Videovigilancia: *ojos* para el control

Estado de la cuestión

PID_00268226

Francesc Guillén Lasierra

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Francesc Guillén Lasierra

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por la profesora: Mònica Vilasau Solana (2019)

Primera edición: septiembre 2019

Avda. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

1. Origen y causas del uso de la videovigilancia

Nuestras sociedades han evolucionado en una dirección que, entre otras cosas, ha **disminuido los tradicionales controles sociales informales**. La enorme movilidad de las personas, la gran diversidad que esto comporta, el debilitamiento de la influencia de la religión y un énfasis muy grande en los derechos individuales han facilitado que las personas tengan una relación menos intensa con su entorno y, en todo caso, no creen que tengan que incidir en las conductas de terceros.

Paralelamente, la criminología ha ido remarcando cada vez más la importancia de la concurrencia de tres factores en la comisión de un delito: un **objeto atractivo**, un **delincuente motivado** y la **ausencia de un guardián** eficaz (Cohen y Felson, 1979). Este posicionamiento bastante mayoritario de la criminología ha venido a dar fuerza a la idea de que es importante que haya alguien que tenga ojos en los lugares más problemáticos para que no se produzcan delitos, por miedo a que sea frustrado el intento o a ser reconocido y poder ser posteriormente identificado con las consecuencias policiales y penales correspondientes.

Este escenario ha coincidido en la segunda mitad del siglo XX con un incremento sostenido de la delincuencia hasta los años noventa, y, posteriormente, una presencia creciente de los comportamientos incívicos o antisociales, asociados a una creciente sensación de inseguridad (seguridad subjetiva baja, Guillén, 2012) y la aparición de la amenaza permanente y generalizada del terrorismo global. Las innovaciones tecnológicas que se suceden con mucha rapidez en la misma época han facilitado que, por un lado, se pensara en el hecho de sustituir la falta de vigilancia humana por vigilancia artificial o tecnológica, y, por otro lado, la industria que produce las herramientas para vigilar también ha promovido esta necesidad para dar salida a sus productos cada vez más sofisticados.

Así, el nacimiento y el desarrollo de la **videovigilancia** ha sido un **elemento omnipresente** en la vida de nuestras ciudades en los últimos años. Algunos (Clarke y Cornish, 2003) ya la consideran una **técnica formal de vigilancia para la prevención del delito**.

Se considera que, teóricamente, la videovigilancia tiene que producir beneficios en varios ámbitos:

1) Reducción del miedo al delito y del sentimiento de inseguridad en general. Este beneficio puede comportar un efecto multiplicador, puesto que si las personas, teóricamente, se sienten más seguras por la presencia de videocámaras, frecuentan más los espacios públicos y aumentan los niveles de control social informal con su presencia.

2) Efecto disuasivo para hipotéticos infractores. La posibilidad de que sus acciones queden grabadas y les puedan comportar consecuencias negativas.

3) Apoyo a las investigaciones policiales. Muy ligadas al punto anterior, las filmaciones pueden ayudar a la policía a identificar a los autores de una infracción y probar su participación en esta.

Ejemplos de apoyo a las investigaciones policiales

Gracias a la videovigilancia se facilitaron las detenciones, muy difundidas por los medios de comunicación, de los asesinos de James Bulger en Liverpool en 1993, del terrorista de Brixton en 1999, también la identificación de los terroristas que llevaron a cabo los atentados del 7 de julio de 2005 en Londres y del asesino de Vanessa Russo en abril de 2006 en Roma.

4) Vigilancia de los servicios de información e inteligencia. Las cámaras pueden ser utilizadas para controlar el comportamiento de delincuentes conocidos en espacios públicos (como, por ejemplo, los traficantes de drogas o delincuentes especialmente peligrosos). Los operadores de las cámaras a menudo conocen los rostros de los delincuentes locales y con las cámaras pueden controlar sus movimientos de forma menos invasiva que con agentes encubiertos (Silverman, 2001).

Las primeras noticias de utilización de cámaras de videovigilancia en Europa parece que se sitúan en la década de 1950, cuando algunos países europeos recurrieron a esta tecnología para controlar el tráfico (Varona, 2012). En el mismo periodo se empezó a usar de forma gradual esta tecnología para controlar la seguridad en bancos y establecimientos comerciales. Sin embargo, no fue hasta los años sesenta que las videocámaras aparecieron en el ámbito urbano. Los primeros países que instalaron sistemas de videovigilancia en sus ciudades (bajo el impulso de las autoridades locales) fueron los Estados Unidos de América y el Reino Unido. La principal función de estos instrumentos era el control de las manifestaciones y desórdenes en espacios públicos. Los altos niveles de urbanización y de consumismo del resto de países del mundo occidental hicieron que estas experiencias se fueran extendiendo (Goold, 2004). En este contexto de crecimiento urbano, económico y demográfico los circuitos de videovigilancia se usaban principalmente para vigilar la propiedad privada, el transporte público, las infraestructuras públicas (como escuelas y hospitales), los acontecimientos masivos y los hurtos (ICPC, 2009).

Francia, España e Italia empezaron a aplicar estas tecnologías a finales de los ochenta y comienzos de los noventa, tanto para la gestión del tráfico, de acontecimientos y grandes concentraciones de personas como para el control de la criminalidad.

2. Desarrollo del uso de la videovigilancia

Ha habido algunos factores que han contribuido a la generalización de la videovigilancia como elemento incluso central en algunos casos de las políticas de seguridad.

En primer lugar, ha habido gobiernos estatales y regionales que han ofrecido una **financiación generosa** para los municipios que decidieran la instalación de circuitos de videovigilancia (CCTV, según las siglas en inglés) para mantener la seguridad, prevenir el delito y calmar a los vecinos. Ante la complejidad de la seguridad, las videocámaras se presentaban como **un instrumento simple**, que disfrutaba **de aprobación popular** y no costaba nada (o poco) a las arcas municipales, debido a los fondos de financiación ofrecidos. En los gobiernos estatales les resultaba una forma fácil (eran tiempos de bonanza económica) de mostrar preocupación por la seguridad de los ciudadanos.

El uso que se hizo en los atentados de Londres de 2005, en que a partir de las videocámaras instaladas en las estaciones de los transportes públicos se consiguió identificar a los autores, hizo que la videovigilancia se considerara un buen instrumento para la prevención y la represión del terrorismo, circunstancia que favoreció todavía más su expansión. Además, la instalación de cámaras es vista por el público como una señal que **el gobierno se preocupa por la protección** de los ciudadanos.

Obviamente, cuando un ayuntamiento o cualquier otra institución instalaba la videovigilancia, los municipios vecinos u otras instituciones no querían ser menos y se incorporaban también a la tendencia vigilantista.

Ejemplos de la instalación de cámaras

En Italia, autoridades regionales, como las de Lombardía, Véneto, Piamonte, Emilia-Romaña, Liguria, Las Marcas, Toscana, Molise, Campania, Lacio y Umbría, desempeñaron un gran papel a la hora de promover los CCTV e invirtieron más de **200 millones de euros** para subvencionar a los municipios que los instalaban en un periodo aproximado de quince años. Actualmente, todos los municipios con más de 20.000 habitantes disponen de circuitos de videovigilancia.

En el Reino Unido, en 2013 ya había más de **cuatro millones de videocámaras**, según datos de la misma industria del sector (British, Security Industry Association). La financiación de los CCTV no recayó normalmente sobre la policía o los negocios locales, puesto que las autoridades se encargaron de ello mayoritariamente. Entre 1994 y 1998 llegó la financiación del gobierno bajo la forma de las *CCTV Challenge Competitions*, que aportaron 38,5 millones de libras para 585 sistemas en todo el país. Entre 1999 y 2003, en el marco del programa para la reducción del delito, el Gobierno puso a disposición de las autoridades **170 millones de libras**, que facilitaron la instalación de 680 sistemas de videovigilancia.

