

AGENCIA CATALANA DE PROTECCIÓN DE DATOS

INSTRUCCIÓN

1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.

La proliferación de dispositivos de videovigilancia en diferentes ámbitos, no sólo con fines de seguridad, pública o privada, sino también con otras finalidades como la regulación y control del tráfico, el control en el ámbito laboral o el control del normal funcionamiento de determinados servicios públicos, junto con la evolución de los medios técnicos de captación, con posibilidades de identificación, manipulación o difusión de gran alcance y con costes económicos cada vez menores, ha dado lugar a la adopción de diferentes iniciativas a nivel internacional. Son ejemplos el Dictamen 4/2004, de 11 de febrero, del Grupo de trabajo previsto en el artículo 29 de la Directiva 95/46/CE, relativo al tratamiento de datos personales mediante vigilancia por videocámara; la Conferencia internacional de autoridades de protección de datos del año 2006 en Londres; o las opiniones adoptadas en fecha 17 de marzo y 2 de junio de 2007 por la Comisión de Venecia, en el seno del Consejo de Europa, sobre videovigilancia en espacios públicos y videovigilancia en espacios privados, que han puesto de manifiesto la necesidad de adecuar la utilización de estos medios de vigilancia a las exigencias derivadas de la privacidad.

De acuerdo con la definición de dato de carácter personal del artículo 3.a) de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD), la imagen o la voz constituyen datos de carácter personal y, por lo tanto, les son de plena aplicación las previsiones de esta Ley orgánica. Ahora bien, la ausencia de previsiones específicas en la normativa de protección de datos con respecto a la captación y al tratamiento de las imágenes, y en su caso de las voces, hace necesaria la concreción en este ámbito de los principios y garantías que establece la LOPD mediante un instrumento que, como la presente Instrucción, aclare el marco jurídico aplicable, en el ámbito de actuación de la Agencia Catalana de Protección de Datos, para aportar seguridad jurídica en esta materia y una mayor concreción de aquellas cuestiones que así lo requieren.

Es preciso hacer referencia a la regulación de los tratamientos de videovigilancia realizada por las fuerzas y cuerpos de seguridad con el fin de contribuir a la convivencia ciudadana, la lucha contra la violencia, la utilización pacífica de las vías y espacios públicos, como también para la prevención de delitos, faltas e infracciones relacionadas con la seguridad pública. 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 ciudadana en lugares públicos, se desarrolló en Cataluña por el Decreto 134/1999, de 18 de mayo, de regulación de la videovigilancia por parte de la policía de la Generalidad y de las policías locales de Cataluña, y por la Orden de 29 de junio de 2001, de regulación de los medios por los que se informa de la existencia de videocámaras fijas instaladas por la policía de la Generalidad y las policías locales de Cataluña en lugares públicos. Con respecto a este ámbito y en virtud de la remisión que hace el artículo 2.2 de esta Ley orgánica, la normativa de protección de datos, y en consecuencia también la presente Instrucción, es sólo de aplicación a aquellas cuestiones que no se regulen específicamente en esa normativa, como el deber de crear el fichero correspondiente y notificarlo al Registro de protección de datos de Cataluña en aquellos supuestos en que no estén sometidos a inscripción en el Registro previsto en aquella normativa específica, la aplicación de las medidas de seguridad o el ejercicio de los derechos de rectificación y oposición.

El tratamiento de imágenes para el control, la regulación, la vigilancia y la disciplina del tráfico que, en virtud de la disposición adicional octava de la Ley orgánica 4/1997, se somete expresamente a la legislación de protección de datos y de protección del derecho al honor, la intimidad y la propia imagen, en el marco de la referida Ley orgánica, merece una mención aparte.

El tratamiento de la imagen y de la voz de las personas físicas con finalidades de vigilancia puede suponer una injerencia en determinados derechos fundamentales

de las personas, regulados en el Título I de la Constitución, fundamentalmente los derechos al honor, a la intimidad y a la propia imagen y el derecho a la protección de datos de carácter personal, pero también otros derechos como la libertad de circulación, el derecho a la no discriminación y, en definitiva, la misma dignidad humana (SSTEDH de 28 de enero de 2003 y de 4 de marzo de 2008). Si bien resulta necesario admitir la posibilidad de recurrir a la videovigilancia cuando concurra alguno de los supuestos legalmente previstos (artículo 6.2 LOPD), entonces adquiere una especial importancia el principio de calidad de los datos y, en concreto, el principio de proporcionalidad. A tenor de este último principio, una medida intrusiva como la que estamos analizando sólo se puede considerar constitucionalmente legítima si resulta proporcionada a través de un triple análisis de la necesidad de la medida, su idoneidad y su carácter proporcional en sentido estricto. Es decir, cuando no se pueda alcanzar la misma finalidad mediante medidas menos intrusivas o que comporten menos riesgos para las personas (STEDH de 28 de enero de 2003, las SSTC 37/1998, 98/2000, o 186/2000, entre muchas otras).

Conscientes de la dificultad con que se encuentran las personas responsables de ficheros o tratamientos de datos a la hora de ponderar los beneficios, los riesgos y las afecciones que, para los diferentes derechos en juego, puede producir la videovigilancia, la presente Instrucción pretende dar más elementos de juicio o de valoración a los responsables, a la hora de tomar la decisión sobre la implantación de estos sistemas.

Precisamente con este objetivo se debe destacar la previsión que hace la presente Instrucción de elaborar una memoria con carácter previo a la aprobación del fichero, como herramienta para realizar un análisis completo y sistemático de las características del tratamiento que se quiere llevar a cabo y de las circunstancias concurrentes, que cumpla no sólo una función formal de motivación de la medida sino que permita una evaluación esmerada con carácter previo a la toma de la decisión, como una garantía para la ciudadanía y al mismo tiempo como una garantía del acierto de la medida para la consecución del interés público.

Por otra parte, se debe destacar también la previsión de la posibilidad de solicitar un informe a la Agencia Catalana de Protección de Datos en el proceso de implantación del sistema de videovigilancia, como medida que ofrece mayores garantías a la hora de asegurar el cumplimiento de la normativa en materia de protección de datos en los tratamientos que se realice.

