Circular /2025 de la Autoridad Catalana de Protección de Datos, sobre el tratamiento de datos personales mediante cámaras con fines de videovigilancia

ÍNDICE

Capítulo 6. Seguridad de los datos personales

Artículo 22. Obligaciones del responsable del tratamiento
Artículo 23. Medidas de seguridad

Disposición transitoria. Carteles informativos
Disposición derogatoria
Disposició final. Entrada en vigor

Anexo

En el año 2009 esta Autoridad aprobó la Instrucción 1/2009, de 10 de febrero de 2009, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia, para concretar la aplicación de los principios y las garantías que establecía la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en relación con la utilización de sistemas de videovigilancia por las entidades sometidas al ámbito de actuación de la Autoridad Catalana de Protección de Datos, con la vocación de ser un instrumento que aclarara el marco jurídico aplicable, aportara seguridad jurídica en esta materia, y una mayor concreción de aquellas cuestiones que, a la luz de los instrumentos internacionales y la jurisprudencia en la materia, así lo requerían.

La evolución jurisprudencial y los importantes cambios normativos producidos desde la aprobación de aquella Instrucción requieren su revisión con el fin de adecuar su contenido al nuevo marco jurídico, constituido, principalmente, por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales (Reglamento 2016/679), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (Ley orgánica 3/2018), la Ley 5/2014, de 4 de abril de seguridad privada y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El Reglamento 2016/679 supone una revisión de las bases legales del modelo europeo de protección de datos. Entre las principales novedades que introduce el Reglamento 2016/679, que tienen un impacto directo en el tratamiento de los datos personales provenientes de la imagen y la voz captadas mediante sistemas de videovigilancia, cabe destacar los principios de responsabilidad proactiva y la protección de datos desde el diseño y por defecto, que determina la necesidad de que los responsables del tratamiento apliquen, tanto en el momento de determinar los medios de tratamiento como en el momento del tratamiento mismo, las medidas técnicas y organizativas adecuadas para aplicar de manera efectiva los principios de protección de datos, e integrar las garantías necesarias en el tratamiento para cumplir los requerimientos del reglamento y, además, poder demostrarlo.

La Instrucción 1/2009 requería que el responsable del tratamiento elaborase una memoria, como herramienta para hacer un análisis completo y sistemático de las características del tratamiento que se pretendía hacer y de las circunstancias concurrentes. Esta medida sigue plenamente vigente a la luz del principio de responsabilidad proactiva establecido por el Reglamento 2016/679, pero debe evitarse

que sea una carga reiterativa en aquellos casos en que el tratamiento deba estar sometido a una evaluación de impacto sobre la protección de datos. Además, el Reglamento incorpora otros mecanismos de responsabilidad proactiva, como la necesidad de designar un delegado de protección de datos o de llevar un registro de las actividades de tratamiento, que deben adoptar los responsables y que pueden presentar una problemática específica en los tratamientos con fines de videovigilancia.

El Reglamento 2016/679, introduce dos nuevas categorías especiales de datos: los datos genéticos y los datos biométricos. En el ámbito de la videovigilancia la imagen o la voz de una persona no constituye un dato biométrico en cualquier caso. Ahora bien, la aplicación de un tratamiento técnico específico que permita o confirme la identificación de una persona conlleva el tratamiento de categorías especial de datos. En este sentido, especial mención merecen las tecnologías de reconocimiento facial que pueden incorporar algunos sistemas de videovigilancia. Al tratarse de datos biométricos, la protección es más reforzada, de manera que como regla general se prohíbe tratar estos tipos de datos, salvo los casos excepcionales previstos en la norma y, con carácter general, habrá que limitar la utilización de estas tecnologías de reconocimiento facial siempre que la finalidad se pueda obtener mediante sistemas menos intrusivos.

En cuanto al derecho de información, el Reglamento ha ampliado el contenido de la información que hay que ofrecer a las personas interesadas. Compatibilizar este mayor contenido, con la necesidad de transparencia, claridad e inteligibilidad de la información en el ámbito de la videovigilancia requiere una adaptación especial de la manera en que se cumple con este deber. Con este objetivo, la Ley Orgánica 3/2018 ha previsto la posibilidad de utilizar un mecanismo de doble capa para dar cumplimiento a las obligaciones de información. Esta previsión está alineada con el mecanismo utilizado en los sistemas de información de videovigilancia, que consiste en mostrar un aviso gráfico sobre el sistema y remitir a un sitio web donde se puede encontrar el resto de la información necesaria para las personas interesadas. Según la Ley Orgánica, los carteles informativos deben indicar la existencia del tratamiento, la identidad del responsable del tratamiento o del sistema de videovigilancia, la posibilidad de ejercer los derechos reconocidos a las personas interesadas por el Reglamento 2016/679, y el lugar donde obtener el resto de la información sobre el tratamiento realizado.

A la luz de la nueva regulación de los derechos de las personas interesadas, es necesario revisar las especialidades de su aplicación en el ámbito de la videovigilancia, especialmente en relación con los derechos de acceso, supresión, oposición y limitación del tratamiento. Hay que tener en cuenta que el derecho de rectificación tiene un margen de aplicabilidad reducido en este contexto, y que el derecho de portabilidad tampoco parece aplicable, dadas las bases jurídicas en que se fundamenta la videovigilancia.

En cuanto a las medidas de seguridad, la nueva regulación no establece un listado de medidas específicas aplicables según la tipología de datos tratados, como hacía la legislación anterior. En cambio, determina que el responsable y el encargado del tratamiento deben adoptar medidas técnicas y organizativas adecuadas al riesgo asociado al tratamiento, basándose en un análisis de los riesgos específicos de cada tratamiento. La Circular recoge los elementos a considerar para minimizar los riesgos y proporciona diferentes aspectos relativos a la seguridad, adaptados a la naturaleza especial de los datos tratados y las características de estos sistemas.

