

ESTUDIOS



VIDEOVIGILANCIA POR SEGURIDAD CIUDADANA EN EL ÁMBITO PÚBLICO DE EUSKADI

Análisis desde la perspectiva de los derechos
fundamentales

ENERO, 2024

ararteko

Herriaren Defendatzailea
Defensoría del Pueblo



Esta obra está bajo una licencia [Creative Commons Reconocimiento 4.0 Internacional](https://creativecommons.org/licenses/by/4.0/) (CC BY 4.0)



Para acceder a las publicaciones del Ararteko:

- [en la web](#)
- [mediante solicitud por correo electrónico](#)
- presencialmente en cualquiera de las tres oficinas, por escrito (Prado 9, 01005 Vitoria-Gasteiz) o por teléfono (945 13 51 18)

ARARTEKO



Índice

I. Acrónimos de normativa y organismos.....	5
II. Presentación.....	7
III. Objetivo, metodología y marco normativo del estudio.....	9
III.1. Objetivo.....	9
III.2. Metodología y estructura del estudio.....	10
III.3. Marco jurídico.....	13
III.4. Pronunciamientos del ararteko en la materia.....	17
IV. Resultados del estudio y evaluación.....	20
IV.1. Estadísticas de número de cámaras, tipo y ubicación.....	20
IV.1.1. Resultados.....	20
IV.1.2. Análisis y valoración.....	23
IV.2. Finalidades y normas habilitantes de la videovigilancia.....	27
IV.2.1. Resultados.....	27
IV.2.2. Análisis y valoración.....	29
IV.3. Régimen de autorización de la videovigilancia.....	32
IV.3.1. Resultados.....	32
IV.3.2. Análisis y valoración.....	35
IV.4. El principio de proporcionalidad.....	41
IV.5. Gestión de las grabaciones de videovigilancia y plazos de conservación.....	47
IV.5.1. Resultados.....	47
IV.5.2. Análisis y valoración.....	51
IV.6. Principio de información.....	54
IV.6.1. Resultados.....	54
IV.6.2. Análisis y valoración.....	56
IV.7. Ejercicio y atención de derechos de la ciudadanía.....	59
IV.7.1. Resultados.....	59
IV.7.2. Análisis y valoración.....	61
IV.8. Obligaciones básicas de protección de datos.....	64
IV.8.1. Resultados.....	64
IV.8.2. Análisis y valoración.....	66
IV.9. Medidas de seguridad.....	71
IV.9.1. Resultados.....	71
IV.9.2. Análisis y valoración.....	72



V. Conclusiones	75
V.1. Aspectos generales y marco regulatorio.....	76
V.2. Finalidades de la videovigilancia y normas habilitantes.....	77
V.3. Sobre el régimen de autorización de la videovigilancia por seguridad ciudadana.....	78
V.4. El principio de proporcionalidad.....	79
V.5. La gestión de las grabaciones y los plazos de conservación...	79
V.6. Publicidad y transparencia en el ámbito de la actuación de la administración.....	80
V.7. Ejercicio y atención de derechos de la ciudadanía.....	81
V.8. Obligaciones básicas de protección de datos.....	82
V.9. Medidas de seguridad.....	83
VI. Recomendaciones	84
VI.1. Aspectos generales y marco regulatorio.....	84
VI.2. Finalidades perseguidas con la videovigilancia y las normas habilitantes.....	85
VI.3. Autorizaciones de videovigilancia por seguridad ciudadana....	85
VI.4. Principio de proporcionalidad.....	86
VI.5. Gestión de grabaciones y plazos de conservación.....	87
VI.6. Publicidad y transparencia.....	87
VI.7. Atención de derechos de la ciudadanía.....	87
VI.8. Protección de datos personales.....	88
VI.9. Medidas de seguridad de la información.....	88
VII. Anexo: Cuestionario	89



I. Acrónimos de normativa y organismos

A continuación, se reseñan con carácter general las normas utilizadas en el presente estudio y los organismos y órganos aludidos con los acrónimos utilizados para hacer las referencias.

NORMAS:

- Constitución Española de 1978 (CE).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD).
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. (LOHP)
- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (LOVFCS).
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- 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 (LO 7/21).
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTBG)
- Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos (LVPD).
- Decreto Legislativo 1/2020, de 22 de julio, por el que se aprueba el texto refundido de la Ley de Policía del País Vasco (LPPV).



- Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos (Real Decreto 596/1999).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Decreto 168/1998, de 21 de julio, desarrolla el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos (Decreto 168/98).
- Orden de 15 de abril de 2011, del Consejero de Interior, por la que se establece el contenido y diseño de los carteles informativos de la instalación y uso de videocámaras fijas por la Policía del País Vasco.
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

ÓRGANOS Y AUTORIDADES

- Agencia vasca de protección de datos (AVPD)
- Agencia española de protección de datos (AEPD)
- Comisión de Videovigilancia y Libertades (CVL)
- Cuerpo de Policía de la Comunidad Autónoma de Euskadi o Ertzaintza y Cuerpos o servicios de Policía local dependientes de las entidades locales del País Vasco o Udaltzaingoa (Policías o Policías del País Vasco)
- Viceconsejería del Departamento de Seguridad de Gobierno Vasco (VCS)



II. Presentación

El rápido desarrollo de la tecnología y su utilización en el ámbito cotidiano está teniendo impacto en el disfrute de los derechos fundamentales, tales como el derecho a la intimidad y a la protección de datos de carácter personal. Los sistemas fijos de videovigilancia y los dispositivos móviles como teléfonos, drones y cámaras disponen de capacidad para tomar imágenes y sonidos en cualquier contexto de relación pública o privada, lo que puede afectar a derechos de terceros. Su utilización debe gozar de legitimación suficiente para la captación de imágenes y sonidos y, muy especialmente para su difusión ulterior en distintos medios y canales de internet y redes sociales.

Las administraciones públicas participan plenamente en el desarrollo tecnológico y, específicamente, en el de los sistemas de videovigilancia. Cuando recurren a la videovigilancia tienen, de igual manera, el deber de hacerlo con pleno cumplimiento del principio de legalidad y pleno respeto del régimen de garantías de los derechos fundamentales y libertades públicas de la ciudadanía.

En ese contexto, el concepto de la seguridad ciudadana¹ ha sido erigido como garantía de que los derechos y libertades reconocidos y amparados por la Constitución puedan ser ejercidos libremente por la ciudadanía. Las policías² son el instrumento primordial para proteger ese ejercicio libre, mediante la prevención de actos delictivos, la protección de las personas y la conservación y custodia de bienes que se encuentren en situación de peligro, especialmente cuando las actuaciones perseguidas suceden en el espacio público.

Así, las administraciones públicas con competencia en materia de seguridad ciudadana se sirven de sistemas de grabación de imágenes y sonidos para incrementar el nivel de protección de los bienes y libertades de las personas y para la protección de la vida e integridad personal.

¹ [Preámbulo](#) de la LOPSC: “La Constitución Española de 1978 asumió el concepto de seguridad ciudadana (artículo 104.1), así como el de seguridad pública (artículo 149.1.29.º). Posteriormente, la doctrina y la jurisprudencia han venido interpretando, con matices, estos dos conceptos como sinónimos, entendiendo por tales la actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad ciudadana”

² De acuerdo con lo previsto en el [artículo 2.1 de la LPPV](#), y a los efectos del presente informe, se considera que las policías del País Vasco se integran por el Cuerpo de Policía de la Comunidad Autónoma de Euskadi o Ertzaintza, dependiente de la Administración de la Comunidad Autónoma de Euskadi, y los Cuerpos o servicios de Policía local dependientes de las entidades locales del País Vasco o Udaltzaingoa.



Sin embargo, el régimen de garantías en materia de videovigilancia afronta nuevos retos surgidos ante la aparición de tecnologías y desarrollos informáticos sin parangón. Se trata de dispositivos novedosos y avanzados que deben utilizarse de acuerdo con los principios básicos de actuación de las policías, por cuanto deben ejercer su función con absoluto respeto a la Constitución y al resto del Ordenamiento Jurídico, tal y como se prevé en el artículo [9.1](#) CE y [5.1.a\)](#) de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad).

La institución del Ararteko está sensibilizada con la garantía de los derechos de la ciudadanía en materia de protección de datos personales y de la intimidad en el marco de las relaciones con la administración cuando se producen captaciones de datos mediante tecnologías que pueden resultar particularmente intrusivas. Así, el uso de tecnologías de grabación de imágenes y sonidos de la ciudadanía para desarrollar las competencias propias de las administraciones, fundamentalmente en materia de seguridad ciudadana, debe de ser ponderado en función de los tipos de cámaras, fijas o móviles, y del ámbito de su utilización. A la hora de ponderar los intereses en juego, será preciso encontrar cual es la base jurídica legitimadora y, por añadidura, evaluar adecuadamente si se cumple, a la hora de utilizar esos instrumentos tecnológicamente avanzados, con el principio de proporcionalidad en su doble versión de idoneidad y de intervención mínima cuando el fin perseguido es la prevención, detección, investigación y enjuiciamiento de infracciones penales o la ejecución de sanciones penales previamente impuestas.

Es en ese marco donde tiene su encaje la elaboración del presente informe. Como resultado de su elaboración quedan identificados aspectos mejorables que podrán servir de base para una adecuada conciliación entre la protección de la seguridad ciudadana y el respeto de los derechos fundamentales de la ciudadanía.

Antes de terminar, el Ararteko desea agradecer sinceramente a todas las personas que, en representación del Gobierno Vasco y de los ayuntamientos de Euskadi (para mayor detalle, ver apartado de metodología), han colaborado en la elaboración de este estudio, facilitando los datos que han permitido llevarlo a cabo y aportando información que ha supuesto un valor añadido al estudio, redactado en clave de derechos fundamentales. Gracias a todos ellos por el espíritu de colaboración con el Ararteko que han demostrado, dedicando, su tiempo, diligencia y esfuerzo a que este trabajo pudiera ver la luz.

El estudio contiene 9 conclusiones y 16 recomendaciones organizadas por títulos en coherencia con las conclusiones alcanzadas.

Manuel Lezertua
Ararteko



III. Objetivo, metodología y marco normativo del estudio

III.1. Objetivo

La protección de los bienes y libertades de las personas mediante la defensa de la seguridad ciudadana puede representar un bien jurídico colectivo superior y por ello gozar de un régimen especial en el que puede encajar la captación de datos personales mediante sistemas de videovigilancia, sin embargo, las normas habilitantes establecen principios y reglas orientadas a garantizar que el tratamiento de datos personales resulte proporcional, oportuno, mínimo y suficiente para el cumplimiento de los fines perseguidos.

En los lugares públicos, la competencia para realizar funciones de videovigilancia con fines de protección de la seguridad de la ciudadanía se encuentra atribuida a las policías por lo que el uso de tecnología ha de acomodarse al régimen de garantías y autorizaciones que establece la normativa de utilización de videocámaras por las policías en lugares públicos.

Sin embargo, la videovigilancia es una medida que por su naturaleza puede resultar especialmente lesiva e intrusiva para las personas, principalmente en espacios públicos, por lo que parece adecuado realizar una reflexión previa sobre el alcance y la finalidad perseguida, a fin de legitimar la captación de imágenes y la grabación de sonidos y lograr su razonable convivencia con los derechos fundamentales que la normativa protege.

En concreto, la captación de imágenes y sonidos, implementados en sistemas fijos de videovigilancia, sistemas móviles instalados en uniformes policiales, teléfonos móviles, drones, báculos portátiles e incluso pistolas eléctricas que permiten grabar por tiempo, en ocasiones ilimitado, en formatos de gran calidad, de ampliación de imagen, de reconocimiento facial, entre otras características, comportan un desafío indudable para los órganos judiciales y entidades independientes como las autoridades de protección de datos, dado que la legislación difícilmente responde a estos novedosos desarrollos tecnológicos.

La ausencia de regulación europea en materia de videovigilancia en lugares públicos con fines de seguridad ciudadana, los escasos pronunciamientos judiciales, y en su caso, las carencias de la regulación de dispositivos **móviles** de videovigilancia,



motivan la realización del estudio, que tiene como fin fundamental ayudar a coherente distintos bienes jurídicos a salvaguardar, a saber, el interés público y misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana por las policías de acuerdo con el [artículo 104.1](#) de la CE y por lo otro lado, el derecho a la intimidad y a la protección de datos ([artículos 18.1 y 18.4](#) CE respectivamente). Asimismo, pretende contribuir a enriquecer y difundir entre las administraciones el conocimiento y aspectos mejorables en materia de garantía de derechos de la ciudadanía y, además, que la sociedad vasca conozca el modo de ejercer esos derechos y libertades públicas en el contexto de la videovigilancia.

El Ararteko ha estimado necesario realizar un estudio dirigido a las administraciones públicas de Euskadi con competencia en materia de seguridad ciudadana con el objetivo de analizar el uso de diferentes sistemas de videovigilancia **en lugares públicos** y el grado de cumplimiento del sistema de garantías establecido en la normativa.

El estudio se centra en analizar elementos relacionados con la toma de decisiones para implantar sistemas de videovigilancia y de las normas que habilitan y regulan su utilización.

En concreto, se estudian las finalidades de la utilización de cámaras de videovigilancia y su impacto en los derechos de la ciudadanía, así como el marco jurídico de la utilización y despliegue de cámaras mediante instalaciones **fijas** y **móviles** con fines de seguridad ciudadana, protección de instalaciones, bienes y personas, disciplina del tráfico y otros ámbitos.

Además, se realiza un contraste del régimen de autorización de las instalaciones **fijas** y **móviles**, los protocolos de atención de derechos de la ciudadanía, medidas de seguridad y conservación de grabaciones y otros aspectos normativos en materia de protección de datos.

III.2. Metodología y estructura del estudio

Para la realización del estudio el Ararteko ha realizado una encuesta a administraciones que disponen de policías; esto es al Departamento de Seguridad de Gobierno Vasco y a 14 ayuntamientos de diferente tamaño y ubicación entre los que se encuentran las capitales de los territorios históricos. En el [apartado VII](#), a modo de anexo, figuran las concretas cuestiones planteadas a las administraciones participantes.



La encuesta se remitió a las siguientes administraciones públicas:

- 1. Departamento de seguridad de Gobierno Vasco*
- 2. Ayuntamiento de Vitoria-Gasteiz*
- 3. Ayuntamiento de Bilbao*
- 4. Ayuntamiento de Donostia/San Sebastián*
- 5. Ayuntamiento de Barakaldo*
- 6. Ayuntamiento de Portugalete*
- 7. Ayuntamiento de Getxo*
- 8. Ayuntamiento de Basauri*
- 9. Ayuntamiento de Errenteria*
- 10. Ayuntamiento de Tolosa*
- 11. Ayuntamiento de Irun*
- 12. Ayuntamiento de Zumarraga*
- 13. Ayuntamiento de Ermua*
- 14. Ayuntamiento de Eibar*
- 15. Ayuntamiento de Llodio-Laudio*

Se ha recibido la encuesta completada por parte de todas las administraciones.

Inicialmente, en la encuesta se han recabado datos cuantitativos y cualitativos relativos al número aproximado de cámaras, tipos (**fijas o móviles**), lugar de ubicación, finalidades perseguidas y motivos para su utilización.

Además, el Ararteko ha planteado cuestiones relativas a las competencias y normas habilitantes de la videovigilancia y del cumplimiento del régimen general de autorizaciones cuando el sistema se utiliza con fines de seguridad ciudadana.

En relación con las grabaciones de imágenes, la institución ha planteado cuestiones relacionadas con la existencia de protocolos internos de custodia, plazos mínimos y máximos de conservación y destrucción.

En materia de información y transparencia, el Ararteko ha planteado preguntas concernientes a los medios para informar a la ciudadanía sobre el uso de sistemas de videovigilancia. Ante el ejercicio de derechos por parte de la ciudadanía, ha requerido conocer qué unidades internas son las encargadas de responder y con qué criterios.



Por otro lado, ha preguntado a las administraciones colaboradoras aspectos relacionados con la protección de datos personales y de medidas de seguridad aplicables al tratamiento de la información para garantizar su confidencialidad.

Finalmente, la institución ha consultado sobre la utilización de cámaras por disciplina de tráfico. De modo específico, ha dirigido al Departamento de Seguridad del Gobierno Vasco preguntas relacionadas con las resoluciones de autorización de la videovigilancia y su comunicación al Comité de Videovigilancia y Libertades.

En cuanto a la **estructura del informe**, en primer lugar, se presentan los datos recabados mediante el cuestionario remitido a las administraciones colaboradoras y una valoración inicial de la información obtenida estructurada por nueve elementos de control.

Los puntos revisados se estructuran como base para analizar y contrastar (1) aspectos generales de cumplimiento normativo en materia de videovigilancia, (2) finalidades y normas habilitantes de las decisiones de implantar sistemas de videovigilancia, (3) el grado de conocimiento y cumplimiento del régimen de autorización de la videovigilancia al cual se somete su utilización, y, además, (4) contrastar los principios generales de la proporcionalidad que debe presidir su utilización.

Por otro lado, se analizan aspectos relacionados con (5) la gestión de las grabaciones de videovigilancia y los plazos de conservación.

Igualmente, (6) el principio de información es un aspecto que se ha estimado oportuno considerar dado que tiene un impacto en la transparencia de la actuación de la administración.

Asimismo, resulta relevante revisar de qué modo se atienden (7) los derechos de la ciudadanía relacionados con las grabaciones en las que figuran sus datos personales.

Por último, la captación de imágenes y, en ocasiones voz de la ciudadanía, comporta la necesidad de revisar algunas (8) obligaciones básicas en materia de protección de datos y las (9) medidas de seguridad que se adoptan para preservar la conservación íntegra y accesible de los datos para los interesados legitimados.

Como resultado, se emiten conclusiones de las evaluaciones realizadas por cada punto o elemento de análisis y recomendaciones generales dirigidas a las administraciones competentes que pueden servir de base para la mejora de la actuación del



sector público en materia de videovigilancia, y en especial, para su utilización con fines de seguridad ciudadana.

III.3. Marco jurídico

La actividad preventiva de las policías en materia de seguridad pública permite el uso e instalación de sistemas de videovigilancia como medio de investigación penal y se encuentra regulada con carácter general en la [LOVFCS](#).

El [Real Decreto 596/1999](#) desarrolla la LOVFCS mediante un reglamento que trata de conseguir la utilización pacífica de vías y espacios públicos y la prevención de delitos, faltas e infracciones relacionadas con la seguridad pública, mediante, entre otras, la captación, reproducción y tratamiento de imágenes y sonido, de forma que no supongan una intromisión ilegítima del derecho a la propia imagen de la ciudadanía así afectados previsto en el [artículo 2.2](#) de la LOHP, por cuanto *“No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley (...)”*.

En Euskadi, la LOVFCS se desarrolló mediante el [Decreto 168/1998](#) y la [Orden de 15 de abril de 2011](#), del Consejero de Interior, por la que se establece el contenido y diseño de los carteles informativos de la instalación y uso de videocámaras fijas por la Policía del País Vasco.

Además, 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 ha introducido aspectos destacables sobre el régimen de garantías a cumplir en materia de videovigilancia y sobre medidas de seguridad y protección de datos en el ámbito del tratamiento de datos personales con los fines de la ley.

En materia de protección de datos, toda vez que la videovigilancia comporta la recogida y tratamiento de datos de imagen, y en su caso voz, por los responsables de tratamiento, resulta preciso atender a aquellas normas y disposiciones aplicables a las administraciones públicas competentes. En concreto, lo previsto en la [LOPDGDD](#), el [RGPD](#) y la [LVPD](#)³.

³ A la fecha de publicación del presente documento se encuentra en fase de tramitación parlamentaria la nueva Ley de protección de datos personales y de la autoridad vasca de protección de datos.



El estudio aborda aspectos de cumplimiento normativo y del sistema de garantías previsto en las normas citadas, en concreto:

a) Finalidades y normas aplicables

Las finalidades perseguidas mediante el uso de la videovigilancia determinan las normas aplicables a cada supuesto. Se ha de distinguir la captación de imágenes con fines de preservar la seguridad de instalaciones, bienes y personas, sometido al régimen general de protección de datos, de aquellos fines de la videovigilancia por motivos de seguridad ciudadana y cuyo régimen especial establece que su utilización únicamente compete a las policías.

b) Régimen de autorizaciones

En Euskadi, el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos se encuentra desarrollado en el [Decreto 168/98](#), el cual establece que es competencia del Viceconsejero de Seguridad del Departamento de Seguridad del Gobierno Vasco autorizar la instalación **fija** de videocámaras por la Ertzaintza y los cuerpos de Policía Local de la Policía del País Vasco, llevar el registro de autorizaciones de instalaciones **fijas** e informar quincenalmente a la CVL. Se trata de un órgano consultivo de protección de la privacidad para reforzar la garantía del derecho a la propia imagen, a la intimidad y dignidad de los ciudadanos respecto del empleo por la Policía del País Vasco de videocámaras en lugares públicos (Más información en: <https://www.euskadi.eus/gobierno-vasco/-/informacion/comision-de-videovigilancia-y-libertades/>).