Pero la concurrencia de uno de los supuestos habilitadores legalmente previstos y el cumplimiento del principio de proporcionalidad no son suficientes para la utilización legítima de cámaras con finalidades de videovigilancia. Además, la captación y el posterior tratamiento se deben realizar de acuerdo con unas garantías que aseguren el respeto a los derechos de las personas y minimicen los riesgos generados por el tratamiento.

Con respecto a los derechos de las personas reconocidos en la normativa de protección de datos, la presente Instrucción pone especial énfasis en el derecho de las personas a ser informadas de la existencia de estos sistemas de videovigilancia. Se trata de un derecho reconocido con carácter general en la LOPD, pero que en este ámbito adquiere unas especiales connotaciones que requieren la adaptación de las previsiones legales a este supuesto concreto, con el fin de hacer posible su cumplimiento. En la presente Instrucción también se concretan las especialidades en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Por otra parte, con el fin de minimizar los riesgos, se recogen aquí las previsiones necesarias para adaptar las medidas de seguridad que prevé la normativa de protección de datos a la especial naturaleza de los datos tratados por estos sistemas. Medidas que, en principio, serán las aplicables a los tratamientos automatizados, aunque cuando se trate de sistemas de grabación que no utilicen tecnología digital, a pesar de la utilización de medios técnicos, resultará más adecuada la implantación de las medidas previstas para los tratamientos no automatizados, en atención a las

posibilidades de tratamiento más limitadas que ofrece la tecnología analógica. En cuanto al nivel aplicable, vista la consideración de la imagen y la voz como datos identificativos, será en principio el nivel básico, sin perjuicio de que cuando en el tratamiento llevado a cabo sea especialmente relevante alguna de las circunstancias que requieren la aplicación de medidas de nivel medio o nivel alto se deba aplicar el nivel que corresponda.

La presente Instrucción se dicta de acuerdo con lo que disponen el artículo 5.1.c) de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, y el artículo 15.1.e) del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos. Para su tramitación se ha sometido a información pública, a informe de la Secretaría de Seguridad del Departamento de Relaciones Institucionales y Participación, del Instituto Catalán de las Mujeres, del Consejo Asesor de Protección de Datos de Cataluña y de la Comisión Jurídica Asesora, cumpliendo lo que establecen los artículos 63 y 64 de la Ley 13/1989, de 14 de diciembre, de organización, procedimiento y régimen jurídico de la Administración de la Generalidad de Cataluña.

Por todo lo expuesto, y de acuerdo con el dictamen de la Comisión Jurídica Asesora, dispongo la siguiente

INSTRUCCIÓN:

CAPÍTULO 1

Disposiciones generales

Artículo 1

Objeto

1.1 La presente Instrucción se aplica al tratamiento de los datos personales consistentes en imágenes, y en su caso, en voces, de personas físicas identificadas o identificables con fines de videovigilancia mediante cámaras u otros medios técnicos análogos.

1.2 Sin perjuicio de la aplicabilidad de la legislación de protección de datos y la de protección del derecho al honor, la intimidad y a la propia imagen, en su caso, quedan excluidas de la presente Instrucción:

- a) Las captaciones de imágenes cuya definición o características no permita identificar personas determinadas.
- b) La captación de imágenes con sistemas de videoportero, siempre que se activen sólo durante el periodo necesario para identificar a las personas que pretendan acceder al inmueble y no se registren las imágenes.
- c) Las captaciones de imágenes con fines exclusivamente periodísticos.
- d) La instalación de cámaras falsas que no sean aptas para captar imágenes.
- e) Los otros tratamientos de imágenes o imágenes y sonidos que no tengan finalidades de videovigilancia.

Artículo 2

Definiciones

A los efectos de la presente Instrucción, se entiende por:

- a) Tratamiento: la captación, incluida la emisión en tiempo real, la grabación, la modificación, la comunicación, el almacenamiento y las elaboraciones posteriores de imágenes, y en su caso de voces, con independencia del soporte utilizado, como también su cancelación, bloqueo y supresión.
- b) Captación: la obtención de imágenes, y en su caso de voces, incluida la emisión en tiempo real, independientemente del sensor utilizado.
- c) Almacenaje: la grabación sobre un soporte reproducible de toda o parte de una imagen o voz.
- d) Persona identificable: una persona se considera identificable cuando puede ser identificada directamente a través de una imagen de su cuerpo, o de su voz,

o indirectamente a través de otras imágenes como por ejemplo códigos, identificadores, matrículas u otras que por ellas mismas, o puestas en relación con otros datos, permitan identificar a una persona sin que ello requiera plazos o esfuerzos desproporcionados.

e) Videovigilancia: captación de imágenes, y en su caso de voces, a través de un sistema de cámaras fijas o móviles que tengan por finalidad la vigilancia o el control en edificios, instalaciones, vehículos u otros espacios públicos o privados, por razones de seguridad pública o privada, control del tráfico, control laboral, aseguramiento del normal funcionamiento de determinados servicios públicos, control de los hábitos, la conducta o el estado de las personas o por otras razones análogas.

f) Cámara: dispositivo, aparato o sensor destinado a captar, impresionar o reproducir imágenes en movimiento o fijas, y también sonidos, en su caso, con independencia de que queden o no registrados y del soporte en que se registren.

g) Sistema de cámaras de videovigilancia: sistema de información integrado por una o más cámaras y otros elementos instalados con una misma finalidad por parte de una persona responsable. El sistema incluye tanto las cámaras como los medios destinados a la monitorización, la grabación, la transmisión o el tratamiento de las imágenes o voces.

h) Disociación de imágenes: tratamiento de las imágenes mediante programas o herramientas informáticas u otras técnicas que, aplicadas sobre una imagen o voz, impide que puedan asociarse a una persona determinada.