En Alemania, la demanda de un uso superior de la videovigilancia pública ha aumentado con el incremento de la amenaza terrorista. No solo los sindicatos policiales, sino también los políticos, el ministro federal del Interior y la Conferencia de ministros estatales del interior se han mostrado varias veces más favorables al uso de esta tecnología. Las estaciones ferroviarias han sido un lugar preferente donde la policía instala cámaras de

videovigilancia, y se ha superado la cifra de tres mil cámaras de videovigilancia en todo el país. Encuestas recientes muestran una tolerancia mayor de la población hacia la videovigilancia.

En Francia en 2007 había 396.000 cámaras autorizadas, de las cuales unas 20.000 en espacios públicos (Efus, 2010). Con el apoyo del Gobierno, en especial con la aprobación de la Ley del 5 de marzo de 2007, las cámaras se multiplicaron por todas partes. Entre 2007 y 2012 el Gobierno financió a **2.335 municipios** con un total de **133,6 millones de euros** (2.500 proyectos de autoridades municipales que comportaron la instalación de 21.742 cámaras). El Gobierno pensaba que la videovigilancia era una forma importante de luchar contra el terrorismo (Klauser, 2009).

En España, la policía local empezó a usar cámaras de videovigilancia en ciertos lugares en días específicos y durante grandes acontecimientos en la década de los noventa (Varona, 2012). El incremento de la delincuencia y el incivismo al finales del siglo XX y comienzos del XXI sirvieron como argumento para extender la videovigilancia. Los atentados de Madrid de 2014 también significaron un gran impulso para la instalación de CCTV en todo el país. Desde entonces, su presencia en fronteras, puertos, aeropuertos, estaciones, carreteras, transportes públicos y centros comerciales ha aumentado notablemente. No hay datos sobre la cantidad de cámaras de vídeo controladas por la policía a nivel global. En Cataluña hay actualmente 169 municipios con sistemas de videovigilancia (DGAS, 2019). En la red del transporte metropolitano de Barcelona hay más de siete mil cámaras (incluidas las instaladas en trenes, autobuses y estaciones).

En segundo lugar, las empresas privadas han recurrido también de forma intensa a la videovigilancia para proteger sus actividades e instalaciones, muy especialmente bancos, comercios y áreas comerciales, y también naves y áreas industriales.

Un desarrollo no de menor importancia ha sido el uso de la videovigilancia para vigilar la buena marcha de grandes acontecimientos deportivos, muy especialmente las competiciones futbolísticas del máximo nivel. Después de incidentes desgraciados como los de Heysel o Sheffield, la instalación de videocámaras en los estadios y sus alrededores se convirtió en una necesidad ineludible para detectar y erradicar los comportamientos violentos. Los estadios se han llenado con miles de cámaras de gran precisión que son capaces de individualizar el rostro de los espectadores incluso en recintos con casi 100.000 espectadores.

3. Privacidad y videocámaras

El uso de la videovigilancia que tanto se ha generalizado y que despierta tanto entusiasmo en todos los ámbitos, no es, sin embargo, inofensivo para los derechos de los ciudadanos que puedan ser afectados por las filmaciones llevadas a cabo por los aparatos. Es bastante evidente que hay derechos como la **intimidad**, el derecho a la **propia imagen** y, en algunos supuestos, el **derecho al honor** que pueden ser afectados, puesto que las videocámaras se apropian (o pueden hacerlo) de esferas de intimidad que solo pertenecen a su titular, con afectaciones al derecho a la propia imagen y, eventualmente, al derecho al honor. Además, el hecho que, como veremos, las grabaciones constituyan datos personales hace que también haya que aplicar las garantías inherentes en este caso. Hay derechos que pueden ser también limitados de forma indirecta, como por ejemplo el derecho de manifestación, de huelga (*vid*. en el caso de España, la STC, 37/1998, de 7 de febrero, mencionada más adelante), o incluso la libertad de expresión, de religión o de pensamiento.

El hecho que las grabaciones se lleven a cabo en espacios públicos no significa que no se pueda vulnerar el derecho a la intimidad de los ciudadanos. Así, cuando estamos **en espacios públicos** también podemos tener una **expectativa razonable de privacidad**, en que aceptamos que nos vean los que están presentes, pero no aquellos que se encuentran a distancia (Guillén, 1997). Si tenemos en cuenta que las grabaciones pueden incluir audio, significa que las conversaciones privadas pueden quedar al alcance de terceras personas, que a pesar de estar en espacios públicos pueden esperar razonablemente que alguien que no esté cerca no tenga acceso a ellas (Guillén, 1997).

Finalmente, hay que tener presente que las grabaciones que son resultado del funcionamiento de las videocámaras tienen, por sus características, la calificación de ***datos personales***, con lo cual le son aplicables todas las garantías propias de la protección de este tipo de datos.

Es cierto que hay mucha gente que no piensa que estas limitaciones de la privacidad que puede provocar el uso de videocámaras pueda tener una incidencia relevante en sus vidas. Es más, hay muchos ciudadanos que no ven ningún inconveniente en su uso. Para combatir esta falsa idea y evitar una difusión incontrolada del uso de la videovigilancia, no solo se han aprobado regulaciones que establecen requerimientos para su utilización, como veremos en los dos apartados siguientes, sino que varias instituciones han aprobado normas y guías que permitan hacer un uso razonable de ella. Hay que destacar en particular la guía/carta elaborada por el Foro Europeo para la Seguridad Urbana para asesorar a sus miembros sobre su uso.

Foro Europeo para la Seguridad Urbana

El Foro Europeo para la Seguridad Urbana (EFUS) es una asociación de colectividades locales y regionales creada en 1987 en Barcelona para promover políticas de seguridad urbana integrales y compartir buenas prácticas. Actualmente forman parte del Foro más de 250 instituciones locales y regionales. Podemos afirmar sin temor a equivocarnos que es la institución más influyente en el ámbito de la seguridad urbana en Europa.

La *Carta para el uso democrático de la vigilancia por vídeo* establece unos principios necesarios para el buen de uso de esta herramienta de vigilancia:

- **Legalidad**. La instalación de cámaras debe hacerse en el marco de la ley, es decir, cuando la ley lo permita (incluye la normativa europea aplicable).

- **Necesidad**. Debe existir una realidad que requiera una reacción de los poderes públicos y la videovigilancia debe ser una respuesta adecuada, que puede satisfacer la necesidad en cuestión.

- **Proporcionalidad**. El problema que se quiere resolver no tiene que ser abordable por otros medios menos intrusivos.

- **Transparencia**. El público tiene que conocer la existencia de los sistemas de videovigilancia, y también el funcionamiento y los resultados.

- **Responsabilidad**. Las autoridades que se encargan de la instalación se hacen responsables de su uso adecuado.

- **Supervisión independiente**. Hay que establecer mecanismos de control del funcionamiento de los sistemas que no sean dependientes de las autoridades que los establezcan.

- **Participación de los ciudadanos**. Las opiniones de los ciudadanos tendrían que ser tenidas en cuenta tanto de cara a decidir los lugares donde las cámaras son necesarias como a evaluar la eficacia de los mecanismos instalados.

4. Regulación y control de la videovigilancia

Como acabamos de decir, hay que someter el uso de la videovigilancia al cumplimiento de requerimientos que puedan garantizar su funcionamiento adecuado, y a una supervisión y control que constaten que su buen funcionamiento es una realidad. De una forma u otra todos los ordenamientos jurídicos han entendido esta necesidad y han intentado aplicar sus principios constitucionales al funcionamiento de los CCTV. Ahora bien, no todos lo han hecho del mismo modo.

4.1. Tendencias en la regulación de la videovigilancia

Seguramente, debido a las especialidades de todos los ordenamientos jurídicos sería muy difícil encontrar dos regulaciones idénticas en el ámbito de la videovigilancia o en ningún otro. De todos modos, sí podemos ver varias tendencias que tienen características comunes. En nuestro contexto, hay básicamente dos respuestas jurídicas a la presencia y el uso de las videocámaras.