El Reglamento elimina la necesidad de crear formalmente los ficheros y de notificarlos al registro de protección de datos de las autoridades de control. Por lo tanto, hay que adaptar la Circular a esta nueva regulación.

La Ley orgánica 3/2018 regula los tratamientos de videovigilancia realizados por un responsable, ya sea una persona física o jurídica, pública o privada, con la finalidad de preservar la seguridad de las personas, los bienes y las instalaciones. Cabe destacar, sin embargo, que las finalidades de la Circular pueden ir más allá de las previstas en la Ley orgánica 3/2018, ya que abarcan también otros supuestos, como la videovigilancia para garantizar el funcionamiento adecuado de determinados servicios públicos.

La Ley orgánica 3/2018 también regula las condiciones de la videovigilancia en el ámbito laboral, reconociendo la facultad de los empresarios de tratar imágenes o datos obtenidos a través de cámaras para ejercer funciones de control sobre los trabajadores o empleados públicos, tal y como prevé la legislación laboral. Asimismo, la Ley Orgánica 3/2018 ha modificado el Estatuto de los Trabajadores y el Estatuto Básico del Empleado Público para incluir el derecho de los trabajadores a la intimidad ante el uso de dispositivos de videovigilancia, como contrapunto a las facultades de control del empresario.

Los tratamientos de los datos personales procedentes de las imágenes y voces obtenidos mediante la utilización de sistemas de videovigilancia por las Fuerzas y Cuerpos de Seguridad, por los órganos competentes para la vigilancia y el control en los centros penitenciarios, y para el control, regulación, vigilancia y disciplina del tráfico con la finalidad de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública, se rigen por la Ley Orgánica 7/2021.

En este ámbito sigue siendo de aplicación 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, y la normativa que la desarrolla, en lo que no contradiga la Ley Orgánica 7/2021.

En Cataluña esta regulación se ha desarrollado mediante 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, 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 y el Decreto 78/2010, de 22 de junio, por el que se regula la instalación de dispositivos de videovigilancia en las dependencias policiales de la Generalitat.

También se aplica supletoriamente el Reglamento 2016/679 y la Ley Orgánica 3/2018, respecto de aquellas cuestiones que no se regulen específicamente en esta normativa, como la aplicación de las medidas de seguridad, el ejercicio de los derechos de rectificación y oposición o el régimen sancionador.

Finalmente, la normativa reguladora de la seguridad privada ha sido modificada mediante la Ley 5/2014, de 4 de abril, de seguridad privada. El tratamiento de los datos provenientes de los sistemas de videovigilancia en el ámbito de la seguridad privada está sometido a la normativa en materia de protección de datos personales, poniendo énfasis en los principios de proporcionalidad, idoneidad e intervención mínima. Se prevé expresamente en este ámbito la aplicación supletoria de la normativa aplicable a la videovigilancia de las fuerzas y cuerpos de seguridad.

Esta Circular se dicta de acuerdo con el artículo 57.2 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, el artículo 5.e) de la Ley 32/2010, de 1 de octubre, de la Autoridad 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 del Departamento de Interior y Seguridad Pública, del Instituto Catalán de las Mujeres, del Consejo Asesor de Protección de Datos de Cataluña y de la Comisión Jurídica Asesora, cumpliéndose así con lo establecido en los artículos 59 a 70 de la Ley 26/2010, de 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña.

Por todo ello, y de acuerdo con el dictamen de la Comisión Jurídica Asesora, dispongo la siguiente:

CIRCULAR:

Capítulo 1
Disposiciones generales

Artículo 1
Objeto

1. Esta Circular tiene por objeto regular las especificidades del tratamiento de datos personales consistentes en imágenes y, en su caso, voces de personas físicas identificadas o identificables con fines de videovigilancia mediante cámaras fijas o móviles, incluidas las instaladas en aeronaves no tripuladas (drones), vehículos o indumentaria de las personas, u otros medios técnicos análogos.

2. Quedan excluidas de esta Circular:

a) Las captaciones de imágenes cuya definición o características no permita identificar personas físicas, directa o indirectamente.

b) El tratamiento de las imágenes en el ámbito personal o doméstico, como sería:

- El tratamiento por una persona física de imágenes o voces del interior de su propio domicilio. Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada contratada para la vigilancia de un domicilio, que tenga acceso a las imágenes o voces. Asimismo, debe interpretarse en el sentido de que afecta únicamente a actividades que se inscriben en el marco de la vida privada o familiar de los particulares. Quedarían excluidas, por tanto, la difusión de estos datos por internet de manera que resulten accesibles para un grupo indeterminado de personas. La grabación debe limitarse a su domicilio y no puede abarcar, ni que sea en parte, el espacio público o una zona ajena a la esfera privada de la persona.

- La captación de imágenes con sistemas de videoportero o con mirillas digitales similares instalados en los domicilios.

c) La instalación de cámaras falsas que no sean aptas para captar imágenes.

3. Sin perjuicio de la aplicabilidad de la legislación de protección de datos personales, quedan fuera del ámbito de aplicación de esta Circular:

a) Las cámaras integradas en vehículos para proporcionar asistencia al estacionamiento o en otros sistemas de ayuda a la conducción, siempre que no se registren las imágenes.

b) Las captaciones de imágenes con fines exclusivamente periodísticos.

c) Las captaciones de imágenes con sistemas de videoportero o con mirillas digitales similares, no incluidas en la letra b) del apartado anterior, 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 y voces.

d) Los otros tratamientos de imágenes o imágenes y voces que no tengan fines de videovigilancia.

