documentos que en materia de videovigilancia han publicado otras Autoridades de Control, ya que el contenido de los mismos es tremendamente útil para cumplir con la protección de datos en la instalación de este tipo de sistemas.

8.1.- "Documento de política de privacidad sobre videovigilancia".

Su objetivo es facilitar información sobre los tratamientos de datos que se realicen mediante la instalación de videocámaras, así como dar transparencia en la utilización de las mismas. La APDCM recomienda que el citado documento esté a disposición de los trabajadores de la organización y que sea accesible al público, en el caso de que se graben imágenes de los mismos.

Con el fin de garantizar aún más la protección de datos, la APDCM también recomienda que se realicen auditorías de seguridad sobre las cámaras –cuando el nivel de las medidas sea básico, ya que si son medias o altas será obligatoria la realización de la misma-, designar un responsable de protección de datos dentro de la organización con la finalidad de canalizar todas las cuestiones referentes a esta materia, y cuando el volumen de los tratamientos a través de imágenes así lo requieran llevar a cabo un "Informe de Impacto de Privacidad".

Este documento se caracteriza por lo siguiente:

- Aprobado por la máxima autoridad del organismo.
- Tiene que publicitarse a los afectados.
- Descriptivo del tratamiento que se realiza por las videocámaras:
    - Identificación del responsable del fichero.
    - Identificación del fichero.
    - Descripción técnica del sistema instalado.
    - Legitimación.
    - Finalidad.
    - Descripción general de la instalación de las cámaras.
    - Existencia de encargado de tratamiento y contrato –en su caso-.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

- Medidas de seguridad adoptadas.
- Cómo se cumple con el artículo 5 de la LOP.
- Período de cancelación de los datos.
- Quién accede a las imágenes.
- Cesiones previstas.
- Formularios para el ejercicio del derecho acceso, cancelación y oposición.
- Informe de auditoría (si se ha realizado).
- Si se han realizado cursos de protección de datos a los trabajadores que controlan las imágenes.

DOCUMENTO DE POLÍTICA DE PRIVACIDAD
NOMBRE DEL FICHERO:
RESPONSABLE DEL FICHERO:
IDENTIFICACIÓN DEL FICHERO: - Disposición general de creación. - Boletín Oficial de publicación de la disposición: - Número de inscripción en el Registro de Fichero de Datos de la APDCM:
FINALIDAD DEL FICHERO:
RELACIÓN DE AFECTADOS POR LA CAPTACIÓN DE IMÁGENES (pj, trabajadores, clientes, ciudadanos…):
NORMATIVA QUE LEGITIMA EL TRATAMIENTO:
DESCRIPCIÓN TÉCNICA DEL SISTEMA:
LUGARES DONDE SE HAN INSTALADO LAS CÁMARAS: - Número de cámaras: - Potencia del zoom: - Tipo de cámaras (pj domo):

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

- Fijas o móviles:
CUMPLIMIENTO DEL DERECHO DE INFORMACIÓN: - Carteles informativos: Contenido: Lugar de colocación: - Información adicional: (Ver Anexo I)
EXISTENCIA DE ENCARGADO DE TRATAMIENTO: - Nombre de la empresa - Adopción de cláusulas del artículo 12 LOPD (Ver Anexo II)
PERÍDO DE CANCELACIÓN DE LAS IMÁGENES:
MEDIDAS DE SEGURIDAD: - Nivel. - Breve descripción de las mismas. - Auditoría (Ver Anexo III)
PERSONAL QUE REALIZA TRATAMIENTO DE IMÁGENES: - Firma de documentos de confidencialidad (Ver Anexo IV). - Cursos de formación recibidos en materia LOPD (nombre).
RESPONSABLE DE PROTECCIÓN DE DATOS: - Identificación. - Funciones.
RESPONSABLE DE SEGURIDAD (obligatorio para medidas medias y altas): - Identificación. - Funciones.
CESIONES PREVISTAS:
FORMULARIOS PARA EL EJERICICO DE LOS DERECHOS ARCO: (Ver Anexo V).
INFORME DE IMPACTO DE PRIVACIDAD (Ver Anexo VI):

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

ANEXOS:

I. Información adicional sobre el cumplimiento del artículo 5 de la LOPD.

II. Copia del contrato del artículo 12 de la LOPD con el encargado del tratamiento.

III. Copia del informe de auditoría (en su caso).

IV. Copia de los documentos de confidencialidad firmados.

V. Modelos para el ejercicio de los derechos ARCO.

VI. Copia del informe de impacto de privacidad.

8.2.- Documentos de otras Autoridades de Control.

8.2.1.- Guía de videovigilancia del Supervisor Europeo de Protección de Datos.

El Supervisor es una autoridad independiente que tiene como función principal que las instituciones y organismos de la Unión Europea cumplan con la normativa de protección de datos. Sus competencias también alcanzan a informar cualquier norma comunitaria que pueda afectar este derecho fundamental.

Su objetivo es ofrecer información práctica destinada a las instituciones y órganos de la Unión Europea que utilicen la videovigilancia para que sean respetuosos con la protección de datos. Lo más destacable de esta Guía es lo siguiente:

- Contiene un apartado sobre la "Privacidad por diseño", que está siendo impulsada por la Unión Europea y otras Autoridades de Control como la canadiense, incluyendo también la posibilidad de realizar "Impactos de privacidad" antes de realizar la correspondiente instalación.

- Contempla el uso de las cámaras, además de por razones de seguridad, con fines de investigación, y "monitorización" y control de empleados, así como el empleo de webcams para diversas funcionalidades como pueden ser cursos de formación, reuniones o actividades recreativas.

- Sobre las obligaciones que tienen que cumplirse por los responsables de ficheros comunitarios, sobresale el apartado de cesiones de imágenes, con dos supuestos específicos:

    - Cesiones a instituciones comunitarias con poderes de investigación, como la Ofician Europea Anti-Fraude (OLAF).
    - Cesiones a las autoridades nacionales de los Estados miembros, como policía, jueces o tribunales.

- Recomienda cumplir con el derecho de información a través de dos métodos diferentes:

    - Mediante el cartel de zona videovigilada.
    - Ofreciendo información adicional en Internet y en la Intranet de cada responsable.

- Introduce el concepto de "Accountability" ("Responsabilidad"), de manera que para cumplir con el mismo el responsable debe:

    - Adoptar una política de privacidad del uso de las cámaras.
    - Realizar y documentar auditorías periódicas.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

La Guía se encuentra disponible en inglés, francés y alemán.

¿Dónde puedo consultar este documento?

http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Guidelines

8.2.2- Informes del Grupo del Artículo 29.

Este Grupo, de carácter consultivo e independiente, fue creado al amparo del artículo 29 de la Directiva 95/46. Está compuesto por un representante de la autoridad o autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Dentro de su función consultiva, elabora informes sobre cualquier asunto a nivel comunitario que afecte al derecho fundamental a la protección de datos.

En materia de videovigilancia, destacan los siguientes informes:

- **Informe 8/2001 sobre el tratamiento de datos en el contexto laboral:**

  En su apartado 12 se analiza la videovigilancia y monitorizacón en el ámbito laboral, que se puede realizar no sólo mediante las cámaras, sino también controlando el correo electrónico del trabajador, el uso que realice de internet y también a través de la localización. La normativa de protección de datos es aplicable a estos supuestos, incidiendo en el cumplimiento de los principios de transparencia (información) y proporcionalidad.

¿Dónde puedo consultar este documento?

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf

- **Informe 4/2004 relativo al tratamiento de datos personales mediante videovigilancia por videocámara:**

Supone un desarrollo mayor de lo contemplado en el anterior informe. Asimismo, el Grupo había elaborado con carácter previo el "Documento de trabajo relativo al tratamiento de datos personales mediante videovigilancia por videocámara". (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67_es.pdf).

Destacar lo siguiente:

- El análisis del principio de proporcional, en el cual inciden diversos elementos:
  - El ángulo visual en relación a los fines perseguidos.
  - Si las cámaras son fijas o móviles.
  - Uso del zoom.
  - Congelación de imágenes.
  - Conexión con un centro de alarmas.
- Los supuestos de no aplicación de la Directiva de protección de datos:
  - Tratamientos de imágenes y sonidos realizados con fines de seguridad pública, defensa, seguridad del Estado o ejercicio de

actividades del Estado en el ámbito del Derecho penal u otras actividades no afectadas por el Derecho comunitario.

- Operaciones de tratamiento de imágenes realizadas por una persona física en el ámbito personal o familiar.
- En consonancia con el artículo 9 de la Directiva, los Estados miembros pueden establecer excepciones y exenciones cuando el tratamiento se realice con fines exclusivamente periodísticos o de expresión literaria o artística, en particular en el sector audiovisual.

- Supuestos en los cuales hay que prestar más atención y evaluarlos caso a caso:

  - Interconexión de la videovigilancia gestionada por diferentes responsables de tratamientos.
  - Asociación de imágenes y datos biométricos.
  - Sistemas de identificación vocal.
  - Sistemas de identificación de reconocimiento fisonómico.
  - Localización de forma automática de itinerarios y pistas.
  - Toma de decisiones basadas en el perfil de una persona.

¿Dónde puedo consultar este documento?

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_es.pdf

- **Informe 4/2007 sobre el concepto de dato personal:**

El objetivo de este informe es alcanzar un acuerdo sobre el concepto de datos personales, utilizando ejemplos extraídos de la práctica nacional de los Estados miembros. Uno de estos ejemplos es el tratamiento de datos mediante la

videovigilancia, ya que las personas pueden ser identificables, teniendo en cuenta, además, que una de las finalidades de la videovigilancia es identificar personas. Incluso, aunque se difumine la cara, el Grupo considera que la persona puede ser identificada por amigos, parientes o vecinos, por la ropa, complexión física o corte de pelo.

¿Dónde puedo consultar este documento?

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

8.2.3.- Guía sobre videovigilancia en el sector privado. Autoridad de Protección de Datos de Canadá.

Como su nombre indica, esta Guía cubre el sector privado, debiendo implementar éstos un documento de "Política de videovigilancia" en el cual se incluya, entre otros:

- Los criterios que han motivado la puesta en funcionamiento de la videovigilancia;
- Que dicha puesta en funcionamiento ha sido decidida por la persona responsable en la organización;
- La finalidad de la grabación;
- El plazo de cancelación de las imágenes;
- Las medidas de seguridad;
- Procedimiento para la comunicación de imágenes y grabaciones a terceros;
- Duración de la instalación de este sistema;
- Quién puede acceder a las imágenes;
- Contrato con un tercero que se ocupe del sistema.

Asimismo, también contiene una serie de recomendaciones para las empresas que se dediquen a la investigación privada y utilicen la videovigilancia, entre otros:

- Debe tratarse de una empresa que tenga reconocida como actividad la investigación de acuerdo a la normativa canadiense;
- La recogida de información tiene que ser limitada en relación a la videovigilancia;
- Descripción clara y concisa del objetivo de la videovigilancia y de la información que se pretende recabar;
- Existencia de instrucciones para la conservación y borrado de las imágenes.
- Prohibición de subcontratar el servicio salvo que exista un contrato escrito.

- Los investigadores deben ser formados sobre el correcto uso del sistema de videovigilancia.

¿Dónde puedo consultar este documento?

http://www.priv.gc.ca/information/pub/gd_cvs_20090527_e.cfm

8.2.4.- Guía sobre videovigilancia en el sector público: utilización por la policía y otros organismos de control. Autoridad de Protección de Datos de Canadá.

Establece quince principios que tienen que tenerse en cuenta el la instalación y uso de cámaras por la policía y otras instituciones. No obstante, estos principios no son de aplicación cuando se trate de una investigación específica al amparo de la normativa de ese país o la misma haya sido autorizada judicialmente, pero sí cuando se hayan instalado las cámaras en una plaza o vía pública.

Entre los principios podemos destacar los siguientes:

- La videovigilancia tiene carácter excepcional, y sólo debe ser instalada cuando no haya más remedio.
- Antes de realizar la instalación, se recomienda llevar a cabo un "Estudio de Impacto de Privacidad" ("Privacy Impact Assesment"), y realizar una consulta pública a los afectados, por ejemplo, a través de asociaciones de vecinos.
- Tiene que existir un cartel en el cual se informe a los afectados de que la zona está siendo controlada por cámaras, indicando quién es el responsable.
- Se prohíbe la instalación en baños, salas para cambiarse de ropa los empleados, o que graben las ventanas de los edificios.

- El sistema instalado debe ser auditado regularmente.
- No necesariamente la videovigilancia tiene que funcionar todos los días del año, sino que se recomienda su uso limitado, cuando pueda existir algún problema por la confluencia de personas.
- El responsable tiene que elaborar un documento de "Política de Privacidad".

¿Dónde puedo consultar este documento?

http://www.priv.gc.ca/information/guide/vs_060301_e.cfm

8.2.5.- Código de Videovigilancia de la Autoridad de Protección de Datos del Reino Unido.

Este Código contempla el uso de la videovigilancia y otros sistemas que permitan la captura de imágenes de personas identificables para las siguientes finalidades:

- Monitorización de personas.
- Uso de las imágenes para tomar acciones legales contra un individuo.

- Uso de imágenes que puedan afectar de alguna forma a la privacidad de un tercero.

Como primera recomendación, al igual que ocurre en alguno de los documentos que hemos citado anteriormente, el responsable debería realizar un "Estudio de Impacto de Privacidad" ("Privacy Impact Assesment"), y en base a los resultados del mismo decidir si es necesario o no la instalación.

Otra de las partes que destacan es la referente a la adecuada administración del sistema de videovigilancia. Para que dicha administración sea realizada de forma efectiva y eficiente, respetando los derechos de los individuos se hace necesario que se clarifiquen los siguientes puntos:

- Quién es el responsable y quién toma las decisiones sobre la utilización del sistema.
- Identificar y definir los objetivos de la videovigilancia.
- Existencia de un documento para manejar las imágenes grabadas.
- Notificación de la creación del fichero al ICO con carácter previo a su puesta en funcionamiento.
- En el caso de que exista un encargado del tratamiento, si se ha firmado el correspondiente contrato.

Por último, mencionar también el apartado dedicado al funcionamiento de las cámaras, ya que en función de los elementos técnicos de las mismas nos encontraremos con cuatro situaciones diferentes:

- "Monitorización": permite "vigilar" el movimiento de las personas pero no tomar imágenes de personas individuales.

- "Detección": la imagen sirve para detectar la presencia de una persona pero sin necesidad de ver su cara.
- "Reconocimiento": como su nombre indica, permite que la imagen sea de una calidad adecuada como para distinguir si uno conoce o no a esa persona.
- "Identificación": la imagen es de gran calidad de manera que puede ser utilizada en un juicio para probar la identidad de una persona.

¿Dónde puedo consultar este documento?

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx

8.2.6.- Decisión sobre videovigilancia de la Autoridad de Protección de Datos de Italia, adoptada el 8 de abril de 2010.

Sobre esta Decisión adoptada por la Autoridad italiana, destacamos la parte referente al"Prior checking", es decir, esa Autoridad realiza con carácter previo al funcionamiento del sistema de videovigilancia un análisis para comprobar si el mismo es respetuoso con la protección de datos personales, pudiendo dirigir instrucciones al responsable para que el sistema se adecúe. Por ejemplo, cuando se trate de un sistema que utilice también datos biométricos o que permitan conocer el comportamiento de una persona.

Sin embargo, hay una serie de supuestos en los que no será necesario realizar el "Prior checking":

- La Autoridad Italiana de Protección de Datos haya emitido una decisión previa sobre categorías de procesamiento de datos;

- Las circunstancias de hecho, la finalidad del tratamiento, el tipo y las modalidades de aplicación del sistema, así como los tipos de datos están en consonancia con una decisión previa de la Autoridad;

Otro de los puntos importantes, es el referente a la cancelación de las imágenes. Con carácter general, el plazo para cancelarlas no será superior a 24 horas, aunque existirán algunas excepciones como el supuesto de que las imágenes hayan sido solicitadas para

una investigación judicial, o cuando se trate de actividades que conlleven un riesgo potencial (el robo de un banco). En todo caso, el período de cancelación no debe ser superior a una semana.

Cuando se trate de cámaras instaladas por los ayuntamientos el período será de siete días cuando la grabación tenga por finalidad la seguridad.

Este período puede ser ampliado mediante una autorización de la Autoridad italiana.

Por otra parte, esta Decisión contempla diversos supuestos, además de la seguridad, de uso de las cámaras:

- Control de empleados.
- Prestación y asistencia sanitaria.
- Escuelas.
- Seguridad en el transporte.
- Turismo.
- Control del tráfico.

