LA VIDEOVIGILANCIA Y LA GARANTÍA DE LOS DERECHOS INDIVIDUALES: SU MARCO JURÍDICO.

Ana Aba Catoira

I. PLANTEAMIENTO DE LA CUESTIÓN

En la sociedad que nos ha tocado vivir las nuevas tecnologías afectan a todos los ámbitos que tienen algo que ver con la vida diaria de sus ciudadanos. Evidentemente, esta aplicación tecnológica plantea, de forma inevitable, una serie de cuestiones jurídico-constitucionales que requieren una solución o respuesta adecuada, habida cuenta que están en juego derechos fundamentales de la persona como la intimidad o el derecho a la protección de sus datos personales.

Pues bien, siguiendo con este orden de cosas, resulta constatable como en los últimos años han proliferado los sistemas de videovigilancia o equipos destinados a la vigilancia de las personas a través de videocámaras, a las que recurren tanto los poderes públicos como organismos de naturaleza privada para ejercer el control de los ciudadanos como medida de seguridad.

Evidentemente, la instalación de estos sistemas de control, de avanzada tecnología, queda sujeta a un conjunto de requisitos que actúan como garantías para los afectados, en protección de sus derechos y libertades individuales. Derechos individuales, como son la intimidad o vida privada y la protección de datos personales, reconocidos y protegidos en diversos instrumentos jurídicos internacionales, como el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[1] (art.8), el Convenio nº 108/1981 del Consejo de Europa, relativo a la

1 Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Instrumento de Ratificación de 26 de septiembre de 1979. (BOE núm.43, de 10 de octubre de 1979).

protección de las personas físicas en lo que respecta al tratamiento automático de datos personales[2] (las voces e imagen se consideran datos personales cuando arrojen información sobre una persona y la hagan identificable) y la Carta de los Derechos Fundamentales de la Unión Europea[3] (art.7 y 8).

Al respecto hemos de añadir que, en la actualidad, el Consejo de Europa está finalizando un conjunto de principios directores para la protección de las personas físicas en relación con la recogida y tratamiento de datos a través de la vigilancia por videocámara. Estos principios deberán profundizar en la especificación de las garantías relativas a los interesados, previstas en los instrumentos del Consejo de Europa.

La legislación comunitaria y, por supuesto, la legislación nacional, protegen los derechos fundamentales de las personas y, en este sentido, no han olvidado la utilización "potencialmente lesiva" de las nuevas tecnologías de vigilancia. En este orden de cosas, la Directiva 95/46/CE, del Parlamento Europeo y del Consejo[4], regula dicha utilización, como hace en España, la Ley Orgánica 4/1997, de 4 de agosto, de Videovigilancia[5] y, por su relación directa con la protección de los datos personales, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales[6], pues se produce el uso y tratamiento automatizado de los datos personales obtenidos a través de las videocámaras.

II. LA VIGILANCIA A TRAVÉS DE LAS VIDEOCÁMARAS: LA VIDEOVIGILANCIA

El aumento considerable de la instalación de videocámaras se constata en diferentes ámbitos, en los que se persiguen fines de lo más variado. Así, en el interior o cercanías de los edificios públicos o abiertos al público para evitar delitos o actos vandálicos; en el interior de estadios o instalaciones deportivas en general; en el sector del transporte y en relación con el tráfico rodado para detectar excesos de velocidad o violaciones de las normas de circulación; para evitar peligros a menores; en el interior de centros sanitarios para el cuidado y vigilancia de los pacientes; en aeropuertos o lugares fronterizos para controlar la entrada ilegal de extranjeros o para la búsqueda de menores o personas desaparecidas; por parte de detectives o investigadores privados; dentro de establecimientos comerciales para evitar robos; en las comunidades de vecinos; con fines periodísticos y publicitarios, etc.

Así pues, la protección de las personas, la protección de la propiedad, el interés público, la detección, prevención y castigo de los delitos y otros intereses legítimos, se erigen como los argumentos esgrimidos para justificar la vigilancia por videocámaras. Una utilización de videocámaras, como sistema de vigilancia a través de la captación y

2 Convenio del Consejo de Europa de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984 (BOE de 15 de noviembre de 1985).

3 Carta de Derechos Fundamentales de la Unión Europea de 2000.

4 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (DOCE serie L. núm.281, de 23 de noviembre de 1995).

5 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 (BOE núm.186, de 5 de agosto). Su Reglamento de desarrollo y ejecución aprobado por Real Decreto 596/1999, de 16 de abril.

6 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (BOE núm.298, de 14 de diciembre). Ley que deroga la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. (BOE núm.262, de 31 de octubre).

grabación de imágenes y sonidos, que puede resultar obligatoria según disponen las leyes en algunos casos, voluntaria en otros y que, incluso, puede llegar a ser ilegal cuando la instalación no cumple los requisitos exigidos por carecer de justificación suficiente.

Ante esta imparable proliferación de estos sistemas de control de las personas, tanto en manos de organismos públicos como de organismos privados, hay que establecer varios elementos que, en todo caso, deben ser tenidos en cuenta para evaluar la legalidad de estas técnicas.

En un primer orden de cosas, la instalación de estos sistemas de captación y grabación de la imagen en zonas públicas y privadas no puede constituir una restricción injustificada de los derechos y libertades de las personas, que pueden acabar teniendo que soportar una recogida de datos abusiva a través de su identificación en lugares públicos y privados.

Además, no se debe variar la tendencia tradicionalmente seguida en la instalación de videocámaras. Su origen está en ser una medida de seguridad para prevenir y evitar conductas delictivas y estas técnicas no deben transformarse en mecanismos de control y exclusión ciudadana, en cuanto formas de estudiar el comportamiento humano y diseñar perfiles individualizados de las personas.

III. EL MARCO JURÍDICO DE LA VIDEOVIGILANCIA:

III.1º. La vigilancia en el marco de la Directiva 95/46/CE

La captación de imágenes y sonidos a través de videocámaras proporcionan datos personales que son fuente de información personal. Esta Directiva tiene como objeto de protección el derecho a la intimidad y la vida privada de las personas, así como sus datos personales.

El carácter sensible de los datos constituidos por la imagen y sonidos relativos a las personas físicas se pone de relieve en los Considerandos de la Directiva y en determinados artículos de la misma. Así, en el Considerando 14 se señala que la Directiva resulta aplicable en este ámbito por la importancia del desarrollo de las técnicas utilizadas para captar, manejar y utilizar los datos personales obtenidos a través de ellas. En este sentido, los principios de protección de datos que en ella se establecen resultan aplicables a toda información, incluída la referente a la imagen y sonido, relativa a personas identificadas o identificables, teniendo en cuenta los medios que puedan ser utilizados por el responsable del tratamiento u otra persona para identificar a aquella (art.2.a y el Considerando 26).

Así, las disposiciones aplicables son:

- Calidad de los datos, que obliga a que las imágenes sean tratadas de manera leal y lícita, destinándose a fines determinados, explícitos y legítimos. En este orden de cosas, los datos deben ser adecuados, pertinentes y no excesivos, no permitiéndose que se traten posteriormente de manera incompatible con dichos fines (art.6).
- Principios relativos a la legitimación del tratamiento de datos: el tratamiento de los datos personales mediante vigilancia por videocámara ha de cumplir alguno de los requisitos establecidos en el art.7: consentimiento inequívoco, necesidad de obligaciones contractuales, necesidad de cumplimiento de obligaciones jurídicas, protección del interés vital del afectado, cumplimiento de intereses públicos, etc.

- Los datos especialmente protegidos, con arreglo al art.8 presentan especialidades en su tratamiento.
- La información que obligatoriamente se ha de facilitar al interesado (arts.10 y 11).
- Los derechos de acceso, rectificación y cancelación y aquellos otros como el de oposición al tratamiento por razones legítimas (art.12.a y art.14).
- Garantías aplicables en relación con las decisiones individuales automatizadas (art.15).
- Seguridad de las operaciones del tratamiento (art.17).
- Notificación de las operaciones de tratamiento (arts.18 y 19).
- Controles previos de las operaciones de tratamiento que puedan presentar riesgos específicos para los derechos y libertades del interesado (art.20).
- Transferencia de datos a terceros países (art.25 y ss.).
- El carácter específico y sensible del tratamiento de datos constituídos por la imagen y sonidos se reconoce en el último artículo de esta Directiva, en el que la Comisión se compromete a estudiar la aplicación de esta norma comunitaria a este ámbito y a presentar las propuestas que puedan ser necesarias en función de los avances que experimenten las tecnologías de la información y la sociedad de nuestros días conocida como Sociedad de la Información (art.33).