Además, con respecto al uso de videocámaras **móviles** se establece una especificidad por cuanto el artículo 2.2 del [Decreto 168/98](#) indica que la autorización podrá otorgarse por los directores del Departamento de Seguridad con responsabilidades en materia de salvaguardia de la seguridad ciudadana y prevención de la criminalidad, que podrán delegar en los responsables policiales de ellos jerárquicamente dependientes con atribuciones al menos en un Territorio Histórico.

c) Principio de proporcionalidad

Las autorizaciones para la instalación de videocámaras **fijas** y **móviles** de seguridad ciudadana deben cumplir una serie de criterios como asegurar la protección de los



edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes, la concurrencia de algún peligro concreto, y fundamentalmente los principios del [artículo 6](#) de la LOVFCS, regulador del principio de proporcionalidad en la doble versión de idoneidad y de intervención mínima, por cuanto:

“- La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.

-La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas”.

Además, el apartado 4 establece la **exigencia** para utilizar videocámaras de que exista *“un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles”.*

d) Gestión y custodia de grabaciones y plazos de conservación

Con respecto a la gestión de grabaciones efectuadas por motivos de seguridad ciudadana y plazos de gestión y conservación, tanto la LOVFCS como la LO 7/21 establecen plazos máximos de conservación y la obligación de custodiar debidamente las grabaciones, así como la necesidad de crear disposiciones reglamentarias que establezcan el órgano o autoridad que custodiará las imágenes.

e) Principio de información

La LOVFCS establece que la ciudadanía debe ser informada *“de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable”* ([artículo 9](#)). Además, en el ámbito territorial de Euskadi, el Decreto 168/98 regula en idénticos términos la citada obligación ([artículo 8](#)).

El [artículo 16.5](#) LO 7/2021 también indica que *“Los ciudadanos serán informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos”* pero se enmarca en el precepto relativo a instalaciones **fijas**.



Además, la [Orden de 15 de abril de 2011](#), de la Consejería de Interior, por la que se establece el contenido y diseño de los carteles informativos de la instalación y uso de videocámaras **fijas** por la Policía del País Vasco desarrolla los preceptos anteriormente citados y regula las características de los carteles que deben advertir sobre la videovigilancia efectuada por la policía de Euskadi en vías y espacios públicos.

f) Ejercicio y atención de derechos

Tanto la LOVFCS como el Decreto 168/98 regulan los derechos de acceso y cancelación de datos que puede ejercer la ciudadanía con respecto a las videograbaciones, el modo de ejercerlos y el régimen de atención a observar por las administraciones públicas.

También la LO 7/21 regula las condiciones generales de ejercicio de los derechos de las personas interesadas.

g) Obligaciones básicas de protección de datos (el registro de actividades de tratamiento)

La normativa de protección de datos en vigor ([artículo 30 RGPD](#) y [31 LOPDGDD](#)) establece la obligación de crear registros de actividades de tratamiento de datos personales que definan la estructura, finalidades y licitud, entre otros aspectos, de los tratamientos de datos personales que efectúen los responsables de la recogida de datos.

En el ámbito del sector público, además, las actividades de tratamiento creadas deben publicarse en los portales de transparencia correspondientes de acuerdo con el [artículo 6 bis](#) de la LTBG.

h) Medidas de seguridad aplicadas al tratamiento de datos personales

El tratamiento de datos personales de imagen y voz comportan la necesidad de aplicar medidas de seguridad de acuerdo con lo dispuesto en la normativa de protección de datos. El RGPD introduce el principio de responsabilidad proactiva, el cual proporciona un marco y deber para el responsable del tratamiento de adoptar medidas oportunas, tanto técnicas como organizativas y eficaces a fin de garantizar la seguridad adecuado al riesgo de los datos tratados.



En concreto el artículo 32 RGPD establece que *“Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”*.

En materia de medidas de seguridad, la normativa de protección de datos se remite a lo dispuesto en el [ENS](#) cuando se produzcan tratamientos de datos por las administraciones públicas tal y como se prevé en la [Disposición Adicional Primera](#) de la LOPDGDD.

Sin embargo, estas medidas se han de coherenstar con aquellas obligaciones específicas que adicionalmente se regulan en el capítulo IV de la LO 7/21 y que fundamentalmente refieren a protección de datos, como las relativas a la creación de registros de actividades de tratamiento, evaluaciones de impacto, consultas previas a la autoridad de control, notificaciones de brechas de seguridad, etc.

III.4. Pronunciamientos del Ararteko en la materia

El presente estudio se centra fundamentalmente en analizar el cumplimiento del sistema de garantías previo a la instalación y utilización de sistemas de videovigilancia tanto **fijos** como **móviles** en espacios públicos.

El Ararteko ha emitido diversa doctrina y resoluciones en materia de uso de cámaras de videovigilancia centrada fundamentalmente en prevenir posibles actuaciones irregulares y proteger al personal policial ante quejas o denuncias infundadas. En este sentido, cabe recordar que el Ararteko, mediante la Recomendación general 7/2011, de 28 de octubre. El sistema de garantías en las actuaciones y prácticas policiales⁴, en el epígrafe 8, ya introdujo elementos a considerar relativos a las grabaciones de las detenciones, como medio para prevenir prácticas contrarias a la integridad y dignidad de las personas detenidas, así como un instrumento idóneo para esclarecer posibles actuaciones irregulares en este ámbito y proteger a los funcionarios policiales frente a eventuales quejas o denuncias infundadas.

⁴ <https://www.ararteko.eus/es/recomendacion-general-del-ararteko-72011-de-28-de-octubre-0>.



En síntesis, en la recomendación general se decía en el citado epígrafe 8 que el sistema de videograbación debía cumplir varios requisitos:

- a) iniciarse la grabación en el mismo momento de la detención;*
- b) comprender todas las dependencias policiales, lugares de detención y espacios de interacción entre los agentes y la persona detenida, salvo que conste la oposición de ésta por razones de protección de su intimidad;*
- c) incluir imágenes y sonido;*
- d) ser accesible a la defensa y a las instituciones de garantía de derechos humanos; y*
- e) observar las exigencias mínimas que fijamos en la recomendación.*

Tenemos que insistir especialmente en el plazo de conservación del material grabado, sobre el que hemos llamado repetidamente la atención, reiterando que tiene que ser un plazo adecuado para que las grabaciones estén disponibles durante el límite máximo de prescripción de las posibles responsabilidades administrativas y penales que pudieran derivarse de las actuaciones grabadas, y para que lo estén también durante el plazo de intervención de las instituciones de garantía de derechos, como la del Ararteko. Es necesario, además, que se garantice la conservación de las grabaciones mientras persista la intervención en los ámbitos señalados”.

Fundamentalmente, la recomendación citada se centraba en aportar garantías a la persona detenida y a las policías mediante una correcta y adecuada gestión y conservación de las imágenes de detenciones, cuestión en la que no se enfoca el presente estudio pero que, de cualquier manera, mantiene una absoluta vigencia en la actualidad, dado que complementa el presente documento.

Se trataba de una recomendación que traía causa de anteriores criterios doctrinales del Ararteko plasmados, en síntesis, en informes anuales presentados al parlamento fruto de diversas actuaciones realizadas.

En concreto, cabe destacar los informes anuales presentados en 2006⁵ y 2007⁶ en los cuales se expusieron los aspectos relevantes de las visitas realizadas a comisarías y centros de detención de la Ertzaintza y policía local y las acciones llevadas a cabo por las administraciones para atender las recomendaciones formuladas por el Ararteko con respecto a los sistemas de control basados en grabaciones de video situadas en pasillos de zonas de calabozos, celdas y demás dependencias interiores.

⁵ <https://www.ararteko.eus/es/informe-al-parlamento-vasco-2006>.

⁶ <https://www.ararteko.eus/es/informe-al-parlamento-vasco-2007>.



En los citados informes y actuaciones, se enfatizaron los elementos y condiciones mínimas de eficacia de estos sistemas de grabación situados en dependencias policiales.

Con posterioridad a la emisión de la recomendación general se ha continuado visitando centros de detención y analizando sistemas de videograbación en dependencias interiores recogiendo en los correspondientes informes los criterios garantistas de protección de los derechos fundamentales a observar ante la utilización de mecanismos de videograbación.



IV. Resultados del estudio y evaluación

IV.1. Estadísticas de número de cámaras, tipo y ubicación

IV.1.1. Resultados

Las administraciones públicas participantes del estudio refieren los siguientes datos aproximados relativos al número de cámaras o sistemas de videovigilancia **fijas** y **móviles** y lugares de ubicación.

Administración	Nº aproximado de cámaras	Cámaras fijas y móviles	Ubicación de cámaras
Departamento de Seguridad de Gobierno Vasco ⁷	Ertzaintza gestiona 2.037 instalaciones fijas en espacios públicos y reporta 134 usos de cámaras móviles por peligro/ evento durante el año 2022.	Ambas	Instalaciones comunes como oficinas, carreteras, calles o espacios públicos (actividad delictiva significativa) cuando resulta oportuno y proporcional para la protección de la seguridad pública. Vías y espacios públicos que requieren especial protección de la seguridad ciudadana por parte de la Ertzaintza.
Ayuntamiento de Vitoria-Gasteiz	600	Ambas	Instalaciones comunes como oficinas, recintos deportivos, edificios culturales, carreteras, casco urbano, otros espacios públicos como escaleras mecánicas, transporte urbano, lugares interiores como lugares de trabajo, pasillos, salas, despachos, bibliotecas, piscinas, ascensores. También cámaras de regulación de tráfico en cascos urbanos que captan matrículas.

⁷ El Departamento de Seguridad no aporta información relativa a cámaras sobre disciplina de tráfico o de videovigilancia fija de dependencias internas sujetas al RGPD.



Ayuntamiento de Bilbao	265	Ambas	Instalaciones comunes como oficinas, edificios culturales y cascos urbanos. Comisaría, e imágenes interiores como lugares de trabajo, pasillos, salas, despachos, bibliotecas, piscinas, ascensores, etc. captación de matrículas para la regulación del tráfico en cascos urbanos o aparcamientos.
Ayuntamiento de Donostia/San Sebastián	350 ⁸	Ambas	Instalaciones comunes como oficinas, recintos deportivos, edificios culturales, carreteras y casco urbano. Imágenes interiores como lugares de trabajo, pasillos, salas, despachos, bibliotecas, piscinas, ascensores, etc. comisaría.
Ayuntamiento de Barakaldo	30	Fijas	Instalaciones comunes como oficinas, carreteras y cascos urbanos y otros espacios públicos como garaje utilizado por miembros de la corporación. Se ha detectado en otros edificios municipales como instalaciones culturales (ver actividad de tratamiento) y algunas cámaras ubicadas en recintos municipales captan imágenes interiores como lugares de trabajo, pasillos, salas, despachos, bibliotecas, piscinas, ascensores, etc.
Ayuntamiento de Portugalete	75	Fijas	Instalaciones comunes como oficinas, edificios culturales, carreteras, parques, ascensores, cascos urbanos, Ayuntamiento-Juzgado de Paz-Policía Local-Oficina Atención a la Ciudadanía dependiente del Ayuntamiento.
Ayuntamiento de Getxo	265	Fijas	Instalaciones comunes como oficinas, recintos deportivos, edificios culturales, carreteras, parques, ascensores, también lugares interiores, aparcamientos.
Ayuntamiento de Basauri	127	Ambas	Instalaciones comunes como oficinas, recintos deportivos, edificios culturales, ascensores, cascos urbanos, y rampas mecánicas. Comisaría. También lugares interiores.

⁸ En otra respuesta al cuestionario se indica 170.



Ayuntamiento de Errenteria	103	Ambas	Instalaciones comunes como oficinas, recintos deportivos, carreteras, ascensores, casco urbano, comisaría, transporte urbano.
Ayuntamiento de Tolosa	14	Fijas	Instalaciones comunes como oficinas, recintos deportivos, edificios culturales (en otro apartado se dice que no) y cascos urbanos.
Ayuntamiento de Irún	84	Fijas	Instalaciones comunes como oficinas, recintos deportivos, carreteras, edificios culturales, parques, cascos urbanos, comisaría, musika eskolan, behobiako adin nagusien zentrua, zubia zentrua, también en lugares interiores.
Ayuntamiento de Llodio-Laudio	28	Fijas	Recintos deportivos, carreteras, ascensores, cascos urbanos, edificios de oficinas. Algunas cámaras ubicadas en recintos municipales captan imágenes interiores como lugares de trabajo, pasillos, salas, despachos, bibliotecas, piscinas, ascensores, etc. No hay en aparcamientos o cascos urbanos.
Ayuntamiento de Zumarraga	71	Fijas	Recintos deportivos, edificios culturales (Antio interpretazio zentroa), ascensores, aparcamiento Zelai Arizti, aparcamiento Intermodal, comisaría.
Ayuntamiento de Eibar	40	Fijas	Recintos deportivos, edificios culturales, ascensores, garbigunes, edificios municipales, comisaría.
Ayuntamiento de Ermua	138	Ambas	Instalaciones comunes como oficinas, edificios culturales, carreteras, ascensores, aparcamientos, edificios públicos, rampas mecánicas, comisaría. Captación de matrículas en casco urbano.



IV. 1. 2. Análisis y valoración

- Número aproximado de cámaras

La institución del Ararteko quiere aproximarse a las razones por las cuales se adopta la decisión de instalar sistemas de captación de imágenes de personas en detrimento de otras medidas o soluciones y comprender si esta responde a criterios técnicos o jurídicos plasmados de antemano en las normas. De hecho, el criterio discrecional del que goza la administración debe ajustarse a aquellos requerimientos previstos en la normativa y previa ponderación de su impacto en otros derechos fundamentales como la intimidad.

Con respecto al número de cámaras reportadas por las entidades públicas participantes en el estudio, interesa destacar la inexistencia de estándares previos y la autonomía competencial que ostentan para adoptar decisiones relativas a su utilización.

Atendiendo al principal objetivo del estudio, analizar el uso de la videovigilancia por motivos de seguridad ciudadana, una hipótesis de correlación con el despliegue de cámaras puede encontrarse en los índices de conflictividad.

Según las estadísticas de delitos publicadas en la página web de la Ertzaintza correspondientes a los últimos años por tipo y municipios, en las poblaciones y capitales de territorios históricos con mayor cantidad de población⁹ parece hallarse escasa correlación entre la actividad delictiva descrita en estadísticas y el uso de la videovigilancia.

Por ejemplo, en Vitoria-Gasteiz, la tasa de infracciones por cada 1.000 habitantes es de 41,09 en 2022 y declaran disponer de aproximadamente 600 cámaras, entre ellas, sistemas **móviles** en uniformes policiales, y, por otro lado, en Bilbao, la tasa es de 66,80 y se declara un uso aproximado de 265 cámaras. En Donostia/San Sebastián, la tasa alcanza un 40,71 y se declara disponer de aproximadamente 350 cámaras. En Barakaldo, refieren la utilización de 30 cámaras fijas según los datos suministrados a esta institución y la tasa de infracciones por habitante en 2022 alcanza a 53,48 y, sin embargo, en Getxo se dispone de aproximadamente 265 cámaras y la tasa de infracciones por 1.000 habitantes en 2022 fue de 34,58.

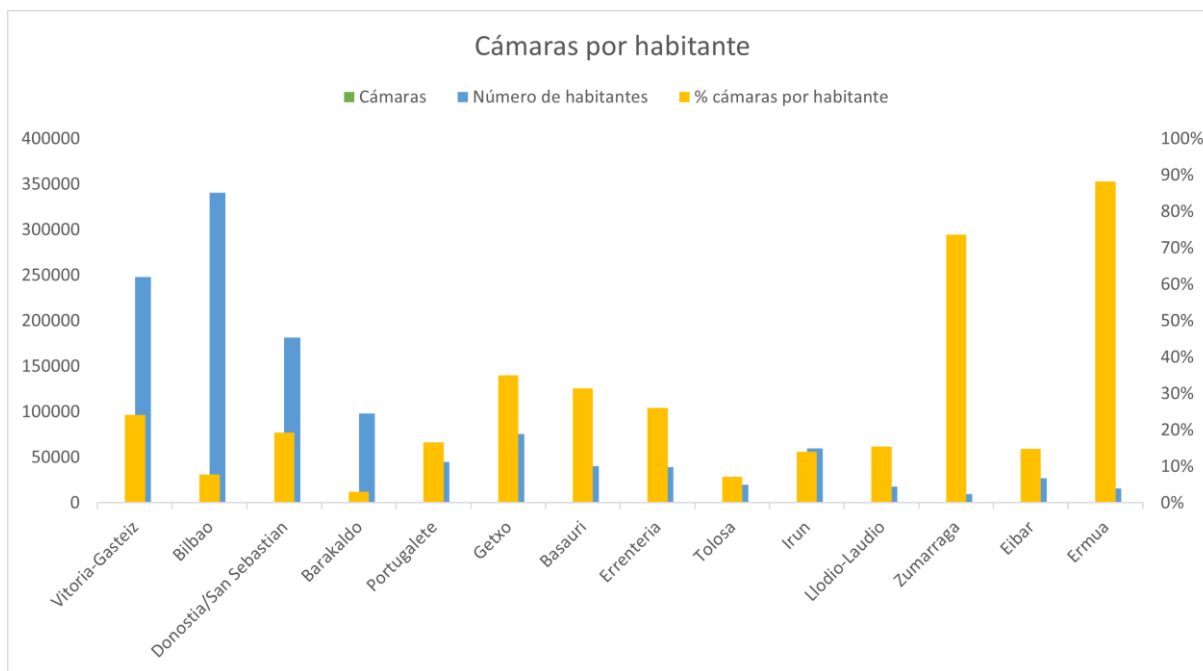
⁹ <https://www.ertzaintza.euskadi.eus/lfr/documents/62347/6356281/Delitos+por+municipios+22+12+c.jpg/cceff0f3-5e30-76ae-7910-a3aa2196820e?t=1676037261891>.



Por otro lado, las estadísticas correspondientes a municipios de entre 20.000 y 50.000 habitantes¹⁰ revelan que la tasa de infracciones en el año 2022 por cada 1.000 habitantes es de 46,57 en Basauri, de 47,39 en Portugalete, de 47,98 en Eibar, de 31,43 en Ermua¹¹ y de 36,21 en Errenteria. El número de cámaras y tipos de uso difiere entre estos municipios, en Basauri se indica que disponen de 127 cámaras y además se utilizan dispositivos **móviles** colocados en uniformes de policía. En Portugalete se dispone de 75 cámaras fijas, en Errenteria y Ermua declaran disponer respectivamente de 103 y 138 cámaras tanto **fijas** como **móviles**. En Eibar únicamente se utilizan 40 cámaras fijas.

La cantidad de instalaciones y lugares en los que se utilizan sistemas de videovigilancia **fijos** y **móviles** por diversas policías de entidades locales arrojan diferencias entre distintas poblaciones. La estadística relativa a la ratio de cámaras por habitantes empadronados no parece ligarse el volumen de población como criterio razonable para garantizar la seguridad ciudadana aun cuando se puede suponer que una menor población puede ocasionar un menor impacto en la seguridad ciudadana.

El siguiente gráfico muestra visualmente lo anteriormente señalado:



¹⁰ <https://www.ertzaingia.euskadi.eus/lfr/documents/62347/6356281/Delitos+por+municipios+2+22+12+c.jpg/c69e7679-e3c1-4efe-a1be-8304cc016702?t=1676037260673>

¹¹ <https://www.ertzaingia.euskadi.eus/lfr/documents/62347/7614212/Memoria+Delicuencia+2022+de+la+Euskal+Polizia.pdf/92da3d71-e776-368b-2726-777c8eb5c00b?t=1679998701819>.



En capitales como Vitoria-Gasteiz existe un despliegue de cámaras superior a Bilbao. En municipios como Getxo, Errenteria, Basauri, Zumarraga o Ermua destacan los porcentajes de implantación de sistemas de videovigilancia en contraste con la población empadronada. El despliegue puede obedecer a criterios objetivos como motivación para extender el uso y alcance de la videovigilancia, por ejemplo, como alternativa temporal a la falta de personal, la extensión del municipio, la afluencia de tráfico, la presencia de empresas o polígonos industriales alejados del núcleo urbano, pero, en cualquier caso, parece reseñable el uso intensivo de la videovigilancia en algunas poblaciones.

Contrasta entre ciudades y grandes poblaciones no sólo el número de cámaras desplegadas sino también el tipo de uso, dado que, en Vitoria-Gasteiz, además, se recurre a la videovigilancia mediante cámaras en uniformes policiales, no así en otras poblaciones con, aparentemente, mayor afección a la seguridad ciudadana. También en municipios como Basauri y Ermua se recurre a la videovigilancia mediante cámaras en uniformes de policía si bien la población y tasa de delincuencia es similar a la de otras poblaciones donde no se utilizan este tipo de sistemas de vigilancia.