¿Dónde puedo consultar este documento?

http://www.garanteprivacy.it/garante/doc.jsp?ID=1734653

8.2.7.- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos.

Se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de videovigilancia 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 aquellas. Recoge las obligaciones que debe cumplir el responsable a la hora de instalar un sistema de videovigilancia:

- Legitimación.
- Derecho de información.
- Principios de calidad, proporcionalidad y finalidad del tratamiento.
- Cancelación.
- Notificación de ficheros.
- Derechos de las personas.
- Seguridad y secreto.

Acompaña a la Instrucción un Anexo con el cartel que hay que instalar para cumplir con el derecho de información, en el que aparecerá:

- Una referencia a la LOPD.
- La finalidad ("Zona videovigilada").

- Identificación del responsable ante el cual pueden ejercitarse los derechos.
-

¿Dónde puedo consultar este documento?

https://www.agpd.es/portalwebAGPD/canalresponsable/videovigilancia/common/Instruccion_1_2006_videovigilancia.pdf

8.2.8.- Guía de Videovigilancia de la Agencia Española de Protección de Datos.

Además de recoger las obligaciones que debe adoptar el responsable del fichero de videovigilancia, a las que hace referencia la Instrucción 1/2006, recoge supuestos específicos del uso de las cámaras como:

- Acceso a edificios y salas de juego.
- Entidades financieras.
- Uso en la vía pública.
- Cámaras conectadas a internet.
- Entornos escolares y menores.
- Espacios públicos de uso privado.
- Taxis.
- Control de tráfico.
- Espacios deportivos.
- Utilización por las Fuerzas y Cuerpos de Seguridad del Estado.

También analiza la utilización de las cámaras para otros usos no ligados a la seguridad, como pueden ser la promoción turística y la investigación científica.

¿Dónde puedo consultar este documento?

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

8.2.9.- Plan Sectorial de Oficio de Videocámaras en Internet. Agencia Española de Protección de Datos.

Mediante este Plan se efectuó un análisis del uso de las llamadas cámaras IP –cámaras de vídeo conectada a Internet que permiten un acceso remoto a través de la Red, pudiendo visionar imágenes en tiempo real-, así como las correspondientes recomendaciones y sugerencias.

En primer lugar, este documento explica cómo funcionan las cámaras IP y cuál es el marco legal aplicable. También realiza un análisis sobre los principios que hay que cumplir como son los de legitimación, información, seguridad y deber de secreto.

Sin lugar a dudas, la parte más destacable de este documento es el análisis y recomendaciones de tipología de webs analizadas:

- Captación de imágenes de paisajes o panorámicas.
- Captación de imágenes de la vía pública.
- Captación de imágenes en el lugar de trabajo.
- Captación de imágenes en el interior de establecimientos comerciales.

Por último, el Plan contiene un Decálogo para usuarios de cámaras conectados a Internet.

¿Dónde puedo consultar este documento?

http://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/plan_sectorial_camaras_internet_2009.pdf

8.2.10.- Instrucción 1/2009, de 10 de febrero, de la Autoridad Catalana de Protección de Datos sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

Destaca la exigencia de, con carácter previo a la creación del fichero o puesta en marcha del sistema de videovigilancia en el caso de que no se registren imágenes, elaborar una Memoria que, entre otros puntos, debe hacer referencia a los siguientes:

- Justificación de:
  - Legitimidad.
  - Finalidad.
  - Proporcionalidad.

- Ubicación y campo de visión de las cámaras.

- Definición de las características del sistema:
  - Número de cámaras.
  - Fijas o móviles.
  - Plano fijo o móvil.

- Período de instalación del sistema.
- Período de almacenamiento de las imágenes.
- Medidas de seguridad.

La Instrucción, como no podría ser de otra forma, también regula otras cuestiones como son los principios aplicables al tratamiento de imágenes, la creación e inscripción de los ficheros, deber de información, derechos de acceso, rectificación, cancelación y oposición, procedimiento para el ejercicio de los mismos, imágenes y voces captadas por las fuerzas y cuerpos de seguridad, y medidas de seguridad.

¿Dónde puedo consultar este documento?

http://www.apd.cat/media/686.pdf

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

9.- LECCIONES RÁPIDAS SOBRE VIDEOVIGILANCIA.

¿Sabía que …. casi un 30% de las resoluciones sancionadores emitidas por la AEPD son en materia de videovigilancia[12]? Es la materia con mayor número de infracciones declaradas y sanciones impuestas.

¿Sabía que…. durante el año 2010 en la AEPD se inscribieron 31.443 ficheros de titularidad privada cuya finalidad es la videovigilancia?[13]

¿Sabía que…. una empresa de seguridad fue sancionada con más de 60.000 Euros porque su personal utilizaba las cámaras de seguridad instaladas en un aeropuerto para enfocar determinadas partes de la anatomía femenina?

¿Sabía que…. el 73% de los españoles se muestra favorable a la instalación de cámaras de seguridad o videovigilancia[14]?

¿Sabía que…. el 10% de los españoles están en contra de la videovigilancia porque consideran que con ella se pierde intimidad y privacidad[15]?

¿Sabía que… el sector de la videovigilancia casi monopoliza el aumento de las denuncias en materia de protección de datos?

¿Sabía que… la videovigilancia supone un tratamiento de datos de carácter personal y que hay que cumplir con la normativa existente en esta materia?

¿Sabía que… antes de instalar un sistema de videovigilancia en la vía pública hay que tener autorización de la Comisión de Videovigilancia?

¿Sabía que…si contrata con un tercero la gestión del sistema de videovigilancia ese tercero se convierte en encargado del tratamiento?

[12] Fuente: Memoria AEPD 2010.
[13] Fuente: Memoria AEPD 2010.
[14] Datos estadísticos extraídos del Barómetro del CIS. Estudio nº 2.812. Septiembre 2009.
[15] Datos estadísticos extraídos del Barómetro del CIS. Estudio nº 2.812. Septiembre 2009.

¿Sabía que…el encargado del tratamiento y el responsable deben firmar un contrato con el contenido del artículo 12 de la LOPD?

¿Sabía que…ese contrato con carácter previo a su perfeccionamiento debe ser enviado a la APDCM?

¿Sabía que… los sistemas de videovigilancia hacen sentir más seguros a los ciudadanos a pesar de que no se ha demostrado que produzcan un descenso de delitos?

¿Sabía que… las cámaras situadas en los accesos a cualquier tipo de establecimiento no deben grabar transeúntes o vehículos?

¿Sabía qué… un grupo de vecinos obligó al Ayuntamiento de su municipio a retirar cámaras de videovigilancia por enfocaban el interior de sus viviendas?

¿Sabía que… la utilización de un cartel informativo que utilice expresiones tipo: "Sonria, le están grabando", no es una forma legítima de cumplir con el deber de información?

¿Sabía que…cuando se instalan cámaras "falsas" o las cámaras no están funcionando no se aplica la LOPD?

¿Sabía que… las imágenes recogidas por un sistema de videovigilancia que cumpla todas las garantías legales pueden tener fuerza probatoria?

¿Sabía que… hay cámaras de videovigilancia que no sólo graban sino que emiten las imágenes en directo en Internet sin informar a las personas que son grabadas?

¿Sabía que… es ilegal ceder imágenes recogidas por una cámara de videovigilancia salvo que exista cobertura legal?

¿Sabía que… en el ámbito laboral los trabajadores tienen derecho a ser informados previamente de la instalación de un sistema de videovigilancia y a saber donde están las cámaras?

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

¿Sabía que… una importante empresa española fue sancionada porque colocó los monitores de supervisión de imágenes captadas por los dispositivos de videovigilancia a la vista de sus clientes?

¿Sabía que… un particular que coloque un sistema de videovigilancia con recogida de imágenes se convierte en responsable de fichero y asume sus obligaciones y responsabilidades?

¿Sabía que… las cámaras instaladas en establecimientos comerciales no deben ser utilizadas para el estudio de hábitos de consumo de los clientes?

¿Sabía que…. instalar cámaras en zonas de descanso como unos vestuarios supone una vulneración grave de los derechos fundamentales de los trabajadores, como la privacidad, la intimidad o la imagen?

¿Sabía que… antes de instalar un sistema de videovigilancia hay que preguntarse si es estrictamente necesario?

¿Sabía que…en vez de instalar un sistema de videovigilancia hay alternativas menos intrusivas para la privacidad?

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

10.- SERVICIOS DE LA APDCM.

LA APDCM pone a disposición de todos los órganos y organismos que están bajo su ámbito de control una serie de servicios de ayuda en materia de protección de datos personales.

La Agencia asesora gratuitamente a los órganos y organismos para el mejor cumplimiento de todas las obligaciones derivadas de la legislación de protección de datos de carácter personal, designando un consultor especialista que trabaja conjuntamente con los responsables de ficheros de datos personales de los mismos.

De igual modo, la Agencia presta también gratuitamente servicios de formación presencial al personal que participe de algún modo en el tratamiento de los datos de carácter personal.

Para el acceso a estos servicios, basta con que lo solicite por cualquier medio a la Agencia de Protección de Datos de la Comunidad de Madrid:

C/Cardenal Marcelo Spínola, 14 - 28016 Madrid
Teléfono: 91-580.28.74
Fax: 91.580.28.76
Correo electrónico: apdcm@madrid.org
Sitio web: www.apdcm.es

La APDCM resuelve también, por escrito, consultas específicas que afecten a la videovigilancia y también a cualquier materia que incida sobre el derecho fundamental a la protección de datos personales.

Existen también publicaciones y herramientas electrónicas a disposición de los órganos de la Administración encargados de la prestación de servicios sociales, tales como:

- Manuales y Guías:

  - "Protección de Datos Personales para Servicios Sociales Públicos".
  - "Protección de Datos Personales para Servicios Sanitarios Públicos"
  - "Protección de Datos Personales para Centros Educativos Públicos"
  - "Protección de Datos Personales para Ayuntamientos".
  - "Protección de Datos Personales para Universidades".
  - "Protección de Datos Personales para Colegios Profesionales".
  - "Seguridad y Protección de datos personales".
  - "Manual de Protección de Datos para las Administraciones Públicas".
  - "Guía de protección de datos personales para empleados públicos".
  - Otros recursos de apoyo, como el programa informático de ayuda (CUMPLE), para la declaración de ficheros, materiales de formación, modelos de disposición, documentos y notificaciones, normativa, extractos de resoluciones de inspección y tutela de derechos en el ámbito de los servicios sociales, y otros, todos ellos contenidos en el sitio Web de la Agencia de Protección de Datos de la Comunidad de Madrid (www.apdcm.es).

    Citar también la aplicación informática DEPD que permite, a través de la web de la Comunidad de Madrid (www.madrid.org, apartado "Registro de ficheros"), ejercitar, on line, los derechos de acceso, rectificación, oposición y cancelación ante los responsables de los ficheros de la Administración

autonómica. Para ello se requiere tener firma electrónica o DNI electrónico, dado que estos derechos exigen poder identificar, de modo indubitado, a la persona que los ejercita.

Si se carece de firma electrónica o certificado digital, no puede realizarse a través de la web ninguna de las actividades de las dos últimas aplicaciones informáticas citadas –declaración y ejercicio de derechos-, al no poder identificarse de modo fehaciente a quien realiza la actividad pero permite obtener los correspondientes modelos y formularios para, una vez rellenos, presentarlos en la APDCM, en el primer caso, o en el correspondiente Registro público, en el segundo.

- Publicaciones periódicas

  - La revista digital www.datospersonales.org, editada con periodicidad bimensual, y que contiene numerosos informes y consultas relativos a protección de datos personales, noticias, normativa nacional e internacional, jurisprudencia, publicaciones y eventos a celebrar. La suscripción es gratuita.

  - El servicio de envío quincenal mediante correo electrónico de novedades de la Agencia de Protección de Datos de la Comunidad de Madrid (nuevas publicaciones, normas, materiales de ayuda, convocatorias de cursos y eventos, servicios, etc…). La suscripción es gratuita a través del sitio web www.apdcm.es (apartado "Servicios" / "Otros servicios y convocatorias").

- Publicaciones monográficas:

  - Colección "Estudios de Protección de Datos", relativa al estudio de la protección de datos de carácter personal, estando editados en la actualidad los siguientes títulos:

    - "El derecho fundamental a la protección de datos. Derecho español y comparado".
    - "La protección de los datos personales".
    - "Datos personales y Administración Pública".
    - "La protección de datos personales en las Administraciones Públicas".
    - "Secreto e intervención de las comunicaciones en internet".
    - "Una aproximación crítica a la autodeterminación informativa".
    - "El impacto de internet en el Derecho Fundamental a la protección de datos de carácter personal".
    - "La Videovigilancia empresarial y la protección de datos personales".
    - "El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión".
    - "Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar".

  - Principios y derechos de protección de datos personales: Doctrina de la Agencia de Protección de Datos de la Comunidad de Madrid 2002-2009.

  - "Repertorio de legislación y jurisprudencia sobre protección de datos". Segunda edición.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

- "Estudios sobre Administraciones Públicas y protección de datos personales. I Encuentro entre Agencias Autonómicas de Protección de Datos".

- "Estudios sobre Administraciones Públicas y protección de datos personales. II Encuentro entre Agencias Autonómicas de Protección de Datos".

- "e-PRODAT: Administración electrónica y protección de datos en regiones y ciudades europeas".

- "An approach to data protection in Europe"

- Memoria del I Premio a las Mejores Prácticas Europeas en materia de protección de datos.

- Memoria del II Premio a las Mejores Prácticas Europeas en materia de Protección de Datos.

- Memoria del III Premio a las Mejores Prácticas Europeas en materia de Protección de Datos.

- Memoria del IV Premio a las Mejores Prácticas Europeas en materia de Protección de Datos.

- Memoria del V Premio a las Mejores Prácticas Europeas en materia de Protección de Datos.

- Memorias anuales de la Agencia de Protección de Datos de la Comunidad de Madrid desde 1998 a 2010.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

- Centro de Investigación y Documentación "Pablo Lucas Murillo de la Cueva", creado en el año 2008 y donde se encuentran a disposición de los responsables de ficheros, estudiosos de la materia y usuarios en general, para su consulta y estudio, un amplio repertorio de legislación y publicaciones nacionales e internacionales especializadas referentes a protección de datos de carácter personal, siendo su consulta gratuita, que habrá de realizarse en la sede de la APDCM.

- Revista en soporte papel, "Revista Española de Protección de Datos", publicación especializada en la materia que recoge información sobre protección de datos tanto nacional como internacional (artículos de responsables de autoridades de control, opiniones de expertos, trabajos académicos y científicos sobre la materia, etc.).

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

11.- BIBLIOGRAFÍA RECOMENDADA SOBRE VIDEOVIGILANCIA.

1. ARZOZ SANTIESTEBAN, Xavier. *Videovigilancia, seguridad ciudadana y derechos fundamentales.* Primera edición. Pamplona. Editorial Aranzadi, S.A. Colección estudios y comentarios. 2010. 356 p. ISBN: 978-84-470-3422-2.

2. BERMEJO BOSCH, Reyes. "Análisis en la doctrina administrativa de la Agencia Española de Protección de Datos en relación con el tratamiento de imágenes a través de sistema de vídeovigilancia". *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2011, núm. 25. p. 61-80.

3. DESDENTADO BONETE, Aurelio y MUÑO RUIZ, Ana Belén. "El control de la prestación del trabajador a través de las nuevas tecnologías: un estudio sobre la videovigilancia en la doctrina judicial". *Revista de Derecho del Trabajo y de la Seguridad Social*. 2010, núm. 44. p. 13-72.

4. ETXEBERRÍA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusco, (Coord.). *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados.* Primera edición. Tirant Lo Blanch. 2010. 333 p. ISBN: 978-84-998-5023-8.

5. ETZIONI, Amitai; et al. *Tendencias en prevención del delito y sus límites: privacidad y dignidad humana frente al uso de las nuevas tecnologías.* AGUSTINA SANLLEHÍ, José Ramón (Dir.); GARCÍA BERMEJO, Mateo (Coord.); SILVA SÁNCHEZ, Jesús (ed. lit.). Madrid. Edisofer S.L.; 2010. ISBN: 978-84-962-6189-1.

6. GOÑI SEIN, José Luis. *La videovigilancia empresarial y la protección de datos personales.* Primera edición. Pamplona. Editorial Aranzadi, S.A. y Agencia de Protección de Datos de la Comunidad de Madrid. Colección Protección de Datos. 2007. 254 p.

7. IGLESIA CHAMARRO, Asunción de la. Las Comisiones de Garantías de la Videovigilancia. *Revista de Derecho Político.* 2008, núm. 68, p. 211-246.