III.1.1º. Excepciones de aplicación de la Directiva

Las disposiciones contenidas en la Directiva no son aplicables al tratamiento de datos constituídos por imágenes y sonidos cuando se realizan con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades estatales en el ámbito penal, así como para el ejercicio de actividades que no están comprendidas en el ámbito de aplicación del Derecho Comunitario. No obstante, muchos Estados miembros se han preocupado por regular estos ámbitos, de manera general, aunque han establecido excepciones específicas.

Así las cosas, en algunos países, estas operaciones de tratamiento de estos datos, excepcionadas del ámbito de aplicación de la Directiva, además de estar sujetas a las garantías establecidas en el Convenio 108 de 1981 y las que responden al cumplimiento de las Recomendaciones del Consejo de Europa, quedan sujetas a disposiciones nacionales determinadas. Todas las operaciones de tratamiento de datos personales, estén o no comprendidas en el ámbito de aplicación de la Directiva, deben responder a motivos de necesidades reales de seguridad pública o para la detección, prevención y control de delitos, cumpliendo con los requisitos establecidos en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

Tampoco resulta aplicable la Directiva a las operaciones de tratamiento realizadas por una persona física en el marco de una actividad meramente personal o familiar (art.3.2º y Considerando 12). Este supuesto adquiere toda su lógica cuando se coloca la cámara de videovigilancia por una persona para controlar a distancia lo que sucede dentro de su casa, ya sea para evitar robos o para cuidar a sus hijos o personas bajo dependencia, pero no es lo mismo cuando su instalación se realiza fuera de la casa con el fin de proteger la propiedad o garantizar la seguridad. En este caso, la instalación pudo ser realizada por los propietarios individuales para vigilar el acceso a su propiedad o por varios propietarios puestos de acuerdo para poder controlar zonas comunes, resultando en este último caso aplicable a las actividades pertinentes. Es decir, el sistema de video-

vigilancia puede dirigirse a la exclusiva protección de un hogar y, por tanto, responder únicamente a fines personales de seguridad y los datos obtenidos no son objeto de publicidad, pero ello no exime, en ningún caso, del respeto de los derechos e intereses de los vecinos y otras personas que pudieran pasar por el lugar vigilado y sometido a grabación. Así, en todo caso, en los Estados miembros, los derechos e intereses siempre están protegidos con independencia de los principios específicos de protección de datos, pues así se establece en las disposiciones generales de naturaleza civil que protegen los derechos personales como la imagen, la intimidad o la vida privada, personal y familiar, de las personas.

La Directiva, en su art.9, establece que los Estados miembros adoptarán excepciones respecto de algunas de sus disposiciones cuando el tratamiento se realice con fines exclusivamente periodísticos o de expresión artística o literaria, contemplando específicamente el sector audiovisual (Considerando 17). Estas excepciones han de responder a la necesidad de conciliar el derecho a la intimidad con las normas que regulan el ejercicio de la libertad de expresión.

III.1.2º. La vigilancia por videocámara y la protección de los Datos Personales

La Directiva 95/46/CE resulta de aplicación al tratamiento automatizado de datos personales, entre los que se incluyen, tal como se ha señalado, los constituidos por imagen y sonido captados por sistemas de vigilancia por videocámara, así como al tratamiento no automatizado de datos personales incluidos en ficheros.

Los datos personales son datos relativos a personas físicas identificadas o identificables y cuando nos concretamos en los constituidos por imagen y sonido es indiferente que:

- las imágenes se utilicen en el marco de un sistema de circuito cerrado y que no estén asociadas a los datos personales del interesado
- se refieran a personas cuyos rostros no hayan sido filmados, aunque contengan otra información captada a través de la videovigilancia
- el método utilizado para el tratamiento (sistemas de video fijos o móviles, como receptores de imagen portátiles, o imágenes en color o en blanco y negro), la técnica (dispositivos de cable o fibra óptica), el tipo de equipo (fijo, móvil o portátil), las características de la captación de imágenes (continua por oposición a discontinua, tal que sucede cuando sólo se realiza en caso de que no se respete el límite de velocidad y no tiene nada que ver con la grabación de imágenes realizada de manera totalmente fortuita y asistemática) y las herramientas de comunicación utilizadas (la conexión con un centro de recepción o el envío de las imágenes a terminales remotos).

A. Garantías a respetar en el tratamiento y obligaciones del responsable

- La legalidad del tratamiento:

El art.6.1º de la Directiva establece los principios relativos a la calidad de los datos, que obligan a los Estados miembros a tratar los datos de manera leal y lícita (letra a). Así, pues, la licitud del tratamiento obliga al responsable del mismo a verificar previamente si la vigilancia efectuada observó la normativa general y específica. En este orden de cosas, se tomarán todas las medidas adecuadas para garantizar que la videovigilancia cumple los principios generales de la protección de datos y se evitará toda lesión de los derechos individuales de los afectados.

Cuando el equipo de vigilancia haya sido instalado por entidades privadas o por organismos públicos, por motivos de seguridad o para la persecución de las actividades delictivas, se prestará especial atención a la fijación de estos motivos, así como a la información sobre los mismos y a las tareas que debe realizar el responsable del tratamiento con arreglo a la normativa. Este último aspecto se plantea de forma más específica con respecto a las autoridades locales, que no tienen competencia directa en asuntos de orden público y seguridad pública y que realizan actividades auxiliares destinadas a la vigilancia.

- Los fines del tratamiento: el responsable del tratamiento de datos ha de asegurarse de que los fines perseguidos y que justifican su realización sean claros e inequívocos con el objeto de ofrecer un criterio preciso para evaluar la compatibilidad exigida por la letra b del art.6.1º de la Directiva.

La claridad de los fines resulta necesaria para mantener convenientemente informados a los interesados cuando se les comunique la notificación pertinente, así como en lo que concierne al control previo que se realiza en relación con el tratamiento de datos (art.20 de la Directiva).

Las imágenes captadas, y, consiguientemente, los datos personales obtenidos a través de estas grabaciones, no podrán ser utilizadas con fines distintos a los establecidos previamente.

- Principios relativos a la legitimación del tratamiento de datos (art.7): el responsable del tratamiento verificará que la vigilancia por videocámara cumple las disposiciones específicas y también los principios establecidos en el art.7 de la Directiva pertinentes a la legitimación del tratamiento con relación específica a la protección de datos personales.

Al margen de aquellos casos en los que se cumple una obligación establecida legalmente, por ejemplo cuando el tratamiento resulta necesario para la protección de intereses vitales (control a distancia de pacientes en unidades de reanimación), con frecuencia es necesario que el responsable del tratamiento cumpla una función de interés público o inherente al ejercicio del poder público, a través del cumplimiento de la normativa específica, tal como prevé el art.7e), o que el tratamiento sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezcan intereses o derechos y libertades fundamentales del interesado que requieran protección de acuerdo con el apartado 1º del art.1 de esta Directiva (art.7f).

En estos casos, y, especialmente, en este último, la naturaleza sensible de las operaciones de tratamiento requiere un análisis detallado de las misiones, los poderes y los intereses legítimos relativos al responsable del tratamiento.

En lo referido al equilibrio entre los diferentes intereses, habrá que estar a la posibilidad de que uno de ellos merezca protección y entre en conflicto con la instalación del sistema o con determinados acuerdos de retención de datos u otras operaciones de tratamiento.

En cuanto a la obtención del consentimiento del interesado (art.7a), deberá ser inequívoco y estar basado en información clara, debiendo ser otorgado por separado y estar específicamente vinculado a las actividades de vigilancia relativas a un lugar en el que se desarrolle la vida privada de una persona. El art.2h) de la Directiva referido al consentimiento válido habla de "toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan".

Cuando las operaciones de tratamiento mediante vigilancia por videocámara sean llevadas a cabo por organismos públicos han de basarse siempre en disposiciones legales específicas.