Artículo 3

Ámbito subjetivo

3.1 La presente Instrucción es de aplicación a todos los órganos, organismos y entidades vinculadas o dependientes de las instituciones públicas de Cataluña, de la Administración de la Generalidad, de los entes locales de Cataluña, de las universidades de Cataluña y de las corporaciones de derecho público que ejerzan sus funciones exclusivamente en Cataluña, que, de acuerdo con el artículo 156 del Estatuto de Autonomía de Cataluña, forman parte del ámbito de actuación de la Agencia Catalana de Protección de Datos.

También es de aplicación a las personas físicas o jurídicas que, en función de cualquier convenio, contrato o disposición normativa, gestionen servicios públicos o ejerzan funciones públicas, siempre que en este último caso el tratamiento se haga en Cataluña y sea en relación con materias de la competencia de la Generalidad de Cataluña o de los entes locales de Cataluña.

3.2 La presente Instrucción se aplica a los tratamientos que realicen las entidades mencionadas en el apartado primero, con independencia de que la totalidad o parte de éstos los lleve a cabo una tercera persona por encargo de alguna de estas entidades. En este caso, son de aplicación las previsiones previstas en la normativa de protección de datos sobre el encargo del tratamiento.

Artículo 4

Régimen aplicable

4.1 Los tratamientos a que se refiere la presente Instrucción se rigen por lo que establece la normativa estatal y de la Generalidad de Cataluña en materia de protección de datos y otra normativa de aplicación, y por lo que establece la presente Instrucción.

4.2 El tratamiento de datos personales procedentes de imágenes y voces obtenidas mediante la utilización de videocámaras por la policía de la Generalidad-mozos de escuadra o por las policías locales de Cataluña se deben regir por sus disposiciones específicas y por lo previsto especialmente, en su caso, en la legislación de protección de datos personales y por la presente Instrucción.

4.3 Lo que establece la presente Instrucción se entiende sin perjuicio del necesario cumplimiento, por parte de las entidades responsables de las cámaras, de los requisitos exigidos por la normativa de seguridad privada y el resto de normativa aplicable.

CAPÍTULO 2

Principios aplicables al tratamiento de imágenes

Artículo 5

Legitimidad del tratamiento

5.1 Para la utilización de cámaras o de sistemas de videovigilancia para el cumplimiento de alguna de las finalidades previstas en el artículo 2.e) de la presente Instrucción hay que contar con el consentimiento libre, inequívoco y específico de las personas afectadas o, en su defecto, con la concurrencia de alguna de las circunstancias previstas en el artículo 6.2 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

La utilización de cámaras o sistemas de videovigilancia por parte de la policía de la Generalidad-mozos de escuadra o por las policías locales de Cataluña requiere la autorización correspondiente en los supuestos previstos en su normativa específica.

5.2 En caso de que se capten imágenes que podrían revelar la ideología, la afiliación sindical, la religión o las creencias de las personas afectadas, el tratamiento sólo será considerado legítimo cuando se cuente con el consentimiento expreso y por escrito de las personas afectadas. Cuando se trate de datos que puedan hacer referencia al origen racial, la salud o la vida sexual de las personas afectadas pueden tratarse cuando, por razones de interés general, lo disponga una ley o la persona afectada consienta expresamente.

Las previsiones de este apartado no son de aplicación a la captación de la imagen de la persona en que, de forma meramente accesorio, se puedan tratar rasgos físicos, la apariencia o incluso determinados hábitos o comportamientos de las personas que puedan considerarse datos especialmente protegidos.

La instalación y la utilización de sistemas de videovigilancia no puede obedecer o dar lugar a prácticas discriminatorias constitucionalmente prohibidas.

5.3 Los trabajos de instalación de aparatos de videovigilancia los deben llevar a cabo empresas autorizadas de seguridad privada. Además, la policía de la Generalidad-mozos de escuadra y la policía local correspondiente pueden instalar sus respectivos sistemas de videovigilancia.

5.4 No se considera legítima:

c) La instalación de aparatos que permitan la grabación del interior del domicilio de otras personas, salvo que se cuente con su consentimiento o concurra alguna otra de las circunstancias previstas en el artículo 18.2 de la Constitución.

d) La captación de imágenes de personas en la vía pública, salvo que la lleven a cabo las fuerzas y cuerpos de seguridad de acuerdo con su normativa específica. La captación incidental de imágenes de la vía pública para la vigilancia de edificios o instalaciones sólo resulta legítima si resulta inevitable para alcanzar la finalidad de vigilancia del edificio o instalación.

5.5 La cesión o comunicación de datos personales consistentes en imágenes, y en su caso voces, obtenidas a partir de la utilización de sistemas de videovigilancia sólo se puede considerar legítima cuando se ajuste a aquello que disponen los artículos 11, 21 y 22 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

La cesión o copia de las imágenes y sonidos captados por la policía de la Generalidad-mozos de escuadra o las policías locales de Cataluña se rige por lo previsto en su normativa específica.

Artículo 6

Finalidad

6.1 De acuerdo con el principio de calidad de los datos, las imágenes, y en su caso las voces, sólo se pueden captar y tratar a través de sistemas de videovigilancia para finalidades determinadas, explícitas y legítimas.

Las imágenes, y en su caso las voces, captadas para una finalidad determinada no pueden utilizarse para una finalidad diferente, salvo consentimiento de la persona titular o que una ley lo autorice.

6.2 Las imágenes captadas con finalidad de difusión cultural o turística, o con el fin de ofrecer información meteorológica u otras análogas no se pueden utilizar con finalidades de videovigilancia y, por lo tanto, no deben poder permitir la identificación de personas concretas.

Artículo 7

Proporcionalidad

7.1 El tratamiento de la imagen, y especialmente de la voz, de las personas físicas con finalidades de vigilancia sólo se puede producir cuando sea adecuado para contribuir de forma clara a la mejora del servicio o actividad, y dicha finalidad no se pueda obtener con otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para los derechos de las personas.

Este mismo principio de intervención mínima también se debe aplicar en la selección de la tecnología utilizada, los lapsos temporales de grabación y en la determinación de las condiciones de conservación y acceso a las imágenes.