8. JIMÉNEZ SEGADO, Carmelo; PUCHOL AIGUABELLA, Marta. La "cámara oculta" frente a los derechos a la intimidad y a la propia imagen (Comentario a la STS, Sala 1ª, Pleno, 1233/2008, de 16 de enero de 2009). *La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Legislación.* 2009, núm. 2, p. 1472-1476.

9. LLÁCER MATACÁS, María Rosa (Coord.). *Protección de Datos Personales en la Sociedad de la Información y la Vigilancia.* Editorial La Ley. 2011. 380 p. ISBN: 978-84-8126-820-1.

10. LYON, David. *The electronic eye: the rise of surveillance society.* [en línea]. United States. University of Minnesota Press. Consulta 29 de septiembre de 2011. Disponible en <http://books.google.com/books?id=0ax3RYomoG0C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false >.

11. MARTÍNEZ-CARANDE CORRAL, Juan Luis. "Videovigilancia y Ley Ómnibus: Legitimación para el tratamiento de datos personales mediante cámaras de videovigilancia".*La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Legislación.* 2010, núm. 2, p. 1818-1820.

12. MARTÍNEZ MARTÍNEZ, Ricard. Videovigilancia y protección de datos personales: la Instrucción 1/2006, de 12 de diciembre, de la Agencia Española de Protección de Datos. *Revista Aranzadi de Derecho y Nuevas Tecnologías*. 2007, núm. 13, p. 73-92.

13. MARZO PORTERA, Ana y MARZO PORTERA, Iciar. *Vigilancia y control de las comunicaciones electrónicas en el lugar de trabajo.* Primera edición. Barcelona. Ediciones Experiencia, S.L. 2009. 263 p. ISBN: 978-84-96283-70-1.

14. MOZO BONAL, José. "Las redes IP y la protección de datos" [en línea]. *Datospersonales.org. La revista de Agencia de Protección de la Comunidad de Madrid*. Número 47 (30 de septiembre de 2010). [Consulta 3 octubre de 3011]. Disponible en < http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142610430251&esArticulo=true&idRevistaElegida=1142605808886&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales&urlPage=RevistaDatosPersonales%2FPage%2Fhome_RDP >.

15. NAVALPOTRO BALLESTEROS, Tomás. Los derechos individuales frente a la videovigilancia pública: una necesaria mirada retrospectiva a la Sentencia Peck del Tribunal Europeo de Derechos Humanos. Civitas. *Revista Española de Derecho Administrativo.* 2007, núm. 135, p. 631-639.

16. NIEVA FENOLL, Jordi. La protección de derechos fundamentales en las diligencias policiales de investigación del proceso penal. *La Ley Penal. Revista de Derecho Penal, Procesal y Penitenciario.* 2008, núm. 5, p. 81-101.

17. PACHECO CIFUENTES, Alfonso. *¿Deben las joyerías instalar obligatoriamente sistemas de grabación de imágenes?*. Privacidad práctica: El blog de Esther Botella, Santiago Bermell y Alfonso Pacheco. Septiembre 2011. [Consulta: 3 octubre de 2011]. Disponible en <http://www.privacidadpractica.com/2011/09/30/deben-las-joyeras-instalar-obligatoriamente-sistemas-de-grabacin-de-imgenes/

18. PACHECO CIFUENTES, Alfonso y BERMELL GIRONA, Santiago. "La Directiva 2006/123/CE, ¿Hacia una pérdida de legitimación en la videovigilancia?". *Datospersonales.org. La revista de Agencia de Protección de la Comunidad de Madrid*. [en línea]. Número 40 (31 de julio de 2009). [Consulta 3 octubre de 3011]. Disponible en < http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142560478549&esArticulo=true&idRevistaElegida=1142557356539&language=es&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales&urlPage=RevistaDatosPersonales%2FPage%2Fhome_RDP >.

19. PAJARES MONTOLÍO, Emilo. "Videovigilancia y constitución". Ministerio de Administraciones Públicas. *Cuadernos de Derecho Público.* 2006. Núm, 29. P. 173-216.

20. RALLO LOMBARTE, Artemi. "La protección de datos en España: análisis de actualidad". *Anuario de la Facultad de Derecho (Alcalá de Henares.* 2009, p. 15-30.

21. SALGUEIRO RODRÍGUEZ, Jorge. *Videovigilancia en la empresa y seguridad privada.* Asociación Europea de Centrales Receptoras de Alarmas (AECRA). Segunda edición. 2009. 97 p. ISBN: 978-84-613-5083-4.

22. SERRA URIBE, Carlos Enrique. *Derecho a la intimidad y videovigilancia policial.* Primera edición. Ediciones del Laberinto. 2006. 160 p. Serie Laberinto Político. ISBN: 978- 88-483-2218-

23. SERRANO GÓMEZ, Alfonso. *Tendencias de la criminalidad y percepción social de la inseguridad ciudadana en España y la Unión Europea.* Primera edición. Madrid. Edisofer S.L.; 2006. 320 p. ISBN: 978-84-962-6132-7.

24. TALENS VISCONTI, Eduardo Enrique y CHAPARRO MATAMOROS, Pedro. "Colisión de los derechos del artículo 18 CE con los métodos modernos de control empresarial: especial referencia a la jurisprudencia, comparación con el derecho francés y el derecho alemán".*Revista de trabajo y seguridad social. Comentarios, casos prácticos. Recursos humanos.* 2009, núm. 311, p. 151-152.

25. VIEIRA MORANTE, Francisco Javier . "Videovigilancia y privacidad, el papel de la comisión de garantías de videovigilancia".*La Ley. Revista Jurídica Española de Doctrina, Jurisprudencia y Legislación.* 2010, núm. 2, p. 1815-1818.

12.- ANEXO.

INSTRUCCIÓN 1/2007, DE 16 DE MAYO, DE LA AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID, SOBRE EL TRATAMIENTO DE DATOS PERSONALES A TRAVÉS DE SISTEMAS DE CÁMARAS O VIDEOCÁMARAS EN EL ÁMBITO DE LOS ÓRGANOS Y ADMINISTRACIONES PÚBLICAS DE LA COMUNIDAD DE MADRID.

I

Entre las diversas formas de tratamiento de datos de carácter personal, la captación y grabación de imágenes de personas físicas identificadas o identificables por medio de sistemas de cámaras o videocámaras, constituye una de las novedades más importantes experimentadas en los últimos años con importante incidencia en materia de protección de datos. La utilización de estos sistemas por parte de los Órganos y las Administraciones Públicas de la Comunidad de Madrid ha provocado frecuentes consultas, planteadas de forma creciente ante la Agencia de Protección de Datos de la Comunidad de Madrid.

El tratamiento de la imagen de las personas se ha convertido así en un elemento permanente de nuestra realidad cotidiana, expandiéndose la utilización de cámaras y videocámaras a un número cada vez mayor de Órganos de la Administración Autonómica, de los Ayuntamientos, de las Universidades Públicas, de las Corporaciones de Derecho público y de otras Instituciones de la Comunidad de Madrid, habiendo proliferado la instalación de estos dispositivos, entre otros sectores, en la educación, en la sanidad, en los transportes y las infraestructuras, y en todo tipo de centros oficiales.

A consecuencia de la existencia de cierto vacío normativo, la instalación de estos sistemas de cámaras y videocámaras se han extendido de manera indiscriminada, lo que ha generado la natural preocupación de los ciudadanos afectados. Aun reconociendo los aspectos positivos que la aplicación limitada de estas técnicas puede aportar a la sociedad, el desarrollo y creciente implantación de sistemas de cámaras y videocámaras puede ocasionar múltiples colisiones con la necesaria garantía y protección de los datos de carácter personal dispensada por la Ley Orgánica 15/1999, de 13 de diciembre.

En consecuencia, se impone la necesaria disciplina y acomodación de estos sistemas a las exigencias derivadas del derecho a la protección de los datos de carácter personal, haciendo más racional y ordenada la captación, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesión de las imágenes, que constituyen el objeto mismo del tratamiento de las imágenes de las personas físicas, realizados por los Órganos y Administraciones Públicas de la Comunidad de Madrid.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

El artículo 2.a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de Datos Personales y a la Libre Circulación de estos Datos, considera identificable a *"toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*. El Considerando 26 de la propia Directiva advierte que para determinar si una persona es identificable, hay que considerar el conjunto de medios que puedan ser razonablemente utilizados por el Responsable del tratamiento, o por cualquier otra persona, para identificar al interesado.

De acuerdo con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y por su normativa de desarrollo, las imágenes captadas o grabadas por cámaras o videocámaras deben ser consideradas datos de carácter personal, definidos en el artículo 3 a) de la citada Ley Orgánica como *"cualquier información concerniente a personas físicas identificadas o identificables"*.

El artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan algunos de los preceptos de la Ley Orgánica, considera datos de carácter personal a *"toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable"*. El artículo 1.5 del citado Real Decreto cierra el concepto, vinculando la identificación del afectado a *"cualquier elemento que permita determinar, directa o indirectamente, la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada"*.

La normativa reguladora del tratamiento de datos personales a través de sistemas de cámaras o videocámaras actualmente vigente, se encuentra contenida en la Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y su Reglamento de desarrollo y ejecución, aprobado por Real Decreto 596/1999, de 16 de abril, en la Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, en la Ley 23/1992, de 30 de julio, de Seguridad Privada, y en el Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre.

En este marco normativo, destaca con luz propia la reciente 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 (BOE de 12 de diciembre). Esta norma de la Agencia Española de Protección de Datos se aplica únicamente al tratamiento de las imágenes de personas físicas identificadas o identificables realizados con fines de vigilancia, teniendo por objeto la regulación y garantía de los derechos de las personas

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

cuyas imágenes son tratadas por medio de sistemas de cámaras y videocámaras dentro del ámbito competencial de la Agencia Española de Protección de Datos.

II

Ante la creciente preocupación expresada por los distintos Grupos Políticos en relación con los tratamientos de imágenes realizados por las Administraciones Públicas madrileñas, el Director de la Agencia de Protección de Datos de la Comunidad de Madrid en sus Comparecencias de 2005 y 2006 ante la Asamblea de Madrid se refirió a la necesidad de acometer la regulación normativa de los tratamientos de imágenes realizados por los responsables de ficheros de titularidad pública de dichas Administraciones, asumiendo el compromiso de llevar a cabo su desarrollo.

Para realizar un correcto estudio de la situación actual, la Agencia ha mantenido reuniones de trabajo con el sector del transporte público madrileño, representado por el Consorcio Regional de Transportes, y con diferentes Ayuntamientos de la Comunidad de Madrid, a las que han asistido representantes de los municipios de San Sebastián de los Reyes, Tres Cantos, Alcobendas, Alcorcón, Pozuelo de Alarcón, Ciempozuelos, Alcalá de Henares y Madrid.

A su vez, en atención a las importantes especialidades existentes en materia sanitaria, se han mantenido reuniones con diversos Centros Hospitalarios públicos de la Comunidad de Madrid, que han contado con la presencia de los responsables de seguridad del Hospital Doce de Octubre, del Hospital de Fuenlabrada y del Hospital Rodríguez Lafora, así como de representantes del Servicio Madrileño de Salud (SERMAS). Asimismo, los Centros Educativos y la propia Administración Educativa han informado a la Agencia de sus experiencias e inquietudes en el marco de una reunión específicamente programada a dicho fin, que ha contado con la presencia de los Directores y Jefes de Estudio de distintos Centros Públicos de educación primaria y secundaria de la Comunidad de Madrid.

Entre otros Órganos, Organismos, Instituciones y demás Entes públicos de la Comunidad de Madrid, también se han mantenido reuniones con la Agencia de Informática y Comunicaciones de la Comunidad de Madrid y con el Canal de Isabel II, en las que se han abordado de manera específica las especialidades que, en materia de seguridad informática y de prestación de servicios básicos a la comunidad, derivan claramente de la actividad propia de dichos organismos.

Las Universidades Públicas madrileñas también han trasladado sus experiencias a la Agencia, haciéndolo de la mano de los representantes de la Universidad Rey Juan Carlos. Asimismo, se han celebrado reuniones de trabajo con representantes de la Dirección General de Seguridad de

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

la Consejería de Justicia, con los responsables de seguridad de la Consejería de Presidencia y con representantes del Centro de Emergencias 112.

A consecuencia de las reuniones mantenidas con los diferentes sectores públicos implicados, se ha constatado que, si bien con carácter general la videovigilancia con fines de seguridad constituye el principal objetivo perseguido por los responsables de los tratamientos, existen también otras finalidades independientes o ajenas a la seguridad que demandan la correspondiente respuesta normativa. Por otro lado, se ha puesto de manifiesto que, en ocasiones, los sistemas de captación de imágenes asociados a fines distintos a la seguridad sirven para complementar los tratamientos realizados para otras finalidades específicas, tal y como ocurre en el ámbito sanitario con los tratamientos de imágenes realizados de manera accesoria en relación con la Historia Clínica de los pacientes.

Como conclusiones principales de estas reuniones se advierte que, en el ámbito de los tratamientos realizados por responsables de ficheros de titularidad pública de la Comunidad de Madrid, el cumplimiento de lo previsto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, exige la clara delimitación de las finalidades y de las diferentes formas de legitimación admisibles para el tratamiento de la imagen de las personas físicas, una regulación detallada de las exigencias derivadas de los principios de calidad y proporcionalidad en el tratamiento de dichas imágenes, y el desarrollo normativo preciso del ejercicio de los derechos a los que se refieren los artículos 15 y siguientes de dicha Ley Orgánica en relación con las personas afectadas por la utilización de los sistemas de cámaras o videocámaras.

A su vez, en el ámbito de actuación de los Responsables de los tratamientos de imágenes sometidos a la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, resulta conveniente establecer las especialidades propias del procedimiento de elaboración de las disposiciones de carácter general y de la inscripción de ficheros relativos al tratamiento de imágenes de personas físicas identificadas o identificables, y proceder al desarrollo concreto de las exigencias derivadas del deber de información previsto en el artículo 5 de la Ley Orgánica de Protección de Datos. Asimismo, la Agencia de Protección de Datos de la Comunidad de Madrid ha apreciado la necesidad de establecer directrices claras y precisas en relación con las medidas de seguridad exigibles para la realización de este tipo de tratamientos.

III

De acuerdo con lo dispuesto en el artículo 2 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, en la NORMA PRIMERA de la presente Instrucción se dispone el *"Ámbito de aplicación"* de la misma, resultando aplicable a los

tratamientos de datos personales realizados por medio de sistemas de cámaras o videocámaras, cuando dichos tratamientos se realicen por las Instituciones de la Comunidad de Madrid, por sus Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de su Administración Pública, así como por los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, y por las Universidades Públicas de la Comunidad de Madrid. Esta Instrucción también se aplica a los tratamientos de imágenes realizados por las Corporaciones de derecho público representativas de intereses económicos y profesionales de la Comunidad de Madrid, siempre y cuando dichos tratamientos se realicen para el ejercicio de potestades de derecho público.

Según dispone el artículo 2.3 e) de la Ley Orgánica de Protección de Datos, los tratamientos de datos procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, se rigen por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999, de 13 de diciembre. En consecuencia, los tratamientos de datos realizados por las Policías Locales de los municipios que integran la Comunidad de Madrid quedan sometidos a esta Instrucción en lo que no se oponga a la regulación específica contenida en la Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y en su Reglamento de desarrollo y ejecución, aprobado por Real Decreto 596/1999, de 16 de abril.

Asimismo, de manera específica, en la NORMA PRIMERA de esta Instrucción se establece el régimen aplicable al tratamiento de imágenes realizado en el ámbito de actuación y bajo la dirección de un Responsable sometido a la disciplina y control de la Agencia de Protección de Datos de la Comunidad de Madrid, cuando la instalación de los sistemas de cámaras o videocámaras se lleve a cabo en edificios, instalaciones o bienes inmuebles afectados a un uso o servicio público cuya vigilancia y protección se encuentren atribuidas legalmente a dicho Responsable en el ejercicio de sus funciones propias, de acuerdo con lo establecido por el artículo 148.1.22 de la Constitución Española y por el artículo 26.1.27 de la Ley Orgánica 3/1983, de 25 de febrero, de Estatuto de Autonomía de la Comunidad de Madrid, que atribuye a la Comunidad de Madrid la competencia exclusiva en materia de vigilancia y protección de sus edificios e instalaciones.

De acuerdo con lo previsto por el artículo 2.2 a) de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, la presente Instrucción no resulta aplicable al tratamiento de datos personales captados y/o grabados para uso o finalidad doméstica, quedando excluidos de la misma la instalación y uso de sistemas de video portero.