En primer lugar, una línea que **no es partidaria de aprobar una normativa específica al tema** y que plantea aplicar los **principios y valores del ordenamiento existentes en varias normas constitucionales o legales** (derecho a la privacidad, protección de datos personales) al uso de las videocámaras. En estos casos el control más cercano lo llevan a cabo las autoridades encargadas de la protección de datos personales, puesto que, como se ha mencionado antes, las grabaciones constituyen datos de carácter personal. Incluso la Unión Europea ha seguido este patrón y la autoridad de protección de datos (European Data Protection Supervisor) aprobó en 2010 unas instrucciones para el uso de las videocámaras que intentan garantizar la protección de los datos personales derivadas de las filmaciones. De hecho, anteriormente ya se había emitido el Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, con lo cual las instrucciones del supervisor europeo no hacían sino consolidar la tendencia de controlar el uso de la videovigilancia por medio de la normativa de protección de datos. Posteriormente, el Comité Europeo para la Protección de Datos ha adoptado las Directrices 3/2019, sobre el procesamiento de datos personales a través de instrumentos de filmación.

Ejemplo del Reino Unido

El ejemplo más paradigmático lo constituye el **Reino Unido**, donde incluso fue la autoridad de protección de datos la que elaboró un código de práctica para los operadores de sistemas de videovigilancia en el año 2000. Posteriormente, en 2012, el modelo ha cambiado ligeramente, al crear un comisionado específico para el control de los datos personales obtenidos por medio de las cámaras de la policía. Un sistema similar es el de Italia, donde ante la ausencia de una ley específica que regule la videovigilancia, la autoridad para la protección de datos (*Garante per la protezione dei date personali*) se encarga de garantizar que el uso de la videovigilancia no utilice los datos personales de forma indebida.

Texto normativo de referencia

Consultad las Directrices 3/2019, sobre el procesamiento de datos personales a través de instrumentos de filmación, en el siguiente enlace: https://bit.ly/2LQ2BMK.

En segundo lugar, una línea que es partidaria de regular **explícitamente el uso y control de la videovigilancia**. En estos países, entre los que están España, Francia y Bélgica, se han establecido requerimientos específicos, con leyes *ad hoc* para el establecimiento de sistemas de videovigilancia, a pesar de que también tienen autoridades y regulaciones sobre protección de datos personales que pueden intervenir en casos en que se produzca una violación de los mismos. A menudo, en estos países la regulación afecta de forma primordial a las videocámaras utilizadas por la policía, y las que tienen un uso y una titularidad **privada** acostumbran a estar únicamente bajo el control de las autoridades de protección de datos.

Ejemplos

En **Francia** hay una ley que regula la *videoprotección* (la denominación fue introducida en 2008 para remarcar la función positiva de la herramienta) que prevé un procedimiento de autorización y de uso bastante estricto: **La autorización es necesaria** cuando la videovigilancia se lleva a cabo en **lugares públicos** (calles, plazas, carreteras, vías de agua) o en **establecimientos abiertos al público** (sobre este concepto existe jurisprudencia que precisa ese término) a cargo de la policía o de entidades privadas. La autoridad competente para dar el visto bueno es:

1) Si se trata de hacer un fichero a efectos de identificación de personas, la CNIL (Commission Nationale de la Informatique et des Libertés), la autoridad competente.

2) En el resto de casos es el **prefecto** (máxima autoridad gubernamental del departamento).

El uso privado (que no afecta a espacios o establecimientos públicos) de la videovigilancia no necesita autorización.

Hay casos en que son los mismos prefectos quienes pueden establecer la videovigilancia como obligatoria en transportes públicos, aeropuertos, instalaciones con riesgo específico (nucleares, eléctricas, depósitos de agua, etc.). También hay ciertas actividades que están obligadas al uso de la videovigilancia, como los casinos o los que se dedican a transportar dinero.

El procedimiento de autorización comprueba que la instalación de los circuitos de videovigilancia no afecte a la intimidad de la persona (prohibición de intromisión en espacios privados).

Debe haber siempre una persona responsable del sistema de videovigilancia, todas las personas que trabajan allí deben tener formación específica y el resto de personas no pueden tener acceso, excepto en los casos previstos por la ley (por ejemplo, investigación de infracciones).

Hay una comisión nacional de videoprotección (en el marco del Ministerio del Interior) y también comisiones en el ámbito departamental o municipal, pero no tienen una influencia directa en el proceso de autorización como en el caso catalán. Hacen informes generales de situación o se interesan por problemáticas concretas. Es decir, son órganos con un carácter predominantemente consultivo.

En **Alemania** y en **Austria** hay una **combinación de legislación de protección de datos y de legislación sobre policía aplicables a la materia**. En Alemania, las leyes de los *Länder* (comunidades autónomas) son las que han acabado regulando su uso policial, después de que en un primer momento solo se trataran como datos personales. De todos modos, la regulación que hacen muchas de estas leyes[1] de policía hace referencia sobre todo a su tratamiento de datos personales. El procedimiento de autorización es interno.

(1)Por ejemplo, ved el artículo 15 de la Ley de Policía de Renania del Norte-Westfalia o el 32 de la Ley de Policía de Baviera

Obviamente, esta regulación no es aplicable a la seguridad privada, pero hay que entender que también debe respetar las normas de tratamiento de datos personales. Ahora bien, algunas instalaciones donde se llevan a cabo actividades comerciales, industriales, culturales o deportivas están obligadas a instalar circuitos de videovigilancia.

En **Austria** recientemente se ha **regulado la videovigilancia privada** pero lo ha hecho la ley de protección de datos.

4.2. Regulación de España

España se encuentra entre los países con legislación específica. La videovigilancia está regulada por la Ley 4/1997, de 4 de agosto, por la cual se regula la **utilización de videocámaras por las fuerzas y los cuerpos de seguridad en lugares públicos**. En consecuencia, como en los demás países, la regulación afecta solo a la policía y todavía no se ha producido el desarrollo reglamentario que aplique los principios de esta ley al uso privado de la videovigilancia.

Se anunció a los medios de comunicación que la nueva Ley 5/2014, de 4 de abril, de seguridad privada, regularía el uso de la videovigilancia de las empresas de seguridad y el artículo 42 contiene algunos mandatos que hay que respetar en estos casos. No hay, sin embargo, regulación para el uso privado que sea llevada a cabo por particulares diferentes a las empresas de seguridad reguladas por la ley en cuestión.

Posteriormente se aprobaron reglamentos de desarrollo de la ley, tanto a escala estatal[2] como autonómica[3] (al ser una competencia compartida en los casos de comunidades autónomas con competencia sobre seguridad ciudadana), pero los reglamentos solo regulan los procedimientos y los requisitos concretos para la instalación y el uso de videocámaras de la policía.

(2)Real decreto 596/1999, de 16 de abril, por el cual se aprueba el Reglamento de desarrollo y ejecución de la LO 4/1997, de 4 de agosto, de uso de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos.

(3)Decreto 134/1999, de 18 de mayo, de regulación de la videovigilancia por la policía de la Generalitat y las policías locales de Cataluña.

De todos modos, todo este procedimiento tiene que respetar, en todos los casos, también las previsiones del nuevo **artículo 22 de la Ley orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales**, que prevé las cautelas que hay que tomar para que las grabaciones no violen las garantías establecidas para los datos de carácter personal.

El ámbito de aplicación de la ley (art. 1) de la Ley 4/1997, que comentamos, es la utilización de videocámaras por **cuerpos policiales** en **lugares públicos** (abiertos o cercados) con el fin de:

- Asegurar la convivencia.
- Erradicar la violencia.
- Utilizar pacíficamente las vías y espacios públicos, o Prevenir
- la comisión de delitos e infracciones relacionadas con la seguridad pública.

Se pueden grabar tanto imágenes como sonidos. En el supuesto de que se graben sonidos e imágenes debe hacerse de forma conjunta, en un mismo soporte. Su uso debe ser proporcional (art. 6.1 de la misma ley) en el sentido que:

- Su uso sea **idóneo** para el objetivo perseguido.
- No sea posible lograr el mismo objetivo con una restricción inferior de derechos (**subsidiariedad** o intervención mínima).
- Sea una medida **limitada** en el tiempo.