7.2 Con carácter previo a la instalación, las personas responsables de la utilización de sistemas de videovigilancia deben ponderar los diferentes derechos y bienes jurídicos en juego, analizando:

- a) La necesidad de utilizar estos sistemas.
- b) La idoneidad de la instalación de sistemas de videovigilancia para alcanzar la finalidad perseguida.
- c) El riesgo que puede suponer para los derechos de las personas, teniendo en cuenta las características del sistema de videovigilancia, las circunstancias de la captación y las personas afectadas.
- d) La ausencia de medidas de vigilancia alternativas que comporten un riesgo menor, en relación con posibles intromisiones en los derechos fundamentales.

Esta ponderación debe quedar documentada en la memoria prevista en el artículo 10 de la presente Instrucción.

7.3 Puede resultar no adecuada al principio de proporcionalidad:

- a) La instalación de cámaras en espacios como baños, servicios, vestuarios, salas de ocio o de descanso con acceso restringido o habitaciones de hoteles y similares, donde, por su propia naturaleza, la captación de imágenes resulta especialmente intrusiva respecto al derecho a la intimidad, a la dignidad personal o al libre desarrollo de la personalidad. Esta previsión también es aplicable a las habitaciones de los centros asistenciales, a menos que sea necesario para proteger un interés vital de la persona afectada. En el caso de celdas de depósito de personas detenidas o de centros penitenciarios o espacios análogos de reclusión, la instalación no resulta proporcionada, salvo que exista un interés legítimo superior que lo justifique.
- b) La utilización de sistemas de videovigilancia en el ámbito laboral con la finalidad exclusiva de controlar el rendimiento de las personas trabajadoras.
- c) La instalación, en el ámbito educativo, de cámaras en el interior de las aulas, gimnasios o espacios de ocio del alumnado para su control.

7.4 La captación y la grabación de la voz de las personas físicas junto con la grabación de la imagen a través de sistemas de videovigilancia sólo puede considerarse legítima, con carácter excepcional, cuando no se trate de conversaciones estrictamente privadas, la finalidad de vigilancia no se pueda conseguir mediante la grabación, de forma exclusiva, de la imagen, y siempre que los motivos que justifican la grabación de la voz figuren en la memoria prevista en el artículo 10 de la presente Instrucción.

Si accidentalmente se registran conversaciones de naturaleza estrictamente privada, hay que cancelarlas, salvo que se cuente con el consentimiento del titular o una norma con rango de ley que habilite la conservación o la comunicación de la información.

Artículo 8

Conservación de las imágenes

8.1 En aquellos supuestos en que no se pueda alcanzar la finalidad perseguida sin almacenar las imágenes, el periodo de conservación no debe ser superior al que

resulte necesario para dar cumplimiento a la finalidad de vigilancia para la que los datos han sido recogidos o registrados. Con carácter general, se recomienda no exceder el plazo máximo de un mes para cancelar las imágenes tratadas.

8.2 La cancelación se produce sin perjuicio del bloqueo, según el cual las imágenes se pueden conservar a disposición de las administraciones públicas, los juzgados y los tribunales para atender a las posibles responsabilidades nacidas del tratamiento durante el plazo de prescripción de estas responsabilidades.

8.3 El bloqueo conlleva que las imágenes, y en su caso las voces, queden fuera de los circuitos de explotación habituales y que se establezca la custodia mediante un sistema que permita el control y la grabación de los accesos que se produzcan, con la finalidad a que hace referencia el apartado anterior.

Cuando se trate de imágenes en soporte digital, conlleva también la encriptación de las imágenes.

Cuando se trate de imágenes registradas en soportes que no sean digitales, el bloqueo se debe garantizar mediante el etiquetado que indique esta circunstancia y la conservación de las imágenes en cajas, contenedores u otros recipientes precintados de acceso restringido. Estos soportes deben quedar bajo la custodia de la persona responsable del fichero o la persona responsable de seguridad, si la hay, o la persona en que deleguen, sin que en ningún caso pueda ser la misma persona operadora del sistema.

8.4 Cuando, accidentalmente, se hayan captado imágenes o voces en circunstancias que comporten su ilicitud, se deben eliminar de manera inmediata en cuanto se tenga conocimiento.

8.5 La conservación de las imágenes y sonidos captados por la policía de la Generalidad-mozos de escuadra o las policías locales de Cataluña se rige por lo que prevé su normativa específica.

CAPÍTULO 3

Creación e inscripción de los ficheros

Artículo 9

Creación de los ficheros

9.1 Para poder iniciar la captación de imágenes debe haberse creado, con carácter previo, el correspondiente fichero, de acuerdo con lo que establece la normativa de protección de datos de carácter personal y la presente Instrucción, salvo que las imágenes se capten sin que haya almacenamiento.

9.2 Sin perjuicio de los supuestos en que la solicitud de informe resulta preceptiva, antes de la creación del fichero o, en su caso, de la puesta en marcha del sistema o de una o varias cámaras, se puede solicitar un informe a la Agencia Catalana de Protección de Datos sobre la adecuación del tratamiento a la legislación en materia de protección de datos. La solicitud de informe se debe acompañar de la propuesta de acuerdo o de disposición general de creación del fichero y de la memoria a que se refiere el artículo siguiente.

9.3 El fichero puede incluir las imágenes referidas a una o varias cámaras, siempre que en este último supuesto las diferentes captaciones presenten suficiente homogeneidad en relación con la finalidad con la que son captadas, las características de la captación y el tratamiento que se prevé hacer.

9.4 En los tratamientos realizados por la policía de la Generalidad-mozos de escuadra o por las policías locales de Cataluña que estén sometidos a inscripción en el registro previsto en su normativa específica, no es necesaria la creación del fichero.