- Proporcionalidad a la hora de recurrir a este tipo de vigilancia: El principio general de que los datos deberán ser adecuados y proporcionados al fin perseguido obliga a que estos sistemas de vigilancia sólo puedan ser utilizados en los siguientes supuestos:

· Con fines que justifiquen recurrir a estos sistemas: evidentemente el recurso a técnicas de vigilancia de control de los ciudadanos debe limitarse, por respeto debido a los derechos y libertades, a los supuestos en los que todos los demás instrumentos de seguridad o de ayuda (a las fuerzas de seguridad por ejemplo) resultan insuficientes. En este sentido, resulta aplicable el principio de idoneidad con respecto a los fines perseguidos, lo que obliga a reducir a lo mínimo e indispensable la captación y tratamiento de datos personales.

Evidentemente, la proporcionalidad preside la instalación de videocámaras, pues no todas las infracciones son de igual intensidad y gravedad y, consecuentemente, no requieren de los mismos medios para su prevención, persecución y sanción que habrán de establecerse de forma gradual y proporcionada.

· Siempre y cuando otras medidas de protección y seguridad, que no implican captación de imágenes, resulten insuficientes o inaplicables.

Evidentemente, estas dos consideraciones afectan directamente a la imparable vigilancia por videocámara con fines de protección privada.

- Proporcionalidad en la realización de actividades de vigilancia: El principio según el cual los datos deben ser adecuados, pertinentes y no excesivos, implica la proporcionalidad de las medidas relativas al tratamiento legal de datos.

Así las cosas, las medidas para la grabación de imagen y sonido, se establecerán teniendo en cuenta:

· El ángulo visual con arreglo a los fines perseguidos: por ejemplo, si la vigilancia se realiza en un lugar público, el ángulo deberá establecerse de manera que no se pueda visualizar detalles o rasgos físicos que sean irrelevantes para los fines perseguidos, o zonas situadas en el interior de lugares privados cercanos.

· El tipo de equipo que se utilizará para filmar, fijo o móvil.

· Medidas reales de instalación, como situación de las cámaras, utilización de plano fijo o cámaras móviles, etc.

· Posibilidad de aumentar las imágenes o realizar primeros planos durante la grabación o una vez almacenadas las imágenes.

· Congelación de imágenes.

· Conexión con un centro para enviar señales de alarma sonoras o visuales.

· Medidas que se toman como resultado de la vigilancia por videocámara, como cierre de entradas, convocatoria del personal de vigilancia, etc.

Además, deberá tenerse en cuenta que se hará con las imágenes grabadas y el tiempo que se conservarán que, en ningún caso, debe ser prolongado.

- Información a los interesados: Los ciudadanos deben estar informados de la instalación y utilización de los equipos de videovigilancia.

Los arts.10 y 11 de la Directiva obligan a informar sobre la vigilancia por videocámara que se está llevando a cabo, incluso cuando ésta se realice en acontecimientos públicos o espectáculos. Es decir, se trata de dar a conocer que se están realizando funciones de vigilancia para que los afectados estén prevenidos al respecto.

En este sentido, la información deberá colocarse a la vista para que pueda ser eficaz, habrán de especificarse los fines de la vigilancia y quién es el responsable del tratamiento.

- Otros requisitos:

La Directiva establece requisitos adicionales, precauciones y garantías en materia de protección de datos, como la necesidad de que el tratamiento de datos personales sea notificado a una autoridad independiente y se someta a la supervisión de la misma con arreglo a los artículos 18, 19 y 28 de la misma.

En relación con esta materia el Grupo de Protección de las Personas[7], en lo que respecta al tratamiento de datos personales, ha adoptado un Documento de trabajo en el que destaca que:

- un número limitado de personas físicas, que deberá especificarse, estará autorizado a visualizar o acceder a las imágenes grabadas, exclusivamente para los fines perseguidos por la vigilancia por videocámara o con vistas al mantenimiento del equipo a fin de verificar su funcionamiento.

Siempre que la vigilancia por videocámara se destine únicamente a prevenir, detectar y controlar infracciones, la solución consistente en utilizar dos claves de acceso (una en posesión del responsable del tratamiento y la otra de la policía) podrá resultar útil para garantizar que las imágenes sólo las verá la policía y no personal sin autorización.

- Deberán aplicarse medidas de seguridad a fin de evitar que se produzcan las eventualidades del art.17 de la Directiva, incluida la difusión de información que pudiera ser útil para proteger un derecho del interesado, a una tercera parte o al propio responsable del tratamiento.
- La calidad de las imágenes grabadas resulta fundamental.
- Los operadores implicados en las actividades de vigilancia por videocámara han de estar formados y al día de las medidas que deben tomar para cumplir los requisitos exigidos.
- Los derechos del interesado: El ejercicio de los derechos contenidos en los arts.13 y 14 de la Directiva, especialmente el derecho de oposición al tratamiento que podrá ejercitarse en cualquier momento oponiéndose al tratamiento de datos que conciernen a uno.

El derecho del interesado al olvido y la brevedad en la conservación de las imágenes reducen el ámbito de aplicación de su derecho a acceder a los datos personales que lo hacen identificable.

- Garantías adicionales relacionadas con operaciones de tratamiento específicas: Se prohíbe la vigilancia por videocámara realizada exclusivamente a causa del origen racial de las personas, sus ideas políticas o religiosas, su pertenencia a sindicatos o sus hábitos sexuales (art.8 Directiva).

El Grupo, anteriormente citado, recalca la necesidad de prestar más atención a determinados contextos en los que se recogen imágenes relativas a personas identificadas o identificables:

- interconexión permanente de sistemas de vigilancia por videocámara gestionados por diferentes responsables del tratamiento

7 Este Grupo de Protección de las Personas se creó en virtud de la Directiva 95/46/CE, siguiendo el art.29 y la letra a) del apartado 1º y apartado 3º del art.30.

- Posible asociación de imágenes y datos biométricos como huellas dactilares
- Utilización de sistemas de identificación vocal
- Introducción, con arreglo a principios de proporcionalidad y en base a disposiciones específicas, de sistemas de indexación relativos a imágenes grabadas o sistemas de recuperación simultánea automática, en particular a través de datos de identificación.
- Utilización de sistemas de reconocimiento fisonómico que no se limiten a la identificación de camuflajes de personas de paso, como barbas y pelucas falsas, sino que se basen en la localización de presuntos delincuentes, es decir, en la capacidad del sistema para identificar automáticamente a determinados individuos, a partir de plantillas o retratos robot que resulten de determinados rasgos externos o con arreglo a comportamientos anormales predefinidos.
- Posibilidad de localizar, automáticamente, itinerarios y pistas, o de reconstruir o prever el comportamiento de una persona.
- Toma de decisiones automatizadas basadas en el perfil de una persona o en análisis inteligentes y sistemas de intervención que no estén relacionados con señales de alarma estándar.

III.2º. Legislación Nacional aplicable a la vigilancia por videocámara

Las videocámaras ayudan a prevenir y a probar comportamientos delictivos y es por esto por lo que su empleo se regula como mecanismo de política criminal, pues se postula su uso como instrumento eficaz en la prevención y persecución del delito y para el mantenimiento de la seguridad ciudadana. En este orden de cosas, la Ley Orgánica 4/1997 regula la utilización de técnicas de videovigilancia en los lugares de tránsito público.

Ciertamente, la videovigilancia plantea numerosos problemas, pero también reporta indudables beneficios, por lo que nos encontramos ante la necesidad de equilibrar unos y otros, intentando que primen los segundos. En el lado de las ventajas se encuentran los fines que justifican su utilización por el Estado y en el de los problemas, los ya sabidos: la proliferación incontrolada de instalación de cámaras, muchas de ellas con fines privados sin contar con una regulación adecuada, el control de los ciudadanos con el consiguiente efecto aparejado de inhibición en lo que respecta a su comportamiento social, y, como a nadie se le escapa, la posibilidad de recopilar, almacenar y transmitir informaciones personales de forma ilimitada.

La conclusión de todo ello es la sensación de control total a la que estamos sometidos, un control o vigilancia que nosotros no podemos controlar, y que, indudablemente, repercute en nuestros derechos y libertades fundamentales.

En algunos países se han desarrollado disposiciones específicas relativas a la vigilancia por videocámaras con independencia de que ésta implique el tratamiento de datos personales. Así, existe una legislación específica que regula su implantación y utilización para captar imágenes y sonidos de las personas al margen de que haya una legislación específica de protección de datos personales, en la que, lógicamente, se regula el tratamiento de los datos que constituyen la imagen y sonidos. En otros países, la vigilancia por videocámaras no es objeto de legislación específica y las autoridades de protección de datos se afanan en garantizar la adecuada aplicación de las disposiciones generales de protección de datos a este ámbito.