Ejemplo del análisis de la proporcionalidad

Una exposición muy clara del significado de la proporcionalidad la encontramos, entre otras, en la STC 186/2000, de 10 de julio, FJ 7), en que el Tribunal avala la instalación de una cámara que enfocaba las manos de una cajera de un supermercado sobre la que había sospechas de apropiación indebida de dinero de la empresa. Previamente, los res-

ponsables de la empresa habían utilizado otras medidas para descubrirla sin resultado, puesto que las cuentas seguían sin cuadrar cada vez que trabajaba la persona en cuestión. Cuando se descubrió por medio de las imágenes que, efectivamente, la señora *distraía* algunos importes a su bolsa, se dieron por acabadas las filmaciones. También en una sentencia anterior, la STC 37/1998, de 7 de febrero, el Tribunal Constitucional había hecho una muy buena explicación de lo que hay que entender como proporcionalidad. El Alto Tribunal consideró **desproporcionado el uso de videocámaras por la Policía del País Vasco (Ertzaintza)** para controlar la acción de unos piquetes en un polígono industrial conflictivo en una jornada de huelga general. El Tribunal no aceptó el uso de las cámaras, basándose en el hecho de que los líderes sindicales que habían pedido que no se llevaran a cabo las filmaciones habían facilitado sus documentos de identidad para que la policía los pudiera responsabilizar si se producía algún incidente. El hecho de que los líderes sindicales aceptaran la responsabilidad de mantener la actuación de los piquetes dentro de la razonabilidad hacía innecesario, a los ojos del Tribunal, el uso de la videovigilancia por la policía, uso que, por otro lado, **podía cohibir tanto a los piquetes como a los trabajadores** que se dirigían a las fábricas.

En la misma dirección, la Agencia Española de Protección de Datos sancionó a El Corte Inglés por la grabación indiscriminada e ilimitada de las cámaras instaladas en su establecimiento en Málaga (según publicó Iustel el 26 de mayo de 2011).

El objetivo de la instalación de videovigilancia tiene que ser uno de los que se mencionan a continuación (art. 4):

- Asegurar la protección de edificios e instalaciones públicas y de sus accesos (a pesar de que quedan exceptuadas de la aplicación de la ley las cámaras de videovigilancia instaladas en los edificios policiales para garantizar la seguridad).
- Salvaguardar las instalaciones útiles para la defensa nacional.
- Constatar infracciones a la seguridad ciudadana.
- Prevenir la causación de daños a las personas y bienes.

La ley también excluye de su aplicación directa las cámaras utilizadas para el control de la seguridad del tráfico (Disposición adicional octava) y remite a la legislación específica sobre tráfico y protección de datos.

En Cataluña se tomó la decisión de someter todas las videocámaras operadas por la policía al control de la Comisión de videovigilancia[4].Una gran novedad en el uso de la videovigilancia en Cataluña (siguiendo en este caso el ejemplo del País Vasco) fue **la instalación de cámaras** en las zonas/**celdas** en que los policías interactúan con los detenidos (Guillén, 2018). La medida, muy impopular entre los sindicatos policiales, se hizo para parar un número apreciable de denuncias por maltrato interpuestas por los detenidos, que los policías calificaban como falsas y sin fundamento. Desde la instalación de las cámaras las denuncias se redujeron prácticamente a cero y hoy nadie se posiciona contra su existencia. En el País Vasco había pasado exactamente lo mismo con la peculiaridad de que aquellos que denunciaban los maltratos eran las personas detenidas por actividades relacionadas con el terrorismo o la lucha en la calle. El éxito de estas experiencias hizo que en 2015 las autoridades del Ministerio del Interior español declararan públicamente la intención de instalarlas en las celdas de la Guardia Civil y la Policía Nacional (Guillén, 2016). No consta, sin embargo, que estas intenciones se hayan traducido en hechos.

(4)Decreto 78/2010, de 22 de junio, sobre la instalación de dispositivos de videovigilancia a las dependencias policiales de la Generalitat.

Los lugares que son objeto de la vigilancia por medio de las cámaras tienen que ser espacios públicos (abiertos o cercados) y quedan expresamente **excluidos** los supuestos siguientes (arte. 6.5):

- **Interior de casa o vivienda**. Excepto supuestos previstos en el artículo 18.2 de la Constitución –consentimiento del titular o autorización judicial.
- **Vestíbulos**.
- Grabación de **conversaciones privadas**.

- **La afectación directa y grave de la intimidad**. Hay que imaginar, por ejemplo, que se daría este supuesto en caso de instalación en unos urinarios públicos, como había señalado el Tribunal Supremo en sentencia de 19 de abril de 1996, FJ5.

El Tribunal Constitucional ha manifestado la existencia de conversaciones privadas en el puesto de trabajo durante la jornada laboral y declaró contrario a la Constitución y, por lo tanto, sin cobertura legal, la grabación de todas las conversaciones de los trabajadores de las cajas de un casino para comprobar si los intercambios de dinero por fichas que hay que utilizar en el casino se llevaban a cabo de forma correcta. El Tribunal lo consideró una intromisión ilegítima en la privacidad de los trabajadores (STC 98/2000, de 10 de abril, FJ 6 y 7). El STC 12/2012, de 30 de enero, reiteró la existencia de espacios de privacidad durante el ejercicio profesional y declaró contraria a derecho la obtención y difusión de una determinada información con una cámara camuflada en la consulta de un terapeuta. El contenido de esta jurisprudencia ha sido recogida en el actual artículo 89 de la Ley orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales que regula los principios que hay que seguir tanto en las grabaciones de imágenes como de sonidos en los puestos de trabajo durante la jornada laboral.

Los instrumentos que la ley permite utilizar son: videocámaras fijas o móviles y cualquier otra herramienta o medio que permita las filmaciones previstas en la Ley. Hay dos procedimientos diferenciados en función de si se trata de cámaras fijas o móviles.

1) Videocámaras fijas. Es necesario en todo caso la existencia de un riesgo razonable para la seguridad que habrá que acreditar en el procedimiento.

- **Fuerzas y cuerpos de seguridad del Estado** (y policías locales en comunidades sin competencia en materia de seguridad): las autoriza el delegado del Gobierno, después de un informe de una comisión presidida por el presidente del Tribunal Superior de Justicia, en el que la administración que autoriza no puede tener mayoría, y tienen que estar representados los municipios.

- **Policías autonómicas** (y policías locales en comunidades autónomas con competencias): las autoriza la autoridad autonómica correspondiente (en el caso de Cataluña, la persona titular de la Dirección general de Administración de Seguridad), después de informe **de una comisión** presidida por el presidente del Tribunal Superior de Justicia (en el caso de Cataluña también forma parte el fiscal jefe) en que la administración que autoriza no puede tener mayoría, y tienen que estar representados los municipios.

La ley exige que el **público** sea **informado de forma visible y permanente** sobre la existencia y el funcionamiento de las videocámaras fijas.

Es importante remarcar, sin embargo, que el Tribunal Constitucional ha matizado que no es necesario que las personas que sean el objetivo particular de la filmación sean advertidas específicamente. El Tribunal estudió un caso en el que se instalaron cámaras para grabar a una persona que trabajaba en la caja de una cadena comercial que era sospechosa de apropiación dineraria de la caja. La instalación de videocámaras se anunció de forma generalizada en el establecimiento, sin advertir a la persona objeto de la vigilancia. Cuando se descubrió que esta persona sustraía de manera ilícita dinero de la caja fue despedida. La persona en cuestión recurrió a los tribunales por falta de notificación personal de las instalaciones de las cámaras, circunstancia que, según ella, invalidaba las pruebas obtenidas. El Tribunal (STC 39/2016, de 3 de marzo) declara suficiente el anuncio

genérico en el establecimiento comercial de la instalación de videocámaras para cumplir con el requisito legal de publicidad.

2) Videocámaras móviles. Hay que acreditar la existencia de un riesgo concreto para la seguridad y diferenciar estos supuestos:

- **Uso en lugares donde ya hay cámaras fijas** (supuesto no previsto en el caso estatal). Las puede autorizar el mando superior de cuerpo en el territorio o el alcalde (en el caso de las policías locales en Cataluña). Hay que informar al órgano competente para la autorización de las fijas y a la Comisión de videovigilancia, establecida por la ley y que acabamos de mencionar, en un plazo máximo de 72 horas.