Artículo 10

Memoria

10.1 Con carácter previo a la creación del fichero, o a la puesta en marcha del sistema de videovigilancia en aquellos casos en que no se registren las imágenes, se debe elaborar una Memoria, que debe hacer referencia a los siguientes puntos:

a) Órgano, organismo o entidad responsable: concreción de la persona responsable del fichero, de las personas operadoras del sistema de videovigilancia, como también, en su caso, de la persona responsable de la instalación y de su mantenimiento.

b) Justificación de la legitimidad de la captación y de los tratamientos posteriores que se prevean: debe hacerse constar si se cuenta con el consentimiento de los afectados o, si no es el caso, cuál de los apartados del artículo 6.2 de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en su caso otra normativa aplicable, concurre en el caso concreto, a efectos de legitimar el tratamiento de las imágenes y voces.

c) Justificación de la finalidad y de la proporcionalidad del sistema, de acuerdo con lo que establecen los artículos 6 y 7 de la presente Instrucción.

d) Datos personales tratados: hay que concretar si se registrará también la voz y si la finalidad conlleva, previsiblemente, la captación de imágenes que revelen datos personales especialmente protegidos u otros que exijan un nivel medio o alto de seguridad.

e) Ubicación y campo de visión de las cámaras: debe hacerse referencia a la ubicación y orientación de las cámaras. En especial, cuando se trate de cámaras en el exterior, debe hacerse constar si en un radio de 50 metros hay centros de salud, centros religiosos, de culto o sedes de partidos políticos o centros educativos donde asistan menores. También debe hacerse referencia a los espacios que entren dentro del campo de visión de las cámaras.

f) Definición de las características del sistema. En este apartado hay que especificar:

Número total de cámaras que forman el sistema.

Condiciones técnicas de las cámaras y de otros elementos.

Si las cámaras disponen de ranuras o conexiones para dispositivos de almacenamiento externo.

Si las cámaras son fijas o móviles.

Si se captan imágenes en un plano fijo o móvil.

Si se dispone de la posibilidad de obtener primeros planos en el momento de la captación o una vez registradas las imágenes.

Si las imágenes se visionan directamente o sólo se registran, con acceso limitado a determinados supuestos previstos en la Memoria.

Si la captación, y en su caso la grabación, se hace de manera continuada o discontinua.

Si las imágenes se transmiten.

Previsiones relativas a los mecanismos de identificación y de disociación para atender al ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Cuando se grabe la voz, también hay que especificar la distancia a la que se puede registrar.

g) Deber de información: hay que incluir una referencia al número y emplazamiento de los carteles informativos, como también a los otros medios adicionales de información, con el fin de acreditar el cumplimiento del deber de información.

h) Periodo por el que se instala el sistema y periodo de conservación de las imágenes.

i) Medidas previstas para evaluar los resultados del funcionamiento del sistema y la necesidad de su mantenimiento.

j) Medidas de seguridad: concreción del nivel de seguridad exigible y descripción de las medidas de seguridad aplicadas.

10.2 La información a que se refieren los apartados e) y g) debe ir acompañada de la información gráfica correspondiente.

10.3 En los ficheros de titularidad pública, esta Memoria puede formar parte de la memoria prevista en el procedimiento de elaboración de disposiciones de carácter general.

10.4 La Memoria se debe elaborar también cuando el tratamiento de la imagen, y en su caso de la voz, sea accesorio de otro tratamiento. En este supuesto, hay especificar y justificar esta circunstancia.

10.5 La Memoria debe estar a disposición de los funcionarios y funcionarias de la Agencia Catalana de Protección de Datos que ejercen tareas de inspección.

Artículo 11

Inscripción de ficheros de videovigilancia

11.1 Cualquier tratamiento de datos personales que comporte la grabación de imágenes de personas físicas identificadas o identificables, captadas mediante una o más cámaras que formen parte de un sistema de videovigilancia, constituye un fichero y se debe notificar al Registro de protección de datos de Cataluña. La notificación se debe hacer una vez se haya creado el fichero, de acuerdo con lo que prevé la normativa de protección de datos, mediante el formulario que se establezca por resolución del director o directora de la Agencia Catalana de Protección de Datos. También debe inscribirse la modificación y la supresión de los ficheros.

11.2 Las captaciones de imágenes que no se almacenen quedan exceptuadas de la obligación de inscripción.

11.3 Si la captación de imágenes constituye un tratamiento accesorio o complementario de otro tratamiento, se puede inscribir como un único fichero.

11.4 La Agencia Catalana de Protección de Datos traslada al Registro general de protección de datos de la Agencia Española de Protección de Datos las inscripciones, modificaciones o supresiones de ficheros de videovigilancia que se producen en el Registro.

11.5 Las previsiones de este artículo no son de aplicación a los tratamientos de datos personales a través de sistemas de videovigilancia llevados a cabo por la policía de la Generalidad-mozos de escuadra o por las policías locales de Cataluña que deban inscribirse en el Registro de autorizaciones previsto por su normativa específica, sin perjuicio de que se puedan establecer fórmulas de colaboración entre este registro y el Registro de protección de datos de Cataluña.

CAPÍTULO 4

Deber de información

Artículo 12

Información

12.1 Las personas responsables del tratamiento de imágenes a través de cámaras fijas deben informar de forma clara y permanente sobre la existencia de las cámaras mediante la colocación de los carteles informativos que sean necesarios para garantizar el conocimiento por las personas afectadas. Esta obligación es exigible igualmente cuando las imágenes captadas no sean registradas.

12.2 Los carteles informativos se deben colocar antes de que empiece la captación de imágenes y voces, incluso si se trata de pruebas, y sólo pueden retirarse una vez sea desinstalado el sistema.

12.3 Los carteles informativos deben colocarse en emplazamientos claramente visibles antes de entrar en el campo de grabación de las cámaras. La ubicación concreta de los carteles dependerá, en cada caso, de la naturaleza y estructura de las zonas y espacios videovigilados. No obstante, hay que tener en cuenta las siguientes condiciones:

Para las cámaras de videovigilancia en edificios o instalaciones, debe colocarse un cartel informativo en cada uno de los accesos al área videovigilada. En caso de que estén divididos por plantas, además, hay que colocar otro cartel informativo en cada una de las plantas que cuenten con videocámaras, ubicados en un espacio de acceso principal en el área o zona videovigilada en la planta.

Para las cámaras de videovigilancia en el transporte público, debe colocarse, como mínimo, un cartel informativo en cada uno de los accesos al área videovigilada, así como en la entrada de los vehículos sometidos a videovigilancia, de tal manera que sea visible para las personas afectadas cuando accedan.