Dentro del grupo de los países con legislación específica se sitúa España, con la Ley Orgánica 4/1997, por la que se regula la utilización de videocámaras por las

Fuerzas y Cuerpos de Seguridad en lugares públicos, exclusivamente, y que, además, cuenta con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, que transpone la Directiva 95/46/CE. Otro país como Suecia cuenta con una regulación específica de la vigilancia por videocámaras en la Ley 1998/150, sobre vigilancia general por videocámaras y la Ley 1995/1506, sobre vigilancia secreta por videocámara, circunscrita a las investigaciones criminales.

En cuanto al segundo grupo, cabe citar el caso de Italia con el Decreto Legislativo nº 467, Sección 20, de 28 de diciembre de 2001, relativa a la adopción de códigos de conducta, y con las resoluciones de la autoridad italiana de protección de datos: nº 2, de 10 de abril de 2002, relativa al fomento de la adopción de códigos de conducta; de 28 de septiembre de 2001, relativa a las técnicas biométricas y de reconocimiento fisonómico aplicadas por los bancos y de 29 de noviembre de 2000, el "decálogo de la vigilancia por videocámara".

Las complejas y delicadas tareas encomendadas a las Fuerzas y Cuerpos de Seguridad del Estado necesitan de todas las ayudas posibles para su realización. En este orden de cosas, las nuevas tecnologías de la información se presentan como un recurso inestimable al que recurren en el desempeño diario de su trabajo en una utilización de las tecnologías que en el contexto democrático se sujeta a un conjunto de garantías legales y constitucionales que controlan el ejercicio del poder en salvaguardia de nuestros derechos e intereses.

La Ley Orgánica 4/1997, de Videovigilancia, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos es buena muestra de ello. Con su aprobación se pone fin a un tortuoso y largo camino que se inició con los sucesos que acontecieron en Bilbao en el verano de 1993, con el linchamiento de un policía autonómico[8].

Evidentemente, la grave realidad que se vive en el País Vasco, quizás más violenta a fines de los noventa, fechas en las que se elabora y aprueba esta Ley, explica la política policial que busca el aprovechamiento de las ventajas que ofrecen las nuevas tecnologías, por lo que la instalación de las videocámaras en los ámbitos de seguridad ciudadana no deben extrañar por ser comunes en los países de nuestro entorno.

Si a la instalación de las videocámaras sumamos la recopilación de datos personales, obtenidos a través de las grabaciones, y su tratamiento automatizado, llegamos a la conclusión de que se han incrementado notablemente las posibilidades de gestionar la información y exprimirla para obtener material con el que luchar para mantener la seguridad ciudadana. Por ejemplo, las posibilidades tecnológicas permiten que una ficha policial contenga, además de las notas básicas que identifican a un sujeto, su imagen y su voz . Además, la conexión entre redes informáticas a lo largo y ancho del planeta suponen la desaparición de los límites temporales y espaciales en la recopilación y transmisión de información.

Evidentemente, el empleo de las nuevas tecnologías acrecienta los riesgos y amenazas que sufren los derechos y libertades individuales, pues la vigilancia en cuanto control, implica una mayor intromisión en ámbitos constitucionalmente protegidos. De ahí la importancia de cumplir escrupulosamente todos los requisitos y garantías establecidas, así como de la formación en el respeto de los derechos fundamentales de

8 GONZÁLEZ URDINGUIO, A. y GONZÁLEZ GUTIÉRREZ DE LEÓN, Mª A.: "La videovigilancia en el sistema democrático español: análisis y crítica de la Ley Orgánica 4/1997, 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos", *Revista de la Facultad de Derecho de la Universidad Complutense de Madrid,* Núm.89, pp.105-124.

aquellas personas encargadas de la utilización de estos medios y del tratamiento de la información[9].

III.2.1º. Los Derechos Fundamentales afectados

Como ya se ha señalado reiteradamente, estudiar la utilización de instrumentos técnicos con fines de vigilancia policial presenta como elemento de dificultad añadida que estamos ante una materia que repercute en el ámbito de los derechos fundamentales, particularmente en el derecho a la intimidad o derecho a la vida privada.

Y es que, efectivamente, no son pocos los casos en los que se han realizado abusos de derechos a través de las técnicas de videovigilancia mediante grabaciones y reproducciones ilícitas de imágenes y sonidos. La cada vez mayor implantación de estas videocámaras en lugares públicos y espacios privados, como por ejemplo en los lugares de trabajo, ya no extraña a nadie e incluso, hemos aprendido a convivir con ese ojo mecánico que sigue nuestros movimientos silenciosamente. La capacidad de vigilar y, por tanto, de controlar a los ciudadanos por los ojos públicos y privados atenta contra los derechos de los ciudadanos, que se ven indefensos ante la imposibilidad de controlar esas actuaciones.

Los derechos fundamentales que resultan más afectados son los derechos de la personalidad reconocidos en el art.18.1º de la Constitución y el derecho de autodeterminación informativa o derecho de protección de datos personales contenido en el art.18.4º. Pero también se ven afectados otros derechos como la inviolabilidad del domicilio, ya que las tecnologías permiten captar las actividades y conductas desarrolladas en el interior de los espacios privados protegidos por la inviolabilidad del art.18.2º de la Constitución, así como el derecho de libre circulación de las personas que se sienten intimidadas y vigiladas por las videocámaras.

En el ámbito del art.18.1º recordar junto al derecho a la intimidad o vida privada de las personas, el derecho a la propia imagen que tutela la representación gráfica de la figura humana y, por tanto, la personalidad. En consecuencia, la persona puede decidir sobre la captación o reproducción de su propia imagen física existan o no motivaciones de naturaleza económica[10].

En palabras del Tribunal Constitucional "Los derechos a la intimidad personal y a la propia imagen garantizados por el art.18.1º de la Constitución, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas. Y en este ámbito de la intimidad, reviste singular importancia la necesaria protección del derecho a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma y de datos y de circunstancias pertenecientes a la intimidad que garantiza este precepto"[11].

9 DAVARA, M. A.: *Guía práctica de Protección de Datos,* Madrid, 1999. Al respecto consultar la Teoría de la limitación de los derechos fundamentales, ABA CATOIRA, A.: *La limitación de los derechos en la jurisprudencia del Tribunal Constitucional,* Valencia, 1999; *Los límites de los derechos por razón del sujeto,* Madrid, 2001.

10 Sobre el derecho a la intimidad HERCE DE LA PRADA, v.: *El derecho a la propia imagen y su incidencia en los medios de difusión,* Barcelona, 1994; ROYO JARA, J.: *La protección del derecho a la propia imagen,* Madrid, 1987; ALEGRE MARTÍNEZ, M. A.: *El derecho a la propia imagen,* Madrid, 1997; PACE, A.: "El derecho a la propia imagen en la sociedad de los mass media" en *Revista Española de Derecho Constitucional,* Núm.52, 1988.

11 STC 170/1987, FJ 4º.

"El derecho a la propia imagen, consagrado en el art.18.1º C.E. junto con los derechos a la intimidad personal y familiar y al honor, contribuye a preservar la dignidad de la persona (art.10.1º C.E.), salvaguardando una esfera de la propia reserva personal frente a intromisiones de terceros. Sólo adquiere así su pleno sentido cuando se le enmarca en la salvaguardia de "un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC 231/1988, FJ 3º). [...] Calificado así, resulta claro que el primer elemento a salvaguardar sería el interés del sujeto en evitar la difusión incondicionada de su aspecto físico, que constituye el primer elemento configurador de su intimidad y de su esfera personal, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como individuo. En este contexto, la captación y difusión de la imagen del sujeto sólo será admisible cuando la propia –y previa- conducta de aquél o las circunstancias en que se encuentre inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que puedan colisionar con aquél [...]"[12].

"El derecho a la propia imagen, reconocido por el art.18.1º de la Constitución a la par de los del honor y la intimidad personal, forma parte de los derechos de la personalidad y como tal garantiza el ámbito de libertad de una persona respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona. En la medida en que la libertad de ésta se manifiesta en el mundo físico por medio de la actuación de su cuerpo y las cualidades del mismo, es evidente que con la protección de la imagen se salvaguarda el ámbito de la intimidad y, al tiempo, el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz"[13].