Artículo 2
Definiciones

A los efectos de esta Circular, se entiende por:

a) Dato personal: cualquier información sobre una persona física identificada o identificable.

b) Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, que permiten o confirman la identificación única de esta persona, como imágenes faciales o datos dactiloscópicos. El tratamiento de imágenes de personas físicas no debe considerarse sistemáticamente como un tratamiento de categorías especiales de datos. Sólo se deben considerar datos biométricos si se tratan con medios técnicos específicos con la finalidad de hacer una identificación o autenticación de una persona física.

c) Persona identificable: la persona que puede ser identificada directamente a través de una imagen de su cuerpo, de una parte del mismo, o de su voz, o indirectamente, sin esfuerzos desproporcionados, a través de otros datos captadas como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea, matrículas, o uno o varios elementos propios de la identidad física, fisiológica, psíquica, económica, cultural o social.

d) Tratamiento: la captación de imágenes y, en su caso, voces de personas físicas, incluida la emisión en tiempo real, la grabación, el registro, la organización, la estructuración, la conservación, la adaptación o la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, así como su limitación, supresión o destrucción.

e) Captación: la obtención de imágenes, y en su caso voces, incluida la emisión en tiempo real, independientemente del sensor utilizado.

f) Almacenamiento: la grabación sobre un soporte reproducible de toda o parte de una imagen o voz.

g) Videovigilancia: captación de imágenes, y si procede 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.

h) Cámara: dispositivo, aparato o sensor destinado a captar, impresionar, o reproducir imágenes en movimiento o fijas, y también voz, si procede, con independencia de que queden o no registradas y del soporte en que se registren.

i) Sistema de cámaras de videovigilancia: sistema de información integrado por una o más cámaras fijas o móviles, incluidas las instaladas en aeronaves no tripuladas (drones), vehículos o indumentaria de las personas, y otros elementos instalados con una misma finalidad de videovigilancia por parte de una persona responsable. El sistema incluye tanto las cámaras como los medios destinados a la monitorización, la grabación, el almacenamiento, la transmisión o el tratamiento de las imágenes o las voces.

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

k) Vía pública: cualquier lugar destinado al tráfico, tanto urbano como interurbano, abierto al público, como por ejemplo calles, avenidas, plazas, caminos o cualquier otro lugar por donde transitar o circular libremente peatones y vehículos.

l) Espacio o lugar público: cualquier área o lugar de acceso abierto destinado a ser utilizado por el público en general como por ejemplo pasajes, parques, jardines y otros espacios o zonas verdes o forestales, puentes, túneles y pasos subterráneos, playas y cualquier otro lugar o espacio público, sea abierto o cerrado, o de uso público.

Artículo 3
Ámbito subjetivo

1. Esta Circular es de aplicación a los tratamientos con fines de videovigilancia que llevan a cabo:

a) Las instituciones públicas de Cataluña.

b) La Administración de la Generalidad.

c) Los entes locales de Cataluña.

d) Las entidades autónomas, los consorcios y las demás entidades de derecho público vinculadas a la Administración de la Generalidad o a los entes locales, o dependientes de ella.

e) Las entidades de derecho privado que cumplan, como mínimo, uno de los tres requisitos siguientes con relación a la Generalidad, a los entes locales o a los entes que dependen de ella:

Primero. Que su capital pertenezca mayoritariamente a dichos entes públicos.

Segundo. Que sus ingresos presupuestarios provengan mayoritariamente de dichos entes públicos.

Tercero. Que en sus órganos directivos, los miembros designados por dichos entes públicos sean mayoría.

f) Las demás entidades de derecho privado que prestan servicios públicos por medio de cualquier forma de gestión directa o indirecta, si se trata de tratamientos vinculados a la prestación de estos servicios.

g) Las universidades públicas y privadas que integran el sistema universitario catalán, y los ente que dependen de ella.

h) Las personas físicas o jurídicas que cumplen funciones públicas con relación a materias que son competencia de la Generalidad o de los entes locales, si se trata de tratamientos destinados al ejercicio de estas funciones y el tratamiento se lleva a cabo en Cataluña.

i) Las corporaciones de derecho público que cumplen sus funciones exclusivamente en el ámbito territorial de Cataluña.

2. Esta Circular 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.

Artículo 4
Régimen aplicable

1. Esta Circular se aplica a los tratamientos de imágenes y voces comprendidos en el ámbito de aplicación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento 2016/679) y la Ley Orgánica 3/2018, de 5 de diciembre.

2. También se aplica, supletoriamente respecto a su normativa específica, a los tratamientos de imágenes y voces obtenidos por las Fuerzas y Cuerpos de Seguridad, por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación y disciplina del tráfico, cuando el tratamiento no tenga como finalidad la prevención, detección, investigación y enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención ante las amenazas contra la seguridad pública.

3. Lo establecido en esta Circular 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 demás normativa aplicable.

Capítulo 2
Principios aplicables al tratamiento de videovigilancia

Artículo 5
Licitud del tratamiento

1. Para el tratamiento de imágenes, o en su caso de voces, mediante cámaras o sistemas de videovigilancia para el cumplimiento de alguna de las finalidades de videovigilancia previstas en el artículo 2.e) de esta Circular, es necesario que concurra alguna de las bases jurídicas previstas en el artículo 6.1 del Reglamento 2016/679.

2. El tratamiento de las imágenes obtenidas a través de cámaras o sistemas de videovigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de las instalaciones puede tener habilitación legal en los términos y condiciones establecidos por el artículo 22 de la Ley Orgánica 3/2018.

3. El tratamiento de las imágenes obtenidas a través de cámaras o sistemas de cámaras para el ejercicio de las funciones de control de los trabajadores o de los empleados públicos puede tener habilitación legal en los términos y condiciones establecidos por el artículo 89 de la Ley Orgánica 3/2018.

4. Sólo se pueden captar imágenes que puedan revelar el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, datos genéticos, datos biométricos destinados a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, si concurre, adicionalmente a lo establecido en el apartado 1 de este artículo, alguna de las excepciones previstas en el artículo 9.2 del Reglamento 2016/679.