Para las cámaras de videovigilancia en espacios abiertos, debe colocarse un cartel informativo a una distancia suficiente para que las personas afectadas ten-

gan conocimiento, de manera clara y permanente, de la existencia de cámaras de videovigilancia en el área o zona a la que acceden. En cualquier caso, la ubicación del cartel informativo debe estar a una distancia inferior a 50 metros desde el límite exterior del área.

12.4 El contenido y el diseño del cartel informativo debe ajustarse a lo que establece el anexo de la presente Instrucción, sin que en ningún caso resulte exigible que se especifique el emplazamiento de las cámaras.

El cartel informativo puede ser sustituido por la información a través de pantallas electrónicas, cuando se ofrezca una imagen fija del cartel o éste aparezca, y pueda ser leído, con una frecuencia que garantice el conocimiento por las personas afectadas.

12.5 Corresponde al responsable del tratamiento velar por la conservación y el mantenimiento de los carteles informativos, a fin de que permitan que las personas afectadas conozcan, en todo momento, la existencia de cámaras.

12.6 La persona responsable del tratamiento, o quien designe en su lugar, también debe proporcionar a las personas afectadas información sobre el resto de puntos previstos en el artículo 5.1 de la LOPD por medio de impresos o a través de su web o sede electrónica, donde deberá constar la finalidad específica de la vigilancia, como también el resto de la información, establecida en los apartados a), d) y e) del artículo 5 de la LOPD.

12.7 Con carácter complementario se pueden utilizar, en su caso, otros medios adicionales para cumplir el deber de información que aseguren el conocimiento por todas las personas, como el uso de sistemas de megafonía.

12.8 En las cámaras fijas para el control, la regulación, la vigilancia y la disciplina del tráfico en la vía pública, el contenido del cartel se puede limitar a informar de la existencia de la cámara o el dispositivo de control de velocidad, sin perjuicio de lo que establece el apartado 6 de este artículo.

12.9 En el caso de las cámaras móviles, salvo que su presencia sea claramente perceptible, hay que informar de su existencia, en la medida en que sea posible, en el mismo acto de la grabación o, si eso no es posible, a través de otros medios.

12.10 El cumplimiento del deber de información en los tratamientos sometidos a la legislación sobre el uso de videocámaras por la policía de la Generalidad-mozos de escuadra o por las policías locales de Cataluña se rige por su normativa específica.

CAPÍTULO 5

Derechos de acceso, rectificación, cancelación y oposición

Artículo 13

Derecho de acceso

Mediante el derecho de acceso, la persona titular de la imagen, y en su caso de la voz, tiene derecho a que la persona responsable del tratamiento le informe sobre si su imagen ha sido captada a través de sistemas de videovigilancia, la finalidad de la captación, si la imagen es registrada en un fichero, si es objeto de algún otro tratamiento, si se ha realizado o se ha previsto alguna comunicación y cuál es el periodo de conservación de las imágenes o voces.

Cuando la persona interesada así lo pida, también tiene derecho a acceder a las imágenes o voces y a obtener copia, como también de las elaboraciones posteriores que se hayan hecho.

En caso de que el ejercicio del derecho afecte también imágenes o voces de terceras personas, salvo que se cuente con su consentimiento, el acceso requiere la disociación previa de las imágenes y sus voces con cualquier medio que impida la identificación. Cuando la disociación exija esfuerzos desproporcionados en atención al lapso temporal registrado o al elevado número de terceras personas afectadas, la persona responsable puede solicitar que se reduzca el periodo de grabación al que se pretenda tener acceso.

Artículo 14

Derecho de rectificación

14.1 Sólo procede el ejercicio del derecho de rectificación de las imágenes o la voz captadas con sistemas de videovigilancia cuando la imagen o la voz hayan sido distorsionadas o alteradas con posterioridad a su captación.

14.2 Con el fin de dar cumplimiento a lo que prevé este artículo, cuando se alteren o distorsionen las imágenes o voces se debe guardar copia de la grabación original o disponer de un mecanismo de recuperación de la información original. La alteración o distorsión debe quedar reflejada en el registro de incidencias, indicando el periodo afectado y el motivo.

Artículo 15

Derecho de cancelación

Mediante el derecho de cancelación la persona titular de la imagen o la voz puede pedir la supresión, previo bloqueo, de sus imágenes o voz cuyo tratamiento sea inadecuado, excesivo o contrario al ordenamiento jurídico.

Artículo 16

Derecho de oposición

16.1 Mediante el derecho de oposición, a menos que una norma con rango de ley o norma de derecho comunitario de aplicación directa disponga lo contrario, la persona titular de la imagen puede pedir la exclusión del tratamiento de su imagen o voz en aquellos supuestos en que no sea necesario su consentimiento. La solicitud de ejercicio de este derecho debe justificarse en motivos fundamentados y legítimos relativos a una situación personal concreta.

16.2 También se puede ejercer el derecho de oposición cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, o cuando el tratamiento tenga por finalidad la adopción de una decisión referida a la persona interesada basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

Artículo 17

Procedimiento de ejercicio de derechos

17.1 Para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, hay que formular una solicitud dirigida al responsable del fichero o, en su caso, al encargado del tratamiento, indicando el lugar, la fecha y la hora aproximada, en franjas no superiores a dos horas, en que su imagen pudo ser captada. La solicitud debe acompañarse de una imagen de la persona solicitante que corresponda al periodo en que se captó, de manera que permita identificarla. Con el fin de comprobar la coincidencia entre la imagen aportada y las imágenes registradas, se pueden utilizar herramientas de reconocimiento de imágenes.

17.2 En los sistemas de videovigilancia que registren la voz, el derecho de acceso se puede ejercer aportando una grabación de la voz de la persona afectada. A estos efectos, la persona responsable de los sistemas de videovigilancia que registren el sonido debe contar con herramientas de reconocimiento de la voz que permitan comprobar la coincidencia de la grabación de voz aportada con alguna de las voces registradas.