En cuanto a su ámbito objetivo, esta Instrucción se aplica tanto al tratamiento de la imagen de las personas físicas identificadas o identificables, como al tratamiento de cualquier otro dato de carácter personal realizado a través de sistemas de cámaras o videocámaras. En consecuencia, las referencias a la imagen de las personas físicas identificadas o identificables contenidas en la Instrucción se entienden hechas también a cualquier otro dato de carácter personal sobre el

que se realicen tratamientos a través de sistemas de cámaras o videocámaras.

A su vez, esta Instrucción resulta también aplicable en el supuesto de que las imágenes captadas no se incorporen y/o registren en un soporte físico, limitándose la captación a los fines de su reproducción o emisión en tiempo real. Dicha aplicación se extiende incluso a la obligación de declarar este tipo de ficheros por parte del Responsable del tratamiento, sin perjuicio de que para este caso se excepcione el ejercicio de los derechos de los afectados recogidos en su NORMA SÉPTIMA.

La NORMA SEGUNDA de esta Instrucción, bajo el título *"Responsable del tratamiento"*, se dirige a la definición de los diferentes actores que pueden intervenir en el tratamiento de imágenes de personas físicas identificadas o identificables realizado a través de sistemas de cámaras o videocámaras, abordando su delimitación en atención a las diferentes especialidades que surgen en el ámbito público objeto de la competencia de la Agencia de Protección de Datos de la Comunidad de Madrid.

En su apartado *"Supuestos especiales"*, la NORMA SEGUNDA regula determinados supuestos especialmente problemáticos y fronterizos, tales como los relativos al arrendamiento de edificios, instalaciones y bienes inmuebles afectados al uso o servicio público, y a la utilización conjunta de edificios, instalaciones y servicios.

A fin de hacer más fácil al Responsable del tratamiento el cumplimiento de sus obligaciones, en la NORMA TERCERA, *"Procedimiento de elaboración de la disposición de carácter general e inscripción del fichero"*, se incorporan las normas específicas relativas al procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros relativos al tratamiento de datos personales realizados mediante cámaras o videocámaras, así como las relativas al procedimiento de inscripción de creación, modificación o supresión de ficheros en el Registro de Ficheros de Datos Personales en el ámbito de los tratamientos de imágenes realizados por los Responsables sometidos a lo dispuesto en la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

El cumplimiento de las obligaciones contenidas en la NORMA TERCERA se exige al Responsable del tratamiento sin perjuicio de que en la instalación de cámaras o videocámaras se respeten el resto de los requisitos técnicos y/o jurídicos exigidos por la legislación específicamente aplicable en relación con este tipo de dispositivos, y sin menoscabo de las competencias que el ordenamiento jurídico atribuya a la Comisión Regional de Coordinación de Policías Locales y a las Juntas Locales de Seguridad en aquellos municipios donde se hayan constituido las mismas.

Como requisito esencial, en su remisión a la Agencia de Protección de Datos de la Comunidad de Madrid, el proyecto de disposición de carácter general deberá ir acompañado de un informe sobre la necesidad del tratamiento de las imágenes realizado mediante sistemas de cámaras o

videocámaras. En dicho informe el Responsable deberá justificar el tratamiento de las imágenes en la concurrencia de alguno de los supuestos que legitiman el tratamiento previstos en la propia Instrucción, razonando especialmente el cumplimiento de lo dispuesto en relación con el principio de proporcionalidad.

Especial mención merece el contenido de la NORMA CUARTA, *"Legitimación y Finalidad en el tratamiento de imágenes"*, y de la NORMA QUINTA, *"Calidad en el tratamiento de las imágenes"*, de la presente Instrucción.

Con pleno respeto a los principios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y, especialmente, con plena observancia del principio de calidad de los datos, la NORMA CUARTA establece de forma concreta los supuestos derivados de la aplicación íntegra de los artículos 6 y 11 de la propia Ley Orgánica que sirven de base a la regulación de la legitimación y la finalidad en el tratamiento de las imágenes.

Entre las diferentes formas de legitimación, destaca la posibilidad de que las imágenes se recojan para el ejercicio de las funciones propias de las Instituciones, Órganos, Organismos y demás Entes y Entidades de la Comunidad de Madrid en el ámbito de sus competencias, no sólo con fines de vigilancia para la seguridad, sino también con la finalidad de control y disciplina del tráfico, circulación de vehículos a motor y seguridad vial, al objeto de controlar el acceso de vehículos a zonas especialmente delimitadas o de estacionamiento regulado, así como para el establecimiento de sistemas de aforo del tráfico, y con la finalidad de prestación de un determinado servicio público o del cumplimiento de funciones públicas de soberanía.

También como novedad, se establecen los supuestos específicos de legitimación para el tratamiento de las imágenes derivados del mantenimiento o cumplimiento de una relación negocial, laboral o administrativa, vinculada al ámbito competencial propio de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere la Instrucción.

A su vez, en la NORMA CUARTA se establecen supuestos concretos de legitimación para el tratamiento de imágenes con fines sanitarios y asistenciales, para el diagnóstico y tratamiento a distancia de enfermedades a través de técnicas de telemedicina o con fines de monitorización de pacientes en Unidades médicas de Cuidados Intensivos.

Asimismo, entre otros supuestos concretos, se recogen los tratamientos de imágenes con fines históricos, estadísticos y científicos, así como la realización de tratamientos de imágenes con fines de investigación y/o docencia.

De otra parte, en relación con la instalación de los sistemas de cámaras o videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, en la NORMA QUINTA se establece que toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos para la

protección de los datos de carácter personal, 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 sus funciones por las Administraciones públicas, debiéndose valorar la utilización de estos sistemas en atención a su proporcionalidad en relación con el fin perseguido.

Los criterios de legitimación y proporcionalidad a la hora de valorar la captación de imágenes a través de cámaras o videocámaras, han sido considerados determinantes por la Jurisprudencia del Tribunal Constitucional, entre otras, en sus Sentencias STC 186/2000, de 10 de julio, FFJJ. 6 y 7, y STC 98/2000, de 10 de abril, FJ. 8. A su vez, con carácter general, dichos criterios han sido considerados como determinantes de cualquier medida restrictiva de derechos fundamentales en otras muchas Sentencias del Alto Tribunal (STC 66/1995, de 8 de mayo FJ. 5; SSTC 55/1996, de 28 de marzo FFJJ. 6, 7, 8 y 9; SSTC 207/1996, de 16 de diciembre FJ. 4.e; y SSTC 37/1998, de 17 de febrero FJ. 8). Así, de acuerdo con dicha Jurisprudencia, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: 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).

La proporcionalidad es un elemento fundamental en la instalación de sistemas de cámaras o videocámaras en el ámbito público, dado que son numerosos los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas. En consecuencia, el Responsable del tratamiento de las imágenes deberá valorar con cautela las implicaciones de la adopción de estos sistemas y la posibilidad de adoptar otros que, siendo igualmente idóneos, resulten menos intrusivos para la protección de los datos de las personas que deben someterse a los mismos.

En la NORMA SEXTA, *"Información"*, se recogen las especialidades derivadas del deber de informar en función de los distintos fines a los que puede responder la instalación de los sistemas de cámaras o videocámaras.

El contenido del distintivo informativo utilizado deberá incorporar una mención a la finalidad para la que se tratan los datos, una información descriptiva de los espacios comprendidos dentro de la zona en la que se instalen los sistemas de cámaras o videocámaras, una referencia a la "LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS", la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y la indicación de la

posibilidad de obtener una información más detallada solicitando la misma en un lugar expresamente señalado al efecto.

El diseño de dicho distintivo podrá ajustarse a lo previsto en el ANEXO de esta Instrucción. Asimismo, a su elección, el Responsable del tratamiento podrá utilizar cualquier otro distintivo que incorpore la información y cumpla con los requisitos establecidos en la misma. Para el supuesto de que la instalación de cámaras se realice con fines de seguridad, el Responsable podrá utilizar, también a su elección, el distintivo informativo previsto por el Apartado 1 del Anexo de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos.

Por su parte, en la NORMA SÉPTIMA, bajo el título *"Derechos de las personas",* se acomete el desarrollo de los derechos de los afectados por el tratamiento de las imágenes, cuya regulación general se contiene en los artículos 15 y siguientes de la Ley Orgánica de Protección de Datos, detallándose las especialidades del procedimiento para el ejercicio de los derechos de acceso, cancelación y oposición.

Como novedad se establece que cuando el Responsable del tratamiento disponga de servicios de información y atención al ciudadano o para el ejercicio de reclamaciones relacionadas con el servicio prestado, deberá concederse al afectado la posibilidad de ejercer sus derechos a través de dichos servicios.

El Responsable del tratamiento deberá atender la solicitud de acceso, cancelación u oposición ejercida por el interesado adoptando las medidas oportunas para garantizar, en todo caso, la debida disociación de la imagen o, en su caso, de cualquier otro dato de carácter personal de las terceras personas afectadas por los tratamientos. A dichos efectos, el Responsable del tratamiento deberá servirse de los programas y/o herramientas informáticas adecuadas que, aplicadas sobre los datos de carácter personal de las terceras personas afectadas, impidan su identificación y la cesión de su imagen a la persona que realice la solicitud.

Las previsiones contenidas en la NORMA SÉPTIMA no resultan aplicables a la mera captación de imágenes realizada por medios analógicos, incluida su reproducción o emisión en tiempo real, salvo que las imágenes así captadas se incorporen a un fichero con datos de carácter personal o estructurado conforme a criterios específicos relativos a personas físicas.

En la NORMA OCTAVA de esta Instrucción, *"Seguridad y Deber de Secreto"*, se procede a la fijación de las debidas garantías en relación con la cancelación, bloqueo o destrucción de las imágenes una vez transcurridos los plazos necesarios exigidos por la normativa aplicable en cada caso.

Con carácter general, se establece que en la instalación de sistemas de cámaras o videocámaras las medidas de seguridad adoptadas por el Responsable del tratamiento serán las calificadas de nivel básico. Sin embargo, en determinados supuestos claramente establecidos deberán implantarse, además de las medidas de seguridad de nivel básico, aquéllas otras de nivel medio o alto que resulten necesarias atendiendo a la finalidad de la información tratada. En todo caso, la transmisión de imágenes a través de redes públicas de comunicaciones se realizará mediante el cifrado de dichas imágenes, o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Asimismo, en la NORMA OCTAVA se establecen reglas específicas en relación con el documento de seguridad, con las medidas de seguridad de nivel básico relativa a control de accesos, identificación y autenticación, con las medidas de seguridad específicamente exigibles para los niveles medio y alto, y con el deber de secreto exigible a quienes intervengan en el tratamiento de las imágenes.

Finalmente, haciéndose eco de las importantes singularidades existentes en relación con los tratamientos de imágenes realizados en espacios y áreas de acceso restringido por motivos de seguridad neurálgica, la Instrucción incorpora en su DISPOSICIÓN ADICIONAL un conjunto de normas específicas que resultan especialmente aplicables a estas áreas de acceso restringido, ubicadas en centros neurálgicos de vital importancia para la población en general.

En concreto, en la DISPOSICIÓN ADICIONAL se contienen reglas especiales relativas a la cancelación de las imágenes, al régimen de acceso a las instalaciones, al deber de información, y a la utilización de los sistemas de cámaras o videocámaras como instrumento de apoyo de los sistemas de control de acceso físico.

IV

En consecuencia, en el ámbito de actuación al que se refiere el artículo 41 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en ejercicio de la competencia que le atribuye el artículo 15 d) de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, esta Agencia de Protección de Datos de la Comunidad de Madrid ha estimado la necesidad de dictar una Instrucción para adecuar los tratamientos de imágenes de personas físicas identificadas o identificables realizados en el ámbito de su competencia a los principios contenidos en dichas normas.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

En su virtud, de conformidad con lo dispuesto en el artículo 15 d) de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, dispongo:

NORMA PRIMERA.- Ámbito de aplicación.

1. Ámbito subjetivo de la norma.

1.1 La presente Instrucción se aplica a los tratamientos de datos personales a los que se refiere el apartado 2 de esta NORMA Primera, realizados por las Instituciones de la Comunidad de Madrid, por sus Órganos, Organismos, Entidades de Derecho público y demás Entes públicos integrantes de su Administración Pública, así como por los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid, y por las Universidades Públicas de la Comunidad de Madrid.

También se aplica a los tratamientos de datos personales a los que se refiere el apartado 2 de esta NORMA Primera, realizados por las Corporaciones de derecho público representativas de intereses económicos y profesionales de la Comunidad de Madrid, siempre y cuando dichos tratamientos se realicen para el ejercicio de potestades de derecho público.

1.2 Los tratamientos de datos personales a los que se refiere el apartado 2 de esta NORMA Primera, realizados por las Policías Locales de los municipios que integran la Comunidad de Madrid, quedarán sometidos a esta Instrucción en lo que no se oponga a la regulación específica contenida en la Ley Orgánica 4/1997, de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, y en su Reglamento de desarrollo y ejecución, aprobado por Real Decreto 596/1999, de 16 de abril.

La recogida y tratamiento para fines policiales de los datos de carácter personal a los que se refiere el apartado 2 de esta NORMA Primera, realizados por las Policías Locales de los municipios que integran la Comunidad de Madrid y que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, quedarán sometidos a esta Instrucción sin perjuicio de lo dispuesto en el artículo 22 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.3 Esta Instrucción también se aplicará a la realización de tratamientos de imágenes mediante cámaras o videocámaras llevados a cabo por parte de otras Fuerzas y Cuerpos de Seguridad, distintas de las Policías Locales, cuando actúen dentro del ámbito de dirección y para el desarrollo de las competencias propias de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere esta NORMA Primera.

A estos efectos, se presumirá realizado el tratamiento en el ámbito de actuación y bajo la dirección de dichas Instituciones, Órganos, Organismos y demás Entes y Entidades, cuando la finalidad, contenido y uso del tratamiento, respondan a la decisión de dichos Responsables,

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

sometidos a lo dispuesto por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, adoptada en el ejercicio de una competencia propia atribuida por el ordenamiento jurídico.

1.4 Esta Instrucción también se aplica a las empresas de seguridad privada que, de acuerdo con lo dispuesto por los artículos 5.1 d) de la Ley 23/1992, de 30 de julio, de Seguridad Privada, y por el artículo 1 del Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre, realicen tratamientos de imágenes u otros datos de carácter personal de personas físicas identificadas o identificables, a través de sistemas de cámaras o videocámaras, siempre que dichos tratamientos se lleven a cabo por cuenta de las Instituciones, Órganos, Organismos, Entes y Entidades a las que se refiere esta NORMA Primera en su calidad de Responsables del tratamiento.

1.5 La presente Instrucción resulta también aplicable a los tratamientos de imágenes realizados mediante sistemas de cámaras o videocámaras por cualquier otro tipo de empresas, entidades o personas jurídico-privadas que presten servicios de tratamiento de imágenes, siempre que dichos tratamientos se lleven a cabo por cuenta de las Instituciones, Órganos, Organismos, Entes y Entidades a las que se refiere esta NORMA Primera, y siempre que la finalidad, contenido y uso del tratamiento, correspondan al ejercicio de una competencia propia atribuida por el ordenamiento jurídico a dichas Instituciones, Órganos, Organismos, Entes y Entidades en su calidad de Responsables del tratamiento.

1.6 Especialmente, a los efectos de lo dispuesto en los apartados 1.3, 1.4 y 1.5 de esta NORMA Primera, se entenderá que el tratamiento se realiza en el ámbito de actuación y bajo la dirección de un Responsable sometido a lo dispuesto por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, cuando la instalación de los sistemas de cámaras o videocámaras se lleve a cabo en edificios, instalaciones o bienes inmuebles afectados a un uso o servicio público cuya vigilancia y protección se encuentren atribuidas legalmente a dicho Responsable en el ejercicio de sus funciones propias, de acuerdo con lo establecido por el artículo 148.1.22 de la Constitución Española y por el artículo 26.1.27 de la Ley Orgánica 3/1983, de 25 de febrero, de Estatuto de Autonomía de la Comunidad de Madrid.

1.7 De conformidad con lo dispuesto en el artículo 2.2 a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la presente Instrucción no resulta aplicable al tratamiento de datos personales captados o grabados para uso o finalidad doméstica, quedando excluidos de la misma la instalación y uso de sistemas de video portero.

1.8 Queda fuera del ámbito de aplicación de la presente Instrucción el tratamiento de imágenes realizado mediante cámaras o videocámaras con fines periodísticos, sin perjuicio, en su caso, de la tutela judicial prevista por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

1.9 La Agencia de Protección de Datos de la Comunidad de Madrid ejercerá la función de control sobre los tratamientos de datos personales realizados en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid en los términos regulados por la presente Instrucción, sin menoscabo de las competencias que el ordenamiento jurídico atribuya a la Comisión Regional de Coordinación de Policías Locales, y a las Juntas Locales de Seguridad en aquellos municipios donde se hayan constituido las mismas.