- **Uso en lugares donde no hay cámaras fijas**. Es necesaria una resolución motivada del órgano competente para la autorización de cámaras fijas y una comunicación a la Comisión de videovigilancia correspondiente en un plazo máximo de 72 horas.

- **Uso en casos de urgencia**. Las autoriza el mando superior del cuerpo policial en el territorio o el alcalde (en el caso de las policías locales en Cataluña). Hay que informar al órgano competente para la autorización de las fijas y a la Comisión de videovigilancia correspondiente en un plazo máximo de 72 horas (los plazos son inferiores en el caso de las FCSE: se informa en 24 horas y se emite un informe motivado en 48 horas). Es decir, se equipara este caso al del uso de cámaras móviles en el que ya existen cámaras fijas.

En todos los casos, las grabaciones tienen que ser eliminadas en el plazo de un mes, excepto en el supuesto de que estén relacionadas con investigaciones de delitos o infracciones graves contra la seguridad pública.

La ley contiene una disposición adicional novena que obliga al Gobierno a elaborar una normativa para el uso de la videovigilancia de las empresas privadas de seguridad en el plazo de un año. Pero, como se ha dicho antes, a estas alturas solo la Ley de seguridad privada del año 2014 ha establecido en un único artículo algunos principios que las empresas de seguridad privada tienen que respetar en el uso de la videovigilancia. La inexistencia de regulación específica para la seguridad privada ha sido parcialmente compensada con la actividad de las agencias de protección de datos (tanto a escala estatal como autonómica) que, al considerarse un dato personal, han hecho algún seguimiento y control de la actividad privada en este ámbito, y han publicado guías de utilización de la videovigilancia que tenían que ser respetadas por la seguridad privada.

La Agencia Española de Protección de Datos publicó ya hace algunos años una guía de videovigilancia que ya adaptaba los principios establecidos en la legislación de protección de datos (y, de alguna manera, también los principios introducidos por la legislación sobre videovigilancia de la policía) al uso de la videovigilancia de la seguridad privada e incluso de los particulares. Hace poco, en 2018, la Agencia adaptó la regulación a la nueva normativa sobre protección de datos y sustituyó la antigua guía por un nuevo documento

titulado ***Protección de datos: Guía sobre el uso de videocámaras para seguridad y otras finalidades***. Por su parte, la Agencia Catalana de Protección de Datos aprobó, en el marco de sus competencias, la instrucción **1/2009**, **de 10 de febrero**, sobre el tratamiento de datos de carácter personal mediante cámaras con finalidad de videovigilancia.

Esta regulación ha sido aplicada de forma irregular en todo el territorio español con intensidades y criterios diferentes, con autoridades y comisiones de videovigilancia muy intervencionistas y estrictas, y otras más pasivas y permisivas. Por otro lado, la realidad tecnológica ha desbordado totalmente los supuestos previstos en el texto. Un caso muy significativo lo constituyen las cámaras instaladas en los vehículos policiales o las que ya se incorporan en los uniformes de algunos cuerpos policiales, especialmente en aquellos casos que implican intervenciones conflictivas, como por ejemplo en el ámbito del orden público. ¿Se trata de cámaras móviles o fijas? ¿Qué requisitos hay que seguir para su aprobación? El caso de las cámaras en los vehículos policiales suscitó un gran debate en la Comisión de videovigilancia de Cataluña, con muchas reticencias para su aprobación. En cambio, en otras comunidades autónomas varias policías locales han anunciado con una gran difusión en los medios la instalación de cámaras en los vehículos policiales y no han trascendido los argumentos utilizados por las comisiones correspondientes para su aplicación (en algún caso, ni siquiera que la comisión correspondiente se haya pronunciado al respecto).

En todo caso, con la cantidad de medios de grabación al alcance de todo el mundo (especialmente en los teléfonos móviles) que existe en la actualidad, es muy posible que la ley requiriera una profunda actualización que, sin dar carta blanca al uso de la videovigilancia, hiciera una regulación razonable y posibilista ante el escenario tecnológico actual. También sería interesante que la legislación se pronunciara sobre las condiciones en que se podrían constituir redes públicas y privadas de videovigilancia que, como veremos en el apartado 6, se plantean cada día más como una necesidad para hacer un uso eficiente de los recursos para una mejor protección de la seguridad del público.

5. Eficacia de la videovigilancia: resultados de la investigación

Uno de los problemas que ha costado más de afrontar ha sido la evaluación de la eficacia de la videovigilancia. Hay una **fe ciega en el público sobre su eficacia**. Sin ninguna base científica, mucha gente tiende a pensar que la videovigilancia es una herramienta muy efectiva para prevenir la delincuencia. En la policía, la situación es la misma, incluso de forma más exagerada, como explicitaba muy bien hace un tiempo un documento de la Police Foundation (citado por Guillén, 2015, 167):

> «A pesar de la falta de una evidencia concreta sobre su eficacia, los escalafones superiores de los servicios de policía apoyan a los circuitos de cámaras de vídeo como una herramienta efectiva en la lucha contra el delito.»

Este tipo de fe indestructible en el instrumento ha dificultado mucho el establecimiento de mecanismos de evaluación serios.

> Francia nos muestra muy claramente esta diversidad: mientras los informes publicados por el Ministerio del Interior, e incluso un informe del Senado del año 2013, apostaban por invertir en videovigilancia y constataban su eficacia en la lucha contra la delincuencia, un famoso informe del Tribunal de Cuentas francés del 30 de junio de 2011 sobre la organización y la gestión de las fuerzas de seguridad pública ponía de relieve la **falta de evidencia científica de la eficacia** de las videocámaras.

Paulatinamente, las inversiones inmensas que hemos visto que se han llevado a cabo en la instalación de sistemas CCTV, especialmente, pero no únicamente, en el mundo anglosajón, han obligado a intentar averiguar la rentabilidad, es decir, la eficacia. Sobre todo con el escenario de falta de recursos públicos de los últimos años debido a la crisis económica.

La dificultad principal constatada para su eficacia la encontramos en el hecho que, en muchos casos, la inversión en videovigilancia se consideraba un ahorro notable en personal policial que reduce globalmente el gasto de las organizaciones. Para muchos, las cámaras, de hecho, sustituían los ojos de los profesionales y la información que aportaban se incorporaba sin más al trabajo policial, sin implicar ningún cambio de estructura o de funcionamiento. Simplemente, había más ojos que actuaban como oficinas de policía virtuales. No solo no había que efectuar ningún tipo de reestructuración para hacer un buen uso de las cámaras, sino que ni había que formar a los agentes de policía para hacerlo. Pero, evidentemente, **una cámara no es un policía**, puesto que cuando *ve* algún incidente no puede actuar directamente, alguien en la sala central de la policía tiene que **procesar la imagen y organizar una respuesta**. En muchos casos, esta falta de previsión ha provocado que los policías no supieran realmente cómo canalizar de la mejor manera posible la información que les llegaba por medio de las videocámaras (Menichellli, 2014; Goold, 2004). Así, el primer paso para incrementar la eficacia de las videocá-

maras fue **reestructurar los procesos de trabajo** de forma que garantizaran un trato adecuado de la información recibida y su rápida transformación en acción policial.