Así, esta institución considera que el número aproximado de cámaras utilizado por las entidades públicas participantes en el estudio no tiene porqué encontrarse exclusivamente correlacionada con índices de conflictividad, sino que pueden existir distintos elementos de juicio o ponderación que han motivado su utilización. Por ejemplo, por razón del lugar y espacio, de los recursos humanos y policiales de los que dispone la administración, índices de peligrosidad o de denuncias presentadas, etc. y en aplicación del principio de proporcionalidad.

- Ubicación de los sistemas de videovigilancia

En el cuestionario, esta institución no ha efectuado una distinción con respecto a la ubicación y finalidades perseguidas por las administraciones para utilizar e implantar sistemas de videovigilancia, pero, como se verá posteriormente, en función del uso elegido, la finalidad y legitimación puede ser diferente a tenor de las normas aplicables y, por lo tanto, deben cumplir criterios y garantías específicas.

Con respecto a la ubicación de las cámaras desplegadas, cabe resaltar lo señalado por el Departamento de Seguridad del Gobierno Vasco, que refiere el uso de la videovigilancia en espacios públicos como instalaciones comunes de oficinas, en



carreteras, calles o vías en las cuales se produce una actividad delictiva significativa y, por lo tanto, resulta adecuado y proporcional recurrir a su uso.

Tal y como se expone en los siguientes apartados, el uso de sistemas de videovigilancia en edificios e instalaciones municipales fundamentadas o amparadas en la seguridad ciudadana deben responder al régimen de garantías y requisitos estrictos, atendiendo al razonable riesgo o peligro concreto para la ciudadanía y, además, cumplir el principio de proporcionalidad. Lógicamente, el uso de cámaras con fines de control y afluencia de tráfico en cascos urbanos o por razones de disciplina y seguridad del tráfico que únicamente captan matrículas o planos generales no comporta una especial afección para la intimidad o la protección de datos personales de la ciudadanía.

Las entidades locales participantes del estudio, atendiendo a las características de los municipios, refieren la localización de sistemas de videovigilancia en diferentes lugares e instalaciones como comisarías, edificios municipales de oficinas, recintos deportivos, edificios culturales y bibliotecas, ascensores, aparcamientos, piscinas, cascos urbanos, escaleras mecánicas, transporte urbano y lugares interiores de trabajo como salas, pasillos, despachos, etc.

Esta institución pone de relieve la captación de imágenes en rampas mecánicas, bibliotecas municipales, transportes urbanos, recintos deportivos o incluso piscinas, lugares en los que no parece existir un razonable riesgo para la seguridad ciudadana.

En estos supuestos, parece oportuno modular la captación de imágenes por razón del lugar, tiempo de observación y ampararla en la normativa de protección de datos con fines de preservar la seguridad de instalaciones, bienes y personas como alternativa que respete la intimidad y los datos personales de toda la ciudadanía, y en especial, de menores y personas con discapacidad.

En este sentido, el presente estudio alude posteriormente a las reglas sobre la proporcionalidad que se consideran elementales para valorar previamente la decisión de captar imágenes porque se considera factible utilizar medios menos intrusivos y lesivos para la intimidad a la hora de proteger instalaciones, bienes y personas.

Además, en lugares interiores de edificios e instalaciones municipales, cuando la captación de imágenes abarca tanto ciudadanía como personal trabajador, ello puede tener su impacto en otros derechos regulados en normas y disposiciones que establecen reglas sobre la legitimidad y proporcionalidad que deben observarse de



antemano. En efecto, el [artículo 89](#) de la LOPDGDD, relativo al derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, establece que *“Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida”*. Y la propia normativa de función pública de Euskadi contempla como derecho individual del personal empleado público vasco el relativo a la intimidad¹².

Por ese motivo, aun no siendo el objeto principal del presente estudio, cabe remarcar que, la videovigilancia en espacios interiores en los cuales se puede encontrar personal trabajador debe respetar la intimidad de las personas, y en el caso de que el fin perseguido resulte el control laboral, debe acomodarse a las reglas y normas al efecto.

Por lo tanto, las cámaras ubicadas en los citados lugares interiores con fines de seguridad deben respetar la intimidad de las personas físicas en todos los supuestos si bien las normas de contraste establecen sus requisitos específicos en función de los bienes jurídicos a proteger.

IV.2. Finalidades y normas habilitantes de la videovigilancia

En el presente apartado se ofrecen los resultados y la evaluación de los fines perseguidos por las administraciones públicas y de las normas habilitantes de la videovigilancia.

IV.2.1. Resultados

Administración	Finalidades y normas habilitantes
Departamento de Seguridad de Gobierno vasco	<ul style="list-style-type: none"> – Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) – Seguridad ciudadana (LOVFCS-LO 7/21) – Disciplina de tráfico (LOVFCS-Decreto 168/98)

¹² Artículo 161.h) de la [Ley 11/2022, de 1 de diciembre, de Empleo Público Vasco](#).



Administración	Finalidades y normas habilitantes
Ayuntamiento de Vitoria-Gasteiz	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Seguridad ciudadana (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Bilbao	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Seguridad ciudadana (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Donostia/San Sebastián	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Seguridad ciudadana (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98) - Monitorización de la línea de costa en climatología adversa¹³
Ayuntamiento de Barakaldo	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Seguridad ciudadana (LOVFCS-No señalan LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Portugalete	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Seguridad ciudadana (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Getxo	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Seguridad ciudadana (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Basauri	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas, control de accesos (LOPDGDD) - Seguridad ciudadana (LOVFCS-LO 7/21)

¹³ El Ayuntamiento de Donostia/San Sebastián refiere que dispone de un sistema de cámaras que les permite monitorizar la línea de costa con objeto de adoptar decisiones ante situaciones de climatología adversa. Cuando el objetivo no es captar imágenes y sonidos de personas y tampoco es posible identificar de manera directa o indirecta a las mismas, quizá no resulten aplicables las normas y criterios emitidos en el presente estudio y la vigilancia encaje en otras competencias como protección civil, misión de interés público diferente de la seguridad pública.



Administración	Finalidades y normas habilitantes
Ayuntamiento de Errenteria	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - No señalan seguridad ciudadana pero sí en las normas aplicables (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Tolosa	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - No señalan seguridad ciudadana pero sí en las normas aplicables (LOVFCS) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Irun	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - No señalan seguridad ciudadana pero sí en las normas aplicables (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Llodio-Laudio	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Seguridad ciudadana (LOVFCS-LO 7/21) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (LOVFCS-Decreto 168/98)
Ayuntamiento de Zumarraga	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - No por seguridad ciudadana ni disciplina de tráfico
Ayuntamiento de Eibar	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Disciplina de tráfico y regulación de tráfico en zonas urbanas (sin referencia normativa).
Ayuntamiento de Ermua	<ul style="list-style-type: none"> - Preservar la seguridad de instalaciones, bienes y personas (LOPDGDD) - Se indica que no se utilizan cámaras con fines de seguridad ciudadana, pero en la práctica, sí se utilizan cámaras móviles con dichos fines y además autorizadas por la VCS.

IV.2.2. Análisis y valoración

Existen distintas normas reguladoras de la videovigilancia en función del fin perseguido y, por lo tanto, distintas obligaciones para los titulares de los sistemas de captación de imágenes.



En este sentido, cabe distinguir entre aquellas cámaras y sistemas de videovigilancia orientadas a **preservar la seguridad de instalaciones bienes y personas** ([art 22 LOPDGDD](#)) de aquellas que claramente tienen una función de **contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública**¹⁴ en lugares públicos, abiertos o cerrados de acuerdo con los siguientes criterios señalados en la LOVFCS: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes.

La LO 7/2021 tiene por objeto regular el tratamiento de datos, y, por lo tanto, también de imágenes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, y establece en el apartado 2 del artículo 15:

“Artículo 15. Sistemas de grabación de imágenes y sonido por las Fuerzas y Cuerpos de Seguridad.

1. [...].

*2. En la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones **propias**; asegurar la protección de edificios e instalaciones públicas y de sus accesos que **estén bajo custodia**; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública.”*

El alcance de la captación de imágenes se amplía mediante esta disposición, puesto que no se circunscribe a asegurar la protección de los edificios e instalaciones públicas y de sus accesos, como señalaba la LOVFCS, sino que parece posible su uso para asegurar *“la protección de los edificios e instalaciones **propias**; asegurar la protección de edificios e instalaciones públicas y de sus accesos que **estén bajo custodia**”*.

Los usos señalados, en principio, deben acotarse a la prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, pero parece complicada su convivencia con el uso basado en el interés legítimo

¹⁴ [Artículo 1 LOVFCS](#).



de preservar la seguridad de bienes, instalaciones y personas reflejado en la normativa de protección de datos.

Independientemente de la aparente falta de armonización de la normativa, resulta menester cumplir las reglas de autorización previa e información a la ciudadanía de espacios y lugares videovigilados por seguridad ciudadana cuando se trata de, por ejemplo, dependencias policiales y otras instalaciones bajo custodia de las policías. Porque en dichas dependencias pueden producirse hechos que motiven una intervención de las policías en los que se encuentre involucrada la ciudadanía, personas detenidas o los propios agentes de policía.

La cuestión no parece trivial¹⁵ porque una falta disciplinaria cometida por un funcionario público en la entrada de una dependencia policial quizá no tendría la misma calificación jurídica en el ámbito disciplinario en función del tipo de cámaras y régimen de autorización. En tal sentido, se podría interpretar que en el marco de protección de datos no se ha producido un acto que atente contra la integridad de personas y, sin embargo, en un contexto de cámaras autorizadas bajo el régimen de la LOVFCS, podría ser calificado de delito leve (no implica puesta disposición de autoridades competentes) o grave (sí implica puesta a disposición de autoridades competentes). Además, los plazos máximos de conservación de las grabaciones serían diferentes y podrían causar perjuicios en los derechos y garantías de las personas. El aspecto relativo a los plazos de conservación de las grabaciones se analizará más adelante ([Apartado IV.5](#)).

Tal y como se ha anticipado anteriormente, se ha de poner de relieve qué régimen resulta aplicable a la videovigilancia en otro tipo de edificios y dependencias de titularidad de la administración cuando el tratamiento de datos no tiene implicaciones en materia de seguridad ciudadana o de prevención de comisión de infracciones de índole penal, sino aquellas relacionadas con **preservar** la seguridad de instalaciones, bienes y personas.

Las autorizaciones de videovigilancia en instalaciones de la administración como centros culturales, bibliotecas, polideportivos, piscinas, algunas oficinas y espacios interiores emitidas al amparo de la LOVFCS deberían respetar el principio de proporcionalidad porque en su dimensión de intervención mínima ([Artículo 6.3 LOVFCS](#)) *“exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas”* y en las citadas instalaciones, habitualmente existen

¹⁵ Ver STS 1564/2021, de 26 de abril ([ECLI:ES:TS:2021:1564](#)).



medios alternativos y menos lesivos para la intimidad para efectuar un control de instalaciones, bienes y personas. A simple vista, parece complicado que en las mismas se produzca un razonable riesgo para la seguridad ciudadana que motive utilizar cámaras **fijas**, o un incluso un peligro concreto, si se opta por utilizar cámaras **móviles**.

En todo caso, se observa que algunas administraciones señalan al Ararteko el tratamiento de datos de videovigilancia únicamente con fines de preservar la seguridad de acuerdo con los requerimientos de la normativa de protección de datos y, sin embargo, disponen de sistemas autorizados por la VCS, por lo que, lógicamente se utilizan con fines de seguridad ciudadana. Se trata de un aspecto esencial que deben dilucidar y distinguir para definir correctamente los fines perseguidos y las normas que corresponde aplicar.

IV.3. Régimen de autorización de la videovigilancia

IV.3.1. Resultados

En relación con el régimen de autorización y utilización de sistemas de videovigilancia **fijos** y **móviles** los resultados obtenidos son los siguientes:

Administración	Autorización de sistemas de videovigilancia
Departamento de Seguridad de Gobierno vasco	<ul style="list-style-type: none"> - Cámaras fijas: Autorizadas por la VCS. Existen otros sistemas fijos sin autorización y bajo régimen del RGPD no gestionadas por la Ertzaintza. - Cámaras móviles: Se solicita autorización previa de uso a los órganos competentes. Se añade que se solicitan y autorizan de modo conjunto, y no por cámaras o unidades policiales. Plazo: 1 mes prorrogable por otro, en la práctica se autoriza para el tiempo que dure el evento concreto o resulte de interés policial respecto del peligro para seguridad pública. <ul style="list-style-type: none"> o En uniformes: SI o Drones: SI o Videocámaras o dispositivos utilizados por la Ertzaintza, ante peligro o evento concreto, para la protección de la seguridad ciudadana en espacios públicos.



Administración	Autorización de sistemas de videovigilancia
	<ul style="list-style-type: none"> - Disciplina de tráfico: las resoluciones autorizadoras identifican las vías públicas o los tramos susceptibles de captación, así como el órgano encargado de su custodia y de resolución de peticiones de acceso y cancelación y que se notifican a la CVL.
Ayuntamiento de Vitoria-Gasteiz	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Cámaras móviles: uniformes de policía y en portátiles de la unidad de investigación de delitos. Se solicita autorización previa a la VCS. - Disciplina de tráfico: las resoluciones identifican las vías públicas o los tramos susceptibles de captación, así como el órgano encargado de su custodia y de resolución de peticiones de acceso y cancelación y que no se notifican a la CVL.
Ayuntamiento de Bilbao	<ul style="list-style-type: none"> - Cámaras fijas: Se encuentran autorizadas por la VCS. - Cámaras móviles: en vehículos. Se dispone de instalaciones móviles con motivo de la celebración de determinados eventos: Aste Nagusia, Santo Tomás, por ejemplo. Una vez finalizado el evento desaparecen. Se cuenta con autorización previa pero también se utilizan para fines distintos a la prevención, detección e investigación de delitos, pero no se especifica para cuáles. - Disciplina de tráfico: las resoluciones autorizadoras identifican las vías públicas o los tramos susceptibles de captación, así como el órgano encargado de su custodia y de resolución de peticiones de acceso y cancelación, pero no se notifican a la CVL.
Ayuntamiento de Donostia/San Sebastián	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Cámaras móviles: drones para la monitorización de eventos con grandes concentraciones en espectáculos culturales, deportivos o festejos, en el marco de aplicación de los planes de protección civil; báculos portátiles o en fachadas de edificios para monitorizar eventos con gran concentración de público (Aste nagusia, Donostia Eguna, Santo Tomás, Regatas de la Concha, etc. Con respecto a cámaras móviles se solicita autorización previa. - Disciplina de tráfico: se dispone de resoluciones al efecto y se comunican a la CVL.



Administración	Autorización de sistemas de videovigilancia
Ayuntamiento de Barakaldo	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Disciplina de tráfico: se encuentran autorizadas por la VCS pero no notificadas a la CVL.
Ayuntamiento de Portugalete	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Disciplina de tráfico: se dispone de resoluciones al efecto y se comunican a la CVL.
Ayuntamiento de Getxo	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - No refieren existencia de cámaras móviles. - Disciplina de tráfico: se dispone de resoluciones al efecto, no se comunican a la CVL.
Ayuntamiento de Basauri	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Cámaras móviles en uniformes de policía, se dispone de autorización previa.
Ayuntamiento de Errenteria	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Cámaras móviles (Domo) en vías, cruces, rotondas principales con gran afluencia de tráfico. No se solicita autorización porque se utilizan para fines distintos a la prevención, detección e investigación de delitos y que no requieren autorización previa. - Disciplina de tráfico: se dispone de resoluciones al efecto y que se comunican a la CVL. Plazo de conservación 1 mes.
Ayuntamiento de Tolosa	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Disciplina de tráfico: se dispone de resoluciones al efecto y que se comunican a la CVL.
Ayuntamiento de Irun	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Disciplina de tráfico: se dispone de resoluciones al efecto y se comunican a la CVL.
Ayuntamiento de Llodio-Laudio	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Disciplina de tráfico: se dispone de resoluciones al efecto y que no se comunican a la CVL.
Ayuntamiento de Zumarraga	<ul style="list-style-type: none"> - Cámaras fijas: sin autorización de la VCS porque no se utilizan por motivos de seguridad ciudadana.



Administración	Autorización de sistemas de videovigilancia
Ayuntamiento de Eibar	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS (se indica que no son cámaras ubicadas en lugares públicos con fines de seguridad ciudadana). - Disciplina de tráfico: se dispone de resoluciones al efecto y que no se comunican a la CVL.
Ayuntamiento de Ermua	<ul style="list-style-type: none"> - Cámaras fijas: autorizadas por la VCS. - Cámaras móviles en uniformes de policía, se dispone de autorización previa. - Disciplina de tráfico: se dispone de resoluciones al efecto y que no se comunican a la CVL.

IV.3.2. Análisis y valoración

La instalación de videocámaras en lugares públicos, tanto **fijas** como **móviles**, es competencia exclusiva de las policías, y el tratamiento de dicha imágenes se rige por su legislación específica, contenida en la LOVFCS, y su normativa de desarrollo, sin perjuicio de que sea aplicable, en su caso, lo especialmente previsto en la normativa de protección de datos en aspectos como la adopción de las medidas de seguridad que resulten de la realización del análisis de riesgos así como el registro de actividades de tratamientos, aspectos que serán analizados posteriormente.

Su utilización en lugares públicos tiene una finalidad de seguridad en beneficio de la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

La instalación de este tipo de dispositivos se encuentra sujeta a requisitos muy estrictos ya que, la autorización de instalación de videocámaras **fija** y la utilización de cámaras **móviles**, se otorga por la Delegación del Gobierno previo informe preceptivo y vinculante de la Comisión de Garantías de la Videovigilancia de la Comunidad Autónoma correspondiente. Dicha autorización tiene una vigencia máxima de un año, debiendo renovarse una vez finalizado éste, llevando las Comisiones de Videovigilancia un registro de instalaciones autorizadas. Para autorizar su instalación se tiene en cuenta, conforme al principio de proporcionalidad, los criterios de intervención mínima e idoneidad de manera que:



- Sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en la Ley.
- Se deberá ponderar, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.
- Su utilización exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las **fijas**, o de un peligro concreto, en el caso de las **móviles**.
- No se podrán utilizar para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni en lugares en lugares públicos, abiertos o cerrados, cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada.

Tal y como se ha expuesto en el apartado relativo al [marco jurídico](#), en Euskadi, el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos se encuentra desarrollado en el [Decreto 168/98](#).

El citado decreto prevé que, los responsables de los servicios y unidades policiales podrán utilizar y obtener imágenes y sonidos con videocámaras **móviles**, *“en casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización”*.

Con carácter general, los responsables de los servicios y unidades policiales pueden solicitar de los órganos competentes autorización para la utilización de videocámaras **móviles** mediante petición razonada en la que justifiquen la necesidad e idoneidad de dicho uso. Sin embargo, no es precisa dicha autorización previa cuando se trata de vías o lugares públicos donde se haya autorizado la instalación de videocámaras **fijas**, o cuando se trate de los supuestos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización anteriormente indicada. En cualquier caso, el [Decreto 168/98](#) citado establece que en tales casos se dará cuenta mediante informe motivado al órgano competente para otorgar la autorización y a la CVL, en el plazo máximo de setenta y dos horas y, el órgano competente para otorgar la autorización debe dar cuenta a su vez de dicho informe al Viceconsejero de Seguridad.

Por último, cabe destacar que la LO 7/21 establece que, en estos supuestos de dispositivos **móviles** *“las autorizaciones no se podrán conceder en ningún caso con*



carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro”.

De los resultados obtenidos en este apartado, parece derivarse que **todas las administraciones públicas competentes encuestadas refieren que recaban y obtienen la autorización previa para la utilización de cámaras fijas y móviles con finalidades de seguridad ciudadana**. En algunos supuestos, quizá no resultaría necesaria dicha autorización cuando el fin perseguido es preservar la seguridad de instalaciones de acuerdo con lo dispuesto en la normativa de protección de datos y se ha reportado a esta defensoría que únicamente se vigilan mediante cámaras en recintos y edificios municipales y no en espacios públicos (Eibar).

En materia de seguridad de tráfico, todas las administraciones indican que solicitan y obtienen autorización previa para la utilización de cámaras al efecto de acuerdo con el régimen previsto en la [disposición adicional tercera del Decreto 168/98](#), si bien **algunas entidades no notifican las resoluciones a la CVL**.

En particular, son autoridades competentes para ordenar la instalación y uso de los dispositivos de videovigilancia el director de Tráfico y Parque Móvil del Gobierno en las vías públicas de la Comunidad Autónoma del País Vasco cuya regulación del tráfico no esté atribuida a los municipios y la autoridad competente del municipio en las vías cuya regulación del tráfico le correspondan.

En principio, las citadas autoridades crean y aprueban las correspondientes resoluciones de ordenación de instalación, pero en varios casos, sin embargo, no parecen notificarse a la Comisión tal y como establece la [disposición adicional tercera del Decreto 168/98](#) (Llodio-Laudio, Getxo, Vitoria-Gasteiz, Barakaldo y Bilbao).