Por lo que respecta al párrafo 4º del citado art.18, nos encontramos ante un nuevo derecho fundamental que ofrece protección frente a la recogida, almacenamiento, utilización y transmisión ilimitada de los datos de carácter personal, permitiendo que sea el individuo afectado, titular de dichos datos, quien decida sobre su difusión y utilización, es decir, que controla personalmente las informaciones que la afectan.

El origen de este derecho de tercera generación está en la Sentencia del Tribunal Constitucional Federal Alemán, dictada a raíz de la Ley del Censo de 1983, en la que el Alto Tribunal acuña el nuevo derecho. La fundamentación constitucional de este nuevo derecho se construye desde el derecho general de la personalidad (art.2.1º) en relación con la dignidad personal (art.1.1º). Todas las personas tienen derecho al libre desenvolvimiento de su personalidad siempre que no vulneren los derechos de los otros ni atenten al orden constitucional o a la ley moral. Así, para el TCFA este derecho de autodeterminación informativa atribuye al individuo la capacidad de decidir, "esta facultad requiere en las condiciones actuales y futuras de la elaboración automática de datos una medida especial de protección [...] hoy día gracias a la ayuda de la elaboración automática de datos, la información individual sobre circunstancias personales u objetivas de una persona determinada o en su caso determinable son técnicamente hablando acumulables sin límite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquiera que sea la distancia. Es más esa información puede –especialmente con el montaje de sistemas integrados de información- refundirse con otras colecciones de datos en un perfil de personalidad parcial o ampliamente definido, sin que el interesado pueda controlar suficientemente su exactitud y su utilización [...].

12 STC 99/1994, FJ 5º.

13 STC 117/1994, FJ 3º.

Ahora bien, la autodeterminación del individuo presupone –también en las condiciones de las técnicas modernas de tratamiento de la información- que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada"[14].

El Tribunal Constitucional español inicia claramente su línea jurisprudencial hacia el reconocimiento de un nuevo derecho fundamental en la STC 254/1993, FJ 7º. Un nuevo enfoque que culminará con la STC 292/2000 en la que se apuesta abiertamente por la consagración de un nuevo derecho fundamental a la protección de datos personales con base en el artículo 18.4º de la Constitución, con lo que se integra en nuestro ordenamiento la tesis alemana de la autodeterminación informativa, mantenida por el Tribunal Constitucional Federal Alemán.

Así las cosas, desde que se reconoce un nuevo derecho fundamental autónomo, ya no es necesario discutir si el derecho a la intimidad incorpora y comprende, junto a la facultad tradicional de exclusión de terceros como forma de protección de la vida privada, una facultad de disposición y control de las informaciones personales que afecten al individuo.

Por lo que respecta a la inviolabilidad domiciliaria (art.18.2º) recordar que la protección del espacio privado donde se desarrollan las vivencias personales y familiares, los comportamientos y relaciones personales, es una prolongación o proyección de la tutela que la Constitución depara al derecho a la intimidad[15].

Las entradas no consentidas por el titular del domicilio, o no autorizadas judicialmente, constituyen una violación de este espacio privado, pero no se requiere la penetración física, siendo suficiente la captación o conocimiento de las actividades o comportamientos que se realizan en su interior. Así las cosas, el Tribunal Constitucional desde su más temprana jurisprudencia veda "toda clase de invasiones incluidas las que puedan realizarse sin penetración directa por medio de aparatos mecánicos, electrónicos u otros análogos"[16].

A. Límites de los Derechos ante las actividades policiales:

En el marco de una sociedad democrática, la garantía de la seguridad ciudadana y el mantenimiento del orden público constituyen una presupuesto para el libre ejercicio de los derechos fundamentales y la tutela de los valores justifica que, en ocasiones, los derechos fundamentales se vean limitados siempre que se den las condiciones de proporcionalidad del sacrificio que se impone y de su establecimiento mediante una ley, amén de la aplicación obligatoriamente restrictiva de la norma de limitación.

Las funciones que desarrollan las Fuerzas y Cuerpos de Seguridad del Estado garantizan los derechos y libertades de los ciudadanos, que se constituyen en objeto y límite de sus actuaciones. Las nuevas tecnologías, a la vez que instrumento útil para la realización de sus funciones, tienen gran capacidad de dañar estos derechos y, por ello, se debe buscar un equilibrio entre las libertades y la protección de la seguridad ciudadana.

---

14 La STCFA de 15 de diciembre de 1983, se encuentra en *Boletín de Jurisprudencia Constitucional,* Núm.33, enero de 1984, pp.126-170, traducida por M. DARANAS.

15 Sobre el derecho a la inviolabilidad domiciliaria GONZÁLEZ TREVIJANO, P.: *La inviolabilidad del domicilio,* Madrid, 1992.

16 STC 22/1984, FJ 5º.

En este orden de cosas, el Tribunal Constitucional ha manifestado que "De la Constitución se deduce que las Fuerzas de Policía están al servicio de la comunidad para garantizar al ciudadano el libre y pacífico ejercicio de los derechos que la Constitución y la Ley les reconocen, y este es el sentido del art.104.1º C.E. que puede considerarse directamente heredero del art.12 de la Declaración de Derechos del Hombre y del Ciudadano, configurando a la Policía como un servicio público para la comunidad, especializado en la prevención y lucha contra la criminalidad, el mantenimiento del orden y la seguridad pública y la protección del libre ejercicio de los derechos y libertades. El art.104.1º C.E. trata de asegurar la adaptación del sistema policial, de sus funciones y de sus principios básicos al orden constitucional, subrayando, en un plano positivo, y en la misma línea que el art.53 C.E., la función de garantía de libertades y derechos fundamentales que también corresponde a la Policía pero, al mismo tiempo, negativamente destacando que la actuación de la fuerza de la Policía debe respetar también y garantizar las libertades y derechos fundamentales del ciudadano"[17].

Evidentemente, las investigaciones policiales procuran la obtención de material probatorio, pero que, como todas las actuaciones que supongan afectación de los derechos, encuentran límites, pues no son admisibles las pruebas obtenidas con vulneración de derechos fundamentales[18]. Desde su más temprana jurisprudencia así lo ha afirmado el Tribunal Constitucional, pues declara que la prohibición de estas pruebas obedece a la posición preferente de los derechos fundamentales en el ordenamiento jurídico y de su afirmada condición de inviolables[19].

En definitiva, las limitaciones de los derechos fundamentales han de ajustarse a los siguientes requisitos: ser una medida legítima, autorizada en su caso por resolución judicial motivada y estar acordada siguiendo los principios de legalidad y proporcionalidad[20]. Además, y, cuando la obtención de pruebas se realiza con técnicas tan invasivas como la videovigilancia, se han de respetar los requisitos y garantías establecidos a tal efecto en la Ley Orgánica 4/1997 y en la Ley Orgánica de Protección de Datos Personales. Así, ya en su Exposición de Motivos, la Ley de Videovigilancia reconoce el potencial lesivo de estas técnicas y su necesaria utilización por las Fuerzas Policiales, cuando señala que: "Las imágenes y sonidos obtenidos por cualquiera de las maneras previstas serán destruidos en el plazo de un mes desde su captación, salvo que se relacionen 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 abierto. El público será informado de la existencia de videocámaras fijas y de la autoridad responsable y todas las personas interesadas podrán ejercer el derecho de acceso y cancelación de las imágenes en que hayan sido recogidos.

Finalmente, se dispone la inmediata puesta a disposición judicial de aquellas grabaciones en las que se haya captado la comisión de hechos que pudieran constituir ilícitos penales y, en previsión de que, por circunstancias que deberán ser justificadas, no sea posible, se establece la entrega de la grabación junto con el relato de los hechos a la autoridad judicial o al Ministerio Fiscal".

17 STC 55/1990, FJ 5º. Consultar BARCELONA LLOP, J.: *Policía y Constitución,* Madrid, 1997.

18 La Ley Orgánica del Poder Judicial en su art.11.1º establece que "En todo tipo de procedimientos se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente violentando los derechos o libertades fundamentales".