La investigación ya ha avanzado notablemente, tanto en el ámbito académico (Piza, 2012) como institucional (hay una investigación notable llevada a cabo por el Ministerio del Interior belga). Las conclusiones más evidentes han sido matizar que el impacto de las videocámaras **varía en función de los lugares y del tipo de delitos e infracciones**. No es sorpresivo: del mismo modo que un medicamento no sirve para tratar todas las enfermedades, ningún instrumento sirve para prevenir todo tipo de delitos en cualquier circunstancia. Veamos las conclusiones más relevantes (EFUS, 2016):

- La videovigilancia funciona **muy bien en espacios cerrados o muy definidos** (Welsh y Farrington, 2002). Por ejemplo, las cámaras en **aparcamientos de vehículos** han reducido bastante los robos de vehículos y dentro de ellos (siempre que las cámaras sean supervisadas por alguien). De hecho, es en este ámbito que el éxito ha sido más destacado y ha llegado a un 51% de reducción en algunos casos (Piza, 2012; Welsh y Farrington, 2007). También han funcionado de forma notable en los grandes estadios deportivos. Concretamente, en los estadios de fútbol se han convertido en un requisito *sine qua non* para participar en las competiciones de más alto nivel y su uso ha servido para identificar los comportamientos antisociales, circunstancia que ha permitido individualizar las sanciones, a menudo consistentes en prohibir a los infractores la entrada al estadio durante un tiempo. Su impacto en la reducción de los comportamientos antisociales y la violencia en los estadios es indudable.

- Los efectos son **inferiores en espacios más grandes e indefinidos**. A pesar de que parece que la instalación de videocámaras en el centro de las ciudades ha reducido la delincuencia, esta reducción ha sido muy poco significativa (como muestra el ejemplo de Málaga, Cerezo y Díaz Ripollés, 2010). Aquello que realmente ha resultado extraño es que un operador de CCTV provoque directamente una detención de un delincuente. Ditton y Short (1999, citados por Piza, E., 2012, 26) muestran que en su estudio de dos sistemas de CCTV en Escocia la actividad del operador comportó únicamente una detención cada 967 horas de funcionamiento). Sarno, Hough y Bulos (1999) (también citados por Piza, E., 2012, 26) informan que una unidad de CCTV en Londres **proporcionaba a la policía imágenes de un delito unas ocho veces el año**.

- Los delitos contra la propiedad **sí parecen afectados** por la presencia de videocámaras, mucho más que los delitos violentos contra las personas, que apenas son influenciados por su presencia.

- Las cámaras instaladas en **viviendas y transportes públicos** han comportado una **reducción de los delitos**, a pesar de que no muy sustancial.

- A pesar de la creencia generalizada de que las cámaras de videovigilancia producen un incremento de la seguridad percibida (una mejora de la **seguridad subjetiva**), que las personas que circulan o están en zonas donde hay instaladas videocámaras se sienten más seguras, **no hay estudios concluyentes**. Mientras que **algunos** estudios muestran un **incremento de la seguridad subjetiva**, **otros** manifiestan que la gente **considera como problemáticos los espacios donde hay cámaras de videovigilancia instaladas** y, en consecuencia, las cámaras no les dan seguridad, sino todo lo contrario, les confirman el carácter peligroso de la zona. Incluso en el ámbito del transporte público solo un 14% de los encuestados en Francia sobre la seguridad en el transporte público manifestaron que la ausencia de videocámaras les provocaba angustia (Vanier y d'Arbois de Jubainville, 2018).

- También es controvertido el hecho de hasta qué punto la videovigilancia puede reducir los actos de vandalismo, a pesar de que la policía lo cree firmemente. Parece que **el efecto significativo en el vandalismo** se produce **solo** cuando detrás de la cámara hay **un operador en tiempo real que es capaz de organizar una respuesta inmediata** cuando identifica un incidente (Poyner, 1988).

Un tema muy debatido en relación con el impacto de la videovigilancia está relacionado con el hecho de si, y en qué medida, la instalación de las cámaras no produce en realidad un **efecto de desplazamiento** mucho más que no una reducción del delito. La investigación muestra, quizás de forma sorpresiva, que la videovigilancia **no provoca un desplazamiento significativo**, a pesar de que puede provocar alguno (Cerezo, 2013), de la delincuencia u otras conductas desordenadas, ni tampoco ninguna difusión de beneficios (extensión de las mejoras en zonas periféricas a las cámaras). En el experimento de Piza (2012) sí se produjo una difusión de beneficios en los casos de delincuencia relacionada con los vehículos.

Parece evidente que los factores fundamentales para que la videovigilancia provoque los efectos esperados son (EFUS, 2016):

- Una **buena iluminación** de los espacios afectados.

- Una **implantación intensa** (un gran número), una **buena cobertura** y un **posicionamiento adecuado**.

- La videovigilancia es más eficaz cuando se establece **junto con otras medidas preventivas**, como, por ejemplo, guardias comunitarios o vigilantes de barrio. Nobili (2009) afirma que en la región italiana de Emilia-Roma-

ña la videovigilancia es más eficaz cuando se aplica conjuntamente con operaciones específicas de vigilancia comunitaria.

- Una **muy buena cooperación con la policía**, a todos los efectos o en el marco de operaciones especiales (por ejemplo, contra el tráfico de drogas).

- Una **buena ubicación y visibilidad** de las cámaras, además de una publicidad suficiente de su existencia, puesto que si el público no es consciente de ellas, el efecto disuasorio no llega a producirse.

6. Tendencias de futuro

Podríamos distinguir las tendencias en tres ámbitos claramente diversos: la finalidad del uso de la videovigilancia, las innovaciones tecnológicas y las tendencias asociativas.

6.1. Nuevas funcionalidades de la videovigilancia

Las relaciones entre la policía y el público proporcionan casos y situaciones francamente conflictivos, a pesar de que la mayoría de las interacciones entre unos y otros son muy pacíficas (Guillén, 2018). En los casos que resultan conflictivos, a menudo es difícil sacar algo en claro más allá de obtener la palabra del miembro del público y del policía que actúa y, normalmente, de dar una cierta presunción de veracidad al agente de la autoridad. La ausencia habitual de testigos (o de testigos que quieran atestiguar) hace difícil una aproximación más objetiva. Este ha sido, por ejemplo, tradicionalmente, el caso de las interacciones de la policía con las personas que están detenidas bajo su custodia. Durante mucho tiempo ha sido habitual escuchar personas que habían sido detenidas por la policía que acusaban a los guardianes de maltratos e incluso de torturas (Guillén, 2018). Como ya se ha mencionado a la hora de hablar de la regulación de la videovigilancia en España, tanto en Cataluña como en el País Vasco se decidió instalar cámaras que grabaran las interacciones entre la policía y los detenidos en los centros donde se mantenían en custodia. Pues bien, como se ha mencionado, los resultados han sido espectaculares en ambos casos y se han reducido las denuncias en contextos de detención prácticamente a cero. Habrá que ver hasta qué punto se generaliza este uso de la videovigilancia tanto en España como otros países de su entorno.

La idea de fondo es que el hecho de sentirse observados necesariamente tiene que afectar a la conducta de ambas partes: del policía, que es consciente que cualquier irregularidad quedará evidenciada por la filmación y por el miembro del público que, por un lado, si provoca al policía para que reaccione con dureza, la conducta quedará grabada, y, por el otro, que si acusa falsamente y, en realidad, es él mismo o ella misma quien se provoca las lesiones, las cámaras evidenciarán el hecho. Es decir, el uso de **videocámaras** en este contexto es un mecanismo de protección **tanto de la policía como de las personas detenidas**.

Hay otros contextos especialmente conflictivos para las relaciones entre la policía y el público (Guillén, 2018). Hay que mencionar el ámbito de la policía de orden público y, en general, a todas aquellas situaciones, a menudo a horas intempestivas, en que los agentes de la policía y los ciudadanos interactúan fuera de los ojos de terceras personas. Aquí la situación de indefensión ha sido a menudo mutua, de los ciudadanos, que alegan abusos que no siempre pue-

den demostrar, y de los policías, que tienen dificultades para defenderse de las acusaciones de conductas violentas o desconsideradas con la ciudadanía. Incluso, en los últimos años, con la proliferación de las nuevas generaciones de teléfonos móviles, es frecuente, por ejemplo en el ámbito del orden público, que cualquier uso de la fuerza de los policías intervinientes sea recogido con toda su crueldad por algún teléfono móvil y se difundan después las imágenes no únicamente por los medios de comunicación, sino también y sobre todo por las redes sociales. Los policías se han quejado a menudo de que se trata de instantáneas perversas, sacadas de contexto, que no explican de manera adecuada la secuencia ni la causa de la intervención y que los desprestigian de forma considerable.