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

5. La utilización de cámaras o sistemas de videovigilancia por parte de la Policía de la Generalidad-Mossos d'Esquadra o por las policías locales de Cataluña requiere la autorización correspondiente en los supuestos previstos en su normativa específica. La cesión o copia de las imágenes y voces captadas por estos sistemas se rige por aquello que prevé su normativa específica.

6. No es considera legítima:

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

b) La captación de imágenes de la vía o lugar público, salvo que:

- La lleven a cabo las fuerzas y cuerpos de seguridad de acuerdo con su normativa específica.
- La lleven a cabo empresas de seguridad privada de acuerdo con su normativa específica.
- Se trate de una captación incidental para la vigilancia de edificios o instalaciones, si resulta inevitable para alcanzar la finalidad de vigilancia del edificio o instalación.
- Sea necesario para garantizar la seguridad de bienes o instalaciones estratégicas o de infraestructuras vinculadas al transporte.

c) La captación de imágenes o voces en baños o vestuarios, ni en lugares destinados al descanso o el recreo de los trabajadores o los empleados públicos como comedores salas de ocio y similares.

d) La captación de imágenes o voces en habitaciones de residencias, albergues, hoteles y similares. Eso 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 puede no ser proporcionada, salvo que exista un interés legítimo superior que lo justifique.

Artículo 6
Limitación de la finalidad

De acuerdo con el principio de limitación de la finalidad, las imágenes, y en su caso las voces, sólo se pueden captar y tratar a través de sistemas de videovigilancia para fines determinados, explícitos y legítimos.

Las imágenes, y si procede las voces, captadas para una finalidad determinada no pueden utilizarse de manera incompatible con aquella finalidad.

Artículo 7
Minimización

1. El tratamiento de la imagen, y especialmente de la voz, de las personas físicas con finalidades de vigilancia sólo se puede considerar proporcionado cuando sea adecuado y necesario para alcanzar la finalidad perseguida. Sólo se puede optar por medidas de videovigilancia si la finalidad del tratamiento no se puede obtener con otros medios que resulten menos intrusivos para los derechos y las libertades fundamentales de las personas.

El factor económico no debe ser el único elemento a tener en cuenta para analizar la proporcionalidad y la conveniencia de establecer un sistema de videovigilancia.

Este mismo principio de intervención mínima también debe aplicarse 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.

2. Con carácter previo a la instalación, el responsable del sistema de videovigilancia debe ponderar los diferentes derechos y bienes jurídicos en juego analizando:

a) La necesidad de utilizar estos sistemas para alcanzar la finalidad perseguida.
b) La idoneidad de la instalación de sistemas de videovigilancia para alcanzar la finalidad perseguida, asegurando que es el medio más efectivo y proporcional para conseguir los objetivos establecidos.
c) El riesgo que puede suponer para los derechos de las personas, dadas 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, considerando otros métodos menos invasivos que podrían ser igualmente eficaces.
e) Si las características de configuración del sistema permiten alcanzar la finalidad perseguida de la manera menos intrusiva por los derechos de las personas afectadas, como, entre otros, el número de cámaras, la utilización de técnicas de reconocimiento facial o de voz, emplear la mera visualización en tiempo real, cajas negras, el campo de visión y la posibilidad de emplear máscaras para enfocar determinadas áreas, la movilidad del campo de visión, el grado de definición de las imágenes o el zoom.

Esta ponderación debe documentarse en la Memoria prevista en el artículo 9 de esta Circular o, en su caso, en la evaluación de impacto relativa a la protección de datos.

3. Puede resultar no adecuada al principio de proporcionalidad:

a) La utilización de sistemas de videovigilancia en el ámbito laboral con la finalidad exclusiva de controlar el rendimiento de las personas trabajadoras de manera continuada.

b) La instalación, en el ámbito educativo, de cámaras en el interior de las aulas, gimnasios o espacios de ocio del alumnado para su control salvo que, excepcionalmente haya un interés superior que lo justifique.

c) La captación de imágenes con finalidad de difusión cultural o turística, o con el fin de ofrecer información meteorológica, del tráfico u otras análogas que permitan la identificación de personas concretas.

d) Tratar de manera generalizada las imágenes o voces obtenidas con sistemas de videovigilancia mediante técnicas específicas de reconocimiento facial o de otros tipos de análisis basados en datos biométricos.

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 proporcionada, con carácter excepcional, cuando no se trate de conversaciones estrictamente privadas, y la finalidad de vigilancia no se pueda alcanzar mediante la grabación, de forma exclusiva, de la imagen. Los motivos que justifican la grabación de la voz deben constar en la Memoria prevista en el artículo 9 de esta Circular o, en su caso, en la evaluación de impacto relativa a la protección de datos.

En el ámbito laboral la grabación de voces en el puesto de trabajo se admite únicamente cuando sean relevantes los riesgos para la seguridad de las instalaciones, los bienes y las personas derivados de la actividad que se lleve a cabo en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías que prevé la normativa de protección de datos.

Si accidentalmente se registran conversaciones de naturaleza estrictamente privada, hay que suprimirlas, salvo que se cuente con el consentimiento de la persona interesada u otra base jurídica que habilite la conservación.

Artículo 8
Conservación

1. Cuando 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. En cualquier caso, las grabaciones deben ser suprimidas en el plazo máximo de un mes desde su captación, salvo que deban conservarse por:

a) Acreditar la comisión de actos que atenten contra la integridad de las personas, bienes o instalaciones. En estos casos las grabaciones deben ponerse a disposición de las autoridades competentes en un plazo máximo de setenta y dos horas desde que se tenga conocimiento de su existencia.

b) Exigir las responsabilidades oportunas.

2. A los tratamientos en materia de videovigilancia no les es de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018.

3. Cuando, accidentalmente, se capten imágenes o voces en circunstancias que comporten su ilicitud, deben suprimirse de manera inmediata tan pronto como se tenga conocimiento.