2. Ámbito objetivo y tipos de tratamiento sometidos a la norma.

2.1 Esta Instrucción se aplica al tratamiento de la imagen de las personas físicas identificadas o identificables, así como al tratamiento de cualquier otro dato de carácter personal realizado a través de sistemas de cámaras o videocámaras, por parte de las Instituciones, Órganos, Organismos, y demás Entes y Entidades mencionados en esta NORMA Primera.

2.2 Se considerará identificable una persona cuando su identidad pueda determinarse mediante la captación, grabación, transmisión, conservación o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, o a través del tratamiento que resulte de los datos personales relacionados con dichas imágenes, sin que ello requiera plazos, actividades o esfuerzos desproporcionados.

2.3 Las referencias a la imagen de las personas físicas identificadas o identificables contenidas en esta Instrucción se entenderán hechas también a cualquier otro dato de carácter personal sobre el que se realicen tratamientos a través de sistemas de cámaras o videocámaras. A dichos efectos, se estará a la definición de dato de carácter personal contenida en el artículo 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre.

2.4 El tratamiento de datos personales objeto de esta Instrucción comprende la captación, grabación, transmisión, conservación y almacenamiento de imágenes, realizados tanto a través de soportes físicos de carácter digital, como mediante soportes analógicos estructurados con arreglo a criterios personales.

2.5 La presente Instrucción resultará aplicable aún cuando las imágenes captadas no se incorporen y/o registren en un soporte físico, limitándose la captación a los fines de su reproducción o emisión en tiempo real, incluido el visionado de dichas imágenes a distancia, sin perjuicio de lo dispuesto en el Apartado 1.7 de la NORMA Séptima.

2.6 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 de datos de carácter personal previstos en la misma.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

NORMA SEGUNDA.- Responsable del tratamiento.

1.1 Norma general.

A los efectos de la presente Instrucción, se considerará Responsable del tratamiento de datos personales realizado a través de sistemas de cámaras o videocámaras, a la persona jurídica de naturaleza pública u órgano administrativo, determinado en su NORMA Primera, que decida sobre la finalidad, contenido y uso previsto en relación con la instalación de cámaras o videocámaras.

En todo caso se entenderá que concurre la condición de Responsable del tratamiento en las Instituciones, Órganos, Organismos y demás Entes y Entidades que, de acuerdo con lo dispuesto por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, ostenten la competencia administrativa a cuyo fin sirva la instalación del sistema de cámaras o videocámaras.

1.2 Encargado del tratamiento.

El Responsable del tratamiento podrá contratar los servicios de otra persona física o jurídica, pública o privada, que trate los datos personales por cuenta de dicho Responsable, en calidad de Encargado del tratamiento. En estos casos, no se considerará comunicación o cesión de datos el acceso del Encargado del tratamiento a las imágenes cuando dicho acceso sea necesario para la prestación de su servicio al Responsable del tratamiento.

La realización de tratamientos de datos mediante cámaras o videocámaras por cuenta de terceros, deberá estar regulada en un contrato que constará por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará las imágenes conforme a las instrucciones del responsable del tratamiento, y que no las aplicará o utilizará con fin distinto al que figure en dicho contrato, ni las comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, que el Encargado del tratamiento está obligado a implementar.

Una vez cumplida la prestación contractual, las imágenes deberán ser destruidas o devueltas al Responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

En el caso de que el Encargado del tratamiento destine las imágenes a otra finalidad, las comunique o las utilice incumpliendo las estipulaciones del contrato, será considerado, también,

Responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

1.3 Supuestos especiales.

1.3.1 Arrendamiento de edificios, instalaciones y bienes inmuebles afectados al uso o servicio público.

En todo caso, se considerará Responsable del tratamiento de datos personales, realizado a través de sistemas de cámaras o videocámaras, a la persona jurídica de naturaleza pública, u órgano administrativo, determinado en la NORMA Primera de esta Instrucción, que decida sobre la finalidad, contenido y uso previsto para en la instalación de cámaras o videocámaras, cuando dicho tratamiento se efectúe en edificios, instalaciones o bienes inmuebles, afectados al uso o servicio público y utilizados en exclusiva, en virtud de cualquier título jurídico válido en derecho, por dicha persona jurídico pública u Órgano administrativo, para el ejercicio de sus funciones propias dentro del ámbito de sus competencias.

1.3.2 Utilización conjunta de edificios, instalaciones y servicios.

En todo caso, se considerará Responsable del tratamiento de datos personales, realizado a través de sistemas de cámaras o videocámaras, a la persona jurídica de naturaleza pública, u órgano administrativo, determinado en la NORMA Primera de esta Instrucción, que decida sobre la finalidad, contenido y uso previsto para en la instalación de cámaras o videocámaras, cuando dicho tratamiento se efectúe en zonas, áreas o espacios claramente delimitados, de los edificios, instalaciones o bienes inmuebles, afectados parcialmente al uso o servicio público y utilizados, en virtud de cualquier título jurídico válido en derecho, por dicha persona jurídico pública u Órgano administrativo, para el ejercicio de sus funciones propias dentro del ámbito de sus competencias.

NORMA TERCERA.- Procedimiento de elaboración de la disposición de carácter general e inscripción del fichero.

1 Normas generales

1.1 La creación, notificación e inscripción de ficheros relativos al tratamiento de imágenes de personas físicas identificadas o identificables, o relativos al tratamiento de cualquier otro dato de carácter personal efectuado mediante sistemas de cámaras o videocámaras, se realizará mediante disposición de carácter general que será publicada en el Boletín Oficial de la Comunidad de Madrid o en el Diario Oficial que corresponda, de acuerdo con lo dispuesto por el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter

Personal, y por el artículo 4 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

1.2 Con carácter general, el procedimiento para la creación, notificación e inscripción de tratamientos de imágenes, realizados mediante sistemas de cámaras o videocámaras, se ajustará a lo dispuesto por el Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales.

1.3 Las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere la presente Instrucción que prevean la realización de tratamientos de la imagen de las personas físicas identificadas o identificables, o el tratamiento de cualquier otro dato de carácter personal efectuado mediante sistemas de cámaras o videocámaras, deberán notificarlo previamente a la Agencia de Protección de Datos de la Comunidad de Madrid, para su inscripción en el Registro de Ficheros de dicha Agencia, quien dará traslado de la misma al Registro General de Protección de Datos en orden a la inscripción prevista en el artículo 39 de la Ley Orgánica 15/1999, de 13 de diciembre.

1.4 El cumplimiento de las obligaciones contenidas en esta NORMA Tercera se exigirá al Responsable del tratamiento sin perjuicio de que en la instalación de cámaras o videocámaras se respeten el resto de los requisitos técnicos y/o jurídicos exigidos por la legislación específicamente aplicable en relación con este tipo de dispositivos, y sin menoscabo de las competencias que el ordenamiento jurídico atribuya a la Comisión Regional de Coordinación de Policías Locales y a las Juntas Locales de Seguridad en aquellos municipios donde se hayan constituido las mismas.

2 Normas específicas relativas al procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros relativos al tratamiento de datos personales realizados mediante cámaras o videocámaras.

2.1 Corresponde a la Mesa de la Asamblea de Madrid, de conformidad con lo previsto en los artículos 2.1 y 78.1 del Reglamento de Régimen Interior de la Asamblea de Madrid, la competencia para la creación, modificación y supresión de sus ficheros que contengan datos de carácter personal relativos a la imagen de las personas físicas identificadas o identificables, por medio de disposición de carácter general aprobada mediante Acuerdo de la Mesa.

En el ámbito de la Administración General de la Comunidad de Madrid y de conformidad con lo previsto en el artículo 4.1 de la Ley 8/2001, de 13 de julio, así como en el artículo 50.3 de la Ley 1/1983, de 13 de diciembre, de Gobierno y Administración de la Comunidad de Madrid, la aprobación de la disposición será por Orden del Consejero respectivo.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

2.2 Por lo que se refiere a los Organismos Autónomos, los Órganos de Gestión y demás Entidades de Derecho Público previstas en la Ley 1/1984, de 19 de enero, Reguladora de la Administración Institucional de la Comunidad de Madrid, así como a aquellos Entes del sector público de la Comunidad dotados de especial autonomía e independencia, y los previstos en el artículo 6 de la Ley 9/1990, de 8 de noviembre, Reguladora de la Hacienda de la Comunidad de Madrid, la competencia para la aprobación de la disposición se ajustará a lo previsto en el artículo 4.1 de la Ley 8/2001, de 13 de julio, así como en la Ley 1/1984, de 19 de enero, o en la normativa específica de creación o regulación de dichos Entes.

2.3 Corresponde a cada uno de los Entes que integran la Administración Local del ámbito territorial de la Comunidad de Madrid la competencia para la creación, modificación y supresión de sus ficheros que contengan datos de carácter personal relativos a la imagen de las personas físicas identificadas o identificables, mediante la aprobación de la correspondiente ordenanza municipal o cualquier otra disposición de carácter general, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de Bases de Régimen Local y, en su caso, en la legislación autonómica. En relación con el Ayuntamiento de Madrid se estará, además, a la regulación específica contenida en la Ley 22/2006, de 4 de julio, de Capitalidad y de Régimen Especial de Madrid.

2.4 Las Universidades Públicas, en los términos señalados en el artículo 2 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, crearán, modificarán y suprimirán sus ficheros que contengan datos de carácter personal relativos al tratamiento de la imagen de las personas físicas identificadas o identificables, realizado a través de sistemas de cámaras o videocámaras, mediante resolución del órgano competente para aprobar disposiciones de carácter general, de acuerdo con lo establecido en sus propios Estatutos.

2.5 Los Colegios Profesionales incluidos en el ámbito de aplicación de la Ley 8/2001, de 13 de julio, siempre y cuando los tratamientos de imágenes de las personas físicas identificadas o identificables se realicen para el ejercicio de potestades de derecho público, crearán, modificarán y suprimirán sus ficheros relativos a dichos tratamientos, mediante disposición de carácter general que elaborarán de conformidad con lo previsto en la Ley 19/1997, de 11 de julio, de Colegios Profesionales de la Comunidad de Madrid.

La Cámara de Comercio e Industria de la Comunidad de Madrid, siempre y cuando los tratamientos de imágenes de las personas físicas identificadas o identificables se realicen para el ejercicio de potestades de derecho público, creará, modificará y suprimirá sus ficheros relativos a dichos tratamientos, mediante Orden del Consejero de Economía e Innovación Tecnológica, de conformidad con la previsión contenida en el artículo 33.1 de la Ley 10/1999, de 16 de abril, de la Cámara de Comercio e Industria en Madrid.

La Cámara Agraria de la Comunidad de Madrid, siempre y cuando los tratamientos de imágenes de las personas físicas identificadas o identificables se realicen para el ejercicio de potestades

de derecho público, creará, modificará y suprimirá sus ficheros relativos al tratamiento de la imagen de las personas físicas identificadas o identificables mediante Orden del Consejero de Economía e Innovación Tecnológica, de conformidad con lo dispuesto en el artículo 4 de la Ley 6/1998, de 28 de mayo, de la Cámara Agraria de Madrid.

2.6 Salvo que el ordenamiento jurídico específicamente aplicable pueda establecer un procedimiento distinto, la iniciativa en la tramitación del procedimiento de elaboración de las disposiciones de carácter general de creación, modificación o supresión de ficheros referidos al tratamiento de imágenes corresponderá al órgano titular de la función específica en que se concrete la competencia sobre la materia a cuyo ejercicio sirva instrumentalmente el tratamiento.

2.7 Durante el proceso de elaboración de la disposición de carácter general se recabarán, además de los informes y dictámenes previos preceptivos, cuantos estudios y consultas se estimen convenientes para garantizar la oportunidad y legalidad del texto del proyecto.

2.8 Las disposiciones de creación o modificación de ficheros de datos de carácter personal, relativas a tratamientos de datos realizados a través de sistemas de cámaras o videocámaras, deberán indicar en todo caso:

a) El Órgano, Ente o autoridad administrativa Responsable del tratamiento de las imágenes.

b) El Órgano, Servicio o Unidad ante el que se deberán ejercitar los derechos de acceso, cancelación y oposición (este apartado se cumplimentará sólo en el caso de que sea diferente al Responsable del tratamiento).

c) El nombre y la descripción del fichero relativo al tratamiento de imágenes que se crea.

d) El carácter informatizado del tratamiento realizado.

e) El sistema de información al que pertenezca el tratamiento de imágenes, así como la descripción de los tipos de imágenes de las personas físicas identificadas o identificables o, en su caso, de cualquier otro dato de carácter personal cuyo tratamiento se realice a través del sistema de cámaras o videocámaras.

f) Las medidas de seguridad que se apliquen, con indicación del nivel básico, medio o alto exigible.

g) Los tipos de imágenes que se incluirán en el mismo.

h) La descripción detallada de la finalidad del tratamiento de imágenes y de los usos previstos para el mismo.

i) Las personas o colectivos sobre los que se pretenda obtener las imágenes o que resulten obligados a suministrarlos.

j) El procedimiento de recogida de las imágenes de las personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal, realizado mediante sistemas de cámaras o videocámaras.

k) Los órganos y entidades destinatarios de las cesiones previstas en relación con las imágenes tratadas, indicando de forma expresa las que constituyan transferencias internacionales.

2.9 En las disposiciones que se aprueben para la supresión de los ficheros se establecerá el destino de las imágenes contenidas en los mismos y no canceladas y, en su caso, las previsiones que se adopten para su destrucción.

2.10 Elaborado el proyecto de disposición de carácter general, se abrirá una fase de alegaciones, durante un plazo no inferior a quince días hábiles. Especialmente, dichas alegaciones podrán referirse a la adecuación, pertinencia y proporcionalidad de la instalación de sistemas de cámaras o videocámaras para la finalidad pretendida por el Responsable del tratamiento.

2.11 Con carácter previo a su aprobación, el proyecto de disposición de carácter general, junto con las alegaciones formuladas, se remitirá a la Agencia de Protección de Datos de la Comunidad de Madrid para informe preceptivo.

2.12 La Agencia de Protección de Datos de la Comunidad de Madrid podrá recabar del Responsable del tratamiento cuanta información estime necesaria al objeto de comprobar la adecuación del proyecto de disposición de carácter general a la normativa vigente en materia de protección de datos. A tal efecto, efectuará los requerimientos necesarios en el plazo de quince días establecido por el artículo 10.3 del Decreto 99/2002, de 13 de junio, al objeto de que el responsable realice las subsanaciones o aportaciones de información solicitadas.

2.13 La falta de información, el no aportar toda la documentación indicada, o la no realización de las subsanaciones requeridas en plazo, será motivo de emisión de informe no favorable al proyecto de disposición de carácter general relativa al tratamiento de datos de carácter personal realizado mediante sistemas de cámaras o videocámaras que se esté tramitando.

2.14 En su remisión a la Agencia de Protección de Datos de la Comunidad de Madrid, el proyecto de disposición de carácter general deberá ir acompañado de un informe sobre la necesidad y oportunidad del tratamiento de las imágenes realizado mediante sistemas de cámaras o videocámaras. De dicho informe quedará constancia en el expediente administrativo instruido al efecto por el Responsable del tratamiento con ocasión de la elaboración de su proyecto de disposición de carácter general de creación, modificación o supresión del fichero.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

En su informe el Responsable fundamentará el tratamiento de las imágenes de personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal realizado mediante sistemas de cámaras o videocámaras, en la concurrencia de alguno de los supuestos que legitiman el tratamiento de las imágenes previstos en la NORMA Cuarta de esta Instrucción.

2.15 El Responsable razonará especialmente en su informe el cumplimiento de lo dispuesto en el Apartado 2 de la NORMA Quinta de esta Instrucción en relación con la proporcionalidad del tratamiento de las imágenes, indicando expresamente que la instalación del sistema de cámaras o videocámaras supera el juicio de idoneidad, el juicio de necesidad y el juicio de proporcionalidad en sentido estricto a los que se refiere dicha NORMA Quinta.

2.16 Una vez que disponga de toda la documentación indicada, la Agencia de Protección de Datos de la Comunidad de Madrid emitirá el informe preceptivo que se le asigna como función en el artículo 15.g) de la Ley 8/2001, de 13 de julio, en el plazo máximo de quince días, notificándoselo al órgano encargado de la tramitación del proyecto de disposición de carácter general y procediendo a devolverle toda la documentación.