17.3 Si la imagen o la voz aportadas no ofrece bastante definición o elementos para permitir la identificación, se debe otorgar un plazo de enmienda de 10 días hábiles para poder aportar otra imagen o grabación de la voz.

17.4 La tramitación y la resolución de la solicitud se rige por lo que establecen la normativa de protección de datos de carácter personal y por la presente Instrucción. La obligación de resolver persiste, con independencia de que las imágenes no hayan sido registradas o que ya hayan sido canceladas en el momento en que se ejerce el derecho. En este último caso, la resolución puede limitarse a exponer esta circunstancia y a informar de la imposibilidad material de dar satisfacción al derecho ejercido.

17.5 Puede denegarse la solicitud de ejercicio de los derechos de acceso, rectificación, cancelación u oposición cuando no concurren los requisitos exigibles, o cuando el nivel de coincidencia entre la imagen o la voz aportada con la solicitud y las que hayan sido objeto de tratamiento no permita asegurar que ésta última corresponde a la persona interesada. También puede denegarse cuando no hayan sido registradas o ya hayan sido canceladas.

6. Ante la denegación del ejercicio del derecho o ante la falta de recepción de respuesta en el plazo establecido, la persona afectada puede formular una reclamación de tutela ante la Agencia Catalana de Protección de Datos.

Artículo 18

Imágenes y voces captadas por las fuerzas y cuerpos de seguridad

18.1 El ejercicio de los derechos de acceso y cancelación de imágenes o voces tratadas por cámaras de las que son responsables la policía de la Generalidad-mozos de escuadra o las policías locales de Cataluña se rige por su normativa específica.

18.2 Los derechos de oposición y de rectificación en relación con imágenes captadas por las cámaras de las que son responsables los cuerpos policiales mencionados se ejercen de acuerdo con lo que establece la normativa estatal y autonómica sobre protección de datos, como también por lo que establece la presente Instrucción.

CAPÍTULO 6

Medidas de seguridad

Artículo 19

Obligaciones de la persona responsable del tratamiento

19.1 La persona responsable del tratamiento debe adoptar las medidas técnicas y organizativas necesarias que garanticen la autenticidad, la integridad y la confidencialidad de las imágenes captadas mediante sistemas de cámaras y que eviten la alteración, pérdida, acceso indebido o tratamiento no autorizado.

19.2 La persona responsable del tratamiento debe informar a las personas que tengan acceso a las imágenes en ejercicio de sus funciones que deben observar el deber de secreto, y que esta obligación subsiste incluso después de haber finalizado su relación de servicio.

19.3 Las previsiones del presente capítulo son exigibles también a los ficheros y tratamientos llevados a cabo mediante sistemas de videovigilancia cuyos responsables son la policía de la Generalidad-mozos de escuadra o las policías locales de Cataluña.

Artículo 20

Nivel de seguridad

20.1 El nivel de seguridad que se debe asignar al fichero es el que resulte de la normativa que regula los niveles de seguridad exigibles en el tratamiento de datos de carácter personal, de acuerdo con lo que resulte de la memoria a que se refiere el artículo 10 de la presente Instrucción.

20.2 La recogida y el tratamiento de imágenes de personas identificadas o identificables requiere, con carácter general, el nivel de seguridad básico, sin perjuicio que en determinados supuestos puedan ser de aplicación las medidas de nivel medio o alto especificadas en esta normativa.

Sin perjuicio del resto de supuestos previstos en la normativa de protección de datos, la captación y el tratamiento de determinadas imágenes o voces que, de manera previsible y significativa y no meramente ocasional, ofrezcan información que permita evaluar aspectos de la personalidad o el comportamiento de las personas, requiere nivel medio de medidas de seguridad. Se requiere nivel alto cuando ofrezcan información sobre datos especialmente protegidos, cuando se trate de imágenes captadas o tratadas para fines policiales sin el consentimiento de las personas afectadas, o cuando sean relativas a actos de violencia de género.

20.3 La captación de la imagen de la persona en que, de forma meramente accesoria, se puedan tratar rasgos físicos, la apariencia, determinados hábitos o comportamientos u otras circunstancias que podrían tener atribuido un nivel de seguridad diferente, no altera el nivel de seguridad que sea de aplicación si aquella circunstancia no es tenida en cuenta en el tratamiento que se realice.

20.4 Los tratamientos de imágenes captadas con sistemas de videovigilancia que sean accesorios de otros tratamientos principales pueden segregarse de éstos últimos, y aplicar el nivel de medidas de seguridad que corresponda al tratamiento de las imágenes, siempre que se determine las personas usuarias que tendrán acceso y conste en el documento de seguridad.

Artículo 21

Medidas de seguridad

21.1 A las imágenes, y en su caso a las voces, obtenidas o tratadas mediante sistemas digitales de videovigilancia, incluso durante el periodo de pruebas, se debe aplicar las medidas de seguridad técnicas y organizativas previstas en la normativa de protección de datos de carácter personal para los ficheros o tratamientos automatizados, según el nivel de seguridad establecido de acuerdo con el artículo anterior.

21.2 A las imágenes, y en su caso a las voces, obtenidas o tratadas con dispositivos que no utilicen tecnología digital o que posteriormente a la captación se incorporen a soportes que no se basen en la tecnología digital, se debe aplicar las medidas técnicas y organizativas previstas para los ficheros y tratamientos no automatizados.

21.3 Sin embargo, la persona responsable, atendiendo a los riesgos inherentes a los sistemas de videovigilancia, puede implantar medidas adicionales o complementarias a las expresamente requeridas por la normativa de protección de datos de carácter personal.