4. Cuando no se pueda atender una solicitud de acceso antes de que transcurra el plazo de conservación de las imágenes o voces, debe conservarse una copia de las imágenes afectadas hasta que se entreguen a la persona afectada o, en caso de desestimación, hasta un plazo de dos meses desde que se notifique la denegación de la solicitud.

5. La conservación de las imágenes y voces sometidas a la legislación sobre videovigilancia de la Policía de la Generalidad-Mossos d'Esquadra o las policías locales de Cataluña se rige por su normativa específica.

Capítulo 3
Obligaciones del responsable

Artículo 9
Memoria

1. Con carácter previo a la puesta en marcha del sistema de videovigilancia debe elaborarse una memoria que debe referirse, como mínimo, a los siguientes aspectos:

a) Órgano, organismo o entidad responsable: identificar a la persona responsable del tratamiento, a las personas operadoras del sistema de videovigilancia, así como, si procede, de la persona responsable de la instalación y de su mantenimiento.

b) Justificación de la licitud de la captación y de los tratamientos posteriores que se prevean: hay que hacer constar cuál o cuáles de los apartados del artículo 6.1 del Reglamento 2016/679 concurre en el caso concreto, para legitimar el tratamiento de las imágenes y voces y, si procede, la norma con rango de ley, o bien disposición de la Unión Europea, en que se basa.

c) Justificación de la finalidad y de la proporcionalidad del tratamiento, de acuerdo con lo establecido en los artículos 6 y 7 de esta Circular. Si se han producido incidentes de seguridad que justifiquen la instalación del sistema, conviene concretarlos.

d) Datos personales tratados: indicar si se registrará también la voz y si la finalidad comporta, previsiblemente, la captación de imágenes que revelen categorías especiales de datos o datos de menores u otros datos sensibles.

e) Ubicación y campo de visión de las cámaras: hay que hacer referencia a la ubicación y orientación de las cámaras. En particular, cuando se trate de cámaras en el exterior, se debe hacer 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 o centros de atención a personas con discapacidad.

También se debe hacer 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:

- El nombre total de càmeres que formen el sistema.
- Las condiciones técnicas de las cámaras y 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, dónde y por quién, o sólo se registran, con acceso limitado a determinados supuestos previstos en la Memoria.
- Si la captación, y si procede la grabación, se hace de manera continuada o discontinua sólo por determinados periodos o franjas horarias.
- Si las imágenes se transmiten.
- Previsiones relativas a los mecanismos de identificación y de anonimización para atender el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, y oposición.
- Cuando se grabe la voz, también hay que especificar la distancia a la que se puede registrar.
- Si se emplearán procedimientos técnicos específicos para el análisis de datos biométricos o de análisis de las conversaciones.

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

h) Periodo de tiempo de instalación del sistema y periodo de conservación de las imágenes.

i) Protocolo para la comunicación de las imágenes o voces a terceras personas que las soliciten.

j) Medidas previstas para evaluar la eficacia del sistema y la necesidad de su mantenimiento dada la finalidad perseguida.

k) Medidas de seguridad: análisis de los riesgos que comporta el tratamiento de videovigilancia que se quiere llevar implantar y la descripción de las medidas de seguridad técnicas y organizativas aplicadas para garantizar un nivel de seguridad adecuado al riesgo.

l) Acciones formativas previstas para el personal que tenga que intervenir en la gestión del sistema.

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

3. Esta memoria debe elaborarse también cuando el tratamiento de la imagen, y en su caso de la voz, sea accesorio de otro tratamiento. En este supuesto, hay que especificar y justificar esta circunstancia.

4. La Memoria debe estar a disposición de la Autoridad Catalana de Protección de Datos.

Artículo 10
Evaluación de impacto relativa a la protección de datos

1. Cuando la videovigilancia implique una observación sistemática a gran escala de una zona de acceso público o cuando pueda conllevar un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento debe hacer una evaluación de impacto relativa a la protección de datos.

Para determinar la posible existencia de un alto riesgo hay que tener en cuenta, entre otras, la concurrencia de alguna de las operaciones de tratamiento incluidas en la lista publicada por esta Autoridad de acuerdo con el artículo 35.4 del Reglamento (UE) 2016/679.

2. La evaluación de impacto relativa a la protección de datos sustituye a la Memoria prevista en el artículo 9 de esta Circular.

3. Cuando el resultado de la Evaluación de impacto indique que, a pesar de las medidas previstas, el tratamiento de datos comporta un alto riesgo, el responsable debe hacer una consulta previa a la Autoridad Catalana de Protección de Datos. La consulta debe ir acompañada de la siguiente información:

a) Responsabilidades respectivas del responsable, de los corresponsables y de los encargados implicados en el tratamiento.
b) Finalidades y medios del tratamiento previsto.
c) Medidas y garantías establecidas para proteger los derechos y las libertades de las personas interesadas.
d) Datos de contacto del delegado de protección de datos, si procede.
e) Documento de evaluación de impacto relativa a la protección de datos.

La Autoridad Catalana de Protección de Datos puede solicitar cualquier información que considere necesaria relativa al tratamiento.

Artículo 11
Registro de actividades de tratamiento

Los responsables y encargados del tratamiento de los sistemas de videovigilancia que capten imágenes o voces, con independencia de que se registren o no, deben incluir el tratamiento en el Registro de actividades de tratamiento a que se refiere el artículo 30 del Reglamento 2016/679.

Se puede incluir como una única actividad de tratamiento un sistema de videovigilancia integrado por una o por varias cámaras en una misma instalación o en varias instalaciones siempre que sean equiparables y con una misma finalidad.

Artículo 12
Delegado de protección de datos

Los responsables del tratamiento que tengan como actividad principal operaciones de tratamiento que por su naturaleza, alcance y/o finalidades requieran la observación habitual y sistemática de interesados a gran escala deben designar un delegado de protección de datos. Ello sin perjuicio de los demás supuestos en que sea exigible de acuerdo con la normativa vigente.

Artículo 13
Encargo del tratamiento.