2.17 Posteriormente, se remitirá toda la documentación a la Secretaría General Técnica de la Consejería correspondiente, o al Órgano que resulte competente en virtud de lo dispuesto en el artículo 11 del Decreto 99/2002, de 13 de junio, para que emitan informe preceptivo de conformidad con el artículo 5.7 de la Ley 8/2001, de 13 de julio, fijándose a tal efecto un plazo máximo de quince días.

3 Normas específicas relativas al procedimiento de inscripción de creación, modificación o supresión de ficheros en el Registro de Ficheros de Datos Personales

3.1 El Responsable del tratamiento, una vez publicada en el Boletín Oficial de la Comunidad de Madrid, o en el diario oficial que corresponda, la disposición de carácter general por la que se cree, modifique o suprima el correspondiente fichero relativo al tratamiento de imágenes de personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal, realizado mediante sistemas de cámaras o videocámaras, vendrá obligado a comunicarla al Registro de Ficheros de Datos Personales, disponiendo para ello de un plazo de quince días.

3.2 Una vez concluidas todas las comprobaciones y realizadas las subsanaciones que pudieran resultar necesarias, el titular del Registro de Ficheros de Datos Personales elevará propuesta de resolución al Director de la Agencia de Protección de Datos de la Comunidad de Madrid, para que proceda a la inscripción de la creación, modificación o supresión de ficheros que contenga la disposición de carácter general publicada, dándose traslado de la misma al Registro General de Protección de Datos de la Agencia Española de Protección de Datos en orden a la inscripción prevista en el artículo 39 de la Ley Orgánica 15/1999, de 13 de diciembre.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

4 Excepciones: Tratamientos accesorios de datos mediante cámaras o videocámaras.

4.1 No será exigible la declaración e inscripción de un fichero independiente con datos de carácter personal en el Registro de Ficheros, cuando el tratamiento de datos realizado por el Responsable a través de cámaras o videocámaras se incorpore, de manera inseparable, a otro fichero con datos de carácter personal debidamente notificado e inscrito en dicho Registro, a cuyo fin general sirva de forma accesoria.

4.2 En todo caso, corresponde al Responsable del tratamiento realizado por medio de cámaras o videocámaras, cuya utilización se asocie de manera inseparable y accesoria a otro fichero con datos de carácter personal, el estricto cumplimiento de lo dispuesto por el artículo 6 del Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales.

4.3 A dichos efectos, sin perjuicio de lo dispuesto por el Decreto 99/2002, de 13 de junio, en la disposición de creación o modificación del fichero principal, a cuyo fin general sirva de forma accesoria la utilización de cámaras o videocámaras, el Responsable del tratamiento deberá señalar especialmente:

a) La descripción detallada de la finalidad y los usos previstos para el fichero principal, indicando expresamente que en relación con dicha finalidad y usos se prevé la utilización de cámaras o videocámaras.

b) Las personas o colectivos sobre los que se pretenda obtener las imágenes o que resulten obligados a suministrarlas.

c) El procedimiento de recogida de la imagen de las personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal, realizado mediante sistemas de cámaras o videocámaras.

4.4 En relación con los tratamientos de datos previamente inscritos por el Responsable, para el cumplimiento de las obligaciones previstas en esta NORMA será exigible la realización de las modificaciones necesarias, siguiendo para ello el procedimiento previsto por el artículo 7 del Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

NORMA CUARTA.- Legitimación y Finalidad en el tratamiento de imágenes.

No será preciso el consentimiento de los afectados para el tratamiento de las imágenes objeto de la presente Instrucción cuando, de acuerdo con lo dispuesto por los artículos 6 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con pleno respeto a los principios establecidos en dicha Ley Orgánica y, especialmente, con plena observancia del principio de calidad de los datos, concurra alguno de los siguientes supuestos:

3. Cuando la imagen se recoja para el ejercicio de las funciones propias de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere el Apartado 1 de la NORMA Primera de la presente Instrucción, en el ámbito de sus competencias.

En concreto se reputará legítima la utilización de sistemas de cámaras o videocámaras:

c) Con fines de vigilancia para la seguridad.
d) Con la finalidad de control y disciplina del tráfico, circulación de vehículos a motor y seguridad vial.
e) Al objeto de controlar el acceso de vehículos a zonas especialmente delimitadas o de estacionamiento regulado, así como para el establecimiento de sistemas de aforo del tráfico.
f) Con la finalidad de prestación de un determinado servicio público o del cumplimiento de funciones públicas de soberanía.

4. Cuando el tratamiento de la imagen por parte de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere la presente Instrucción, se habilite de manera expresa por una norma con rango de Ley o por una norma de derecho comunitario de aplicación directa.

5. Cuando 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, resulten necesarios para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa, vinculada al ámbito competencial propio de las Instituciones, Órganos, Organismos y demás Entes y Entidades a los que se refiere la presente Instrucción.

En concreto se reputará legítima la utilización de sistemas de cámaras o videocámaras:

a) Cuando el tratamiento de la imagen tenga por objeto el seguimiento, control y garantía del cumplimiento de la relación laboral, funcionarial o estatutaria.
b) Cuando el tratamiento de la imagen se realice en el marco de una relación jurídica derivada del sometimiento del afectado a una relación administrativa de sujeción especial.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

c) Cuando el tratamiento de la imagen se dirija a la mejora en la calidad de la gestión de los servicios públicos.
d) Cuando se realice cualquier otro tratamiento que resulte necesario para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa, vinculada al ámbito competencial del Responsable del tratamiento en el ejercicio de sus funciones.

6. Cuando el tratamiento de la imagen del afectado o, en su caso, el tratamiento de cualquier otro dato de carácter personal realizado mediante sistemas de cámaras o videocámaras por las Instituciones, Órganos, Organismos y demás Entes y Entidades a las que se refiere esta Instrucción:

a) Tenga por objeto proteger el propio interés vital del afectado o el de otra persona.
b) Resulte necesario para la prevención o para el diagnóstico médico, incluida la evaluación y diagnóstico médicos a distancia mediante la Telemedicina.
c) Tenga por objeto la prestación de asistencia sanitaria o tratamientos médicos, incluido el tratamiento a distancia a través de la Telemedicina.
d) Se realice mediante la monitorización de pacientes en Unidades médico-sanitarias y, especialmente, en Unidades de Cuidados Intensivos.
e) Tenga por objeto la gestión de los servicios sanitarios, siempre que dicho tratamiento se realice por profesionales sanitarios sujetos al secreto profesional o por otras personas sujetas a una obligación equivalente de secreto.
f) Resulte necesario para solucionar una urgencia médica o para realizar estudios epidemiológicos en los términos establecidos en la legislación estatal o autonómica sobre sanidad.

7. Cuando el tratamiento realizado a través de sistemas de cámaras o videocámaras por las Instituciones, Órganos, Organismos y demás Entes y Entidades enumeradas en la NORMA Primera de esta Instrucción, se refiera a imágenes que figuren en fuentes accesibles al público y su tratamiento resulte necesario para la satisfacción del interés legítimo perseguido por el Responsable del tratamiento o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

8. Cuando la transmisión, comunicación o cesión de la imagen realizada por las Administraciones, Órganos, Entes y Entidades a las que se refiere esta Instrucción, tenga por destinatario al Defensor del Pueblo, al Ministerio Fiscal, a los Jueces o Tribunales o al Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas, o a las Instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

9. Cuando el tratamiento de imágenes realizado a través de sistemas de cámaras o videocámaras por las Fuerzas y Cuerpos de Seguridad a los que se refiere la NORMA Primera de esta Instrucción, tenga por objeto el mantenimiento de la seguridad pública que legalmente les corresponda en relación con las siguientes competencias:

a) La protección y custodia de autoridades, edificios, instalaciones, dependencias, infraestructuras y equipamientos cuando lo tengan legalmente atribuido, así como la colaboración con las Administraciones competentes en materia de seguridad.
b) En colaboración con las Administraciones competentes, cuando lo tengan legalmente atribuido, la prevención, mantenimiento y restablecimiento de la seguridad ciudadana y tratar de garantizarla en lo referente a aquellos actos que ocasionen molestia social o daños sobre bienes y personas en la vía pública.
c) El ejercicio de las competencias que en materia de policía administrativa y policía de seguridad les atribuya la normativa estatal, así como, en su caso, la denuncia en las materias de policía administrativa especial de competencia estatal.
d) El ejercicio de las competencias que en materia de policía judicial les atribuya la normativa estatal.

10. Cuando la transmisión, comunicación o cesión de la imagen realizada por las Administraciones, Órganos, Entes y Entidades a las que se refiere esta Instrucción, tenga por destinatarios a las Fuerzas y Cuerpos de Seguridad, de acuerdo con las siguientes condiciones:

a) La comunicación se limitará a las imágenes concretas, debidamente individualizadas, solicitadas por las Fuerzas y Cuerpos de seguridad en el marco de las competencias que tengan atribuidas por la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.
b) La obtención de las imágenes por parte de la Policía deberá basarse en la prevención de un peligro real y grave para la seguridad pública o en la represión de infracciones penales y, tratándose de datos especialmente protegidos, las imágenes deberán resultar absolutamente necesarias para los fines de una investigación concreta. En todo caso la cesión quedará limitada al uso derivado de la función de mantenimiento de la seguridad pública.
c) La petición policial, debidamente motivada, se dirigirá al Responsable del tratamiento, acreditándose la existencia de una investigación policial en curso.
d) La solicitud deberá cursarse a través de un soporte documental que permita dejar constancia de la misma, resultando admisible a dichos efectos la expedición de un oficio u orden de servicio extendidos por parte de la propia Policía encargada de las actuaciones.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

e) Corresponderá a las Fuerzas y Cuerpos de Seguridad cesionarios garantizar la confidencialidad y seguridad de las imágenes cedidas en los términos previstos en esta Instrucción.

11. Cuando el tratamiento de las imágenes por las Administraciones, Órganos, Entes y Entidades a las que se refiere esta Instrucción tenga por objeto la investigación y docencia, o se realice para finalidades históricas, estadísticas o científicas.
Para la determinación de dichos fines se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, la Ley 13/1986, de 14 de abril de Fomento y Coordinación General de la Investigación Científica y Técnica, la Ley 5/1998, de 7 de mayo, de Fomento de la Investigación Científica y la Innovación Tecnológica de la Comunidad de Madrid, la Ley 16/1985, de 25 junio, del Patrimonio Histórico Español, la Ley 10/1998, de 9 de julio, de Patrimonio Histórico de la Comunidad de Madrid, la Ley 12/1989, de 9 de mayo, reguladora de la Función Estadística Pública y la Ley 12/1995, de 21 de abril, de Estadística de la Comunidad de Madrid, así como al resto de la normativa estatal y autonómica sobre estas materias.

NORMA QUINTA.- Calidad en el tratamiento de las imágenes.

1. Adecuación y pertinencia de los datos.

1.1 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, declaradas por el Responsable del tratamiento.

1.2 Las imágenes objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidas mediante los sistemas de cámaras o videocámaras.

El Responsable del tratamiento se limitará a tratar imágenes concretas de los afectados o, en su caso, a tratar otros datos de carácter personal de los mismos, evitando la recogida y tratamiento de imágenes que permitan identificar a terceros.

1.3 Los sistemas de cámaras o videocámaras emplazados en edificios, instalaciones y bienes inmuebles afectados al uso o servicio público por las Instituciones, Órganos, Organismos y demás Entes y Entidades a las que se refiere el Apartado 1 de la NORMA Primera, no podrán obtener imágenes del exterior de aquéllos salvo que resulte imprescindible para la finalidad que se pretenda. Sin perjuicio de lo anterior, las cámaras o videocámaras se instalarán de forma que no capten imágenes del exterior o, si ello resultare imposible, de manera que se minimice

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

al máximo la captación de dichas imágenes. En todo caso, deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

La instalación de cámaras y videocámaras con fines de seguridad en la vía pública corresponde en exclusiva a las Fuerzas y Cuerpos de Seguridad.

1.4 Queda prohibida la instalación de sistemas de cámaras o videocámaras en aquellos espacios, áreas y zonas, tales como aseos, baños, vestuarios y otros similares, en los que, de acuerdo con su propia naturaleza, la captación, grabación y tratamiento de imágenes resulte claramente incompatible con el respeto a la intimidad, a la dignidad personal o al libre desarrollo de la personalidad.

1.5 Cuando se pretenda utilizar las imágenes captadas con fines estadísticos o científicos, salvo que concurra el consentimiento del afectado, se evitará la identificación del mismo. En este supuesto podrán conservarse las imágenes, una vez disociadas, siguiéndose para ello el procedimiento definido en el artículo 3 f) de la Ley Orgánica 15/1999, de 13 de diciembre. A dichos efectos, el Responsable del tratamiento se servirá de los programas y/o herramientas informáticas adecuadas que, aplicadas sobre los datos de carácter personal de los afectados, impidan su identificación.

1.6 Los sistemas de captación de imágenes asociados a fines distintos de la seguridad, que sirvan para complementar los tratamientos realizados para otra finalidad principal, sólo podrán destinarse por el Responsable del tratamiento a dicha finalidad a la que sirvan de manera accesoria.

En estos supuestos el Responsable del tratamiento se limitará a tratar imágenes concretas de los afectados o, en su caso, a tratar cualquier otro dato concreto de carácter personal de los mismos, evitando la recogida y tratamiento de imágenes que permitan identificar a terceros.

2 Proporcionalidad del tratamiento de imágenes.

2.1 Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad perseguida 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.

2.2 En el informe que acompañe al proyecto de disposición de carácter general de creación, modificación o supresión de ficheros al que se refiere la NORMA Tercera de esta Instrucción, el Responsable del tratamiento justificará suficientemente que la instalación del sistema de cámaras o videocámaras resulta necesaria en consideración a los hechos y a las circunstancias concurrentes, motivando que la elección de este tipo de tratamiento de datos personales resulta la medida más adecuada, pertinente y proporcional de las que pueda adoptar.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

En dicho informe, el Responsable del tratamiento deberá hacer expresa referencia a:

a) Si el tratamiento de datos personales a través de sistemas de cámaras o videocámaras constituye una medida susceptible de conseguir el objetivo que se pretende (juicio de idoneidad).

b) Si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva, teniendo en cuenta la protección de los datos de carácter personal. A dichos efectos, el Responsable del tratamiento argumentará que dicha medida es necesaria, por no existir otra más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad). En la fundamentación para la adopción de dicha medida, el Responsable del tratamiento podrá valorar la existencia una experiencia, previamente contrastada y consolidada, que aconseje la utilización de sistemas de cámaras o videocámaras para el tratamiento de los datos de carácter personal.

c) Si la medida adoptada es proporcional, resultando equilibrada en atención a la ponderación entre la finalidad perseguida y el grado de restricción del derecho fundamental a la protección de datos de carácter personal, con expresa mención a si de dicha medida derivan más beneficios o ventajas para el interés general que perjuicios sobre la protección de los datos de carácter personal (juicio de proporcionalidad en sentido estricto).

3 Cancelación de las imágenes.

3.1 Los datos de carácter personal recogidos mediante sistemas de cámaras o videocámaras serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, y en todo caso en el plazo máximo de un mes desde su captación, sin perjuicio de las excepciones contenidas en esta NORMA.

Con carácter general, el Responsable del tratamiento procederá a la supresión y borrado de las imágenes cuando dejen de ser necesarias o pertinentes en relación con dicha finalidad, sin que la existencia del plazo máximo al que se refiere el apartado anterior en relación con la cancelación de dichas imágenes pueda servir de base para la conservación de las mismas por un periodo de tiempo mayor del estrictamente necesario.

3.2 Las imágenes captadas para finalidades distintas a la seguridad podrán conservarse hasta que hayan dejado de ser necesarias, dentro de los plazos máximos establecidos por la normativa sectorial específicamente aplicable.

En particular, se estará a lo dispuesto en la legislación estatal y autonómica sobre sanidad, reguladora de la autonomía del paciente y de sus derechos y obligaciones en materia de información y documentación clínica, en relación con la conservación de las imágenes cuyo tratamiento se encuentre asociado, de manera accesoria y/o complementaria, a los datos de salud y/o a la documentación clínica de los afectados por los tratamientos.

3.3 Cuando el tratamiento no se ajuste a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, la imagen deberá ser cancelada en el plazo de diez días desde que se tuviese conocimiento de dichas circunstancias.

Si la imagen hubiera sido comunicada previamente, el Responsable del tratamiento deberá notificar al cesionario, en el plazo de diez días, la cancelación efectuada.

Las actuaciones comprendidas en este apartado, no requerirán comunicación alguna al afectado, sin perjuicio del ejercicio de los derechos reconocidos a dicho afectado en la Ley Orgánica 15/1999, de 13 de diciembre.