Este contexto de conflictividad en las distancias cortas entre el público y la policía ha planteado la necesidad de considerar, aprovechando los grandes adelantos tecnológicos, si la incorporación de pequeñas videocámaras en los uniformes de la policía (en ciertos países, las cámaras en los vehículos policiales hace años que funcionan) sería una garantía del desarrollo pacífico de los encuentros entre la policía y los ciudadanos. En Cataluña, por ejemplo, en materia de orden público ya se acordó hace algunos años que las intervenciones de la brigada móvil serían grabadas para evidenciar el comportamiento de los ciudadanos violentos y justificar la conducta de los agentes actuantes (o exigir responsabilidades cuando se diera el caso). Varias organizaciones policiales se han planteado, además, equipar a los policías con **cámaras incorporadas en el uniforme** (*body worn cameras*, en la terminología inglesa) en servicios especialmente complicados. Por ejemplo, el uso de armas conductoras de energía o, de una forma más común, pistolas eléctricas, se acostumbra a autorizar con la exigencia de que se graben todas las intervenciones en las que se usen. Esta exigencia generalizada ha comportado que los mismos fabricantes de estas armas hayan incorporado una pequeña videocámara que se pone en marcha en el momento en que el policía procede a utilizarla (Guillén, 2018).

Ha habido casos en los que el uso de las cámaras incorporadas en el uniforme ha sido **impuesto por una sentencia judicial** para establecer mecanismos de control sobre el comportamiento de los agentes de la autoridad en la calle. Hay, como mínimo, una sentencia de la jueza federal de distrito Shira A. Sheidlin en el caso Floyd v. Ayuntamiento de Nueva York del 12 de agosto de 2013. 959 F. Supp. 2d 540, 562 (S.D.N.Y. 2013) en la que obligaba a la policía local a instalar videocámaras en los uniformes de las patrulleras para constatar si su comportamiento con el público era el adecuado (Guillén, 2018). Hay que recordar que, a partir de la implantación de las políticas policiales de tolerancia cero en la década de 1990, las acusaciones de comportamientos agresivos con el público de los policías de Nueva York han estado a la orden del día (Guillén, 2012).

Antes de la mencionada sentencia ya se habían puesto en marcha experimentos con cámaras integradas en el uniforme (predominantemente en el mundo anglosajón), hasta el punto de que las reformas de las leyes estatales de policía (un total de 34) que se llevaron a cabo en el bienio 2014-2016 en los Estados Unidos de América se dedicaron, entre otras cosas, a la regulación del uso de este tipo de cámaras (Subramanian y Skrzypiec, 2017, citados por Guillén, 2018). Existen estudios empíricos sobre los experimentos llevados a cabo en ciudades como Palo Alto, Orlando, otras ciudades americanas y alguna policía inglesa. Estos estudios muestran que el uso de cámaras incorporadas en el uniforme ha **provocado un gran descenso de la conflictividad** en las interacciones entre el público y la policía (disminuyen las quejas) (Farrar, 2013) y una cierta tendencia a reducir el uso de la fuerza de la policía. Se detecta, sin embargo, una excepción en la reducción del uso de la fuerza: en los casos en los que se requiere un uso muy intensivo de la fuerza por la gravedad de la situación no se reduce su uso (Guillén, 2018). Es evidente que, por

ejemplo, en casos en los que la policía debe afrontar a una persona muy agresiva y con armas letales que plantea un riesgo inminente para ellos o para terceras personas, por mucho que sean objeto de videovigilancia, no dudarán en hacer uso de la fuerza necesaria para evitar que el riesgo se concrete en lesiones de alguna persona.

Esta influencia de la videovigilancia en los agentes de policía hace que algunos defiendan que la verdadera finalidad del uso de las cámaras incorporadas en el uniforme es controlar cada vez más a los agentes de policía (Menichelli, 2014).

Por lo que se puede ver en los ambientes profesionales (sindicatos policiales muy favorables a su uso), en la opinión pública y en las autoridades, y por el coste cada vez más asumible de las cámaras en cuestión, parece razonable pensar que **los uniformes de policía tenderán a incorporar las videocámaras** con más frecuencia en las próximas décadas.

Finalmente, sería adecuado también mencionar el uso combinado de las videocámaras modernas de dimensiones muy reducidas con **los drons**. La combinación de estos dos elementos (dron y cámara) hace que se pueda acceder en espacios sin acceso a nivel de tierra (patios interiores de edificios o de instalaciones deportivas, industriales o recreativas) y que se pueda hacer el seguimiento de grandes concentraciones de masas o de grandes accidentes o catástrofes a un precio mucho más reducido que hasta ahora (hacían falta aviones o helicópteros), e incluso se pueden utilizar en los grandes estadios deportivos. Su proliferación provoca, sin embargo, algunos problemas de seguridad, sobre todo en las cercanías de los aeropuertos, además de violación de la intimidad, que ha espoleado la regulación de su uso.

Texto normativo de referencia

Consultad el documento *Privacy and data protection implications of the civil use of drones* elaborado por el Parlamento Europeo en 2015. https://bit.ly/1fuwmsf

Denominación de *dron*

Es importante tener en cuenta la denominación en inglés de los drons para poder comprender la amplia literatura sobre el tema en esta lengua. Hasta hace unos años la denominación técnica era *unmanned aerial vehicles* (UAV), y actualmente predomina *remotely piloted aircraft* (RPA).

6.2. Las innovaciones en la videovigilancia: hacia los Smart CCTV

La utilización práctica de la videovigilancia ha puesto de manifiesto dos dificultades (o necesidades, según como se mire). La primera, relacionada con la práctica imposibilidad de tener personas que visionen en directo los registros de todas las cámaras que están en funcionamiento en cada momento y, la segunda, la importancia de poder combinar la información obtenida de las grabaciones videográficas con otras fuentes de datos, de forma que el efecto de ambas fuentes sea multiplicador y las cámaras puedan acabar funcionando de forma *inteligente*.

Las salas de control de las videocámaras en funcionamiento acostumbran a tener multitud de pantallas **que no pueden ser vistas en el momento por los operadores disponibles en la sala**. Incluso a menudo las diversas pantallas van alternando imágenes de varias cámaras porque su número es tan grande que es imposible tener una pantalla para cada una de ellas. En esta situación es poco probable que el operador detecte los incidentes de seguridad que las cámaras constatan en el mismo momento en que se producen, lo cual dificulta la gestión de la necesaria respuesta de los actores de seguridad.

Para dar respuesta a esta necesidad ha aparecido la nueva generación de ***Smart CCTV***, es decir, de cámaras inteligentes, que, a partir de la información previa introducida en el sistema y en función de las conductas o hechos que aparecen en pantalla, son capaces de **detectar** delitos, infracciones o cualquier otra anomalía que tenga implicaciones en la seguridad, **priorizarlas** y **pasarlas** a las pantallas que son visualizadas por los operadores.

Ejemplos de innovaciones en la videovigilancia

Por ejemplo, ya hace algunos años, uno de los problemas más frecuentes que tenía el servicio de transporte público del área metropolitana de Múnich eran los grafitis que pintaban en el exterior de los vagones. Una vez decidido que había que actuar con intensidad ante estos hechos, introdujeron en el sistema información, de forma que diera preferencia a las imágenes con personas que se agachaban en los lados exteriores de los vagones y que estas imágenes (indiciariamente sospechosas de que alguien intentaba pintar el exterior del vagón) pasaran a las pantallas que eran visualizadas por los operarios, de forma que visionaran los hechos, comprobaran si realmente alguien pintaba el vehículo o simplemente se abrochaba los zapatos, y, en caso necesario, pudieran organizar la respuesta correspondiente. En los aeropuertos hay sistemas que dan preferencia a piezas de equipaje abandonadas que pueden representar un hipotético riesgo de explosivo terrorista. Si los operadores identifican rápidamente estas maletas o bolsas pueden tomar las medidas oportunas para aislarlas y comprobar el contenido. De hecho, la misma Comisión Europea ha financiado varios proyectos dirigidos a elaborar estos detectores de conductas problemáticas o irregulares, como, por ejemplo, la *Automatic Detection of Antisocial Behaviour and Threads in Crowded Spaces* (ADABTS), o el proyecto INDECT, que perseguía la identificación de amenazas reales para la seguridad. Consulteu aquest enllaç: https://cordis.europa.eu/project/rcn/89374/factsheet/en.