1. En el caso de que se produzca un acceso a las imágenes o voces captadas por un sistema de videovigilancia, por terceras personas que actúan por cuenta del responsable del tratamiento, es necesario formalizar un contrato de encargo del tratamiento entre el responsable y el tercero autorizado con el contenido previsto en el artículo 28.3 del Reglamento 2016/679. En el caso de entidades sometidas a la normativa de contratación pública, hay que incluir también las previsiones que establece esta normativa.

El responsable del tratamiento está obligado a escoger un encargado del tratamiento que ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas de acuerdo con el Reglamento 2016/679. La adhesión a códigos de conducta u otros mecanismos de certificación se pueden utilizar como prueba para demostrar que el encargado del tratamiento ofrece garantías suficientes.

2. Cuando un responsable del tratamiento implante un sistema de videovigilancia que comporte el acceso de una empresa de seguridad privada a las imágenes o voces que se capten, ésta tendrá la consideración de encargado del tratamiento.

Cuando se trate de un sistema instalado en una vivienda para una finalidad personal o doméstica y el control del sistema se haga a través de una central de alarmas de una empresa de seguridad, ésta tendrá la consideración de responsable del tratamiento.

Capítulo 4
Transparencia

Artículo 14
Información a las personas afectadas

1. Los responsables del tratamiento de sistemas de videovigilancia deben informar de manera clara y permanente sobre la existencia de las cámaras mediante la colocación de los carteles informativos que sean necesarios para garantizar su conocimiento por las personas afectadas. Esta obligación es exigible igualmente cuando las imágenes captadas no se registren.

2. Los carteles informativos deben colocarse antes del inicio de la captación de imágenes y voces, incluso si se trata de pruebas, y sólo se pueden retirar una vez que el sistema haya sido des instalado.

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 condiciones siguientes:

- Para las cámaras de videovigilancia en edificios o instalaciones, hay que colocar un cartel informativo en cada uno de los accesos al área videovigilada. Si los edificios están divididos por plantas con diferentes responsables o con finalidades diferentes, también hay que colocar otro cartel informativo en cada una de las plantas con cámaras, ubicado en un espacio de acceso principal al área o zona videovigilada de la planta.

- Para las cámaras de videovigilancia en el transporte público, hay que colocar, 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, es necesario colocar un cartel informativo a una distancia suficiente para que las personas afectadas tengan 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.

La ubicación de los carteles debe permitir a las personas afectadas prever cuáles son las áreas vigiladas.

4. El contenido y el diseño del cartel informativo debe ajustarse a lo establecido en el Anexo de esta Circular. Debe incluir, como mínimo, la existencia del tratamiento de datos, la identidad del responsable del tratamiento, el lugar donde se puede obtener más información y la posibilidad de ejercer los derechos previstos en el Reglamento 2016/679, sin que en ningún caso sea exigible que se especifique el emplazamiento de las cámaras. Asimismo, se puede incluir un código de conexión o una dirección de internet para acceder al resto de información que hay que facilitar a las personas interesadas.

5. El cartel informativo se puede sustituir por información ofrecida a través de pantallas electrónicas, siempre que éstas muestren una imagen fija del cartel o éste aparezca, de manera legible con una frecuencia que garantice su conocimiento por las personas afectadas.

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

7. La persona responsable del tratamiento, o quien designe en su lugar, debe mantener a disposición de las personas afectadas, en un lugar fácilmente accesible, información sobre la finalidad del sistema de videovigilancia y sobre el resto de aspectos establecidos en el artículo 13 del Reglamento 2016/679. Esta información se puede ofrecer a través de impresos o en un apartado o espacio del sitio web o sede electrónica.

8. De manera complementaria, se pueden utilizar otros medios adicionales para cumplir el deber de información como el uso de sistemas de megafonía, para asegurar que todas las personas tengan conocimiento de ellos.

9. En el caso de los sistemas de videovigilancia para control laboral, además, se informará con carácter previo y de manera expresa clara y concisa a los trabajadores o empleados públicos y, en su caso, a sus representantes. Cuando se capte la comisión flagrante de actos ilícitos por parte de los trabajadores o empleados públicos, se entenderá cumplido el deber de informar mediante el cartel a que se refieren los apartados 1 a 5 de este artículo.

10. En las cámaras fijas para el control, la regulación, la vigilancia y la disciplina del tráfico en la vía pública, el contenido del cartel puede limitarse a informar de la existencia de la cámara o el dispositivo de control de velocidad o de control del tráfico, sin perjuicio de lo establecido en el apartado 7 de este artículo.

11. En el caso de las cámaras móviles, incluidas las instaladas en aeronaves no tripuladas (drones), vehículos o indumentaria de las personas, hay que informar de su existencia mediante carteles en los accesos a las zonas videovigiladas o, si esto no es posible, a través de otros medios.

12. El cumplimiento del deber de información en los tratamientos sometidos a la legislación sobre videovigilancia de la Policía de la Generalidad-Mossos d'Esquadra o por las policías locales de Cataluña se rige por su normativa específica.

Capítulo 5
Derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición

Artículo 15
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 el responsable del tratamiento le informe sobre si su imagen o voz ha sido captada a través de sistemas de videovigilancia y, en caso afirmativo, a la siguiente información:

a) Las imágenes o voces registradas y, en su caso, las elaboraciones posteriores que se haya hecho.

   Si el acceso afecta también a imágenes o voces de terceras personas, salvo que se cuente con su consentimiento, el acceso requiere la previa anonimización de las imágenes y las voces de las mismas con cualquier medio que impida su identificación, como por ejemplo el enmascaramiento. Cuando la anonimización exija esfuerzos desproporcionados en atención al lapso temporal registrado o el elevado número de terceras personas afectadas, el responsable puede solicitar que se reduzca el periodo de grabación al que se pretenda tener acceso.

b) La finalidad del tratamiento.

c) Si la imagen o la voz se almacenan o sólo se visionan.

d) El período de conservación de las imágenes o voces.

e) Si se ha hecho o se ha previsto hacer alguna comunicación, incluidas las transferencias a un tercer país o una organización internacional.

f) La existencia del derecho a solicitar la rectificación, la supresión, la limitación del tratamiento o a oponerse a este tratamiento.

g) El derecho a presentar una reclamación ante una autoridad de control.

h) La existencia de decisiones automatizadas, incluida la elaboración de perfiles, en su caso.