A su vez, algunas administraciones indican que las grabaciones se conservan por tiempo indefinido (Vitoria-Gasteiz) y cabe destacar que el plazo máximo que establece la normativa es de 1 mes salvo excepciones previstas en la propia disposición adicional tercera.

Por otro lado, la tramitación de la autorización para la instalación de cámaras **fijas** es posible iniciarla a través de la sede electrónica de Gobierno Vasco, a fin de obtener la autorización gestionada por la Dirección de Coordinación de Seguridad y a resolver por la Viceconsejería de Seguridad, tal y como figura en el siguiente enlace <https://www.euskadi.eus/autorizacion/video-vigilancia/web01-tramite/es/>. En



aparición, **no parece prever la posibilidad de solicitar autorizaciones para utilizar cámaras móviles.**

Con respecto a los resultados de la encuesta, en particular, el Departamento de Seguridad de Gobierno Vasco indica que las autorizaciones para el uso de cámaras **móviles** se solicitan de modo conjunto, y no por cámaras o unidades policiales. Este hecho, podría comportar una dificultad para apreciar con carácter previo la concurrencia de un peligro concreto y el cumplimiento del principio de proporcionalidad tal y como establece el [artículo 17 de la LO 7/21](#) relativo al uso de dispositivos **móviles**.

Además, la posibilidad que ofrece el apartado 3 del artículo 9 del [Decreto 168/98](#) de no precisar autorización previa *“cuando se trate de vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, o cuando se trate de los supuestos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización”* puede generar cierta inseguridad jurídica, debido a que los supuestos habilitantes para el uso de cámaras **fijas** quizá no encajen en la misma causa justificativa de peligro para la seguridad ciudadana que para el uso de dispositivos **móviles**. Es más, la tecnología de calidad, alcance, capacidad, etc. incorporada en la actualidad a los dispositivos **móviles** podría permitir la captación de elementos de modo excesivo y, por lo tanto, no superar el juicio de proporcionalidad.

Por ejemplo, el uso de cámaras **móviles** en uniformes de la policía o mediante drones en un casco urbano donde ya existen sistemas fijos, entre otros ejemplos, quizá deban someterse a un control más estricto y exhaustivo que encaje en supuestos de peligro concreto y evaluable para la seguridad ciudadana, y, además, como medio para ponderar la necesidad e idoneidad caso por caso.

Por otro lado, algunas entidades locales utilizan cámaras **móviles** autorizadas por la VCS como báculos portátiles y drones ante la celebración de eventos con gran afluencia de personas, que posiblemente deberían añadir más elementos de valoración y ponderación previa para acreditar la necesidad e idoneidad de su utilización.

Se trata de dispositivos cuyo desarrollo tecnológico es constante y parece razonable someter su utilización a elementos de valoración previa e interna sobre su proporcionalidad que podrían concretarse en instrumentos jurídicos. Es decir, mediante protocolos o instrucciones internas se podrían definir el tipo de eventos y supuestos específicos que pueden motivar la necesidad del uso de dispositivos **móviles**, como la celebración de eventos masivos, y, además, establecer criterios temporales y de espacio a vigilar.



En relación con las cámaras **móviles** utilizadas mediante uniformes policiales, es relevante la ausencia de concreción apriorística que permita evaluar el supuesto de peligro concreto para la seguridad ciudadana y la proporcionalidad de su uso. Con carácter general, parece un supuesto de uso de captación de imágenes y, en su caso, sonidos, en espacios públicos cuya ponderación ante un posible conflicto con otros derechos fundamentales como la intimidad puede afectar no sólo a la ciudadanía, sino también al propio personal trabajador de la administración. Ciertamente, esta defensoría no dispone de elementos para valorar los supuestos de hecho y el alcance temporal y espacial que motiven positivamente la iniciativa de su uso o la decisión de su activación en un momento concreto, pero sí cabe señalar aspectos sobre su utilización que pueden impactar en los derechos fundamentales de las personas.

En lo que respecta a los cuerpos de la policía local, parece recomendable tener en cuenta la Disposición Adicional Primera del [Decreto 168/98](#), que establece unos requisitos específicos ante la utilización de cámaras **móviles** sin autorización previa, en cuyo caso, *“los responsables policiales habrán de dar cuenta mediante informe motivado al Director de Seguridad Ciudadana del Gobierno Vasco, que lo comunicará al Viceconsejero de Seguridad, y a la Comisión de Vigilancia y Libertades y en el plazo máximo de setenta y dos horas”*. En todo caso, parece deseable que los cuerpos de la policía local, a tenor del apartado 2 de la citada DA1ª, recaben e interesen informes de la CVL sobre la adecuación de los registros de imágenes y sonidos que se obtengan o pretendan obtener mediante cámaras **móviles** con objeto de reforzar las garantías jurídicas que deben presidir la toma de datos de imágenes de la ciudadanía en lugares públicos.

En materia de plazos autorizados para el uso de cámaras de videovigilancia por motivos de seguridad ciudadana, existe un aspecto que llama la atención del Ararteko, dado que la normativa establece con respecto a las cámaras **fijas** que serán autorizadas para su uso por un plazo máximo de un año y que podrán renovarse a la expiración del mismo por un período equivalente. Sin embargo, ni la LOVFCS ni el Decreto 168/98 establecen límite temporal para el uso de cámaras **móviles**.

La LO 7/21 viene a establecer, en su [artículo 17.2](#), criterios y límites temporales a observar en las autorizaciones. En este sentido, el apartado citado establece que *“las autorizaciones no se podrán conceder en ningún caso con carácter indefinido o permanente, siendo otorgadas por el plazo adecuado a la naturaleza y las circunstancias derivadas del peligro o evento concreto, por un periodo máximo de un mes prorrogable por otro”*.



Como se ha expuesto anteriormente, algunas peticiones de utilización de cámaras **fijas** y **móviles** se presentan conjuntamente, lo cual, a juicio del Ararteko, puede encajar en un supuesto de hecho concreto que comporte un razonable riesgo o peligro concreto para la seguridad ciudadana y que, además, supere el pertinente juicio de proporcionalidad. Sin embargo, pueden crearse disfunciones y usos no deseados o no previamente autorizados en el caso de que se capten imágenes mediante sistemas **móviles** si no se especifican supuestos, usos y plazos aplicables en las resoluciones autorizadoras.

En último término, parece oportuno comprobar la proporcionalidad de la instalación cuando transcurran los plazos para la renovación de las autorizaciones relativas a instalaciones **fijas**, dado que pueden ser revocadas atendiendo a los criterios de idoneidad y de intervención mínima, y a la exigencia de que exista un razonable riesgo para la seguridad ciudadana y peligro concreto, en el caso de las **móviles**.

El artículo 7 del [Decreto 168/98](#) regula la creación del **registro de autorizaciones** de instalaciones **fijas**. Nada indica con respecto a las autorizaciones relativas a cámaras **móviles** y su posible inscripción en el citado registro, lo cual constituye un vacío que quizá pueda colmarse en aras a la transparencia de la actuación de la administración, especialmente ante la proliferación de diferentes sistemas de cámaras **móviles** como drones, cámaras en uniformes, báculos portátiles y tecnologías similares.

El apartado 3 del citado artículo 7 establece que *"El acceso a los datos contenidos en dicho registro se efectuará de conformidad con lo dispuesto en la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común"*.

En opinión de esta institución, la remisión al acceso de acuerdo con los términos expuestos en la derogada Ley 30/92 se corresponde con el derecho de acceso a la información pública, archivos y registros contemplado en el [artículo 13](#) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y, por lo tanto, cualquier petición de acceso al registro planteado por la ciudadanía se estima que debería tramitarse de acuerdo con las reglas de la [LTBG](#).

Sin perjuicio del cumplimiento de la vertiente pasiva de la transparencia, en aras de la publicidad y transparencia de la actuación de las administraciones públicas, quizá deberían publicarse como medida activa las resoluciones de autorización de instalaciones **fijas** y **móviles** y, como se razonará posteriormente, con objeto de



complementar el deber de informar o de reforzar las reglas de publicidad sobre la captación de imágenes, dado que, parece complicado colocar carteles informativos o advertir a la ciudadanía sobre la presencia de cámaras **móviles** ubicadas en drones, báculos o uniformes de agentes sin acudir a otros medios o elementos informativos.

IV.4. El principio de proporcionalidad

Este Ararteko, en el marco de la encuesta realizada a las distintas entidades públicas, no ha planteado cuestiones específicas sobre el principio de proporcionalidad, en la medida en que los resultados no aportarían elementos de juicio para valorar la doble versión de idoneidad y de intervención mínima que debe presidir el cumplimiento del citado principio.

Sin perjuicio de lo anterior, la encuesta incluye cuestiones particulares planteadas al Departamento de Seguridad del Gobierno Vasco. En concreto, se preguntó si las autorizaciones para la instalación y uso de cámaras tanto **fijas** como **móviles** incluían una valoración de la necesidad e idoneidad de las solicitudes planteadas por los responsables de los servicios y unidades policiales, a lo cual se respondió afirmativamente.

Como punto de partida, conviene apuntar elementos fundamentales relacionados con el principio de proporcionalidad, que, según el Tribunal Constitucional, intérprete supremo de la Constitución y garante de las libertades y derechos fundamentales, es una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, especialmente cuando afectan al derecho a la intimidad.

Según doctrina del Tribunal Constitucional sentada mediante sentencias 56/1996, de 21 de mayo de 1996 ([ECLI:ES:TC:1996:56](#)) y 207/1996, de 22 de enero de 1997 ([ECLI:ES:TC:1996:207](#)), entre otras, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".



En materia de utilización de videocámaras con fines de seguridad ciudadana, el principio de proporcionalidad debe presidir todo supuesto de uso, como se prevé en el propio preámbulo de la LOVFCS:

“Las garantías que introduce la presente Ley en el uso de sistemas de grabación de imágenes y sonidos por parte de las Fuerzas y Cuerpos de Seguridad parten del establecimiento de un régimen de autorización previa para la instalación de videocámaras inspirado en el principio de proporcionalidad, en su doble versión de idoneidad e intervención mínima.”

De acuerdo con lo previsto en la legislación sobre videovigilancia con fines de seguridad ciudadana (LOVFCS), las autorizaciones para la instalación de videocámaras **fijas** y **móviles** deben cumplir una serie de criterios como asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes, la concurrencia de algún peligro concreto, y **fundamentalmente el artículo 6 de la LOVFCS, regulador del principio de proporcionalidad en la doble versión de idoneidad y de intervención mínima**, por cuanto:

“- La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.

- La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas”.

Además, el apartado 4 del citado artículo 6 establece la **exigencia** para utilizar videocámaras de que exista *“un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles”*.

También la LO 7/21 establece que *“la instalación de sistemas de grabación de imágenes y sonidos se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones propias; asegurar la protección de edificios e instalaciones públicas y de sus accesos que estén bajo custodia; salvaguardar y proteger las instalaciones útiles para la seguridad nacional y prevenir, detectar o investigar la comisión de infracciones penales y la protección y prevención frente a las amenazas contra la seguridad pública”* ([artículo 15.2](#)).



El principio de proporcionalidad, por tanto, constituye la garantía constitucional de juicio y ponderación y establece los requisitos y límites para la protección de la seguridad ciudadana como bien colectivo constitucionalmente protegido, así como su equilibrio con otros derechos fundamentales como la intimidad. Si bien el derecho a la intimidad no es absoluto, debe observarse escrupulosamente la ley de videovigilancia a fin de que cualquier límite al derecho sea necesario, proporcionado y respetuoso con el contenido esencial del derecho fundamental.

Atendiendo a las respuestas de las distintas administraciones sobre la ubicación de las cámaras de videovigilancia, cabe señalar que deberían distinguirse distintas normas aplicables en función del fin perseguido. Así, como se ha señalado anteriormente, el Ararteko considera que no siempre es preciso aplicar las disposiciones relativas a la seguridad ciudadana dado que, en algunos casos, probablemente bastará con acudir a lo dispuesto en el [artículo 22](#) de la LOPDGDD para legitimar la captación de imágenes con fines de preservar la seguridad de personas, bienes e instalaciones de titularidad pública. Se trata de una base de legitimación que podría aplicarse interiores, pasillos, oficinas a los cuales accede únicamente personal de la administración, recintos deportivos, bibliotecas, edificios culturales, escuela de música, rampas mecánicas, residencias de personas mayores, piscinas o lugares similares, previo cumplimiento de los requisitos de proporcionalidad, información y demás derechos y garantías para la ciudadanía que establece la normativa de protección de datos.

En particular, este Ararteko quiere llamar la atención sobre la videovigilancia efectuada en lugares en los que puede producirse una captación de imágenes que pueden afectar a la intimidad tanto para la ciudadanía como personal trabajador, dado que el principio de proporcionalidad exige una justificación y ponderación de derechos en juego con objeto de evaluar cuáles prevalecen y, si existen elementos o medios menos lesivos o intrusivos para la intimidad, deben utilizarse al margen de las posibilidades que ofrece la videovigilancia.

Durante los últimos años, diversas instituciones han planteado consultas a la AVPD relacionadas con la captación de imágenes en instalaciones municipales cuya revisión y consulta pueden proporcionar elementos de juicio y ponderación sobre el principio de proporcionalidad previamente a la utilización de cámaras con la finalidad de preservar la seguridad de instalaciones, bienes y personas en consideración a la normativa de protección de datos. Entre otros, los dictámenes [D17-002](#) y [D10-015](#) abordan aspectos destacables sobre el principio de proporcionalidad en el marco de



la protección de datos personales y también refieren a la normativa de seguridad ciudadana a fin de delimitar los ámbitos protegibles y competenciales.

Asimismo, la AEPD publicó una *Guía sobre el uso de videocámaras para seguridad y otras finalidades*¹⁶ que aporta elementos de juicio y valoración previos a la implantación de sistemas de videovigilancia en los cuales el interés legítimo de preservar la seguridad de instalaciones, bienes y personas es la base jurídica aplicable al control de la seguridad por parte de la administración.

Por otro lado, como se ha indicado, las policías pueden efectuar la videovigilancia mediante instalaciones **fijas o móviles** cumpliendo requisitos específicos y el principio de proporcionalidad cuando el fin perseguido tiene su encaje en la seguridad pública. Las peticiones de autorización, con carácter general deben incluir una justificación de la instalación y, en cualquier caso, las resoluciones de autorización deben motivarse. En este sentido, refiere el Departamento de Seguridad de Gobierno Vasco que las autorizaciones para la instalación y uso de cámaras tanto **fijas** como **móviles** incluyen una valoración de la necesidad e idoneidad de las solicitudes planteadas por los responsables de los servicios y unidades policiales.

Un elemento de preocupación para el Ararteko es la autorización de cámaras **fijas** en lugares e instalaciones públicas con fines de seguridad ciudadana en zonas en las que quizá no concurre un razonable riesgo para la seguridad ciudadana como zonas interiores de polideportivos, aulas de cultura e instalaciones análogas y cuyos accesos no se custodian por las policías.

En el supuesto de uso de cámaras **móviles**, resulta precisa la concurrencia de un peligro concreto a fin de autorizar su utilización, aspecto que difícilmente encaja con la proporcionalidad debida si se utilizan de manera cotidiana o masiva como en uniformes de policía, mediante drones o báculos portátiles sin realizar una ponderación previa caso por caso, tal y como exige la vertiente de intervención mínima en contraposición al derecho al honor, a la propia imagen y a la intimidad de las personas.

Esta institución es consciente de que pueden existir situaciones de urgencia para atender hechos que requieren una toma y captación de datos ante un eventual peligro concreto, pero en otros supuestos se utilizan cámaras **móviles** en eventos masivos que se celebran periódicamente, por lo que, *a priori*, el régimen de utilización de los medios como drones o báculos portátiles, y especialmente las cámaras en uniformes policiales, quizá debería ponderarse con mayores garantías si cabe, sin

¹⁶ <https://www.aepd.es/es/documento/guia-videovigilancia.pdf>.



perjuicio de cumplir el régimen general de autorización, como se abordará posteriormente. En particular, esta institución estima que el uso de cámaras **móviles**, a tenor del principio de proporcionalidad y a falta de regulación expresa relativa al alcance y supuestos concretos de utilización, deberían someterse a un previo control interno de la administración en el que se fundamente y motive expresamente la necesidad de su utilización y en su caso, se articulen protocolos, instrucciones o medidas que permitan conocer los límites aplicables para salvaguardar la intimidad de la ciudadanía, dado que, en puridad, los citados medios electrónicos tienen capacidad para captar elementos de la esfera personal como domicilios, locales interiores, o contextos en los que pueden primar otros derechos fundamentales y especialmente, de los menores.

En definitiva, el Ararteko quiere poner de relieve la debida observancia que debe realizarse del principio de proporcionalidad previamente a la petición y autorización de instalaciones **fijas** y **móviles** de videovigilancia en su doble vertiente de idoneidad e intervención mínima, puesto que, en algunos supuestos referentes a instalaciones **fijas**, quizá no resulte preciso legitimar la videovigilancia en las competencias de seguridad pública, sino en el interés legítimo de preservar la seguridad de instalaciones, bienes y personas de acuerdo con las reglas de la normativa de protección de datos. O, en su caso, pueden existir medios menos lesivos o intrusivos para la intimidad para efectuar el control o modular la captación de la imagen, esencialmente de menores o personas con discapacidad en lugares en los que, probablemente no exista un razonable riesgo para la seguridad ciudadana.

Por otro lado, resulta deseable reflexionar y ponderar caso por caso la utilización de sistemas **móviles** de videovigilancia, dado que las posibilidades de vulneración de derechos fundamentales de la ciudadanía parecen aumentar ante la ausencia de parámetros que acoten el alcance, la duración, el espacio y los concretos supuestos de hecho que motiven su uso.

Por ese motivo, parece adecuado que las administraciones públicas competentes regulen mediante instrucciones y protocolos los supuestos que motivan la necesidad de utilización de cámaras y, en la práctica, que se produzca un doble control, interno de la propia administración y externo cuando se solicitan las autorizaciones de instalación y uso a las autoridades competentes. Ello facilitaría, seguramente, la supervisión de la CVL como órgano consultivo de protección de la privacidad para reforzar la garantía del derecho a la propia imagen, a la intimidad y dignidad de los ciudadanos respecto del empleo por la Policía del País Vasco de videocámaras en lugares públicos.



Ello, redundaría en un mejor cumplimiento del principio de proporcionalidad y, además, a conciliar con otros derechos fundamentales de la ciudadanía¹⁷.

¹⁷ STSJG 11/2010 de 14 de enero de 2010 ([ECLI:ES:TSJGAL:2010:185](#)).

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

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

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



IV.5. Gestión de las grabaciones de videovigilancia y plazos de conservación

IV.5.1. Resultados

Administración	Gestión de grabaciones y plazos
Departamento de Seguridad de Gobierno vasco	<ul style="list-style-type: none"> – Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: Se dispone de protocolo y las autorizaciones determinan la unidad policial o administrativa encargada de la custodia material de las grabaciones. – Plazos: No se establecen plazos mínimos, y si se establecen plazos máximos según marco regulador (1 mes por protección de datos; 3 meses según LO 7/21; tráfico 1 mes; 1 mes para instalación fija en vías públicas por seguridad ciudadana según criterio acordado por la Comisión Videovigilancia y Libertades. – Disciplina de tráfico: plazo de 1 mes de conservación. – Cámaras móviles con fines de seguridad ciudadana: El plazo máximo previsto en ley es 1 mes prorrogable por otro. En la práctica la autorización se reduce al plazo de tiempo que dure el evento concreto o resulte de interés policial respecto del peligro para seguridad pública, sin superar el plazo establecido en la ley. – Sin perjuicio de los plazos máximos de conservación de las grabaciones, dicho mantenimiento se ve modulado en determinados ámbitos para mayor garantía de los derechos de la ciudadanía, como por ejemplo el criterio acordado por la CVL de limitar a 1 mes el plazo máximo para la conservación de las imágenes concernientes a la videovigilancia de vías públicas. Más allá de plazos máximos (salvo relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto), el mantenimiento de las imágenes se ve condicionado por la capacidad de almacenaje de los dispositivos técnicos.



Administración	Gestión de grabaciones y plazos
Ayuntamiento de Vitoria-Gasteiz	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo de gestión y la unidad u órgano de gestión es el departamento de seguridad ciudadana. - Plazo de conservación mínimo: no. - Plazo máximo: 1 mes con carácter general. En materia de disciplina de tráfico, conservación indefinida.
Ayuntamiento de Bilbao	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo y la unidad u órgano interno de gestión es el laboratorio de audiovisuales de la Policía Municipal. - Se establece plazo mínimo de conservación. - Plazos máximos: Cámaras instaladas en edificios, el plazo es de 1 mes; en el caso de las cámaras de tráfico y de control de acceso de vehículos al Casco Viejo 15 días, conservadas en el Área de Movilidad y Sostenibilidad, transcurrido ese plazo, las nuevas grabaciones se realizan sobre las anteriores. En el caso de las grabaciones realizadas por cámaras utilizadas por Seguridad Ciudadana, se aplica lo establecido en cada una de las autorizaciones emitidas para cada una de las instalaciones. Las cámaras que no están bajo el paraguas de esas autorizaciones se ajustan al periodo marcado por las cámaras sí recogidas, dentro de cada una de las instalaciones. - Disciplina de tráfico: plazo inferior a 1 mes
Ayuntamiento de Donostia/San Sebastián	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: existe protocolo de gestión y órgano gestor guardia o jefatura municipal. - Se establece plazo mínimo de conservación. - Plazo máximo: 1 mes. En materia de disciplina de tráfico se conservan grabaciones por plazo inferior a 1 mes.
Ayuntamiento de Barakaldo	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo y el órgano de gestión es la jefatura de policía local. - Se establece plazo mínimo de conservación. - Plazo máximo: con carácter general, se establecen en 1 mes. Por disciplina de tráfico 1 mes.