19 STC 114/1984, FJ 4º.

20 SSTC 85/1994; 54/1996; 228/1997, FJ 11º.

B. Límites a las actividades policiales en protección de los Derechos Fundamentales:

La Ley Orgánica 4/1997 establece en el párrafo 5º de su art.6, dedicado a los principios de utilización de las videocámaras, una limitación a la actividad policial estableciendo que "No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de los vestíbulos salvo consentimiento de su titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley (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. Las imágenes y sonidos obtenidos accidentalmente deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia".

Así pues, este artículo de la Ley Orgánica de Videovigilancia se dirige a la protección de los derechos reconocidos por el artículo 18 de la Constitución, la intimidad y todos aquellos que son una proyección de ésta y que amplían la protección otorgada a la intimidad personal y familiar. La vida privada en general opera como límite frente a las actuaciones policiales que se sirven de estos artificios técnicos para el buen desarrollo de sus funciones de seguridad pública.

No obstante lo anterior, la Ley precisa que no se podrán grabar cuando "se afecte de forma directa y grave a la intimidad de las personas" y que las conversaciones sean "de naturaleza estrictamente privada", con lo que se está limitando o condicionando la protección de los derechos fundamentales a favor de los fines que justifican la vigilancia a través de las técnicas de videovigilancia.

III.2.2º. Análisis del marco jurídico español

A. La Ley Orgánica de videocámaras (LOV)

El art.2.2º de la LOV señala que "Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento Automatizado de los Datos de Carácter Personal".

Evidentemente, en cuanto que la Ley Orgánica de Protección de Datos Personales de 1999 derogó la Ley de 1992, esta remisión queda sin efecto. Además, hay que tener presente que el art.2.3ºe) excluye de su ámbito de aplicación tratamientos de datos personales "procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia. No obstante, estos tratamientos se regirán también "por lo especialmente previsto, en su caso, por esta Ley Orgánica".

Si se interpretan las previsiones legales concluyendo que la LOPD excluye el registro de imágenes y sonidos creados por las Fuerzas y Cuerpos de Seguridad, automatizados o no, también se entenderá que quedan excluidos de su ámbito los tratamientos derivados de esas imágenes y sonidos. Por tanto, quedarían excluidos un gran número de tratamientos de datos personales.

No obstante, también se podría entender que cualquier tratamiento de los datos personales realizado a partir de estas imágenes y sonidos quedaría sujeto a "lo especialmente previsto, en su caso, por la Ley Orgánica de Protección de Datos". Si se atiende a lo dispuesto en el art. 3 de la citada Ley se entiende que "datos personales" son "cualquier información concerniente a personas físicas identificadas o identificables" y "tratamiento" es el conjunto de "operaciones y procedimientos técnicos de carácter

automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

El Reglamento que desarrolla la Ley de Videovigilancia facilita el uso de estas técnicas por las Fuerzas y Cuerpos de Seguridad en el ámbito público en el que desarrollan sus funciones de seguridad. De un estudio de la regulación de esta materia se puede concluir como la opción legislativa se inclina por limitar los derechos fundamentales en aras a fortalecer o favorecer la seguridad pública y la prevención del delito y deja sin solventar las no pocas lagunas que ponen en peligro los derechos de los ciudadanos.

En garantía de los derechos fundamentales la Ley Orgánica 4/1997 crea en su art.3.1º las Comisiones de Garantías de la Videovigilancia, en plural, pues se creará una en cada Comunidad Autónoma con la función de elaborar un informe previo a la instalación de videocámaras, cuya autorización es competencia del Delegado de Gobierno en la Comunidad Autónoma.

Estas Comisiones son órganos colegiados, presididos por un Magistrado, y en su composición no predominan los miembros dependientes de la Administración autorizante. Se habilita en el art.3.2º al Reglamento para determinar su composición y funciones, estando presidida por el Presidente del Tribunal Superior de Justicia y con participación de los municipios.

La Comisión podrá recabar las grabaciones, en caso de uso de videocámaras móviles, y emitir un informe que, de ser negativo, podrá conllevar la destrucción de lo grabado (art.5.2º).

En cualquier caso, señalar que el Reglamento no ha respondido a las expectativas creadas, pues su Capítulo III no ofrece una completa regulación de estas Comisiones de Garantías. Por lo que respecta a sus competencias, decir que se le permite un control previo del uso de las videocámaras y verificar posteriormente la utilización de las mismas, además de destruir las grabaciones cuando no se ajusten a las previsiones de la Ley Orgánica.

En lo concerniente a la solicitud de autorización para instalar videocámaras, hay que decir, en primer lugar, que la Ley de Videovigilancia (arts.3-5) y el Reglamento distinguen entre cámaras fijas y cámaras móviles. En este sentido, la autorización para instalar cámaras fijas se obtiene a través de una solicitud que pueden formular el Subdelegado del Gobierno, el Jefe de la Comisaría Provincial de Policía y el Jefe de la Comandancia de la Guardia Civil o sus inmediatos inferiores en los casos previstos, el Alcalde o el concejal en materia de seguridad ciudadana (art.3 del Reglamento).

La solicitud se dirige al Delegado del Gobierno y ha de contener: la identificación del solicitante, los motivos que la justifican, la definición del ámbito físico susceptible de ser grabado, la necesidad o no de grabar sonido con sujeción a las limitaciones legales, la cualificación de las personas encargadas de la explotación del sistema de tratamiento de las imágenes y sonidos, el tipo de cámaras y sus condiciones técnicas y el período de tiempo en el que se pretenda grabar.

El Delegado del Gobierno encargado de autorizar su instalación cursará la petición a la Comisión de Garantías de la Videovigilancia para que informe previamente en el plazo de un mes. Se trata de un informe vinculante cuando considere que la instalación supondría una vulneración de los criterios establecidos en el art.4 de la Ley, en cuyo caso no podrá conceder la autorización solicitada e, igualmente, cuando siendo favorable a la instalación, se condicione a restricciones, limitaciones o prevenciones en cumplimiento de lo dispuesto en el citado artículo (art.16 del Reglamento).

La solicitud se encuentra obligada a respetar el principio de proporcionalidad y ha de "asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones de la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes".

El principio de proporcionalidad se consagra en el art.6 de la Ley, referido a idoneidad e intervención mínima. La idoneidad supone que "Sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana". La intervención mínima obliga a ponderar en 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, la Ley exige la presencia de "un razonable riesgo para la seguridad ciudadana" para la autorización de las videocámaras fijas.

La resolución por la que se acuerde la autorización ha de ser motivada, referida en cada caso al lugar público concreto que ha de ser objeto de vigilancia, con las condiciones y limitaciones de uso, particularmente "la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes [...]".

Se deberá precisar el ámbito físico y la duración de la autorización con una vigencia máxima de un año "a cuyo término habrá de solicitarse su renovación". El plazo para la resolución, según el art.5 del Reglamento, es de dos meses a contar desde el día siguiente al de la solicitud. Si no se dicta resolución, en su plazo, se entiende denegada.

En referencia a las instalaciones ya existentes, la Disposición transitoria única previó que "Con excepción de lo dispuesto en el apartado 1 y en el párrafo 2º del apartado 1 del artículo 2 y en la Disposición adicional quinta, las Fuerzas y Cuerpos de Seguridad que tengan instalaciones fijas de videocámaras con anterioridad a la entrada en vigor del presente Reglamento y pretendan seguir utilizándolas, deberán, de acuerdo con lo previsto en el mismo, solicitar la correspondiente autorización, que tendrá prioridad en su tramitación".

En principio, parece que la Ley ofrece garantías suficientes para evitar excesos en la instalación de videocámaras.

En lo que respecta a las videocámaras móviles la Ley, atendiendo al espacio público en que se instalen y las circunstancias en que se utilicen, habla de tres categorías. Así las cosas, el art.5.1º autoriza su uso, ya que "En las vías o lugares públicos donde se haya autorizado la instalación de videocámaras fijas, podrán utilizarse simultáneamente otras de carácter móvil para el mejor cumplimiento de los fines previstos en esta Ley, quedando, en todo caso, supeditada la toma, que ha de ser conjunta, de imagen y sonido, a la concurrencia de un peligro concreto y demás requisitos exigidos en el artículo 6".