Artículo 16
Derecho de rectificación

1. Se puede ejercer el derecho de rectificación de las imágenes o la voz captadas con sistemas de videovigilancia cuando:

a) La imagen o la voz hayan sido distorsionadas o alteradas con posterioridad a su captación.

b) Los sistemas de datación hayan asociado una hora o fecha incorrectas a la imagen.

2. Para dar cumplimiento a lo previsto en la letra a) del apartado anterior, 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, con indicación del periodo afectado y el motivo.

Artículo 17
Derecho de supresión

Mediante el derecho de supresión la persona titular puede solicitar al responsable del tratamiento la supresión de las imágenes o voces registradas, de acuerdo con lo establecido en el artículo 17 del Reglamento 2016/679.

Cuando el motivo de supresión lo requiera, el responsable debe comunicar la solicitud de supresión a los demás responsables del tratamiento a quienes haya comunicado las imágenes o voces.

Artículo 18
Derecho a la limitación del tratamiento

Mediante el derecho de limitación del tratamiento la persona titular de la imagen o la voz puede solicitar al responsable del tratamiento que conserve las imágenes o la voz cuando:

a) La persona interesada ha impugnado la exactitud de sus datos personales, durante el plazo que permita al responsable verificar su exactitud.

b) El tratamiento es ilícito y la persona interesada se opone a la supresión de sus datos personales y, en lugar de suprimirlos, solicita que se limite su uso.

c) El responsable ya no necesita los datos personales para las finalidades del tratamiento, pero la persona interesada los necesita para formular, ejercer o defender reclamaciones.

d) La persona interesada se ha opuesto al tratamiento basado en un interés legítimo o en el ejercicio de una misión en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los de la persona interesada.

Artículo 19
Derecho de oposición

1. Mediante el derecho de oposición la persona titular de la imagen o voz puede solicitar, antes de la captación o una vez que se haya producido, por motivos relacionados con su situación particular, la exclusión o el cese del tratamiento de su imagen o voz, salvo que el responsable del tratamiento acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los derechos o intereses legítimos de la persona interesada o por la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de la imagen o voz tiene por objeto el marketing, la persona interesada tiene derecho a oponerse en cualquier caso al tratamiento de los datos personales que le afectan, incluida la elaboración de perfiles con esta finalidad.

Artículo 20
Procedimiento de ejercicio de los derechos

1. Para ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición, es necesario formular una solicitud dirigida al responsable del tratamiento o, en su caso, al encargado del tratamiento. La solicitud debe indicar el lugar, la fecha y la hora aproximada, en franjas no superiores a dos horas, en las que su imagen pudo ser captada. Debe acompañarse de una imagen de la persona solicitante que corresponda al período en que se captó, de manera que permita identificarla.

2. En los sistemas de videovigilancia que registran la voz, el derecho de acceso se puede ejercer aportando una grabación de la voz de la persona afectada.

3. Si la imagen o la voz aportada no ofrece suficiente definición o elementos para permitir la identificación, se debe otorgar un plazo de enmienda de 10 días hábiles para que pueda aportarse otra imagen o grabación de la voz.

4. La tramitación y la respuesta de la solicitud se rige por lo establecido en la normativa de protección de datos personales y por esta Circular. La obligación de responder existe incluso si las imágenes no han sido registradas o ya han sido suprimidas en el momento de ejercer el derecho. En este último caso, la respuesta puede limitarse a exponer esta circunstancia y a informar de la imposibilidad material de satisfacer el derecho ejercido.

5. La solicitud de ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición puede ser denegada si no concurren los requisitos exigibles, o si el nivel de coincidencia entre la imagen o la voz aportada con la solicitud y las que hayan sido objeto de tratamiento no permiten asegurar que se trata de la misma persona. También puede denegarse cuando no hayan sido registradas o ya hayan sido suprimidas.

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 para la tutela de sus derechos ante la Autoridad Catalana de Protección de Datos.

7. Previamente, y con carácter potestativo, las personas interesadas pueden dirigirse al delegado de protección de datos del responsable del tratamiento que debe responder en el plazo de dos meses.

Artículo 21
Imágenes y voces captadas por las Fuerzas y Cuerpos de Seguridad

1. Cuando el tratamiento no tenga como finalidad la prevención, detección, investigación y enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención ante las amenazas contra la seguridad pública, el ejercicio de los derechos de acceso y supresión de imágenes o voces tratadas por cámaras sometidas a la legislación sobre videovigilancia de la Policía de la Generalidad-Mossos d'Esquadra o las policías locales de Cataluña se rige por su normativa específica.

2. Los derechos de limitación del tratamiento, rectificación y oposición en relación con imágenes captadas por las cámaras de las que son responsables los cuerpos policiales mencionados se ejercen de acuerdo con lo establecido en el Reglamento 2016/679 como también por lo establecido en la presente Circular.

3. Cuando el tratamiento tenga como finalidad la prevención, detección, investigación y enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención ante las amenazas contra la seguridad pública, el ejercicio de los derechos de los interesados se rige por la Ley Orgánica 7/2021.