Administración	Gestión de grabaciones y plazos
Ayuntamiento de Portugalete	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo y el órgano gestor tal y como figura en las Resoluciones del Gobierno Vasco es Alcalde, Jefe de Policía Local y sus sustitutos en periodo de ausencia. - Se establece plazo mínimo de conservación. - Plazo máximo de conservación: 1 mes. En materia de disciplina de tráfico se conservan grabaciones por plazo inferior a 1 mes.
Ayuntamiento de Getxo	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo y es la jefatura de policía local el órgano gestor. - Se establece plazo mínimo de conservación. - Plazo máximo de conservación: 1 mes con carácter general, incluida disciplina de tráfico
Ayuntamiento de Basauri	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo y el órgano gestor es la jefatura de policía local - Se establece plazo mínimo de conservación. - Plazo máximo de conservación: 1 mes.
Ayuntamiento de Errenteria	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo y el órgano gestor es la jefatura de policía local - Se establece plazo mínimo de conservación. - Plazo máximo de conservación: 1 mes con carácter general, incluida disciplina de tráfico.
Ayuntamiento de Tolosa	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: Se dispone de protocolo y el órgano gestor es la policía municipal, sin concreción de la unidad. - Se establece plazo mínimo de conservación. - Plazo máximo de conservación: 8 días en función de la capacidad del disco duro. Plazo inferior a 1 mes por disciplina de tráfico.



Administración	Gestión de grabaciones y plazos
Ayuntamiento de Irun	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: se dispone de protocolo y el órgano gestor es la jefatura de policía local. - Se establece plazo mínimo de conservación. - Plazo de conservación máximo: 7 días. Plazo inferior a 1 mes por disciplina de tráfico.
Ayuntamiento de Llodio-Laudio	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: no se dispone de protocolo que establezca a disposición y custodia de qué unidad u órgano interno quedan las grabaciones. - Se establece plazo mínimo de conservación . - Plazo máximo de conservación: 1 mes. Plazo inferior a 1 mes por disciplina de tráfico.
Ayuntamiento de Zumarraga	<ul style="list-style-type: none"> - No existe protocolo interno. - No existe plazo mínimo de conservación. - El plazo máximo lo determina la capacidad del sistema informático, aproximadamente 10 días.
Ayuntamiento de Eibar	<ul style="list-style-type: none"> - Protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones: jefatura de policía local. - Existe plazo mínimo de conservación. - Plazo máximo de conservación: 1 mes con carácter general, incluida disciplina de tráfico.
Ayuntamiento de Ermua	<ul style="list-style-type: none"> - Se indica la existencia de protocolo interno pero no se informa de la unidad u órgano, sino que se describe el sistema informático de gestión. - Se establece plazo mínimo de conservación - Plazo máximo de conservación: 1 mes. Plazo inferior a 1 mes por disciplina de tráfico.



IV.5.2. Análisis y valoración

Con respecto a la gestión de grabaciones efectuadas por motivos de seguridad ciudadana y plazos de gestión y conservación, el artículo 8 de la LOVFCS establece:

- “1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto.*
- 2. Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley.*
- 3. Se prohíbe la cesión o copia de las imágenes y sonidos obtenidos de conformidad con esta Ley, salvo en los supuestos previstos en el apartado 1 de este artículo.*
- 4. Reglamentariamente la Administración competente determinará el órgano o autoridad gubernativa que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. Dicho órgano será el competente para resolver sobre las peticiones de acceso o cancelación promovidas por los interesados”.*

Además, el artículo 18.3 de la LO 7/21 dispone:

- “(…) 3. Las grabaciones serán destruidas en el plazo máximo de tres meses desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, sujetas a una investigación policial en curso o con un procedimiento judicial o administrativo abierto”.*

Es posible observar en las disposiciones citadas cómo los plazos de conservación difieren aun cuando el objeto de captación tiene el mismo fin, prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

Se trata de un aspecto que genera inseguridad jurídica y que tiene su reflejo en las contestaciones proporcionadas por las administraciones públicas participantes en el estudio.

Por ejemplo, el Departamento de Seguridad del Gobierno Vasco refiere distintos plazos de conservación en función de las normas aplicables, 3 meses de acuerdo con



la LO 7/21 y, sin embargo, se indica la conservación como máximo de 1 mes para instalación **fija** en vías públicas por seguridad ciudadana según criterio acordado por la CVL.

Todas las entidades locales refieren aplicar un plazo máximo de 1 mes de conservación de imágenes relacionadas con la seguridad ciudadana o incluso inferior en función de las características técnicas de los dispositivos para grabar y conservar datos.

En cualquier caso, resulta deseable una aclaración y concreción de los citados plazos de conservación desde el punto de vista normativo, lo cual no impide que las propias policías establezcan igualmente criterios concretos de conservación mediante protocolos específicos.

En este sentido, el apartado 4 del [artículo 8](#) de la LOVFCs establece que debe determinarse el órgano o autoridad que tendrá a su cargo la custodia de las imágenes obtenidas y la responsabilidad sobre su ulterior destino, incluida su inutilización o destrucción. De las respuestas recibidas al cuestionario, se desprende que prácticamente la totalidad de las administraciones públicas consultadas disponen de protocolos de gestión de grabaciones. En el caso del Departamento de Seguridad del Gobierno Vasco, se explica que sus propias autorizaciones de instalación detallan la unidad policial o administrativa encargada de la custodia material de las grabaciones.

Sin embargo, en el caso de las entidades locales, en la mayoría de las ocasiones se refiere que no existe un órgano o unidad administrativa específica encargada de la gestión de las grabaciones, y bien se responde que es el área o departamento de seguridad ciudadana o la jefatura de policía local. Destaca Bilbao, cuyo Ayuntamiento especifica que la unidad u órgano interno de gestión es el laboratorio de audiovisuales de la policía municipal, lo cual parece una buena práctica para mantener la independencia como garantía de custodia y trazabilidad ante supuestos de puesta a disposición de terceros legitimados. En otros supuestos, a falta de una estructura similar al cuerpo de policía de Bilbao, parece aconsejable establecer protocolos específicos de custodia y conservación de grabaciones con objeto de garantizar la independencia de las actuaciones policiales, especialmente, de la trazabilidad de la custodia, ante peticiones de acceso por terceros legitimados y así evitar la pérdida o destrucción no autorizada.

De este modo, se podrán aportar más garantías para la protección de los derechos de la ciudadanía en supuestos que afecten al ejercicio de derechos (estableciendo



plazos mínimos y máximos de conservación) y para su puesta a disposición ante órganos judiciales u otras policías, o incluso, de esta institución.

Por último, cabe destacar que **la normativa no establece plazos mínimos de conservación de imágenes**, lo cual provoca que, las decisiones de conservación y en su caso, puesta a disposición de terceros, quede al albur de la tecnología, porque el sistema no permite grabar más tiempo del deseado hasta alcanzar los plazos máximos, o de decisiones discrecionales del personal interno que, a falta de protocolos de custodia y trazabilidad, permitirían la destrucción de imágenes en cualquier momento.

Así, se puede pensar en la posibilidad de que un sistema de videovigilancia únicamente permita la grabación de imágenes durante 48 horas, pasadas las cuales, el historial grabado se borra con las imágenes captadas y así sucesivamente, por lo que, salvo que exista algún tipo de denuncia o infracción que motive su conservación y puesta a disposición, se destruyan definitivamente las grabaciones de modo automatizado. En este sentido, esta institución estima que los protocolos e instrucciones de gestión y conservación de grabaciones deberían establecer reglas claras de custodia y trazabilidad de las imágenes por personal debidamente autorizado que permitan esclarecer cualquier duda sobre la integridad de los videos, y, además, para su puesta a disposición de otros órganos internos o externos competentes o legitimados.

Además, el acceso a los datos personales de videovigilancia quizá deba atender a criterios claros sobre el personal autorizado para su tratamiento a tenor de lo previsto en la normativa de protección de datos y en el ENS, como se verá en posteriores apartados, con objeto de garantizar la seguridad y confidencialidad de la información y también la transparencia, integridad y legalidad de la actuación de la administración.

Ciertamente, un uso indebido de las imágenes puede comportar consecuencias jurídicas para el personal interno tal y como se prevé en [Disposición adicional séptima](#) de la propia LOVFC:

- “1. Se considerarán faltas muy graves en el régimen disciplinario de las Fuerzas y Cuerpos de Seguridad del Estado, las siguientes infracciones:*
- a) Alterar o manipular los registros de imágenes y sonidos siempre que no constituya delito.*



b) Permitir el acceso de personas no autorizadas a las imágenes y sonidos grabados o utilizar éstos para fines distintos de los previstos legalmente.”

Disposición que tiene su previsión específica en el [artículo 139](#) de la LPPV por lo que, parece recomendable detallar exhaustivamente los protocolos de gestión, conservación y traza de imágenes de videovigilancia durante un plazo mínimo por el personal autorizado exclusivamente, para su uso interno o puesta a disposición de terceros legitimados en concordancia con lo previsto en el [artículo 12](#) del Decreto 168/98 relativo custodia y conservación de imágenes.

IV.6. Principio de información

IV.6.1. Resultados

Administración	Principio de información (medios y canales)
Departamento de Seguridad de Gobierno vasco	Se utilizan carteles de protección de datos y de seguridad ciudadana para informar sobre cámaras fijas y también se utilizan carteles para advertir sobre existencia de cámaras móviles y también mediante distintivos visibles en uniformes, vehículos, o lugar de ubicación del dispositivo, pero no mediante páginas web, redes sociales, y canales análogos.
Ayuntamiento de Vitoria-Gasteiz	Se informa mediante ambos tipos de cartelería para avisar de las cámaras fijas y se utilizan distintivos visibles en uniformes, vehículos, o lugar de ubicación del dispositivo para las cámaras móviles, pero no mediante páginas web, redes sociales, y canales análogos. También se informa de cámaras de regulación de acceso a casco urbano, pero no graban.
Ayuntamiento de Bilbao	Se utilizan carteles de fondo azul para cámaras fijas y móviles. Se disponen carteles informativos para otro tipo de videovigilancia.
Ayuntamiento de Donostia/San Sebastián	Se utilizan carteles por protección de datos y de fondo azul por seguridad ciudadana. Sobre cámaras móviles (drones, báculos) se informa con carteles azules.
Ayuntamiento de Barakaldo	Carteles de fondo azul por seguridad ciudadana



Administración	Principio de información (medios y canales)
Ayuntamiento de Portugalete	Carteles de ambos tipos por protección de datos y seguridad ciudadana.
Ayuntamiento de Getxo	Carteles informativos de protección de datos y de seguridad ciudadana.
Ayuntamiento de Basauri	Carteles informativos de protección de datos y de seguridad ciudadana. Se utilizan distintivos visibles para informar sobre grabación mediante cámaras en uniformes.
Ayuntamiento de Errenteria	Ambos tipos de cartelería en función de las finalidades perseguidas, de protección de datos y de fondo azul por seguridad ciudadana.
Ayuntamiento de Tolosa	Carteles de fondo azul por seguridad ciudadana y se informa con carteles al efecto en instalaciones y recintos municipales.
Ayuntamiento de Irun	Carteles de fondo azul por seguridad ciudadana.
Ayuntamiento de Llodio-Laudio	Ambos tipos de cartelería en función de las finalidades perseguidas, de protección de datos y de fondo azul por seguridad ciudadana.
Ayuntamiento de Zumarraga	Ambos tipos de cartelería en función de las finalidades perseguidas, de protección de datos y de fondo azul por seguridad ciudadana.
Ayuntamiento de Eibar	Ambos tipos de cartelería en función de las finalidades perseguidas, de protección de datos y de fondo azul por seguridad ciudadana.
Ayuntamiento de Ermua	Cámaras fijas: Carteles informativos de fondo amarillo o similar por protección de datos. Cámaras móviles: Se informa mediante distintivos visibles en uniformes, vehículos, o lugar de ubicación del dispositivo y a través de páginas web, redes sociales, y canales análogos.



IV.6.2. Análisis y valoración

Las modalidades reguladas de publicidad e información que se debe aportar a la ciudadanía concernientes a la existencia de sistemas de videovigilancia no siempre establecen adecuadamente el alcance y contexto de la misma.

En materia de videovigilancia con fines de seguridad ciudadana, la LOVFCS establece que la ciudadanía debe ser informada *“de manera clara y permanente de la existencia de videocámaras fijas, sin especificar su emplazamiento, y de la autoridad responsable”* ([artículo 9](#)), además, en el ámbito territorial de Euskadi, el Decreto 168/98 regula en idénticos términos la citada obligación ([artículo 8](#)), si bien se añade en el apartado 2, que *“cuando lo aconsejen razones de interés público apreciadas por el órgano competente se podrá publicar en el Boletín Oficial del País Vasco un extracto de la resolución autorizante conteniendo la fecha de autorización y su plazo de vigencia, la localización genérica de los lugares observados sin especificar el emplazamiento de las cámaras, así como el órgano y autoridad de custodia y resolución de las peticiones de acceso y cancelación”*. Fórmula que, en ciertos supuestos y en aras de ese interés público aludido, podría complementar la falta de regulación específica, si bien este Ararteko no ha detectado en boletines oficiales ninguna publicación al respecto.

El [artículo 16.5](#) LO 7/2021 también indica que *“Los ciudadanos serán informados de manera clara y permanente de la existencia de estas videocámaras fijas, sin especificar su emplazamiento, así como de la autoridad responsable del tratamiento ante la que poder ejercer sus derechos”* pero se enmarca en el precepto relativo a instalaciones fijas.

Además, la [Orden de 15 de abril de 2011](#), del Consejero de Interior del Gobierno Vasco, por la que se establece el contenido y diseño de los carteles informativos de la instalación y uso de instalaciones **fijas** por la Policía del País Vasco desarrolla los preceptos anteriormente citados y regula las características de los carteles que deben advertir sobre la videovigilancia efectuada por la policía de Euskadi en vías y espacios públicos.

Resulta destacable que la orden mencionada, hace referencia al modo de informar cuando se realice la videovigilancia mediante instalaciones **fijas**. Cabe indicar que la fundamentación de la norma se basa en los criterios adoptados por la CVL, que, en sesión de 7 de octubre de 2009, estableció que la información al público *“se debe de producir mediante la colocación de carteles informativos instalados de una*



manera clara, visible y permanente de manera que avisen al público de que se entra en una zona videovigilada. Estos carteles deben de ser de un número suficiente de modo que el público pueda verlos, acceda desde donde acceda, y esté informado en todo momento de que pasa por una zona videovigilada”.

Con carácter general, de acuerdo con las respuestas aportadas por las administraciones participantes del estudio, parece cumplirse el deber de informar ante la existencia de instalaciones **fijas** de videovigilancia dado que se reconoce la existencia y colocación de carteles de fondo azul con las características establecidas en la [Orden de 15 de abril de 2011](#) del Consejero de Interior de Gobierno Vasco. En el supuesto del Ayuntamiento de Zumarraga, se refiere la existencia de carteles de fondo azul por seguridad ciudadana si bien ha reportado anteriormente que no se utilizan con ese fin ni disponen de autorización al efecto.

La orden citada, como se ha expuesto, únicamente refiere al deber de informar sobre instalaciones **fijas**, aspecto este que deja fuera del ámbito de aplicación a los dispositivos **móviles**, por lo que parece conveniente una revisión y actualización de la disposición.

En cualquier caso, parece recomendable que las administraciones vascas revisen los carteles utilizados y colocados periódicamente, dado que deben informar sobre la autoridad responsable de la instalación a efectos de que la ciudadanía pueda ejercer sus derechos.

El deber de informar establecido en la normativa y conforme al criterio formulado por la CVL parece complicado de cumplir cuando se utilizan dispositivos **móviles** como los reportados por las administraciones participantes en el estudio. Evidentemente, existe un vacío legal que no establece el modo de informar a la ciudadanía sobre el uso y captación de imágenes mediante cámaras **móviles** utilizadas por motivos de seguridad ciudadana, y ello conlleva una inseguridad jurídica dado que cada cuerpo elige el modo y medio para informar, o en muchos supuestos, no se informa.

Es indiscutible la necesidad de disponer de una regulación específica sobre el deber de informar a la ciudadanía acerca del uso de dispositivos **móviles** como los reportados por las distintas administraciones cuando se utilizan en uniformes policiales, mediante drones o báculos portátiles, entre otros ejemplos.



En cualquier caso, a falta de regulación, resulta deseable resolver esta cuestión en aras de garantizar el derecho de información de la ciudadanía sobre el tratamiento y captación de sus datos personales con carácter previo. En este sentido, el desarrollo de protocolos o instrucciones internas que aborden el principio de información como un aspecto ineludible a desarrollar y garantizar, constituye una medida factible, en opinión del Ararteko, para cumplir con el deber de informar sobre la captación y tratamiento de imágenes de la ciudadanía mediante dispositivos **móviles** dado que, en la práctica, son sistemas que pueden producir mayores afecciones al derecho al honor, a la propia imagen y a la intimidad de las personas.

Existen supuestos de urgencia, que quizá no cabe prever con antelación, sin embargo, en la mayoría de los casos de usos reportados ante la celebración de eventos masivos, parece plausible articular medios para informar a la ciudadanía con carácter previo o en su defecto, para la creación de disposiciones internas que permitan a la ciudadanía conocer el responsable y contexto o naturaleza de la captación, y especialmente los motivos que concurren ante un peligro concreto o evento concreto tal y como se dispone en el [artículo 6.4](#) de la LOVFC y en el [artículo 17.1 de la LO 7/2021](#).

Por otro lado, la publicación de actividades de tratamiento de datos personales por motivos de videovigilancia es una obligación, pero también un adecuado modo de informar a la ciudadanía sobre el objetivo pretendido, fines y legitimación. Los aspectos relativos a las obligaciones en materia de protección de datos se analizan en el apartado relativo a "[obligaciones de protección de datos](#)" del presente estudio.

Por último, cabe señalar que, la omisión del deber de informar a la persona interesada acerca del tratamiento de sus datos de carácter personal conforme a lo dispuesto en la LO 7/21 puede comportar una infracción muy grave ([artículo 58.f](#)), y evidentemente la captación de imágenes resulta un tratamiento de datos de carácter personal.



IV.7. Ejercicio y atención de derechos de la ciudadanía

IV.7.1. Resultados

Administración	Ejercicio y atención de derechos
Departamento de Seguridad de Gobierno vasco	<p>La unidad u órgano interno encargado de atender el ejercicio de derechos relacionados con las grabaciones (como acceso o supresión) es:</p> <p>VCS para videovigilancia gestión policial; así como el correspondiente órgano responsable (Dirección) cuando dispone de una actividad de tratamiento de videovigilancia</p> <p>Órgano responsable de cada actividad de tratamiento de videovigilancia:</p> <ul style="list-style-type: none"> - Viceconsejería Seguridad para videovigilancia de gestión de la Ertzaintza y sus instalaciones; - Dirección de Trafico en su ámbito. <p>Se dispone de un protocolo o procedimiento de atención de derechos relacionado con las grabaciones.</p>
Ayuntamiento de Vitoria-Gasteiz	<p>Unidad u órgano interno encargado de atender el ejercicio de derechos: La jefatura de la policía local. Disponen de protocolo.</p>
Ayuntamiento de Bilbao	<p>Unidad u órgano interno encargado de atender el ejercicio de derechos: Las Direcciones de las unidades responsables del tratamiento de los datos: Dirección de Presupuestos (cámaras en edificios), Dirección de Policía Municipal (cámaras de Seguridad Ciudadana) y Dirección de Movilidad y Sostenibilidad (cámaras de tráfico).</p> <p>Se dispone de un protocolo o procedimiento de atención de derechos relacionado con las grabaciones.</p>
Ayuntamiento de Donostia/San Sebastián	<p>Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local.</p> <p>Se dispone de protocolo de atención de derechos.</p>
Ayuntamiento de Barakaldo	<p>Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local.</p> <p>Se dispone de protocolo de atención de derechos.</p>
Ayuntamiento de Portugalete	<p>La unidad u órgano interno encargado de atender el ejercicio de derechos relacionados con las grabaciones (como acceso o supresión) es Alcaldía - para los Derechos de acceso y cancelación.</p> <p>Se dispone de protocolo de atención de derechos.</p>



Administración	Ejercicio y atención de derechos
Ayuntamiento de Getxo	Unidad u órgano interno encargado de atender el ejercicio de derechos: Delegada de protección de datos del ayuntamiento. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Basauri	Unidad u órgano interno encargado de atender el ejercicio de derechos: Se encarga la jefatura, dirección o responsable del área que dispone de los medios de grabación y de cuya instalación es responsable. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Errenteria	Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Tolosa	Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Irun	Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Llodio-Laudio	Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Zumarraga	Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Eibar	Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local. Se dispone de protocolo de atención de derechos.
Ayuntamiento de Ermua	Unidad u órgano interno encargado de atender el ejercicio de derechos: jefatura de la policía local. Se dispone de protocolo de atención de derechos.