21.4 Con el fin de adecuar las medidas previstas en la normativa en materia de protección de datos a las exigencias de seguridad derivadas del tratamiento de imágenes y voces, hay que tener en cuenta lo siguiente:

a) El documento de seguridad debe definir a las personas o a los perfiles de personas usuarias que pueden manipular las cámaras y también a las que pueden visualizar las imágenes, en tiempo real o grabadas. Asimismo, debe definir a las personas que puedan llevar a cabo operaciones de bloqueo, borrado, destrucción, conservación, identificación, distorsión o cualquier otra manipulación de las imágenes, como también el personal que puede autorizar, modificar o revocar el acceso de terceros. Cuando se establezca a partir de perfiles de personas usuarias, el número de éstas debe ser limitado en el mismo documento de seguridad.

b) Los equipos de visionado de las imágenes deben estar situados en áreas restringidas al público o, si eso no es posible, dispuestos de forma que las imágenes no sean visibles por personas no autorizadas.

c) La persona responsable del fichero o tratamiento debe adoptar las medidas necesarias para asegurar la formación de las personas operadoras del sistema para la custodia, reserva y seguridad de las imágenes, como también para atender al ejercicio de los derechos de las personas mediante un procedimiento ágil.

d) En las operaciones de borrado de ficheros digitales o de reutilización de los soportes para grabaciones analógicas hay que adoptar las medidas necesarias para asegurar la destrucción total de su contenido.

e) En los ficheros automatizados, la realización de copias de soporte se debe hacer semanalmente, salvo que el periodo de conservación de las imágenes sea inferior a una semana.

f) Cuando se deban aplicar medidas de nivel alto a ficheros o tratamientos automatizados, el registro de acceso debe registrar la identificación del usuario que intenta acceder al sistema o archivo, su perfil de usuario, la fecha y hora del intento, las funciones que intenta realizar y si ha sido autorizado o no. En caso de haber sido autorizado, también es necesario registrar las imágenes a las que se ha accedido, identificadas con la fecha y el intervalo horario que se ha visualizado.

Si el tratamiento no se hace con sistema digital, el registro de accesos debe ser operativo a partir del día siguiente al de la fecha en que se produzca la grabación. Este registro lo debe llevar la persona encargada de la custodia de las grabaciones, que debe ser una persona diferente a las personas operadoras del sistema.

21.5 A efectos de garantizar la integridad y al mismo tiempo facilitar el ejercicio de los derechos, las imágenes deben incorporar un sistema de datación que indique el día y hora en que han sido captadas.

21.6 En aquellos supuestos en que no se almacenan las imágenes, las medidas de seguridad se deben adoptar igualmente en aquello que sea aplicable.

Artículo 22

Documento de seguridad

22.1 Las medidas de índole técnica y organizativa exigibles para el tratamiento de imágenes deben estar previstas en el documento de seguridad. Cuando el tratamiento de la imagen tenga carácter accesorio, debe estar previsto en el documento de seguridad correspondiente al tratamiento principal.

22.2 El documento de seguridad debe contener los aspectos previstos en la normativa de protección de datos.

DISPOSICIONES TRANSITORIAS

Ficheros y tratamientos preexistentes

—1 Los ficheros de videovigilancia existentes con anterioridad a la entrada en vigor de la presente Instrucción disponen de un plazo de 3 meses, a contar desde su publicación, para adaptarse a lo que establece el artículo 12 de la presente Instrucción.

Para las cámaras que sólo capten las imágenes, los carteles informativos que a la entrada en vigor de la presente Instrucción estaban colocados y se ajustaban a lo que establece la Instrucción 1/2006 de la Agencia Española de Protección de Datos siguen siendo válidos. En este caso, el plazo previsto en el párrafo anterior no es de aplicación mientras no se sustituyan.

—2 La conservación y el tratamiento de imágenes y voces, incluidas las registradas con anterioridad a la entrada en vigor de la presente Instrucción, deben adaptarse a las nuevas medidas de seguridad, obligaciones y garantías previstas en la presente Instrucción en el plazo de 3 meses, contados a partir de su entrada en vigor.

—3 Las previsiones del artículo 10 de la presente Instrucción sólo son exigibles en los ficheros de sistemas de videovigilancia que se creen a partir de la entrada en vigor de la presente Instrucción.

DISPOSICIÓN FINAL ÚNICA

Entrada en vigor

La presente Instrucción entrará en vigor el día siguiente a su publicación en el *Diari Oficial de la Generalitat de Catalunya*.

Barcelona, 10 de febrero de 2009

ESTHER MITJANS PERELLÓ
Directora

ANEXO

—1 En el cartel informativo a que se refiere el artículo 12 de la presente Instrucción se debe hacer constar de forma claramente visible, de arriba a abajo, como mínimo, la siguiente información:

Mención a la finalidad para la cual se tratan los datos (“Zona videovigilada”).

Pictograma que simboliza una cámara de videovigilancia dentro de un rectángulo blanco. Cuando se capte la voz, el pictograma debe reflejar esta circunstancia.

El texto informativo “Protección de datos”.

Mención expresa a la identificación de la persona responsable ante la que se pueden ejercer los derechos de acceso, rectificación, cancelación y oposición.

Indicación del lugar o web donde se puede conseguir la información a que se refiere el artículo 12.6 de la presente Instrucción.

—2 El diseño del cartel informativo debe ajustarse a los requisitos siguientes:

a) Tiene que ser de forma rectangular y con las aristas en ángulo recto. Las dimensiones estándar del cartel son, aproximadamente, 21 cm de base y 29,7 cm de altura.

Estas dimensiones pueden aumentar o disminuir según sea el área o la zona sometida a videovigilancia y la distancia que sea necesaria para que el cartel informativo resulte visible para las personas afectadas.

b) Tiene como color de fondo el amarillo, en cuyo extremo superior izquierdo puede constar el logotipo de la Agencia Catalana de Protección de Datos.

c) Centrado dentro de un rectángulo blanco de unas dimensiones aproximadas de 1/3 de la altura del cartel y 4/5 de la anchura que, en el cartel estándar, se sitúa aproximadamente a 6 cm del lado superior, debe constar el pictograma al que se refiere el apartado 1 de este Anexo.

En todo caso, estas indicaciones se deben mantener proporcionales en atención a las posibles variaciones en las dimensiones del cartel informativo.

—3 En la página web de la Agencia Catalana de Protección de Datos, www.apd.cat, hay disponibles modelos de cartel ajustados a los requisitos que establece este anexo, que pueden ser descargados.

(09.034.046)