3.4 No obstante, las imágenes podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica, de la ejecución de un contrato, o de la aplicación de medidas precontractuales solicitadas por el interesado, siempre que la concurrencia de dichas circunstancias quede suficientemente probada a través del correspondiente soporte documental. En estos supuestos, la conservación se referirá únicamente a las imágenes afectadas por dichas responsabilidades, debiendo extraerlas el Responsable del tratamiento de su soporte originario.

3.5 Una vez concluido el período al que se refieren los párrafos anteriores la imagen no podrá conservarse, sin perjuicio de la obligación de bloqueo prevista por el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, a disposición de las Administraciones Públicas y los Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de las correspondientes responsabilidades y/o acciones.

Asimismo, la conservación de la imagen podrá traer causa de la atención por el Responsable del ejercicio de sus derechos por el afectado por el tratamiento.

3.6 En el supuesto de conservación de las imágenes en cumplimiento de la obligación de bloqueo prevista por Ley Orgánica 15/1999, de 13 de diciembre, a disposición de las Administraciones Públicas y los Jueces y Tribunales para la atención de las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción correspondiente, el Responsable del tratamiento retendrá y bloqueará únicamente las imágenes afectadas a dichas responsabilidades, extrayéndolas de su soporte originario, sin perjuicio de la cancelación del resto de las imágenes contenidas en dicho soporte o, en su caso, de la destrucción física del mismo.

3.7 También podrán conservarse las imágenes, previa disociación de las mismas, siguiéndose para ello el procedimiento definido en el artículo 3 f) de la Ley Orgánica 15/1999, de 13 de diciembre.

3.8 En relación con la cancelación de las imágenes cuyo tratamiento se realice mediante sistemas de cámaras o videocámaras instaladas en áreas de acceso restringido, ubicadas en

centros neurálgicos de vital importancia para la población en general, se estará especialmente a lo dispuesto en la DISPOSICIÓN ADICIONAL de esta Instrucción.

NORMA SEXTA.- Información.

1. Normas generales.

1.1 El deber de información en relación con el tratamiento de la imagen del afectado o, en su caso, en relación con el tratamiento de cualquier otro dato de carácter personal del mismo realizado mediante sistemas de cámaras o videocámaras, se exigirá en todo caso al Responsable del tratamiento.

1.2 De acuerdo con lo dispuesto por el artículo 4.7 de la Ley Orgánica 15/1999, de 13 de diciembre, el Responsable del tratamiento velará por la recogida leal y lícita de las imágenes. Se prohíbe la recogida de imágenes por medios fraudulentos, desleales o ilícitos.

1.3 Lo dispuesto en esta NORMA en relación con el deber de información no resultará aplicable cuando el tratamiento de la imagen, realizado mediante sistemas de cámaras o videocámaras, se encuentre vinculado a los fines policiales recogidos en el artículo 22.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.4 En relación con la información en el tratamiento de las imágenes realizado mediante sistemas de cámaras o videocámaras instaladas en áreas de acceso restringido, ubicadas en centros neurálgicos de vital importancia para la población en general, se estará especialmente a lo dispuesto en la DISPOSICIÓN ADICIONAL de esta Instrucción.

2. Instalación de cámaras con fines de seguridad.

Los responsables que cuenten con sistemas de videovigilancia instalados con fines de seguridad deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre.

A tal fin deberán:

I) Colocar, en emplazamientos claramente visibles de las zonas videovigiladas, tantos distintivos informativos como resulten necesarios para garantizar que en todo momento los afectados conozcan la presencia de la cámara o videocámara, y el tratamiento de datos realizado.

La ubicación concreta de dichos distintivos dependerá, en cada caso, de la naturaleza y estructura de las zonas y espacios videovigilados. A dichos efectos, resultará admisible la

utilización de un único distintivo, ubicado en un espacio de acceso principal, cuando al mismo se incorpore información suficientemente descriptiva del ámbito físico y espacial al que se refiera la zona videovigilada.

Asimismo, para el supuesto de edificios divididos en plantas, será admisible la utilización de un único distintivo informativo por cada una de ellas, ubicado en un espacio de acceso principal al área o zona videovigilada en dicha planta, cuando a dicho distintivo se incorpore información suficientemente descriptiva del ámbito físico y espacial al que se refiera la zona videovigilada.

En ningún caso resultará exigible que los carteles informativos especifiquen el emplazamiento de las cámaras o videocámaras, ni que coincidan con el lugar físico destinado a la colocación de estas.

II) Tener a disposición de los/las interesados/as documentación comprensible, ofrecida en cualquier soporte inteligible, en la que se proporcione la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.

En concreto, a través de en dicha documentación, deberá informarse a los afectados de modo expreso, preciso e inequívoco:

a) De la existencia de un tratamiento de datos de carácter personal realizado por medio de cámaras o videocámaras.

b) De la finalidad de la recogida de las imágenes y de los destinatarios de dichas imágenes.

c) Del carácter obligatorio o facultativo de la captación y tratamiento de las imágenes a través de cámaras o videocámaras.

d) De las consecuencias de la obtención de las imágenes a través de las cámaras o videocámaras, y de las consecuencias de la negativa a su obtención.

e) De la posibilidad de ejercitar los derechos de acceso, cancelación y oposición.

f) De la identidad y dirección del Responsable del tratamiento o, en su caso, de su representante.

III) El contenido del distintivo informativo deberá incluir:

a) Una mención a la finalidad para la que se tratan los datos ("ZONA VIDEOVIGILADA").

b) Una información descriptiva de los espacios comprendidos dentro de la zona videovigilada.

c) Una referencia a la "LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS".

d) Una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

e) La indicación de la posibilidad de obtener una información más detallada solicitando la misma en un lugar expresamente señalado al efecto.

El diseño del distintivo informativo podrá ajustarse a lo previsto en el Anexo de esta Instrucción. Asimismo, a su elección, el Responsable del tratamiento podrá utilizar el distintivo informativo previsto por el Apartado 1 del Anexo de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, o cualquier otro que incorpore la información y cumpla con los requisitos establecidos en el párrafo anterior.

3. Instalación de cámaras por las Fuerzas y Cuerpos de Seguridad.

Las Fuerzas y Cuerpos de Seguridad a las que se refiere la NORMA Primera de esta Instrucción que realicen tratamientos de imágenes mediante cámaras o videocámaras en lugares públicos, abiertos o cerrados, 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, deberán cumplir con el deber de información de acuerdo con lo dispuesto por 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.

A tal fin, el público será informado de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable.

4. Instalación de cámaras con fines distintos de la seguridad.

Los responsables que cuenten con sistemas de cámaras o videocámaras instaladas para finalidades distintas de la seguridad deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre.

I) A tal fin, con carácter previo a la recogida de las imágenes, deberán informar a los afectados de modo expreso, preciso e inequívoco:

a) De la existencia de un tratamiento de datos de carácter personal realizado por medio de cámaras o videocámaras.

b) De la finalidad de la recogida de las imágenes y de los destinatarios de dichas imágenes.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

c) Del carácter obligatorio o facultativo de la captación y tratamiento de las imágenes a través de cámaras o videocámaras.

d) De las consecuencias de la obtención de las imágenes a través de las cámaras o videocámaras, y de las consecuencias de la negativa a su obtención.

e) De la posibilidad de ejercitar los derechos de acceso, cancelación y oposición.

f) De la identidad y dirección del Responsable del tratamiento o, en su caso, de su representante.

II) Alternativamente, el deber de información al que se refiere el punto anterior de esta NORMA podrá cumplirse, a elección del Responsable del tratamiento, mediante la colocación, en emplazamientos claramente visibles de las zonas, áreas o espacios en los que se instalen los sistemas de cámaras o videocámaras, de tantos distintivos informativos como resulten necesarios para garantizar que en todo momento los afectados conozcan la presencia de dichos sistemas y el tratamiento de imágenes realizado.

En el supuesto de que el Responsable del tratamiento optase por este sistema, el contenido del distintivo informativo deberá incluir:

a) Una mención a la finalidad para la que se tratan los datos (del tipo "Captura de imágenes con fines de ……").

b) Una información descriptiva de los espacios comprendidos dentro de la zona en la que se instalen los sistemas de cámaras o videocámaras.

c) Una referencia a la "LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS".

d) Una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

e) La indicación de la posibilidad de obtener una información más detallada solicitando la misma en un lugar expresamente señalado al efecto.

El diseño del distintivo informativo podrá ajustarse a lo previsto en el Anexo de esta Instrucción. Asimismo, a su elección, el Responsable del tratamiento podrá utilizar cualquier otro distintivo que incorpore la información y cumpla con los requisitos establecidos en el párrafo anterior.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

NORMA SÉPTIMA.- Derechos de las personas.

1. Normas generales.

1.1 En tanto no proceda su cancelación, las imágenes serán tratadas de forma que permitan el ejercicio por parte de los afectados de los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Las referencias a la imagen de las personas físicas identificadas o identificables contenidas en esta NORMA, se entenderán hechas también a cualquier otro dato de carácter personal sobre el que se realicen tratamientos a través de sistemas de cámaras o videocámaras. A dichos efectos, se estará a la definición de dato de carácter personal contenida en el artículo 3 a) de la Ley Orgánica 15/1999, de 13 de diciembre.

1.2 Los derechos de acceso, cancelación y oposición son personalísimos y serán ejercidos por el afectado. Cuando dicho afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrá hacerlo en su nombre su representante legal, siendo necesario que acredite tal condición. Asimismo, estos derechos podrán ejercitarse a través de representante voluntario expresamente designado al efecto.

Los derechos de acceso, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

1.3 Sin perjuicio de lo dispuesto en la presente Instrucción, el ejercicio por parte de los afectados de los derechos a los que se refieren esta NORMA se llevará a cabo de conformidad con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, y por su normativa de desarrollo, y sin más limitaciones que las previstas por dicha normativa.

En relación con las imágenes objeto de tratamiento, deberá concederse al interesado un medio sencillo para el ejercicio de los derechos de acceso, cancelación y oposición. El ejercicio por el afectado de sus derechos en relación con las imágenes no podrá suponer un ingreso adicional para el Responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en la presente Instrucción, los supuestos en que el Responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional o cualesquiera otros medios que impliquen un coste adicional para el interesado.

Cuando el Responsable del tratamiento disponga de servicios de información y atención al ciudadano o para el ejercicio de reclamaciones relacionadas con el servicio prestado, deberá

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

concederse al afectado la posibilidad de ejercer sus derechos de acceso, cancelación y oposición a través de dichos servicios.

1.4 El Responsable del tratamiento deberá atender la solicitud de acceso, cancelación u oposición ejercida por el interesado adoptando las medidas oportunas para garantizar, en todo caso, la debida disociación de la imagen o, en su caso, de cualquier otro dato de carácter personal de las terceras personas afectadas por los tratamientos. A dichos efectos, el Responsable del tratamiento se servirá de los programas y/o herramientas informáticas adecuadas que, aplicadas sobre los datos de carácter personal de las terceras personas afectadas, impidan su identificación y la cesión de su imagen a la persona que realice la solicitud.

1.5 En todo caso, el Responsable del tratamiento resolverá sobre la solicitud del afectado aún cuando, en cumplimiento de lo dispuesto en el Apartado 3 de la NORMA Quinta de esta Instrucción, hubiera procedido a la cancelación de los datos por haber dejado de ser necesarios o pertinentes para la finalidad perseguida.

1.6 Para el ejercicio de los derechos reconocidos por la Ley Orgánica 15/1999, de 13 de diciembre, el afectado deberá remitir al Responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada, indicando el lugar, fecha y hora aproximada en los que su imagen fue captada por el sistema de cámaras o videocámaras del Responsable del tratamiento. A dichos efectos, se entenderá por hora aproximada la referida a una franja horaria inferior a sesenta minutos.

1.7 Lo previsto en esta NORMA Séptima no resultará aplicable a la mera captación de imágenes realizada por medios analógicos, incluida su reproducción o emisión en tiempo real, salvo que las imágenes así captadas se incorporen a un fichero con datos de carácter personal o estructurado conforme a criterios específicos relativos a personas físicas.

Tampoco resultará aplicable cuando el tratamiento de la imagen, realizado mediante sistemas de cámaras o videocámaras, se encuentre vinculado a los fines policiales recogidos en el artículo 22.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.8 Cuando el Responsable del tratamiento tuviera fundadas dudas en relación con la coincidencia existente entre las imágenes tratadas y la correspondiente a la persona que ejercite sus derechos, deberá denegar la solicitud del interesado, fundamentando su resolución motivada en la carencia de la certidumbre necesaria exigida por la presente NORMA.

En el supuesto de que el sistema de cámaras o videocámaras disponga de herramientas u otros productos de software adecuados para el reconocimiento de imágenes, el Responsable del tratamiento podrá denegar la solicitud del interesado si el porcentaje de coincidencia entre la

imagen aportada en su solicitud y la imagen objeto de tratamiento no permite asegurar que esta última corresponda al interesado.

1.9 El interesado al que se deniegue total o parcialmente el ejercicio de los derechos señalados en esta NORMA, podrá reclamar su tutela ante el Director de la Agencia de Protección de Datos de la Comunidad de Madrid.

1.10 Para el ejercicio de los derechos de acceso, cancelación y oposición en relación con las imágenes cuyo tratamiento se realice mediante sistemas de cámaras o videocámaras instaladas en áreas de acceso restringido, ubicadas en centros neurálgicos de vital importancia para la población en general, se estará especialmente a lo dispuesto en la DISPOSICIÓN ADICIONAL de esta Instrucción.

2. Derecho de Acceso.

2.1 El afectado tendrá derecho a obtener información concreta sobre si su imagen, recogida a través de sistemas de cámaras o videocámaras, está siendo tratada por parte del Responsable, sobre el origen de dicha imagen, y sobre las cesiones y comunicaciones realizadas o previstas en relación con la misma.

2.2 El Responsable del tratamiento resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de dicha solicitud. El Responsable deberá responder a la solicitud del afectado en todo caso, aún cuando no disponga de la imagen del mismo, debiéndole comunicar dicha circunstancia en idéntico plazo.

Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la presentación de la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre, y en el artículo 3 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.

2.3 Si la resolución del Responsable fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla.

La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se ofrecerá en forma inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Dicha información comprenderá al menos una copia de la imagen del afectado que haya servido de base para el tratamiento, los datos de dicho afectado resultantes de cualquier elaboración o proceso informático realizado a través de su imagen, la información disponible sobre el origen de la imagen, el día y hora en que se realizó la captura de la misma, los cesionarios de la

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

imagen y la especificación de los concretos usos y finalidades para los que se almacenó.

2.4 Con carácter general, el Responsable del tratamiento podrá facilitar el derecho de acceso mediante comunicación realizada por escrito, por correo electrónico o por otros sistemas de comunicación electrónica, en la que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen la información y los datos que han sido objeto de tratamiento, de acuerdo con lo dispuesto en el apartado 2.3 de esta NORMA Séptima, acompañando a dicho escrito una copia de la imagen del afectado.

Asimismo, dicha información y datos podrán obtenerse de forma verbal, incluyendo en todo caso la visualización en pantalla de la imagen en relación con la cual se ejercita el derecho de acceso, o por cualquier otro procedimiento que sea adecuado a la configuración e implantación material del tratamiento de la imagen realizado a través de cámaras o videocámaras.

2.5 El Responsable del tratamiento podrá denegar el acceso a la imagen del afectado cuando exista una norma con rango de Ley o una norma de derecho comunitario de aplicación directa que impida conceder dicho acceso a la imagen a la que se refiera la solicitud.

Asimismo, cuando el sistema de cámaras o videocámaras disponga de herramientas u otros productos de software adecuados para el reconocimiento de imágenes, podrá denegarse el derecho de acceso a la imagen del afectado cuando el porcentaje de coincidencia entre la imagen aportada en su solicitud y la imagen objeto de tratamiento no permita asegurar que esta última corresponda al interesado. En este supuesto deberá ofrecerse al afectado la información relativa al porcentaje de coincidencia que el sistema de reconocimiento haya facilitado en el procedimiento de búsqueda.

Podrá también denegarse el derecho de acceso a la imagen del afectado cuando dicho derecho se haya ejercitado con anterioridad, dentro de los doce meses anteriores a la solicitud, salvo que el afectado acredite un interés legítimo al efecto.

En todo caso, el Responsable del tratamiento deberá justificar su denegación con expresión del precepto legal en que se ampare, informando al interesado de los motivos de la misma y de su derecho a recabar la tutela de la Agencia de Protección de Datos de la Comunidad de Madrid, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre, y en el artículo 3 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

3. Derecho de Cancelación.

3.1 En todo caso, los afectados por el tratamiento de su imagen realizado a través de sistemas de cámaras o videocámaras, podrán ejercitar el derecho de cancelación ante el Responsable, cuando dicho tratamiento no se ajuste a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

3.2 Si el acceso a la imagen por parte del afectado revelare que los datos son inadecuados o excesivos, podrá este solicitar del Responsable del tratamiento la cancelación de dichos datos, teniendo el Responsable la obligación de hacer efectivo el derecho de cancelación.