IV.7.2. Análisis y valoración

Las disposiciones en materia de videovigilancia regulan los derechos de la ciudadanía para acceder y, en su caso, cancelar las imágenes de videovigilancia efectuadas por motivos de seguridad ciudadana. De igual modo, la legislación establece de qué modo y qué criterios han de observar las administraciones a la hora de atender el ejercicio de los citados derechos.

Así, el artículo 9.2 de la LOVFCS establece:

“Toda persona interesada podrá ejercer los derechos de acceso y cancelación de las grabaciones en que razonablemente considere que figura. No obstante, el ejercicio de estos derechos podrá ser denegado por quien custodie las imágenes y sonidos, en función de los peligros que pudieran derivarse para la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando”.

El [artículo 15](#) del Decreto 168/98 amplía las condiciones para solicitar los derechos de acceso y cancelación, y los criterios de atención de estos. Cabe destacar que, se regulan los motivos para su posible denegación, el plazo de atención (1 mes) y que mediante “Orden del Consejero de Interior se desarrollará el procedimiento y las modalidades en las que se hagan efectivos los derechos de acceso y cancelación”, disposición que no se ha aprobado hasta la actualidad.

Asimismo, el [artículo 20](#) de la LO 7/21 regula las condiciones generales de ejercicio de los derechos de las personas interesadas y, por lo tanto, abarca igualmente la posibilidad de ejercicio de derechos sobre las grabaciones de videovigilancia. Cabe destacar que, la citada norma regula el modo y atención del derecho de acceso con mayor detalle y también los derechos de rectificación, supresión, limitación y supresión, por lo que desaparece el derecho de cancelación.

Con respecto a las respuestas aportadas por las administraciones públicas participantes, cabe destacar en primer lugar que, prácticamente todas las administraciones públicas participantes refieren que disponen de protocolos o procedimientos de atención de derechos de la ciudadanía en relación con los tratamientos de datos relacionados con la videovigilancia. Aspecto que se considera positivo si bien se desconoce el grado de despliegue interno de los citados protocolos y su coherencia con los distintos supuestos de la videovigilancia. En este sentido, se ha de diferenciar los derechos de acceso y supresión de datos comprensivos de datos personales objeto



de tratamiento de acuerdo con fines de preservar la seguridad de instalaciones, bienes y personas, de aquellos tratamientos cuyo objeto tiene como fin la seguridad ciudadana, puesto que las normas relativas a la videovigilancia por seguridad ciudadana tienen sus particularidades.

Cabe advertir que las normas actuales en protección de datos y también la LO 7/2021 regulan nuevos derechos que pueden ser ejercidos por la ciudadanía que no se contemplan en las disposiciones de 1997 y 1998. En concreto, en la actualidad, la ciudadanía puede ejercer, en relación con la videovigilancia de seguridad ciudadana, el derecho de acceso, pero también de rectificación, limitación o el de supresión, que no se prevén en las disposiciones anteriores. Aspecto normativo fundamental a tener en cuenta para que los protocolos desarrollados por las administraciones públicas respondan a la realidad jurídica de los derechos de la ciudadanía.

Por otro lado, destaca que las administraciones atribuyen la gestión y atención de derechos de la ciudadanía a distintos órganos internos y en función del tipo de sistema de videovigilancia y objeto de control o protección. En algunos supuestos, son distintas áreas o direcciones municipales las responsables de atención de derechos en función de si se trata de cámaras de instalaciones municipales, de seguridad ciudadana o carretera (Ayuntamiento de Bilbao). En otros, es directamente la persona delegada de protección de datos la figura que atendería el ejercicio de derechos.

En el caso del Departamento de Seguridad de Gobierno Vasco, se indica que es cada órgano diferenciado según las actividades de tratamiento definidas, el que responde, bien la Viceconsejería Seguridad en materia de gestión policial o de videovigilancia de gestión de la Ertzaintza y sus instalaciones, bien la Dirección de Tráfico en su ámbito de control y competencia.

En este sentido, tal y como se señala posteriormente, en el registro de actividades del Gobierno Vasco¹⁸ no existe una actividad de tratamiento de datos personales en materia de videovigilancia con fines de seguridad ciudadana bajo titularidad del Departamento de Seguridad de Gobierno Vasco por lo que se desconoce el órgano ante el cual ejercer los derechos al efecto.

¹⁸ <https://www.euskadi.eus/web01-aprat/es/ac34aRatWebWar/control/arboll?locale=es>.



Sin embargo, en la página web bajo el dominio de internet [Ertzaintza.euskadi.eus](https://www.ertzaintza.euskadi.eus)¹⁹ sí que se define una actividad de tratamiento denominada videovigilancia cuya responsabilidad se atribuye a la VCS, y que refiere como lugar de ejercicio de derechos el Centro de Elaboración de Datos de la Policía de Euskadi (CEDPE) en Erandio y se ofrece una dirección de correo electrónico para atender el ejercicio de derechos: dpd-dbo@ertzaintza.eus.

Parece recomendable unificar criterios con respecto a la atención de derechos en materia de videovigilancia que permita a la ciudadanía discernir si se deben plantear ante la persona delegada de protección de datos de la CAE, como se contempla para el resto de las actividades de tratamiento de titularidad de la VCS que figuran en el registro del Gobierno, o bien es preciso acudir a la persona delegada de protección de datos de la Ertzaintza.

De manera proactiva y positiva, la página web²⁰ de la delegada de protección de datos, unidad adscrita orgánicamente a la Viceconsejería de Régimen Jurídico del Departamento de Gobernanza Pública y Autogobierno, ofrece información específica sobre videovigilancia²¹ y medios para ejercer los derechos y en concreto, aspectos particulares aplicables a los tratamientos realizados por la Ertzaintza²², pero, en la práctica, no se distingue adecuadamente el órgano competente ante el cual ejercer derechos en el ámbito de la videovigilancia y en función de las finalidades perseguidas por la administración..

En opinión del Ararteko, resulta fundamental conocer y distinguir las normas y disposiciones aplicables a cada supuesto de ejercicio y atención de derechos, dado que los plazos de conservación pueden ser diferentes y los límites al acceso y supresión igualmente diversos en función de la finalidad del tratamiento. Así, en materia de seguridad ciudadana existe un régimen especial de atención de derechos relativos a videovigilancia que difiere del régimen establecido en la normativa de protección datos.

¹⁹ <https://www.ertzaintza.euskadi.eus/lfr/web/ertzaintza/protecci%C3%B3n-de-datos-de-car%C3%A1cter-personal>

²⁰ <https://www.euskadi.eus/gobierno-vasco/delegada-proteccion-datos/inicio/>.

²¹ <https://www.euskadi.eus/tratamiento-de-datos-de-las-cameras-de-videovigilancia/web01-a2datuba/es/>.

²² <https://www.euskadi.eus/ejercicio-derechos-ante-ertzaintza/web01-a2datuba/es/>.



IV.8. Obligaciones básicas de protección de datos

IV.8.1. Resultados

Administración	Ejercicio y atención de derechos
Departamento de Seguridad de Gobierno vasco	<ul style="list-style-type: none"> - Se dispone de actividades de tratamiento creadas para legitimar el tratamiento y publicadas en el portal de transparencia. - Licitud: seguridad ciudadana, preservar seguridad de instalaciones bienes y personas en base a interés legítimo y disciplina de tráfico. - Se prevé la cesión de datos a otras policías y órganos judiciales.
Ayuntamiento de Vitoria-Gasteiz	<ul style="list-style-type: none"> - Se dispone de actividades de tratamiento, pero no publicadas en el portal de transparencia. - Licitud: Interés legítimo, seguridad ciudadana y disciplina de tráfico. - Se prevé cesión a policías y órganos judiciales.
Ayuntamiento de Bilbao	<ul style="list-style-type: none"> - Se dispone de actividades de tratamiento creadas para legitimar el tratamiento y publicadas en el portal de transparencia. - Licitud: seguridad ciudadana, preservar seguridad de instalaciones bienes y personas en base a interés legítimo y disciplina de tráfico. - Se prevé la cesión de datos a otras policías y órganos judiciales.
Ayuntamiento de Donostia/San Sebastián	<ul style="list-style-type: none"> - Refieren que se han creado varias en función de los fines perseguidos (seguridad ciudadana, disciplina de tráfico, protección de bienes e instalaciones, etc.) y que no se encuentran publicadas en el portal de transparencia. - Licitud: Interés legítimo, seguridad ciudadana, disciplina de tráfico. - Cesiones a órganos judiciales y otras policías (en la actividad de tratamiento no se contempla).
Ayuntamiento de Barakaldo	<ul style="list-style-type: none"> - No disponen de actividades de tratamiento de datos creadas pero posteriormente refieren que sí se encuentran publicadas en el portal de transparencia. - Licitud: seguridad ciudadana, disciplina de tráfico. - Se prevé cesión a policías y órganos judiciales, es correcto también en la actividad de tratamiento.



Administración	Ejercicio y atención de derechos
Ayuntamiento de Portugalete	<ul style="list-style-type: none"> - Se han creado varias actividades en función de los fines perseguidos (seguridad ciudadana, disciplina de tráfico, protección de bienes e instalaciones, etc.) - Licitud: Interés legítimo, seguridad ciudadana, disciplina de tráfico. - Cesiones a órganos judiciales y otras policías.
Ayuntamiento de Getxo	<ul style="list-style-type: none"> - Refieren la creación de distintas actividades en función de las finalidades (seguridad ciudadana, disciplina de tráfico, protección de bienes e instalaciones, etc.) y que se encuentran publicadas en el portal de transparencia. - Cesiones: órganos judiciales y también otras policías.
Ayuntamiento de Basauri	<ul style="list-style-type: none"> - Se dispone de actividades de tratamiento, pero no publicadas en el portal de transparencia. - Licitud: Interés legítimo, seguridad ciudadana. - Cesiones a órganos judiciales y otras policías.
Ayuntamiento de Errenteria	<ul style="list-style-type: none"> - No se han creado actividades de tratamiento de datos ni se han publicado en el portal de transparencia. - Licitud: interés legítimo, seguridad ciudadana y disciplina de tráfico. - Cesiones a órganos judiciales y otras policías.
Ayuntamiento de Tolosa	<ul style="list-style-type: none"> - No se han creado actividades de tratamiento ni se han publicado en el portal de transparencia. - Licitud: interés legítimo y disciplina de tráfico. - Cesiones a órganos judiciales.
Ayuntamiento de Irun	<ul style="list-style-type: none"> - Se han creado actividades y figuran en el portal de transparencia - Licitud: interés legítimo, seguridad ciudadana y disciplina de tráfico. - Cesiones a órganos judiciales y otras policías.
Ayuntamiento de Llodio-Laudio	<ul style="list-style-type: none"> - Refieren que no hay actividades de tratamiento y que no se encuentran en el portal de transparencia. - Licitud: interés legítimo, seguridad ciudadana, (no disciplina de tráfico). - Se diferencia plazo (1 mes en el ámbito de seguridad por protección de datos. 3 meses por prevención, detección, investigación y enjuiciamiento de infracciones penales.)



Administración	Ejercicio y atención de derechos
	<ul style="list-style-type: none"> - Cesiones contempladas a órganos judiciales y otras policías.
Ayuntamiento de Zumarraga	<ul style="list-style-type: none"> - Se dispone de actividad de tratamiento, pero no publicada en el portal de transparencia. - En materia de protección de datos sí se señala que la base jurídica del tratamiento es seguridad ciudadana, pero, sin embargo, no se contempla en la pregunta relativa a las finalidades de la videovigilancia. - Se prevé la cesión a órganos judiciales.
Ayuntamiento de Eibar	<ul style="list-style-type: none"> - Se dispone de actividad de tratamiento, pero no publicada en el portal de transparencia. - Licitud: interés legítimo, disciplina de tráfico. - Se prevé la cesión a órganos judiciales y otras administraciones competentes.
Ayuntamiento de Ermua	<ul style="list-style-type: none"> - Se dispone de actividad de tratamiento, pero no publicada en el portal de transparencia. - Licitud: interés legítimo, disciplina de tráfico. - Se prevé la cesión a órganos judiciales y otras administraciones competentes.

IV.8.2. Análisis y valoración

La normativa de protección de datos en vigor ([artículo 30 RGPD](#) y [31 LOPDGDD](#)) establece la obligación de crear registros de actividades de tratamiento de datos personales que definan la estructura, finalidades y licitud, entre otros aspectos, de los tratamientos de datos personales que efectúen los responsables de la recogida de datos.

En el ámbito del sector público, además, las actividades de tratamiento creadas deben publicarse en los portales de transparencia correspondientes de acuerdo con el [artículo 6 bis](#) de la [LTBG](#).

De acuerdo con las respuestas aportadas, en la mayoría de los casos no se han creado actividades de tratamiento con fines de preservar la seguridad de instalaciones, bienes y personas. Es decir, o bien no existen o se indica que la licitud encaja en algún fin de interés público como la seguridad ciudadana.



El Ararteko estima que en determinados supuestos, la base jurídica habilitante para tratar datos puede ser el interés legítimo para preservar la seguridad de algunas instalaciones o bienes a tenor del [artículo 22.1 LOPDGDD](#), como pueden ser edificios que simplemente se destinan a la prestación de servicios públicos en los que difícilmente puede concurrir un peligro real y efectivo para la seguridad ciudadana o el objeto de control es el propio bien o instalación como escaleras mecánicas, algunos recintos deportivos, edificios culturales, oficinas, aparcamientos de bicis o interiores de algunos elementos.

En este sentido, parece recomendable crear actividades de tratamiento de datos personales diferenciadas en función del objeto de control y las normas habilitantes, o bien protección de datos o bien fines de seguridad ciudadana.

Con respecto a las actividades de tratamiento en materia de videovigilancia, cabe destacar que el Departamento de Seguridad de Gobierno Vasco refiere que ha creado actividades de tratamiento legitimadoras de la videovigilancia y que se encuentran publicadas en el Portal de Transparencia de la administración. Sin embargo, de la consulta efectuada por esta institución al citado registro²³ no se ha podido detectar una actividad de tratamiento denominada videovigilancia con fines de seguridad ciudadana. Sin embargo, sí existe una actividad de tratamiento relativa a videovigilancia de tráfico creada y publicada en el Portal de Transparencia bajo la dependencia de la Dirección de Tráfico del departamento.

Ciertamente, en otra página web denominada ertzaintza.euskadi.eus²⁴ se han encontrado descritas actividades de tratamiento de datos personales, entre las cuales figura una relativa a videovigilancia con la finalidad declarada de *“Tramitar y gestionar las solicitudes, actuaciones y procedimientos relacionados con el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos; así como la gestión de las grabaciones (imagen y sonido) cuya responsabilidad recae en la Viceconsejería de Seguridad.”*

En opinión del Ararteko, sería deseable unificar criterios que permitan a la ciudadanía conocer en qué concreto registro de actividades figurarán los tratamientos de datos bajo responsabilidad del Departamento de Seguridad, puesto que, el responsable del tratamiento es en todos los casos la VCS, también en el supuesto de la videovigilancia.

²³ <https://www.euskadi.eus/web01-aprat/es/ac34aRatWebWar/control/arboll?locale=es>.

²⁴ <https://www.ertzaintza.euskadi.eus/lfr/web/ertzaintza/proteccion-de-datos-de-car%C3%A1cter-personal>.



Con respecto a la finalidad del tratamiento declarada en materia de videovigilancia, parece desprenderse que únicamente le corresponde al responsable la mera gestión de grabaciones, y es evidente que la decisión de implantar esos sistemas se toma por la administración. En este sentido, el Ararteko considera que se debería detallar con más precisión el tratamiento de datos en instalaciones, espacios públicos con fines de seguridad ciudadana, con qué tipo de sistemas fijos y móviles se realiza, y en este último supuesto, qué tipo de dispositivos se utilizan. O en su caso, quizá resultaría oportuno describir más actividades de tratamiento de datos por videovigilancia diferenciadas por tipos de sistemas utilizados, fijos o móviles, espacios públicos o instalaciones públicas, bases jurídicas diferenciadas, etc.

Por otro lado, en el apartado denominado videovigilancia del registro de actividades de Gobierno Vasco se indica que el régimen aplicable es el interés público y la ley de seguridad privada, normativa que quizá no cabe aplicar directamente a la administración, y sí a una empresa de seguridad privada contratada al efecto para realizar las labores previstas en el [artículo 42](#) de la Ley 4/2014 de seguridad privada, para "*prevenir*" la comisión de infracciones y evitar daños a las personas o bienes.

En todo caso, se considera que la mera implantación de sistemas de videovigilancia con fines de preservar la seguridad de instalaciones, bienes y personas encontraría su amparo jurídico en el interés legítimo de acuerdo con el [artículo 22](#) de la LOPDGDD cuando el control de acceso y el aseguramiento de su protección no se realiza por policías.

Lógicamente, las policías dispondrían de otra licitud aplicable a la captación de imágenes cuando el fin perseguido se basa en la seguridad ciudadana y control y disciplina de tráfico.

En cuanto al resto de entidades públicas participantes refieren, en unos casos que no disponen de actividades de tratamiento creadas que definan el tratamiento de datos en materia de videovigilancia o que no se encuentran publicadas en el portal de transparencia Sin embargo, de la consulta de diversos portales de transparencia se ha podido constatar que efectivamente se encuentran creadas y publicadas



(Barakaldo²⁵, Donostia/San Sebastián²⁶, Tolosa -no se indica la finalidad relativa a seguridad ciudadana-²⁷ y Laudio-Llodio²⁸).

En Donostia/San Sebastián se han detectado varias actividades de tratamiento de videovigilancia cuya gestión y finalidad se desconoce a qué órgano interno competente, se trata de las actividades correspondientes a grabación de imágenes en el servicio de acogida nocturna "Gaueko aterpea", en ascensores o en aparcamientos de bicis, cuya licitud se encaja en el interés público (Art 6.1.e) RGPD) pero también se alude a la Instrucción 1/2006 de la AEPD como base jurídica aplicable para atender derechos, por lo que, se entiende que o bien debe aplicarse el interés público por seguridad ciudadana o bien el interés legítimo de proteger esos bienes en base a la normativa de protección de datos. De hecho, la entidad local sí que dispone de una actividad relativa a cámaras por vigilancia policial que correctamente establece la licitud del tratamiento en la LOVFCs.

En otros supuestos, se traslada a esta institución que se han creado actividades al efecto y que se encuentran publicadas por transparencia, pero no se ha podido verificar su existencia (Portugalete²⁹). Los Ayuntamientos de Basauri y Ermua refieren que disponen de actividad de tratamiento en materia de videovigilancia pero que esta no se encuentra publicada en el portal de transparencia, aspecto que, teniendo en cuenta los tratamientos de datos mediante cámaras **fijas** y **móviles** que realizan esas administraciones parece a todas luces mejorable. Igualmente, Vitoria-Gasteiz³⁰ refiere que la actividad de tratamiento en materia de videovigilancia se ha creado pero que no se encuentra publicada en el portal de transparencia, sin embargo, esa administración dispone de una actividad de tratamiento denominada *seguridad ciudadana policía* por la cual se recaban datos con fines de videovigilancia, es decir, no existe una actividad de tratamiento diferenciada *sino que se subsume con carácter general en actuaciones de seguridad ciudadana efectuadas por la policía municipal como otras como por ejemplo, gestión de programas de educación vial o de licencias de taxi*. El Ararteko considera deseable que se diferencie el tratamiento en función de los tipos de datos objeto de captación y normas específicas aplicables al ámbito competencial.

²⁵ https://www.barakaldo.eus/portal/c/document_library/get_file?uuid=47e224d0-7fb5-4eb9-a040-8855fd34de14&groupId=10317

²⁶ <https://www.donostia.eus/ataria/es/web/info/politica-de-privacidad#registroTratamiento>.

²⁷ <https://udala.tolosa.eus/sites/default/files/1Politica%20de%20Privacidad%20y%20Registro%20de%20Actividades%20de%20Tratamiento.pdf>.

²⁸ https://laudio.eus/doc/gardentasuna/Registro_Actividades_Tratamiento_Laudio_Udala_v05_2022.pdf.

²⁹ <https://www.portugalete.org/es-ES/Institucional/Paginas/informacion-adicional.aspx>.