Cuando se trata de grabar imágenes en lugares públicos que no cuenten con instalación de videocámaras fijas, la autorización para el uso de videocámaras móviles le corresponde "al máximo responsable a nivel provincial de las Fuerzas y Cuerpos de Seguridad del Estado", atendiendo a la naturaleza de los hechos susceptibles de filmación y adecuando la utilización del medio a los principios del art.6 de la Ley. En este caso la Comisión actúa *a posteriori*, ya que la resolución que se dicte autorizando el uso de videocámaras móviles se pondrá en conocimiento de aquella en el plazo máximo de setenta y dos horas, la cual podrá recabar el soporte físico de la grabación a efectos de emitir el correspondientes informe (art.5.2º).

El art.6 establece las condiciones de la solicitud que podrá realizarse por "los mandos operativos de las Fuerzas y Cuerpos de Seguridad del Estado por el conducto reglamentario" y también por "el Alcalde o el concejal competente en materia de seguridad ciudadana respecto de la policía local de su municipio". La resolución se dictará en "el plazo máximo de un mes, contado a partir del día siguiente al de la presentación de la solicitud" y deberá ser motivada siguiendo los criterios del art.4 de la Ley.

Si la resolución autoriza el uso de videocámaras "se pondrá en conocimiento de la Comisión de Garantías de la Videovigilancia correspondiente en el plazo máximo de setenta y dos horas a contar desde su adopción, por cualquier medio telemático, informático o documental que acredite su recepción".

En último lugar, el párrafo 3º del art.5.2º prevé que "En casos excepcionales de urgencia máxima o de imposibilidad de obtener a tiempo la autorización indicada en razón del momento de producción de los hechos o de las circunstancias concurrentes, se podrán obtener imágenes y sonidos con videocámaras móviles, dando cuenta, en el plazo de setenta y dos horas, mediante un informe motivado, al máximo responsable provincial de las Fuerzas y Cuerpos de Seguridad y a la Comisión aludida en el párrafo anterior, la cual, si lo estima oportuno, podrá requerir la entrega del soporte físico original y emitir el correspondiente informe".

En estos dos supuestos, la participación del Gobierno, a través del Delegado o Subdelegado, y de la Comisión se produce *a posteriori* dejándose en manos del responsable policial la adopción de una medida potencialmente restrictiva de derechos fundamentales. En veinticuatro horas se comunicará la realización de las grabaciones a los dos primeros, en la notificación a la Comisión de Garantías se incluirán la comunicación de la realización de la grabación y copia del informe motivado dictado al respecto. Además, la Comisión tiene derecho a estar informado quincenalmente del uso de videocámaras móviles, pudiendo recabar, cuando lo estime oportuno el soporte físico de la grabación y emitir el correspondiente informe. No hay previsión similar respecto de las cámaras fijas.

El Reglamento de Videovigilancia excluye, en su art.2.2º, su aplicación a las instalaciones fijas de videocámaras usadas por las Fuerzas Armadas en sus inmuebles y el uso de estos medios por la Policía Judicial. No obstante, se aplicará lo previsto en la Ley y en el Reglamento cuando la utilización de las videocámaras no se realice directamente por las Fuerzas y Cuerpos de Seguridad y sea la policía quien realice "un control y dirección efectiva del proceso completo de captación, grabación, visionado y custodia de las imágenes y sonidos".

Estas excepciones se justifican en razón de la seguridad nacional y por la naturaleza especial del trabajo policial que se desempeña. Ahora bien, la Ley de Videovigilancia resulta de aplicación en el primero de los supuestos, pues en su art.9.2º se establece una excepción al denegar el acceso cuando éste pudiera afectar a "los peligros que pudieran derivarse para la defensa del Estado". Asimismo, los registros de imágenes tomadas por la Policía Judicial quedarían integradas en la excepción que deniega el acceso en base a "las necesidades de las investigaciones que se estén realizando".

Por otro lado, se exceptúan las instalaciones fijas de videocámaras que tengan como única finalidad "garantizar la seguridad y protección interior o exterior de los inmuebles que se encuentren bajo la vigilancia de las Fuerzas y Cuerpos de Seguridad". Estas instalaciones están sujetas a autorización según la Disposición adicional quinta del Reglamento que señala que "No obstante lo establecido en el apartado 1 y en el párrafo segundo del artículo 2 del presente Reglamento, las unidades policiales que pretendan realizar instalaciones fijas de videocámaras, en el exterior de sus inmuebles o de

los que se encuentren bajo su vigilancia, exclusivamente para la protección de éstos, lo comunicarán, con carácter previo, a la correspondiente Delegación del Gobierno, junto con un informe descriptivo.

Si el Delegado del Gobierno, en el plazo de siete días, no hace manifestación en contrario, se entenderá concedida la correspondiente autorización".

Ciertamente, cuando las grabaciones se realizan en el exterior de las instalaciones policiales pueden verse afectados derechos fundamentales de las personas que circulan por la vía pública, por lo que esta última excepción no parece tener fundamentación en el hecho de que estas cámaras se destinen a la protección de los edificios e instalaciones públicas, así como de sus accesos.

Por lo que respecta al control de las grabaciones, el art.8.4º de la Ley Orgánica dispone que "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".

En su Disposición adicional segunda se ordena la creación, por las autoridades competentes para autorizar la instalación fija de videocámaras, de un registro en el que consten todas las que se haya autorizado. En el conjunto de datos que han de figurar en estos registros se contarán los que permitan identificar al responsable de su utilización. Así, se podrá conocer a quien exigir las debidas responsabilidades y controlar la instalación de estos artefactos de vigilancia.

Los derechos de los afectados quizás sean lo que más interesa a efectos de este trabajo, en el que venimos poniendo de manifiesto que la instalación y utilización de las videocámaras, con el debido cumplimiento de los requisitos legales, persigue la protección de los derechos fundamentales de los ciudadanos afectados. La Ley de Videovigilancia establece el derecho de los sujetos objeto de grabación a obtener la información, el acceso y, en su caso, la cancelación de las imágenes obtenidas (art.9.2º).

Ya se ha hecho referencia a la distinción entre el tratamiento de datos personales que se realice a partir de las imágenes y sonidos obtenidos y lo que es la estricta utilización de éstos. Así, el primer supuesto se sujeta a los "especialmente previsto, en su caso," por la Ley Orgánica 15/1999, independientemente de que el tratamiento sea manual o automatizado. En el segundo de ellos, se aplican las disposiciones establecidas en materia de videovigilancia, tanto en la Ley como en el Reglamento.

El Reglamento dedica su Capítulo V a los "Derechos de los ciudadanos", pero sus disposiciones no facilitan el ejercicio de los derechos de los afectados sino todo lo contrario. Se establecen requisitos que dificultan su ejercicio, tal como sucede con el art.23.1º que declara que "Toda persona que considere razonablemente que figura en grabaciones efectuadas con videocámaras, podrá ejercer el derecho de acceso a las mismas, mediante solicitud dirigida a la autoridad encargada de su custodia.

En la solicitud, además de los requisitos generales establecidos en la legislación general del procedimiento administrativo común, deberá constar la identificación del interesado mediante fotografías, preferentemente de cuerpo entero, y en todo caso de la cara, así como el día, hora y lugar en que presumiblemente fue grabada su imagen".

Por tanto, cuando se quiere acceder a las imágenes grabadas hay que dirigirse a las autoridades (art.17 Reglamento), después de considerar razonablemente que se figura en las grabaciones efectuadas con videocámaras y tras indicar el día, hora y lugar en que presumiblemente fue grabada la imagen.

El derecho de acceso se concreta en el art.23.4º que señala que "Sin perjuicio de cualquier otro sistema de consulta, el sistema ordinario de acceso a las grabaciones será la visualización en pantalla". No obstante, la realidad parece aconsejar la utilización de cualquier otro sistema de consulta que resulte apropiado para satisfacer este derecho de acceso a las imágenes grabadas, con lo que satisfaría el derecho de elección del soporte en el que desee acceder a la grabación.

El derecho a la información no se explicita en el Reglamento, pero su art.21.1º establece que "La información al público de la existencia de instalaciones fijas de videocámaras será responsabilidad de la autoridad que haya otorgado la autorización, y deberá ser efectiva desde el mismo momento en que se proceda a la utilización de las mismas, debiendo mantenerse actualizada de forma permanente.

Dicha información, que no especificará el emplazamiento concreto de las instalaciones fijas de videocámaras deberá contener en todo caso una descripción genérica de la zona de vigilancia y de las autoridades responsables de la autorización y custodia de las grabaciones".