3.3 En su caso, el Responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de cancelación del interesado en el plazo de diez días.

El Responsable deberá responder a la solicitud del afectado, en todo caso, aún cuando no disponga de la imagen del mismo, debiéndole comunicar dicha circunstancia en idéntico plazo.

Transcurrido el plazo sin que de forma expresa se responda a la petición de cancelación, ésta podrá entenderse desestimada a los efectos de la presentación de la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre, y en el artículo 3 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.

3.4 Si la imagen cancelada hubiera sido cedida previamente, el Responsable del tratamiento deberá notificar la cancelación efectuada a quien se haya comunicado, debiendo este último proceder también a la cancelación en el caso de que mantenga el tratamiento de la imagen.

3.5 El Responsable del tratamiento podrá denegar la cancelación de la imagen del afectado cuando exista una norma con rango de Ley o norma de derecho comunitario de aplicación directa que impida a dicho Responsable cancelar la imagen a la que se refiera la solicitud.

Asimismo, cuando el sistema de cámaras o videocámaras disponga de herramientas u otros productos de software adecuados para el reconocimiento de imágenes, podrá denegarse la cancelación de la misma cuando el porcentaje de coincidencia entre la imagen aportada en su solicitud y la imagen objeto de tratamiento no permita asegurar que esta última corresponda al interesado. En este supuesto deberá ofrecerse al afectado la información relativa al porcentaje de coincidencia que el sistema de reconocimiento haya facilitado en el procedimiento de búsqueda.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

Podrá también denegarse la cancelación de la imagen del afectado en el supuesto en que dicha pretensión resulte de materialmente imposible. En este supuesto bastará la mención motivada a dicha circunstancia.

En todo caso, el Responsable del tratamiento deberá justificar su denegación con expresión del precepto legal en que se ampare, informando al interesado de los motivos de la misma y de su derecho a recabar la tutela de la Agencia de Protección de Datos de la Comunidad de Madrid, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre, y en el artículo 3 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.

4. Derecho de Oposición.

4.1 En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de su imagen, y siempre que una Ley o una norma de derecho comunitario de aplicación directa 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 excluirá del tratamiento la imagen del afectado.

4.2 En su caso, el Responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de oposición del interesado en el plazo de diez días.

El Responsable deberá responder a la solicitud del afectado en todo caso, aún cuando no disponga de la imagen del mismo, debiéndole comunicar dicha circunstancia en idéntico plazo.

Transcurrido el plazo sin que de forma expresa se responda a la petición de oposición, ésta podrá entenderse desestimada a los efectos de la presentación de la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre, y en el artículo 3 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.

4.3 El Responsable del tratamiento podrá denegar el derecho de oposición cuando exista una norma con rango de Ley o norma de derecho comunitario de aplicación directa que impida a dicho Responsable excluir del tratamiento a la imagen a la que se refiera la solicitud.

Asimismo, podrá denegarse la oposición al tratamiento de la imagen del afectado en el supuesto en que dicha pretensión resulte materialmente imposible. En este supuesto bastará la mención motivada a dicha circunstancia.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

En todo caso, el Responsable del tratamiento deberá justificar su denegación con expresión del precepto legal en que se ampare, informando al interesado de los motivos de la misma y de su derecho a recabar la tutela de la Agencia de Protección de Datos de la Comunidad de Madrid, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre, y en el artículo 3 del Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.

NORMA OCTAVA.- Seguridad y Deber de Secreto.

1. Normas sobre nivel de seguridad exigible.

1.1 El Responsable del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de las imágenes de las personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal, captados mediante sistemas de cámaras o videocámaras, y eviten su alteración, pérdida, y tratamiento o acceso no autorizado.

1.2 En la instalación de sistemas de cámaras o videocámaras con fines de seguridad, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo relativa a seguridad en el tratamiento de datos de carácter personal.

1.3 En relación con la instalación de sistemas de cámaras o videocámaras, el Responsable del tratamiento deberá adoptar en todo caso las medidas de seguridad calificadas de nivel básico por la normativa de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, relativa a seguridad en el tratamiento de datos de carácter personal.

1.4 Además de las medidas de seguridad de nivel básico, el Responsable del tratamiento deberá implantar las medidas de nivel medio en los siguientes tratamientos de imágenes realizados mediante sistemas de cámaras o videocámaras:

a) Los relativos a la comisión de infracciones penales o administrativas.
b) Los que requieran el tratamiento de un conjunto de imágenes que ofrezcan una definición de las características o de la personalidad de los afectados y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
c) Los que, de manera directa y específica, se dirijan a la captación y tratamiento de imágenes de personas menores de edad.

1.5 Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes tratamientos de imágenes realizados mediante sistemas de cámaras o videocámaras:

a) Los que, de manera directa y específica, se dirijan a la captación y tratamiento de

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

imágenes relacionadas con la salud, la vida sexual y el origen racial de las personas, así como las relacionadas con la ideología, la afiliación sindical, la religión o las creencias.
b) Los que, de manera directa y específica, se dirijan a la captación y tratamiento de imágenes recabadas para fines policiales.
c) Aquellos que, de manera directa y específica, se dirijan a la captación y tratamiento de imágenes relacionadas o derivadas de actos de violencia de género.
d) Aquellos que, de manera directa y específica, se dirijan a la captación y tratamiento de imágenes en centros de reeducación y reinserción de menores.

1.6 La realización de tratamientos de las imágenes fuera de los locales de la ubicación del Responsable principal deberá ser autorizada expresamente por dicho Responsable del tratamiento y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de tratamiento realizado.

1.7 Sobre los ficheros temporales deberá implantarse el nivel de seguridad que les corresponda con arreglo a los criterios establecidos en la presente NORMA. Todo fichero temporal al que se incorpore la imagen de una persona física identificada o identificable, o cualquier otro dato de carácter personal captado a través de sistemas de cámaras o videocámaras, será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

1.8 En relación con las medidas de seguridad a adoptar en el tratamiento de imágenes realizado mediante sistemas de cámaras o videocámaras instaladas en áreas de acceso restringido, ubicadas en centros neurálgicos de vital importancia para la población en general, se estará especialmente a lo dispuesto en la DISPOSICIÓN ADICIONAL de esta Instrucción.

1.9 Sin perjuicio de lo establecido en esta NORMA Octava, la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos técnicos y jurídicos exigidos por la legislación sectorial específicamente aplicable sobre esta materia.

2. Cifrado de imágenes.

2.1 Las medidas de seguridad exigibles a los accesos a las imágenes objeto de tratamiento a través de redes públicas de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

La transmisión de imágenes a través de redes públicas de comunicaciones electrónicas se realizará mediante el cifrado de las mismas, o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

2.2 Deberá evitarse el tratamiento de imágenes en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el

documento de seguridad y se adoptarán las medidas necesarias que eviten los riesgos de realizar el tratamiento en entornos desprotegidos.

2.3 La identificación de los soportes que contengan datos de carácter personal considerados especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

3. Normas específicas relativas al documento de seguridad.

3.1 El Responsable del tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes con la normativa de seguridad vigente. Dicho documento será de obligado cumplimiento para el personal con acceso a los sistemas de cámaras o videocámaras y su contenido deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

3.2 El documento de seguridad podrá ser único y comprensivo de todos los tratamientos de imágenes, o bien individualizado para cada tratamiento realizado por el Responsable. También podrán elaborarse distintos documentos de seguridad agrupando tratamientos según el sistema de cámaras o videocámaras utilizado, o bien atendiendo a criterios organizativos del propio Responsable.

3.3 Sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo, el documento de seguridad deberá contener además una referencia específica a los siguientes aspectos:

a) Ámbito de aplicación del documento, con especificación detallada de los sistemas de cámaras o videocámaras mediante los que se realicen los tratamientos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en cada caso por esta Instrucción.
c) Descripción de los sistemas de cámaras o videocámaras utilizados para la realización del tratamiento de imágenes.
d) Procedimiento de notificación, gestión y respuesta ante las incidencias que surjan durante el tratamiento de las imágenes.
e) Procedimientos de realización de copias de respaldo y de recuperación de los tratamientos de imágenes realizados.
f) Medidas que sea necesario adoptar para el transporte de soportes en los que se contengan las imágenes, así como para la destrucción de dichos soportes, o en su caso, la reutilización de estos últimos.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

g) Funciones y obligaciones del personal en relación con el tratamiento de las imágenes de personas físicas identificadas o identificables, o de cualquier otro dato de carácter personal realizado mediante sistemas de cámaras o videocámaras.
A dichos efectos, en el documento de seguridad se señalará de manera concreta:
1) La identificación de las personas y el número de las mismas que podrán acceder a las imágenes captadas mediante su visualización en tiempo real, incluido el visionado de imágenes a distancia, con indicación de la categoría o función profesional desempeñada por dichas personas. El detalle de la identificación requerida podrá establecerse de forma nominativa o por perfiles profesionales.
2) La identificación de las personas y el número de las que podrán acceder al contenido de las imágenes grabadas, una vez realizada la captación de las mismas y durante el periodo de su conservación, con indicación de la categoría o función profesional desempeñada por dichas personas. El detalle de la identificación requerida podrá establecerse de forma nominativa o por perfiles profesionales.
3) La identificación de la persona o personas que queden facultadas para realizar, en su caso, las labores necesarias relativas a la cancelación, supresión, borrado, destrucción, conservación, retención, bloqueo, extracción y/o expurgo de las imágenes en los supuestos previstos por esta Instrucción. El detalle de la identificación requerida podrá establecerse de forma nominativa o por perfiles profesionales. El número de personas autorizadas para llevar a cabo estas tareas se limitará al mínimo imprescindible.
4) Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los sistemas de cámaras o videocámaras quedarán claramente definidas y documentadas en el documento de seguridad. También se definirán las funciones de control o autorizaciones delegadas por el Responsable del tratamiento.
5) El Responsable del tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias y responsabilidades en que pudiera incurrir en caso de incumplimiento.

3.4 Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los tratamientos que se realicen en concepto de encargo, con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del Responsable y del período de vigencia del encargo. En aquellos casos en que las imágenes objeto de tratamiento se incorporen y traten de modo

exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad.

3.5 El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los tratamientos realizados mediante cámaras o videocámaras o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

4. Medidas de seguridad de nivel básico relativas a control de accesos, identificación y autenticación.

4.1 Los usuarios de los sistemas de cámaras o videocámaras tendrán acceso únicamente a aquellas imágenes que precisen para el desarrollo de sus funciones.

4.2 El Responsable del tratamiento se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos, estableciendo los mecanismos necesarios para evitar que un usuario pueda acceder a imágenes con derechos distintos de los autorizados.

4.3 Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los sistemas de cámaras o videocámaras y sobre las imágenes objeto de tratamiento, conforme a los criterios establecidos por el Responsable del tratamiento.

4.4 El Responsable del tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

5. Medidas de seguridad específicas para los niveles medio o alto.

5.1 En caso de que resultaran de aplicación al tratamiento de imágenes realizado mediante sistemas de cámaras o videocámaras las medidas de seguridad de nivel medio o alto, previstas en la Ley Orgánica 15/1999, de 13 de diciembre, en su normativa de desarrollo y en la presente Instrucción, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.
b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5.2 Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos y lógicos que den soporte a los sistemas de cámaras o videocámaras con los que se realicen los tratamientos de las imágenes.

6. Medidas de seguridad específicas de nivel alto.

6.1 De cada acceso a las imágenes grabadas por los sistemas de cámaras o videocámaras se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, la imagen o imágenes accedidas, el tipo de acceso y si ha sido autorizado o denegado. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

6.2 Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y de los problemas detectados.

6.3 La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte. Asimismo, se cifrarán las imágenes que se contengan en dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del Responsable del tratamiento.

7. Normas sobre deber de secreto.

7.1 Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las imágenes objeto de tratamiento deberá observar la debida reserva en relación con las mismas. Esta obligación subsistirá aún después de que finalice la vinculación de las personas que intervengan en el tratamiento con el Responsable del mismo.

7.2 El Responsable deberá informar a las personas con acceso a las imágenes tratadas del deber de secreto al que se refiere el apartado anterior.

7.3 El deber de secreto será exigible en todo caso, con independencia de que el acceso a las imágenes captadas mediante sistemas de cámaras o videocámaras, se produzca mediante la simple visualización realizada en tiempo real, o sobre el contenido de las imágenes una vez grabadas y almacenadas.

7.4 La vulneración del deber de guardar secreto sobre las imágenes tratadas dará lugar, en su caso, a la exigencia de las responsabilidades administrativas o penales legalmente previstas.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

DISPOSICIÓN ADICIONAL.- Normas específicas en relación con la videovigilancia de espacios y áreas de acceso restringido por motivos de seguridad neurálgica: Centros, espacios y áreas vitales para la comunidad.

Especialmente, en relación con las áreas de acceso restringido, ubicadas en centros neurálgicos de vital importancia para la población en general, se aplicarán las siguientes normas específicas:

a) Cancelación de las imágenes: En la cancelación de imágenes cuyo tratamiento se realice en espacios y áreas de acceso restringido por motivos de seguridad neurálgica, el Responsable del tratamiento atenderá al cumplimiento de los plazos que, en su caso, establezca la normativa sectorial específicamente aplicable.

b) Régimen de acceso a las instalaciones: El personal autorizado para el acceso a las dependencias en donde se realicen los tratamientos de imágenes a través de cámaras o videocámaras quedará taxativa y específicamente definido en el documento de seguridad.

c) Información: Adicionalmente a la instalación de carteles informativos, el Responsable del tratamiento establecerá protocolos de información, a través de los cuales se informe sobre el tratamiento de imágenes con carácter general y sobre las condiciones específicas que concurran en las zonas de acceso restringido.

Dicha información adicional se ofrecerá en todo caso a los empleados del Centro en el momento de incorporarse a su destino y periódicamente con carácter trimestral. Asimismo, dicha información adicional se ofrecerá por el Responsable del tratamiento a todas aquellas personas vinculadas al mismo y que, en cumplimiento de cualquier tipo de relación negocial, laboral o administrativa, pudieren acceder a las referidas zonas.

En todo caso la información adicional incluirá una referencia sobre la imposibilidad de ejercitar el derecho de oposición en relación con el tratamiento de las imágenes.

d) Utilización de sistemas de cámaras o videocámaras como apoyo de los sistemas de control de acceso físico: Mediante los sistemas de cámaras o videocámaras el Responsable del tratamiento podrá supervisar adicionalmente, a través de la captación de imágenes, la identidad de las personas que accedan a los espacios o áreas restringidas utilizando cualquier otro tipo de sistema o dispositivo de control de acceso físico.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es

DISPOSICIÓN TRANSITORIA PRIMERA.- Tratamientos inscritos.

Los Responsables de los tratamientos realizados mediante sistemas de cámaras o videocámaras ya inscritos en el Registro de Ficheros de la Agencia de Protección de Datos de la Comunidad de Madrid deberán adaptarse a lo dispuesto en la presente Instrucción en el plazo de seis meses a contar desde su entrada en vigor.

DISPOSICIÓN TRANSITORIA SEGUNDA.- Información.

Lo dispuesto en la NORMA Sexta de esta Instrucción en relación con el deber de Información, resultará exigible en el plazo de tres meses a contar desde la entrada en vigor de esta Instrucción.

DISPOSICIÓN TRANSITORIA TERCERA.- Medidas de seguridad.

Las previsiones contenidas en la NORMA Octava de esta Instrucción en relación con la implantación de las medidas de seguridad de nivel medio y alto resultarán exigibles para el Responsable del tratamiento en el plazo de seis meses a contar desde la entrada en vigor de esta Instrucción.

DISPOSICIÓN FINAL.- Entrada en vigor.

La presente Instrucción entrará en vigor el día siguiente al de su publicación en el Boletín Oficial de la Comunidad de Madrid.

ANEXO

El contenido del distintivo informativo al que se refiere la NORMA Sexta en sus Apartados 2 III y 4 II se ajustará a lo dispuesto en la misma. El Responsable del tratamiento podrá utilizar el modelo que se encuentra disponible en la página Web de la Agencia de Protección de Datos de la Comunidad de Madrid, www.apdcm.es, de donde podrá ser descargado, especificando los datos del responsable.

Cardenal Marcelo Spínola, 14, 3ª planta
28016 Madrid
Tfno: 91 580 28 74 / 75
Fax: 91 580 28 76
apdcm@madrid.org
www.apdcm.es