³⁰ <https://www.vitoria-gasteiz.org/docs/wb021/contenidosEstaticos/adjuntos/es/88/83/88883.pdf>.



El ayuntamiento de Errenteria refiere que no ha creado actividades de tratamiento al efecto en materia de videovigilancia, lo cual, dada la captación que efectúa de imágenes parece una práctica mejorable en materia de protección de datos personales y de transparencia en su vertiente activa.

Por otro lado, los ayuntamientos de Bilbao³¹, Getxo³² e Irun³³ refieren que disponen de actividades de tratamiento de datos en materia de videovigilancia con distintos fines y bases de legitimación y así se constata positivamente del análisis de los portales de transparencia de las citadas entidades locales.

En los casos de Zumarraga y Eibar, se dispone de actividad de tratamiento de datos por videovigilancia, pero no se encuentran publicadas en los portales de transparencia de las citadas entidades locales.

Por otro lado, de las actividades revisadas por esta institución es posible resumir que, con carácter general, las bases jurídicas habilitantes del tratamiento se encuentran correctamente definidas en base a lo previsto en el artículo 6 RGPD y que debe coherenciarse con las normas aplicables en materia de seguridad ciudadana cuando el fin perseguido es la seguridad pública. En otros supuestos, quizá debería reflexionarse sobre la conveniencia de diferenciar actividades de tratamiento y licitudes cuando el fin perseguido es el interés legítimo de preservar la seguridad de instalaciones, bienes y personas, en especial cuando la videovigilancia no se realiza por las policías con objeto de asegurar la protección de los edificios e instalaciones públicas y de sus accesos.

Finalmente, cabe advertir que, en la mayoría de las actividades de tratamiento de las entidades públicas consultadas, no se define la recogida del dato de voz, por lo que la tecnología utilizada quizá no capte sonidos. En caso contrario, parecería recomendable añadir el dato de voz en la estructura de la actividad de tratamiento relativa a videovigilancia.

³¹ <https://www.bilbao.eus/cs/Satellite/transparencia/es/ambitos/el-ayuntamiento/proteccion-de-datos>

³² https://www.getxo.eus/DocsPublic/proteccion_datos/castellano/rat_ayuntamiento_cas_12.pdf.

³³ <https://www.irun.org/es/rgpds/399-videovigilancia-instalaciones?idr=109>.
<https://www.irun.org/es/rgpds/399-videovigilancia-via-publica?idr=110>.



IV.9. Medidas de seguridad

IV.9.1. Resultados

Administración	Medidas de seguridad
Departamento de Seguridad de Gobierno vasco	Se aplican según lo previsto en el ENS.
Ayuntamiento de Vitoria-Gasteiz	Medidas técnicas basadas en credenciales de acceso a los sistemas de custodia.
Ayuntamiento de Bilbao	Se aplican según lo previsto en el ENS y además se realizan controles de acceso físicos y lógicos basados en niveles de acceso.
Ayuntamiento de Donostia/San Sebastián	Medidas de seguridad basadas en el ENS y en materia de protección de datos
Ayuntamiento de Barakaldo	Se aplican según lo previsto en el ENS.
Ayuntamiento de Portugalete	Se aplican medidas de acuerdo con las resoluciones del Gobierno Vasco.
Ayuntamiento de Getxo	Se aplican según lo previsto en el ENS y en materia de protección de datos.
Ayuntamiento de Basauri	Se aplican las normas relativas a seguridad ciudadana y la Orden de Servicio ORG004 de fecha 6 de agosto de 2021.
Ayuntamiento de Errenteria	Medidas de seguridad basadas en protección de datos.
Ayuntamiento de Tolosa	Se aplican según lo previsto en el ENS.
Ayuntamiento de Irun	Medidas de seguridad basadas en el ENS y en materia de protección de datos.
Ayuntamiento de Llodio-Laudio	Medidas de seguridad basadas en el ENS y en materia de protección de datos.
Ayuntamiento de Zumarraga	No se han implementado medidas de seguridad específicas.
Ayuntamiento de Eibar	Medidas de seguridad basadas en el ENS y en materia de protección de datos.
Ayuntamiento de Ermua	Medidas de seguridad basadas en el ENS.



IV.9.2. Análisis y valoración

En primer lugar, la videovigilancia comporta, con carácter general, un tratamiento de datos personales de imagen y, en su caso, de voz. Quizá aquellas cámaras destinadas a la disciplina de tráfico no captan sonidos si bien cabe señalar que los datos de matrículas se consideran datos personales de acuerdo con las interpretaciones de las autoridades de protección de datos.

En cualquier caso, el tratamiento de datos personales de imagen y voz comportan la necesidad de aplicar medidas de seguridad de acuerdo con lo dispuesto en la normativa de protección de datos. El RGPD introduce el principio de responsabilidad proactiva que fundamentalmente proporciona un marco y deber para el responsable del tratamiento de adoptar medidas oportunas, técnicas, organizativas y eficaces a fin de garantizar la seguridad adecuado al riesgo de los datos tratados.

En concreto el artículo 32 RGPD establece que *“Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”*.

El citado artículo parece otorgar un margen de discrecionalidad a los responsables de tratamiento de datos para adoptar medidas que, en cualquier caso, deben tener capacidad para demostrar la adopción de dichas medidas y de que realmente funcionan.

Como se ya se ha señalado, en materia de medidas de seguridad, la normativa de protección de datos se remite a lo dispuesto en el [ENS](#) cuando se produzcan tratamientos de datos por las administraciones públicas tal y como se prevé en la [Disposición Adicional Primera](#) de la LOPDGDD.

En este punto, cabe destacar que ni la LOVFCS ni el Decreto 168/98 establecen las concretas medidas de seguridad a aplicar, sino que refieren a aspectos genéricos sobre la conservación de grabaciones. El Decreto 168/98 simplemente indica que las resoluciones autorizantes especificarán *“las medidas de seguridad a adoptar para garantizar el respeto de las disposiciones legales vigentes y la preservación de la disponibilidad, confidencialidad e integridad de las grabaciones, así como los órganos que hayan de asumir la custodia material y efectiva de dichas grabaciones”*.



Pero nada indica con respecto al encaje con las medidas de seguridad internas de la organización y qué medidas específicas han de aplicarse y, en definitiva, cómo garantizar la efectiva y correcta disponibilidad, confidencialidad, integridad, adecuada custodia y destrucción y el personal autorizado para su ejecución.

De este modo, con carácter general, las administraciones públicas deben aplicar medidas de seguridad reflejadas en el ENS que establece “los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias” ([artículo 1 ENS](#)). Se entiende pues, que se deben aplicar las medidas de seguridad a toda la información y servicios que gestionen en el ejercicio de sus competencias, por lo que se han de aplicar igualmente a todos los sistemas de captación de imágenes y vídeos independientemente de la finalidad perseguida.

Las medidas previstas en el ENS se han de amoldar a aquellas obligaciones específicas de protección de datos que adicionalmente se regulan en el [capítulo IV](#) de la LO 7/21 cuando el fin perseguido es la prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Por lo tanto, los responsables de tratamiento de datos personales sobre videovigilancia con los fines antedichos, deben cumplir aquellos aspectos reflejados en la ley referentes a la seguridad que se reflejan en el [artículo 37](#), fundamentalmente, sin perder de vista las previsiones relativas a la creación de registros de actividades de tratamiento, evaluaciones de impacto, consultas previas a la autoridad de control, notificaciones de brechas de seguridad, etc.

En concreto, el capítulo IV regula aspectos de seguridad que, aparentemente, se cumple por la mayoría de las entidades públicas participantes en el estudio puesto que refieren que las medidas adoptadas para gestionar y garantizar la confidencialidad de las grabaciones se basan en lo dispuesto en el ENS y cabe señalar que el [artículo 37](#) de la LO 7/21 establece con respecto a la seguridad del tratamiento, entre otros aspectos:

“Artículo 37. Seguridad del tratamiento.

1. El responsable y el encargado del tratamiento, teniendo en cuenta el estado de la técnica y los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades



de las personas físicas, aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado, especialmente en lo relativo al tratamiento de las categorías de datos personales a las que se refiere el artículo 13. En particular, deberán aplicar a los tratamientos de datos personales las medidas incluidas en el Esquema Nacional de Seguridad.

2. (...):”.

En cualquier caso, parece recomendable establecer prácticas periódicas de evaluación de riesgos con objeto de mantener actualizadas las medidas de seguridad aplicadas internamente con fines de garantizar la correcta custodia, trazabilidad, disponibilidad, integridad y adecuada conservación y destrucción de las grabaciones.

Finalmente, cabe destacar que el uso de dispositivos privados o personales de captación de imágenes pueden comportar un riesgo no deseado para la organización, dado que no es posible aplicar medidas de seguridad adecuadas bajo el ámbito y alcance de las disposiciones internas.

En este sentido, la AEPD ha publicado informes jurídicos³⁴ en los cuales recomienda aplicar medidas de seguridad adecuada al riesgo y advierte sobre la problemática de utilizar dispositivos no profesionales para captar imágenes y sonidos.

³⁴ <https://www.aepd.es/sites/default/files/2019-09/informe-juridico-rgpd-uso-camaras-privadas-por-la-policia.pdf>.



V. Conclusiones

La institución del Ararteko tiene como fin primordial defender los derechos y libertades de la ciudadanía vasca y garantizar el principio de legalidad de acuerdo con sus atribuciones previstas en la [Ley 3/1985, de 27 de febrero, por la que se crea y regula la Institución del Ararteko](#).

El [artículo 9.3](#) de la CE proclama el *principio de legalidad*, que también aparece enunciado en el [artículo 9.1](#) CE, al disponer que “*Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico*”.

En el principio de legalidad encuentran los poderes públicos al mismo tiempo un principio de legitimidad, en cuanto su actuación queda apoyada en un Derecho democráticamente consentido, y un principio de limitación formal o jurídica, en cuanto que su actividad tiene en tal Derecho la frontera de su obrar legítimo. Como ha afirmado el Tribunal Constitucional en su Sentencia 108/1986, de 29 de julio de 1986 ([ECLI:ES:TC:1986:108](#)), el principio de legalidad es un dogma básico del sistema liberal democrático.

El mandato constitucional que atribuye a la policía la misión de proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana ([Art 104 CE](#)) debe cohererarse con el resto de las normas y principios que legitiman esa actuación con objeto de respetar los derechos fundamentales de la ciudadanía y, por lo tanto, mediante una estricta observancia de los límites y garantías establecidas en las normas.

En este contexto, el cumplimiento de las normas y disposiciones en materia de videovigilancia devienen fundamentales no sólo motivadas en cumplir el principio de legalidad, sino también con objeto de aportar una mayor transparencia y confianza para la ciudadanía en la legitimación y proporcionalidad de la actuación de las policías.

Del análisis de los datos efectuados por esta institución en el presente estudio, este Ararteko conviene en exponer las siguientes conclusiones.



V.1. Aspectos generales y marco regulatorio

Las administraciones competentes realizan un esfuerzo por proteger la seguridad ciudadana mediante la utilización de medios tecnológicos actuales y su conciliación con otros derechos fundamentales. De este modo, con carácter general, las entidades participantes en el estudio refieren solicitar y obtener la autorización previa para la instalación y uso de cámaras de videovigilancia cuando el fin perseguido es la seguridad ciudadana. Además, suelen disponer de procedimientos de atención de derechos de la ciudadanía en relación con los tratamientos de datos personales relacionados con la videovigilancia.

Sin embargo, la evolución tecnológica de los sistemas de videovigilancia y su despliegue y uso a través de distintos medios no parece encontrar un correcto acomodo en la normativa actual por lo que parece necesario reflexionar sobre la necesidad de crear disposiciones, en el marco regulatorio que corresponda a las administraciones públicas de Euskadi, que colmen ese vacío legal.

Por ejemplo, la legislación vigente no define el concepto y los posibles usos de los dispositivos **móviles** como drones, báculos o cámaras en uniformes de agentes por lo que, una descripción de los concretos supuestos de uso y alcance de la captación en tiempo y espacio, anticiparían una previa ponderación de derechos en juego que cumplan con el principio de proporcionalidad.

Cabe destacar que no siempre se encuentra una correlación entre el despliegue de cámaras reportado por las administraciones públicas participantes en el estudio y los índices de conflictividad que se producen en Euskadi. Así, el número de cámaras y tipos de usos reportados (**fijas y móviles**) quizá obedecen a otros criterios como los lugares públicos objeto de control, instalaciones, afluencia de personas, tráfico, características de una localidad, recursos humanos, etc., sin perjuicio de que siempre debe cumplirse el principio de proporcionalidad y concurrir un razonable riesgo para la seguridad ciudadana, en el caso de las instalaciones **fijas**, o un peligro concreto, en el caso de las cámaras **móviles**.

Relacionado con lo anterior, las administraciones participantes en el presente estudio refieren la utilización de cámaras en lugares, instalaciones y bienes en los que, aparentemente, no existe un razonable riesgo para la seguridad ciudadana o un peligro concreto. Este es el caso de lugares interiores, oficinas, piscinas, bibliotecas, recintos deportivos en los cuales quizá deba optarse por alternativas menos intrusivas o



lesivas para la intimidad para proteger instalaciones, bienes o personas. ([Ver apartado de análisis y valoración](#)).

V.2. Finalidades de la videovigilancia y normas habilitantes

Las finalidades perseguidas por la administración determinan las normas aplicables y la licitud para la captación de imágenes y en su caso, sonidos.

La mayoría de las administraciones públicas participantes en el estudio habilitan en la seguridad ciudadana la decisión de utilizar la videovigilancia y, como el Ararteko ha señalado anteriormente, no siempre resulta preciso acudir a dicho régimen para legitimar la captación de imágenes de personas. En algunos supuestos, incluso, las administraciones señalan la legitimación del tratamiento de imágenes en base a la dispuesto en la normativa de protección de datos y, sin embargo, recaban autorizaciones para la instalación de sistemas de videovigilancia por seguridad ciudadana, lo cual denota una falta de distinción entre las bases de legitimación aplicables según la finalidad de la captación.

Cuando la finalidad es contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública entonces podrá acudirse a la normativa de videovigilancia por seguridad pública como norma habilitante que legitime la captación de imágenes. Sin embargo, dicha legitimación en lugares cerrados como instalaciones y edificios públicos debe respetar el principio de proporcionalidad y, por lo tanto, su utilización exige como criterio de ponderación la existencia de un razonable riesgo para la seguridad ciudadana.

Cuando no concurre un razonable riesgo para la seguridad ciudadana cabe utilizar medios menos intrusivos para la intimidad de las personas y modular el control sobre instalaciones, bienes y personas por interés legítimo de la administración, acomodando el uso de la videovigilancia en base a la normativa de protección de datos. ([Ver apartado de análisis y valoración](#)).



V.3. Sobre el régimen de autorización de la videovigilancia por seguridad ciudadana

La utilización de cámaras **fijas** y **móviles** con fines de seguridad ciudadana debe cumplir una serie de requisitos establecidos en la legislación de videovigilancia por las policías.

Todas las administraciones participantes en el estudio refieren solicitar y obtener la autorización previa para su instalación y uso cuando el fin perseguido es la seguridad ciudadana.

En materia de disciplina de tráfico, todas las administraciones indican que solicitan y obtienen autorización previa para la utilización de cámaras al efecto de acuerdo con el régimen previsto en la [disposición adicional tercera del Decreto 168/98](#), si bien algunas entidades refieren que no se notifican las resoluciones a la CVL ([Ver apartado de análisis y valoración](#)).

El Ararteko observa con preocupación el régimen de autorización y uso de **dispositivos móviles** como báculos, drones y cámaras en uniformes de agentes ([Ver apartado de análisis y valoración](#)). En concreto, las cámaras **fijas** se autorizan por el plazo de 1 año, renovable, a cuyo término tendría encaje la revisión del cumplimiento de los mismos criterios que motivaron la instalación. Sin embargo, en el supuesto de los **dispositivos móviles** únicamente se prevé en la [LO 7/21](#) que podrán autorizarse por un período máximo de 1 mes prorrogable por otro. Se trata de un límite que aparentemente no tendría buen encaje con el uso de cámaras en uniformes de policía si se utilizan de manera continuada y no acotada a un supuesto de riesgo concreto. En definitiva, parece oportuno que las autorizaciones determinen el plazo concreto de tiempo y ajustado al supuesto que motiva la petición de autorización. Las autorizaciones para el uso de cámaras **móviles** se solicitan de modo conjunto, no acotada a cámaras o unidades policiales, lo cual podría comportar cierta dificultad para valorar la concurrencia de un peligro concreto y el cumplimiento del principio de proporcionalidad.

La tramitación de la autorización para la instalación de cámaras **fijas** es posible iniciarla a través de la sede electrónica del Gobierno Vasco, que en apariencia, no parece prever la posibilidad de solicitar autorizaciones para utilizar cámaras móviles.



V.4. El principio de proporcionalidad

El Ararteko considera que se debe observar escrupulosamente el principio de proporcionalidad previsto en la normativa de videovigilancia con fines de seguridad ciudadana, *en su doble versión de idoneidad e intervención mínima, previamente a la decisión de utilización de cámaras.*

Esta defensoría estima que existen criterios y elementos de valoración y ponderación previas que permiten evaluar si la medida de videovigilancia puede suponer una posible injerencia en el derecho a la intimidad. Con carácter general, esa reflexión no parece efectuarse previamente a la remisión de solicitudes de autorización de videovigilancia por seguridad ciudadana o para implantar cualquier dispositivo de captación de imágenes ([Ver apartado 4.4](#)).

Este escrutinio previo permitiría comprobar si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La realización de un juicio de proporcionalidad, a juicio de esta institución, añadiría más elementos de garantías y transparencia a las decisiones adoptadas por la administración.

De este modo, se podría comprobar si el hecho objetivo concreto y evaluable, como la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes, o la concurrencia de algún peligro concreto, superan el citado juicio de proporcionalidad.

V.5. La gestión de las grabaciones y los plazos de conservación

Los **plazos máximos** de conservación de las grabaciones de videovigilancia por seguridad ciudadana difieren entre las administraciones públicas consultadas aun cuando el objeto de captación tiene el mismo fin: prevenir la comisión de delitos,



faltas e infracciones relacionados con la seguridad ciudadana. ([Ver apartado de análisis y valoración](#)).

La falta de armonización normativa tiene su reflejo en las respuestas aportadas por las entidades participantes en el estudio al señalar distintos plazos máximos de conservación de grabaciones.

Resulta deseable que se establezcan plazos máximos de conservación iguales, pero también, **plazos mínimos**, porque existe un vacío legal que puede producir una falta de garantías y de seguridad jurídica que puede afectar internamente a la administración y a derechos de terceras personas interesadas. Una correcta gestión de las grabaciones durante un plazo mínimo adecuado permitiría acreditar mejor la proporcionalidad de las actuaciones de las policías, la defensa de derechos legítimos de las personas interesadas y, además, facilitaría la labor de terceros legitimados para acceder a las grabaciones como órganos judiciales y el propio Ararteko.

Los plazos mínimos de conservación no deben quedar al albur de una decisión interna o del sistema informático de videovigilancia de que se trate.

V.6. Publicidad y transparencia en el ámbito de la actuación de la administración

Con carácter general, de acuerdo con las respuestas aportadas por las administraciones participantes del estudio, parece cumplirse el deber de informar ante la utilización de **instalaciones fijas** de videovigilancia por motivos de seguridad ciudadana de acuerdo con lo previsto en la [Orden de 2011](#) de la Consejería de Seguridad de Gobierno Vasco. Sin embargo, no parece correcta la utilización de carteles de videovigilancia por seguridad ciudadana cuando el fin perseguido es preservar la seguridad de instalaciones, bienes y personas, en cuyo supuesto, se deberían seguir los criterios de información establecidos en la normativa de protección de datos tal y como se expone en el [apartado de análisis y valoración](#) de los resultados.

En cualquier caso, resulta deseable avanzar en otras fórmulas y medios de información y transparencia, especialmente en el marco de la utilización de dispositivos **móviles** de videovigilancia por seguridad ciudadana, dada la falta de regulación normativa específica ([Ver apartado de análisis y valoración](#)).



En este sentido, existen medios y canales complementarios que permitirían a la ciudadanía conocer el supuesto y objeto de la videovigilancia mediante información a través de los portales de internet, redes sociales, publicación de resoluciones al efecto en boletín oficial, creación de actividades de tratamiento de datos personales y su inclusión en el portal de transparencia, y mediante señales visibles presencialmente.

V.7. Ejercicio y atención de derechos de la ciudadanía

Prácticamente todas las administraciones públicas participantes refieren disponer de protocolos o procedimientos de atención de derechos de la ciudadanía en relación con los tratamientos de datos relacionados con la videovigilancia. Se trata de un aspecto positivo en la medida en que, ante el ejercicio de un derecho de la ciudadanía, el órgano responsable dispondrá de elementos de valoración e impulso de la tramitación y gestión de la solicitud.