Capítulo 6
Seguridad de los datos personales

Artículo 22
Obligaciones del responsable del tratamiento

1. El responsable del tratamiento, así como el encargado del tratamiento, teniendo en consideración el estado de la técnica, los costes de su aplicación y los riesgos para los derechos y libertades de las personas, deben adoptar las medidas técnicas y organizativas necesarias para alcanzar un nivel de seguridad adecuado al riesgo, que permita garantizar la autenticidad, la integridad, la disponibilidad y la confidencialidad de las imágenes captadas mediante sistemas de cámaras de videovigilancia, así como la resiliencia de estos sistemas y que eviten su alteración, pérdida, acceso indebido o tratamiento no autorizado.

2. Los responsables a que se refiere el artículo 77 de la Ley Orgánica 3/2018, al determinar las medidas de seguridad aplicables deben tener en cuenta el Esquema Nacional de Seguridad.

3. Si se produce una violación de la seguridad que afecte a los tratamientos de videovigilancia que pueda comportar la destrucción, la pérdida o alteración accidental o ilícita de las imágenes o voces, la comunicación o el acceso no autorizado a estos datos, el responsable del tratamiento, debe notificarlo a la Autoridad Catalana de Protección de Datos sin dilación indebida y siempre antes de 72 horas desde que tenga constancia, salvo que sea improbable que constituya un riesgo para los derechos y las libertades de las personas.

Cuando comporte un alto riesgo, también debe comunicarlo a las personas afectadas, salvo que concurra alguna de las excepciones previstas en el artículo 34.3 del Reglamento 2016/679.

4. Las previsiones contenidas en este capítulo son exigibles también a los tratamientos llevados a cabo mediante los sistemas de videovigilancia de los que son responsables la Policía de la Generalidad-Mossos d'Esquadra o las policías locales de Cataluña, cuando el tratamiento no tenga como finalidad la prevención, detección, investigación y enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención ante las amenazas contra la seguridad pública, en defecto de normativa específica.

Artículo 23
Medidas de seguridad

1. En la definición de las medidas a aplicar de acuerdo con lo establecido en el apartado primero del artículo anterior, hay que tener en cuenta, entre otros, los siguientes aspectos:

a) Documentar a las personas o perfiles de personas usuarias que pueden manipular las cámaras y también las que pueden visualizar las imágenes, en tiempo real o grabadas. También hay que definir a las personas que puedan llevar a cabo operaciones de borrado, destrucción, conservación, identificación, distorsión o cualquier otra manipulación de las imágenes, así como el personal que puede autorizar, modificar o revocar el acceso de terceros. En caso de perfiles que incluyan un alto número de personas usuarias, hay que limitar su número.

b) Disponer de un registro de accesos a las imágenes conservadas que permita la identificación del usuario que intenta acceder al sistema o archivo, su perfil de usuario, la fecha y la hora del intento, las funciones que intenta realizar y si ha sido autorizado o no. Si el acceso ha sido autorizado, también hay que registrar las imágenes a las que se ha accedido, identificadas con la fecha y el intervalo horario que se ha visualizado.

c) La persona responsable del 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, así como para atender el ejercicio de los derechos de las personas mediante un procedimiento ágil.

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

e) El responsable debe informar a las personas que tengan acceso a las imágenes en ejercicio de sus funciones, que deben observar el deber de confidencialidad, y que esta obligación subsiste incluso después de haber finalizado su relación de servicio.

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

g) Garantizar la seguridad física de los sistemas ante cualquier manipulación o robo.

h) Usar sistemas de encriptación de las imágenes que se conservan y software antivirus. Si el sistema está conectado a internet o a otro sistema de información hay que usar cortafuegos, software de detección de intrusiones y, si es necesaria la comunicación, establecer canales seguros de comunicación. También hay que tener en cuenta las actualizaciones de seguridad del sistema disponibles.

i) Para garantizar la integridad de las imágenes y facilitar el ejercicio de los derechos, es necesario incorporar un sistema de datación que indique el día y hora en que han sido captadas.

j) Establecer mecanismos de revisión periódica del registro de accesos y del funcionamiento del sistema.

2. Cuando no se almacenan las imágenes, las medidas de seguridad deben adoptarse igualmente, en lo que sea aplicable.

Disposición transitoria

Carteles informativos

La utilización del cartel a que se refiere el artículo 14, con el contenido y el diseño que se concreta en el Anexo de esta Circular, es exigible a los carteles que deban instalarse a partir de su entrada en vigor.

Los carteles existentes que se adecuen a lo establecido en la Instrucción 1/2009 mantienen su vigencia hasta que se produzca su sustitución.

Disposición derogatoria

Se deroga la Instrucción 1/2009, de 6 de febrero de 2009, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia,

Disposición final
Entrada en vigor

Esta Circular entrará en vigor el día siguiente a su publicación en el Diari Oficial de la Generalitat de Catalunya.

Barcelona, ... de ..... de

Directora

ANEXO

1. En el cartel informativo a que se refiere el artículo 14 de esta Circular debe hacerse constar de forma claramente visible, de arriba abajo, como mínimo la siguiente información:

- La indicación "ZONA VIDEOVIGILADA"
- El texto informativo "PROTECCIÓN DE DATOS"
- Un pictograma que simboliza una cámara de videovigilancia dentro de un rectángulo blanco. Cuando se capte la voz, el pictograma debe reflejar esta circunstancia.
- La identificación del responsable del tratamiento
- La posibilidad de ejercer los derechos de acceso, rectificación, limitación, supresión y oposición.
- Indicación del sitio o web, o código de conexión (QR o de otro tipo) para conseguir de manera fácil la información a que se refiere el apartado 6 del artículo 14 de esta Circular.

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

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

Estas dimensiones pueden aumentar o disminuir según sea el área o zona sometida a videovigilancia y la distancia que sea necesaria para que el distintivo 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 Autoridad 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 (DIN A4), se sitúa aproximadamente a 6 cm. del lado superior, debe constar el pictograma a que se refiere el apartado 1 de este Anexo.

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

3. En la página web de la Autoridad Catalana de Protección de Datos (incluir enlace), hay disponibles modelos de cartel ajustados a los requisitos que establece este Anexo, que se pueden descargar.