Así pues, el ciudadano conoce la existencia de videocámaras y la autoridad pública ante la que puede ejercer su derecho de acceso. El art.22 concreta que "Para informar al público de la existencia de instalaciones fijas de videocámaras se utilizará una placa informativa, en la cual figurará el pictograma de una cámara de vídeo, y un panel complementario con el contenido especificado en el artículo anterior.

El diseño y formato de la placa informativa y el del panel complementario se ajustará a lo establecido en el Anexo al presente Reglamento.

Cuando por razones debidamente justificadas no puedan emplearse los medios descritos en los apartados anteriores, se utilizarán cualesquiera otros instrumentos de información para garantizar la efectividad de lo previsto en el apartado primero del artículo noveno de la Ley Orgánica 4/1997"[21].

Evidentemente, para la protección de los datos personales y, en definitiva, de los derechos fundamentales de los ciudadanos afectados, las imágenes y sonidos grabados no se pueden conservar indefinidamente, así como tampoco se pueden conservar cuando se hayan obtenido de forma incorrecta o ilícita.

El art.8 de la Ley de Videovigilancia establece que el plazo máximo de conservación de las grabaciones es de un mes y, una vez transcurrido, se destruirán, 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".

La cesión o copia de las grabaciones están prohibidas, 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". En este caso, se pondrán a disposición judicial "con la mayor inmediatez posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación", comunicándose "verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación" cuando no pueda redactarse el atestado en tal plazo. Si se constata la comisión de una infracción administrativa "se

21 MARTÍNEZ MARTÍNEZ, R.: *Tecnologías de la información, policía y Constitución,* pág.382, considera que "No sería en absoluto descabellada la realización de campañas públicas de información ciudadana por las autoridades policiales nacionales, autonómicas o municipales que indicasen al ciudadano la decisión de instalar videocámaras, los espacios a los que afecta y los datos de la autoridad responsable de las grabaciones en los términos en que la LOPD regula el derecho de información en la recogida de datos".

remitirán al órgano competente, igualmente de inmediato, para el inicio del oportuno procedimiento sancionador".

Sobre la destrucción y cancelación de imágenes, el Reglamento establece en su art.18 que "Las grabaciones deberán ser destruidas por la autoridad que tenga encomendada su custodia material conforme a lo previsto en el artículo anterior, en el plazo máximo de un mes a contar desde el mismo día de su captación [...].

La destrucción podrá hacerse efectiva por cualquier modalidad que permita el borrado o inutilización de las grabaciones, o de las imágenes y sonidos concretos que deban ser cancelados".

Las excepciones al ejercicio de este derecho se concretan en aquellos casos en los que las grabaciones desvelen la comisión de un ilícito o cuando se haya interpuesto algún recurso administrativo o jurisdiccional.

Cuando se trate de grabaciones ilegales, el art.20 establece el deber del responsable de custodiar las grabaciones de destruir inmediatamente las imágenes y sonidos así obtenidos. Si no se respetaron los principios que rigen la utilización de las videocámaras móviles, o se grabó sin el consentimiento del titular o autorización judicial imágenes o sonidos del interior de las viviendas o de sus vestíbulos, o las registradas en lugares públicos, abiertos o cerrados, cuando se afecte de forma directa y grave la intimidad de las personas, y cuando se hayan grabado conversaciones privadas, se deben destruir las grabaciones.

El art.24 regula el régimen de cancelación de grabaciones cuando, tras ejercer su derecho de acceso a lo grabado, el interesado considera que las imágenes y sonidos no se ajustan a lo previsto en la LOV. En este caso podrá solicitar a la autoridad de custodia la cancelación o podrá ésta acordarla de oficio.

Además de la cancelación de las grabaciones el Reglamento contempla la posibilidad de bloquear las imágenes y sonidos, lo que supondrá su cancelación parcial (art.25). Se trata de casos en los que ésta es procedente y no sea posible o conveniente su destrucción total, por razones técnicas o por causa del procedimiento o soporte utilizado. A través de este bloqueo parcial se consigue impedir su ulterior utilización sin que se suprima o borren las demás imágenes o sonidos.

B. La Ley Orgánica de Protección de Datos (LOPD)

La Ley establece dos tipos de ficheros de datos de carácter personal mantenidos por las Fuerzas y Cuerpos de Seguridad en atención al fin para el que éstos han sido recogidos. Así, existen los ficheros con fines administrativos sujetos al régimen general establecido en esta Ley Orgánica y los ficheros con fines policiales que presentan mayores problemas.

Estos ficheros al ser de naturaleza pública quedan sujetos a los requisitos contenidos en el art.20 de esta Ley Orgánica 15/1999. Éstos se refieren a la creación, modificación o supresión de los ficheros de las Administraciones Públicas, que sólo se podrá hacer por disposición general publicada en el BOE o diario oficial correspondiente. Las disposiciones de creación o de modificación han de indicar la finalidad del fichero y los usos previstos para el mismo; las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrar; el procedimiento de recogida de los datos; la estructura básica del fichero y la descripción de los tipos de datos de carácter personal que en él se incluyen; las cesiones de datos y, en su caso, las transferencias que se prevean a terceros países; los órganos de las Administraciones responsables del fichero; los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición; las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

De entre los requisitos señalados destacamos en relación con la disposición de creación del fichero policial, dada su especial naturaleza, la determinación de "las medidas de seguridad con indicación del nivel básico, medio o alto exigible"[22]. En este sentido, el art.4.2º del Reglamento señala que "Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales" deberán tener nivel medio y según su apartado 3º "Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual, así como los que contengan datos recabados para fines policiales sin consentimiento de las personas" deberán reunir un nivel de seguridad alto.

El art.22 LOPD señala en su párrafo 1º que "Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley".

Sin embargo, en el párrafo 2º se prevé "La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad".

En el art.7 párrafos 2º y 3º se establecen como datos especialmente protegidos los de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, que sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento, y, junto a estos, los de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, los que sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. En relación a estos datos personales el párrafo 3º del art.22 declara que su recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad se podrá realizar exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad (art.22.4º).

El régimen especial al que se someten estos datos se comprueba cuando se ejercitan los derechos de acceso, rectificación y cancelación, tal como regula el art.23 de la LOPD. En este sentido, el párrafo 1º señala que "Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando".

22 Sobre las medidas de seguridad Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

"El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación".

En el art.24 se contienen otras excepciones a los derechos de los afectados, pues dispone que "Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas".

Por tanto, el derecho a la información en la recogida de datos no será aplicable cuando se den las circunstancias mencionadas, es decir, poner en peligro una serie de investigaciones.

IV. ÁMBITOS PROCLIVES A LA VIDEOVIGILANCIA

Como ejemplo de lugares públicos vigilados a través de los sistemas de videovigilancia señalaremos como el Ayuntamiento de A Coruña está estudiando la ampliación de sus dispositivos de control –ojos electrónicos- a fin de prevenir, perseguir y castigar el vandalismo, la pequeña delincuencia y controlar el tráfico rodado. Estos tres ámbitos son competencia de la Concejalía de Seguridad Ciudadana que ha decidido invertir más dinero en cámaras que permiten que las imágenes viajen en tiempo real a través de la fibra óptica.

En espacios privados nos encontramos con la utilización de las técnicas de vigilancia por videocámaras con el objetivo de controlar la calidad y cantidad de las actividades laborales, con lo que se producen tratamientos de datos personales. Por tanto, estamos de nuevo ante la protección de los derechos y libertades de las personas en el contexto laboral.

El objetivo no es otro que, cuando sea lícita su utilización, ésta se haga con sujeción a las garantías adecuadas. Así, además del respeto a lo establecido en la legislación sobre la protección de datos, es necesario respetar los acuerdos colectivos que se firman con los trabajadores o los sindicatos, representantes de los intereses de éstos, que deberán hacer constar la existencia y ubicación de estos sistemas de control o vigilancia de los empleados cumpliendo así con el derecho de información de los afectados y la obligación de información de los responsables.

En todo caso, la vigilancia no debe recaer sobre lugares reservados al uso privado de los empleados, es decir, que no se destinen a la realización del trabajo exclusivamente (zona de descanso, baños, etc). Por tanto, estos sistemas de vigilancia se destinarán a la protección de la propiedad o para detectar infracciones.