En todo caso, cabe advertir que las normas vigentes en materia de protección de datos y la [LO 7/2021](#) regulan nuevos derechos no previstos en la legislación en materia de videovigilancia en vigor, como el de rectificación, de limitación del tratamiento y el derecho de supresión. En este sentido, de las respuestas aportadas por las administraciones participantes en el estudio, parece desprenderse la necesidad de revisar los protocolos de atención de derechos y su adaptación a las disposiciones vigentes tal y como se ha expuesto en el [apartado de análisis y valoración](#).

Por otro lado, la normativa de videovigilancia en materia de seguridad ciudadana establece que debe ser **el órgano competente** el que atienda y resuelva las solicitudes de ejercicio de derechos. Esta falta de concreción comporta que las entidades públicas participantes en el estudio describan diferentes órganos, unidades, perfiles e incluso departamentos como encargados de atender derechos, como Ertzaintza en el caso de la videovigilancia cuya responsabilidad recae en la VCS, alcaldía, la persona delegada de protección de datos o el departamento de seguridad de una entidad local. En este sentido, resulta deseable una actualización normativa que concrete a la ciudadanía ante qué órgano de una administración pública se pueden plantear las solicitudes de ejercicio de derechos. ([Ver apartado de análisis y valoración](#)).

Conviene pues, clarificar a la ciudadanía cuál es el órgano competente para atender derechos que afecten a datos de videovigilancia por seguridad ciudadana, y en su caso, examinar internamente los medios para coordinar la tramitación dado que, las



particularidades de ese tratamiento se diferencian de otros datos personales objeto de gestión administrativa en el seno de la administración pública. Por ejemplo, los límites para la denegación del acceso a datos de videovigilancia pueden fundamentarse en la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, se trata de límites específicamente contemplados en la legislación de videovigilancia.

En definitiva, en ausencia de disposiciones concretas que regulen procedimientos de atención de derechos relativos a tratamientos de imágenes por motivos de seguridad ciudadana, parece necesario desarrollar y especificar más si cabe los protocolos internos de atención de derechos.

V.8. Obligaciones básicas de protección de datos

Con respecto a las obligaciones básicas en materia de protección de datos, el Ararteko centra su análisis en el cumplimiento de elementos fundamentales previstos en la normativa de protección de datos y en la [LO 7/2021](#) que disponen la necesidad de crear actividades de tratamiento que reflejen correctamente la estructura de los datos personales objeto de captación, finalidades, licitud y otros elementos que proporcionen, además, información transparente para la ciudadanía en sus relaciones con las administraciones. En este sentido, las administraciones públicas deben crear actividades de tratamiento en materia de videovigilancia cuando capten imágenes y voz de la ciudadanía y, además, publicarlas en sus portales de transparencia.

Del análisis de las respuestas aportadas por las entidades públicas participantes se constatan algunos aspectos destacables como se ha expuesto en el [apartado de análisis y valoración](#). A saber, que algunas administraciones públicas no han creado y publicado actividades de tratamiento referentes a videovigilancia. En unas ocasiones, no se distingue la licitud aplicable entre interés legítimo y fines públicos y disposiciones en materia de seguridad ciudadana. En otros casos, algunas entidades parecen desconocer la existencia de registros de actividades de tratamiento publicadas en los portales de transparencia y si existe una actividad de videovigilancia creada al efecto.

Con carácter general se informa correctamente sobre la posibilidad de efectuar cesiones de datos a los órganos judiciales u otras policías.



V.9. Medidas de seguridad

Las administraciones públicas deben aplicar las medidas de seguridad reflejadas en el ENS para asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos personales objeto de tratamiento mediante sistemas de videovigilancia.

Resulta positiva la respuesta mayoritaria de las entidades públicas participantes en el estudio con respecto a las medidas de seguridad aplicadas para garantizar la seguridad de la información, dado que refieren aplicar medidas y en muchos supuestos atendiendo a lo dispuesto en el ENS.

Esta institución desconoce el alcance de las medidas jurídicas y técnicas desplegadas internamente, pero conviene en señalar que son deseables prácticas de revisión y actualización periódicas de las medidas ante la evolución de la tecnología y elementos diversos utilizados para captar imágenes como se ha señalado en el [apartado de análisis y valoración](#) de resultados.

Por otro lado, la formación interna del personal con atribuciones de gestión y tratamiento de datos personales relacionados con la videovigilancia es una medida de seguridad adecuada con objeto de demostrar una responsabilidad proactiva con la protección de la información de la ciudadanía y evitar brechas de seguridad no deseadas. En atención al perfil del personal interno, las formaciones en materia de videovigilancia pueden orientarse a complementar aspectos jurídicos o bien técnicos en materia de seguridad de la información.



VI. Recomendaciones

En el presente apartado el Ararteko formula las recomendaciones dirigidas a las administraciones públicas con objeto de facilitar el cumplimiento del régimen de garantías en materia de videovigilancia y de salvaguardar los derechos fundamentales de la ciudadanía vasca.

RECOMENDACIONES:

VI.1. Aspectos generales y marco regulatorio

Primera

Reflexionar sobre la necesidad de aprobar, en el espacio regulatorio y de desarrollo que corresponde a las administraciones públicas vascas, normas de propósito común y armonizador que aclaren, definan y establezcan los supuestos, criterios y elementos de ponderación necesarios para la toma de decisiones sobre la implantación de sistemas de videovigilancia fijos o móviles.

Segunda

De manera transitoria ante la ausencia de una regulación más específica y actualizada, el Ararteko recomienda desarrollar e implantar instrumentos jurídicos internos como protocolos e instrucciones que añadan más garantías a la actuación proporcional de las policías y, por ende, de protección de los derechos fundamentales de todas las personas. Los citados instrumentos jurídicos podrían definir fases de valoración de la decisión de implantar un sistema de videovigilancia. Por ejemplo, primeramente, podrían definirse los supuestos de hecho que pueden requerir el uso de un sistema de videovigilancia. En segundo lugar, en función del lugar y tipo de instalación (fija o móvil) requerida, el protocolo o instrucción podría configurar un sistema de ponderación previa que contemple alternativas de seguridad menos intrusivas para la intimidad (vigilancia privada, otro personal interno, sistemas de acceso restringido a instalaciones propias, etc.). En último término, superadas las valoraciones precedentes, la última fase comprendería la necesidad acotada y específica de requerir videovigilancia por motivos de seguridad ciudadana y proceder al chequeo y cumplimiento de requisitos legales para su implantación. ([Véase apartado VI.4](#)).



Tercera

Desarrollar instrumentos jurídicos internos que colmen la ausencia de regulación y definición de **dispositivos móviles** y el alcance de su utilización, entre otros aspectos. En concreto, ante el uso de cámaras como drones, báculos o en uniformes de agentes recomienda describir los supuestos de uso y alcance de la captación en tiempo y espacio, previamente a la remisión de la solicitud de autorización a la autoridad competente, con el objetivo de realizar una previa ponderación de derechos en juego que cumplan con el principio de proporcionalidad en su doble vertiente de idoneidad e intervención mínima. Además, los citados instrumentos jurídicos internos, pueden desarrollar los supuestos de utilización de cámaras en lugares, instalaciones y bienes en los que no existe un razonable riesgo para la seguridad ciudadana o un peligro concreto y, por lo tanto, la legitimación de la captación de imágenes podría tener su encaje en la LOPDGDD.

VI.2. Finalidades perseguidas con la videovigilancia y las normas habilitantes

Cuarta

Reflexionar previamente a la utilización de cámaras de videovigilancia sobre la finalidad perseguida con objeto de distinguir adecuadamente las normas habilitantes para la captación de imágenes.

Por un lado, la videovigilancia con fines de seguridad pública por las policías de Euskadi en espacios públicos, abiertos o cerrados encuentra su legitimación en la LOVFCSS y demás disposiciones complementarias o de desarrollo. En otros supuestos, cuando el fin es preservar la seguridad de instalaciones, bienes y personas en espacios públicos cerrados, es posible legitimar la captación en el interés legítimo de acuerdo con la normativa de protección de datos y modular la videovigilancia por tiempo y lugar.

VI.3. Autorizaciones de videovigilancia por seguridad ciudadana

Quinta

Concretar los plazos de tiempo ajustados al supuesto de peligro concreto en las solicitudes de autorización de uso de cámaras **móviles** con fines de seguridad ciudadana.



Sexta

Publicar las autorizaciones de utilización de sistemas **fijos** y **móviles** de videovigilancia por motivos de seguridad ciudadana emitidas por la Viceconsejería de Seguridad del Gobierno Vasco como medida de transparencia activa.

VI.4. Principio de proporcionalidad

Séptima

Implantar protocolos o instrumentos jurídicos internos de valoración y ponderación de derechos (juicio de proporcionalidad) que permitan evaluar previamente a la petición de autorización de videovigilancia, si la medida puede suponer una injerencia en el derecho a la intimidad. Las administraciones competentes podrían elaborar una matriz de elementos de valoración y ponderación que facilitarían la decisión de adoptar la medida de videovigilancia o acogerse a otras fórmulas menos invasivas o que produzcan menores injerencias en la intimidad. Se trataría de definir elementos objetivos y los detalles correspondientes de la potencial captación de imágenes como los siguientes:

- supuestos de hecho (definición del espacio público, edificio o instalación pública, sujeta a control de acceso o custodia)
- temporalidad (definido en tiempo de captación)
- espacio o lugar (definido como lugar de captación y elementos adyacentes, como domicilios o locales privados)
- existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las **fijas**, o de un peligro concreto, en el caso de las **móviles** (por ejemplo, índice de conflictividad, denuncias, etc.).

Elementos concurrentes todos ellos que, una vez concretados, deberían someterse al correspondiente juicio de proporcionalidad, en la doble vertiente de idoneidad (La medida es adecuada, susceptible de conseguir el objetivo propuesto de seguridad ciudadana) e intervención mínima (ponderación entre la finalidad pretendida y la posible afectación al derecho al honor, a la propia imagen y a la intimidad de las personas). El resultado de la valoración comportaría la base para la toma de decisiones y aportaría más garantías de cumplimiento normativo y conciliación con otros derechos fundamentales.



VI.5. Gestión de grabaciones y plazos de conservación

Octava

Implantar instrumentos jurídicos internos de gestión y custodia de grabaciones que garanticen la conservación, trazabilidad, integridad, accesos autorizados, plazos mínimos y máximos de conservación y unidades u órganos independientes de gestión con el objetivo de garantizar la transparencia de la actuación de la administración y en su caso, facilitar la puesta a disposición a terceras personas interesadas o legitimadas para acceder a las imágenes.

VI.6. Publicidad y transparencia

Novena

Definir en los protocolos internos de uso y gestión de imágenes las fórmulas y canales a través de los cuales se informará a la ciudadanía de la existencia de cámaras de videovigilancia. Por ejemplo, el protocolo podría comprender de qué modo colocar carteles en lugares visibles, cómo informar mediante publicaciones en portales de transparencia, redes sociales, boletines oficiales y otros medios análogos cuando se capten imágenes, especialmente, cuando se utilicen cámaras **móviles**. Estos aspectos de mejora permitirían a la ciudadanía conocer cómo se toman las decisiones relacionadas con la protección de la seguridad ciudadana.

VI.7. Atención de derechos de la ciudadanía

Décima

Desarrollar o actualizar los protocolos internos de atención de derechos de la ciudadanía y que concreten el órgano competente para tramitar, definan los nuevos derechos derivados de la regulación actual como rectificación, limitación y supresión, y distingan las particularidades de los tratamientos por seguridad ciudadana a la hora de atender los derechos.

Undécima

Designar órganos de atención de derechos que dispongan de un nivel jerárquico y criterios técnicos y jurídicos que permitan tramitar adecuadamente el ejercicio de derechos de la ciudadanía relacionados con el tratamiento de su imagen por motivos de seguridad ciudadana.



VI.8. Protección de datos personales

Duodécima

Revisar, y en su caso crear, actividades de tratamiento con fines de videovigilancia que reflejen adecuadamente la licitud aplicable.

Decimotercera

Publicar en los portales de transparencia de cada administración las actividades de tratamiento de datos de videovigilancia para su consulta y escrutinio por la ciudadanía.

VI.9. Medidas de seguridad de la información

Decimocuarta

Revisar y actualizar las medidas de seguridad jurídicas y técnicas implantadas para garantizar la seguridad de la información.

Decimoquinta

Aplicar medidas específicas para asegurar la conservación de las grabaciones y evitar la destrucción no autorizada de datos.

Decimosexta

Capacitar en materia de seguridad al personal interno con atribuciones de gestión y tratamiento de datos personales relacionados con la videovigilancia.



VII. Anexo: Cuestionario

A continuación, se expone el cuestionario planteado a las administraciones públicas participantes en el estudio:

Cuestiones comunes a todas las Administraciones

- 1) Número aproximado de cámaras totales desplegadas en la organización
- 2) Tipo de cámaras utilizadas
 - Fijas
 - Móviles
 - Ambas
- 3) Finalidades perseguidas mediante el uso de cámaras de videovigilancia
 - Preservar la seguridad de instalaciones, bienes y personas
 - Seguridad ciudadana
 - Disciplina de tráfico
 - Regulación de tráfico en zonas urbanas
 - Otras (indicar)
- 4) Competencias y normativa habilitante de la videovigilancia realizada por esa administración.
 - Protección de datos personales (Ley orgánica 3/2018 de protección de datos y garantía de los derechos digitales)
 - Seguridad ciudadana en lugares públicos (Ley orgánica 4/1997 por la que se regula la utilización de videocámaras por las policías en lugares públicos y Decreto 168/1998 por el que se desarrolla el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos)
 - Prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (Ley Orgánica 7/2021)
 - Otras (indicar)
- 5) Lugar de ubicación de cámaras fijas
 - Instalaciones comunes como oficinas
 - Recintos deportivos
 - Edificios culturales
 - Espacios públicos (indicar cuáles, como carreteras, parques, ascensores, garbigunes, etc)
 - Cascos urbanos



- 6) ¿Se dispone de cámaras fijas en lugares públicos con fines de seguridad ciudadana?
- Si
 - No
- 7) La instalación de cámaras fijas de videovigilancia con fines de seguridad ciudadana ¿Se encuentran autorizadas por la Viceconsejería de Seguridad del Gobierno Vasco?
- Si
 - No
- 8) ¿Existe un protocolo interno que establece a disposición y custodia de qué unidad u órgano interno quedan las grabaciones?
- Si (Indicar unidad u órgano)
 - No
- 9) ¿Se ha establecido internamente el plazo mínimo de conservación de las grabaciones?
- Si (Indicar)
 - No
 - Se desconoce
- 10) El plazo máximo establecido de conservación de las grabaciones es de
- 1 mes
 - 3 meses
 - Indefinido
 - Otro (Detallar si existen protocolos diferentes en función del contexto)
- 11) Descripción de las medidas de seguridad implementadas para la correcta custodia, conservación, gestión de accesos autorizados y en su caso para la destrucción de grabaciones, basadas en:
- El esquema nacional de seguridad
 - Medidas de seguridad de protección de datos como análisis de riesgo, evaluaciones de impacto y similares.
 - Otras (describir)
 - No se han implementado
- 12) Medios para informar a la ciudadanía sobre la recogida y tratamiento de datos de imagen y en su caso sonidos mediante cámaras fijas.
- Se han colocado carteles de fondo azul por motivos de seguridad ciudadana
 - Se han colocado distintivos con fondo amarillo u otros con fines de preservar la seguridad de instalaciones, bienes y personas.
 - Ambos tipos en función de los fines perseguidos
 - No se han colocado carteles o distintivos al efecto.



- 13) Medios para informar a la ciudadanía sobre captación de imágenes de videovigilancia mediante cámaras móviles
- Se han colocado carteles de fondo azul por motivos de seguridad ciudadana
 - Se informa mediante distintivos visibles en uniformes, vehículos, o lugar de ubicación del dispositivo.
 - Se utilizan página web, redes sociales, y canales análogos
 - No se informa
- 14) La unidad u órgano interno encargado en esa administración de atender el ejercicio de derechos relacionados con las grabaciones como acceso o supresión es:
- La Viceconsejería del Departamento de Seguridad de Gobierno Vasco en todos los supuestos.
 - La Viceconsejería del Departamento de Seguridad de Gobierno Vasco sólo para las grabaciones realizadas por la Ertzaintza.
 - La delegada de protección de datos de Gobierno Vasco.
 - La jefatura de la policía local.
 - Es indiferente, puede atender cualquier persona perteneciente a la entidad pública.
 - Otro (indicar)
- 15) ¿Se dispone de un protocolo o procedimiento de atención de derechos relacionado con las grabaciones?
- Si
 - No

Cuestiones específicas de protección de datos

- 1) ¿Se han creado actividades de tratamiento de datos personales con fines de videovigilancia?.
- Si
 - No
 - Se han creado varias en función de los fines perseguidos (seguridad ciudadana, disciplina de tráfico, protección de bienes e instalaciones, etc.)
- 2) ¿La o las actividades de tratamiento de datos en materia de videovigilancia se encuentran publicadas en el registro de actividades en el portal de transparencia de la entidad pública?.
- Si
 - No



- 3) Indicar el número de cámaras utilizadas con las siguientes bases legitimadoras del tratamiento de datos en materia de videovigilancia
- Interés legítimo (seguridad de instalaciones, bienes y personas): _____
 - Seguridad ciudadana: _____
 - Disciplina de tráfico: _____
 - Otros fines administrativos: _____
- 4) Administraciones u órganos a las que se prevé ceder datos relativos a la videovigilancia
- Órganos judiciales
 - Otras administraciones con competencia en la materia
 - Otros (indicar)
- 5) La gestión del uso y conservación de imágenes se realiza mediante:
- Medios propios
 - Empresas subcontratadas
 - Ambas opciones

Cuestiones relativas a disciplina de tráfico y seguridad vial

- 1) ¿Se dispone de videocámaras y otros medios de captación y reproducción de imágenes para el control, regulación, vigilancia y disciplina del tráfico en las vías públicas?
- Si
 - No
- a) En caso afirmativo a la cuestión anterior, las resoluciones de instalación de sistemas de videovigilancia identifican las vías públicas o los tramos susceptibles de captación, así como el órgano encargado de su custodia y de resolución de peticiones de acceso y cancelación;
- Si
 - No
- b) ¿Las resoluciones sobre instalación de sistemas de videovigilancia con fines de disciplina de tráfico se notifican a la CVL?
- Si
 - No
- c) El plazo de conservación de imágenes en materia de disciplina de tráfico es de:
- Menos de 1 mes
 - 1 mes
 - 1 mes prorrogable por otro
 - 3 meses
 - Indefinido



Cuestiones específicas para administraciones locales

- 1) Se dispone de cámaras fijas en instalaciones municipales como:
 - Edificios de oficinas
 - Recintos deportivos
 - Culturales
 - Comisaría
 - Garbigune
 - Transporte urbano
 - Otros (indicar)

- 2) ¿Algunas cámaras ubicadas en recintos municipales captan imágenes interiores como lugares de trabajo, pasillos, salas, despachos, bibliotecas, piscinas, ascensores, etc?
 - Si
 - No

- 3) ¿Se dispone de cámaras de captación de matrículas para la regulación del tráfico en cascos urbanos o parkings?
 - Si
 - No

- 4) ¿Se informa a la ciudadanía acerca de la captación de imágenes en instalaciones y recintos municipales mediante carteles y avisos?
 - Si
 - No

Cuestiones específicas para el Departamento de Seguridad de Gobierno Vasco

- 1) ¿La Viceconsejería de Seguridad del Departamento de Seguridad de Gobierno Vasco remite las autorizaciones de instalación de cámaras fijas a la CVL previamente a la resolución autorizante?
 - Si
 - No

- 2) El plazo de autorización para el uso de cámaras móviles con fines de seguridad ciudadana es de:
 - 1 mes
 - 1 mes prorrogable por otro
 - 3 meses
 - Indefinido
 - Otro (indicar)



- 3) Las autorizaciones de uso de cámaras móviles se emiten:
- Por cada cámara
 - Por unidad, servicios, jefaturas, etc.
 - De manera conjunta
- 4) ¿La Viceconsejería de Seguridad dispone de un protocolo, instrucción o instrumento jurídico análogo que permite analizar el alcance y supuestos de uso de las cámaras móviles, especialmente ante supuestos de máxima urgencia?
- Si
 - No
- 5) ¿Las autorizaciones para la instalación y uso de cámaras tanto fijas como móviles incluyen una valoración de la necesidad e idoneidad de las solicitudes planteadas por los responsables de los servicios y unidades policiales?
- Si
 - No

Comentarios o informaciones complementarias que se consideren de interés

ararteko

Herriaren Defendatzailea
Defensoría del Pueblo

Oficinas de atención directa

En Álava

Prado, 9 • 01005 Vitoria - Gasteiz
Tel.: 945 13 51 18 • Fax: 945 13 51 02

En Bizkaia

Edificio Albia. San Vicente, 8 – Planta 8
48001 Bilbao
Tel.: 944 23 44 09

En Gipuzkoa

Arrasate 19, 1.a
20004 Donostia/San Sebastián
Tel.: 943 42 08 88

www.ararteko.eus