Otra variante de uso inteligente de la videovigilancia es el conocido sistema tutor de control de disciplina viaria en las carreteras y autopistas. Fundamentalmente se utiliza para controlar la velocidad media en tramos en lugar de centrarse en picos de velocidad en espacios concretos. Se usa mucho en Italia y también últimamente en España. Hay versiones que también detectan los cambios de carril, con los que los sistemas tradicionales tenían problemas.

Un sistema especialmente desarrollado de videovigilancia inteligente es el conocido como **análisis del contenido del vídeo** (VCA, en su denominación inglesa), que permite **reconocimientos faciales** o el **rastreo** de una persona en un mapa a partir del análisis de las imágenes ofrecidas por las videocámaras que están instaladas (Efus, 2016). La conexión entre los rostros identificados por las cámaras y las bases de datos de personas buscadas por la policía y la justicia permite detectar las coincidencias y tomar las medidas oportunas. Su uso es más habitual en aeropuertos y puertos marítimos para buscar sospechosos de terrorismo. Uno de los primeros sistemas de reconocimiento facial de este tipo lo encontramos en Londres a finales del siglo pasado. Se trataba de un total de 140 cámaras vinculadas a un banco de fotografías de sospechosos o perseguidos administrado por la policía (EFUS 2016). De todos modos, la afectación de los derechos fundamentales que pueden provocar estas cámaras ha provocado ciertas reticencias e, incluso, las autoridades de San Francisco prohibieron a la policía de la ciudad el uso de las cámaras de reconocimiento facial para proteger adecuadamente los derechos de las personas objeto de su uso. Otras ciudades podrían seguir el ejemplo. En el Reino Unido, en la misma dirección, un ciudadano se querelló contra la policía del sur de Gales por usar las cámaras de reconocimiento facial sin ningún tipo de regulación, sin ninguna garantía para proteger los derechos de las personas afectadas. En el momento de escribir este material, el caso se encontraba visto para sentencia.

Hay software que ha desarrollado paquetes de identificación y analítica automáticos que pueden reconocer sonidos y maneras de caminar, y también otras sistemas avanzados de identificación y seguimiento de sospechosos. Hay reconocimientos de audio que permiten aislar de forma automática tanto sonidos como disparos, cristales rotos, discusiones o voces agresivas, además de enviar alertas al operador de videovigilancia. La Universidad de Kingston ha desarrollado un sistema innovador de etiquetado y seguimiento. El sistema identifica al sospechoso por su apariencia y otras características, lo etiqueta y todas la cámaras de la red proceden a su seguimiento.

Encontramos otro ejemplo bastante extendido en el que se aplica la conexión de las imágenes con otras bases de datos en los casos de las **cámaras que leen las matrículas de los vehículos de motor** y están conectadas a las bases de datos de tráfico y de la policía (en terminología inglesa se denominan *Automatic License Number Plate Recognition*, ANPR), y en tiempo real pueden saber si el vehículo ha pasado la inspección técnica de vehículos (ITV), si el titular ha pagado los impuestos correspondientes, si tiene algún antecedente penal o el seguro en vigor, si el vehículo ha sido robado, y, muy importante, si la matrícula está autorizada a circular aquel día en el caso de las ciudades que alternan los vehículos autorizados a circular por cuestiones medioambientales.

En Cataluña y el resto del territorio español varios servicios de policía usan este sistema y parece que con total satisfacción sobre su eficacia. Las policías de Londres y de Nueva York hace años que utilizan este tipo de lectores de matrículas. También en Italia ha experimentado una implantación notable.

Una variante de este uso de la videovigilancia conectada a bases de datos externas lo encontramos con las conocidas como **comunidades cerradas** (*gated communities*), que a menudo tienen accesos con identificación de matrículas de vehículos que solo se abren cuando detectan la matrícula de alguno de los residentes. Este sistema también lo usa la policía cuando establece barreras o columnas que impiden el acceso motorizado a determinadas calles para identificar a los vehículos de los residentes que sí pueden tener acceso (sistema utilizado, entre otros, en Barcelona).

Entre otras innovaciones tecnológicas podemos mencionar **las cámaras infrarrojas** para uso nocturno que ya están suficientes extendidas. También hay que mencionar las **cámaras termales** para identificar fuentes de calor, incluidos los seres humanos (un helicóptero o una avioneta que vuele a poca altura puede identificar con una de estas cámaras a una persona que esté perdida, secuestrada o escondida en un determinado territorio durante la noche). **Los escáneres de retrodispersión con rayos X** de baja intensidad permiten ver a través de la ropa para detectar armas u otros materiales prohibidos (empiezan a generalizarse en los aeropuertos). También hay cámaras que pueden detectar movimientos a través de una pared (EFUS, 2016).

6.3. La necesidad de partenariados: el trabajo en red

A comienzos del siglo XXI se produjo una **digitalización** generalizada de los sistemas de videovigilancia. Esta innovación proporcionó una serie de nuevas posibilidades, como, por ejemplo, la **creación de sistemas policéntricos**, que permitan a autoridades locales y otros usuarios **agrupar varios sistemas en grandes redes de videovigilancia**. Esto se traduce en la fusión de varias fuen-

tes de información en las mismas salas de control y requiere una gran homogeneización de los protocolos de trabajo para conseguir grabaciones compatibles que puedan ser tratadas conjuntamente.

En periodos de crisis o, como mínimo, de recursos escasos, es difícil explicar a los contribuyentes la existencia de varios sistemas de videovigilancia cuya la información no puede ser intercambiada. No es fácil explicar que las redes de videovigilancia del transporte, de los centros comerciales, museos públicos y privados, teatros, cines, de las instituciones financieras, de los edificios públicos y privados no puedan integrarse con las de las diferentes policías (que tampoco son compatibles entre ellas), con la consiguiente pérdida de información, de recursos y, de hecho, del prestigio de la coherencia del sistema.

Son ya numerosos, cuantitativa y cualitativamente, los casos de ciudades donde se han creado redes únicas de videovigilancia. Quizás el ejemplo más conocido es el sistema de videoprotección de la **ciudad de París** que se puso en marcha en 2012, que engloba todas las cámaras bajo el control de la policía, los municipios, edificios emblemáticos como el Museo del Louvre y áreas comerciales. Se trata de un **sistema policéntrico con varias fuentes y varios niveles de acceso**, con el cual, en caso de necesidad, la policía nacional tiene siempre acceso a las imágenes de todas las fuentes, que, en primera instancia, son supervisadas por ellas. Es decir, las cámaras del Museo del Louvre o del transporte son, en primer lugar, monitorizadas por sus responsables que, en caso de incidencia relevante, las reenvían a la policía nacional (o esta las puede requerir). Un caso similar se da en la ciudad de **Londres**, donde la policía metropolitana solo posee 500 de las 12.000 cámaras a las que tiene acceso (EFUS, 2016).

Ejemplos fuera de Europa

Fuera de Europa destaca el caso de la Ciudad de México con su Sistema Tecnológico de Videovigilancia, que dispone de 15.000 cámaras en los espacios públicos de la ciudad más 6.000 al servicio del metro. Todas están bajo el control de varios centros de control integrados en el Centro de Comando, Control, Cómputo, Comunicación y Contacto Ciudadano. Entre estas cámaras, hay muchas que identifican matrículas de vehículos y avisan rápidamente en casos de vehículos robados o que presentan cualquier peligro o anomalía. El centro de control está en contacto y puede movilizar cualquier servicio de policía, de emergencias, de extinción de incendios, de protección civil e incluso el ejército. Uno de los datos que ofrecen las autoridades para mostrar el éxito de este sistema es que, desde su implantación, el precio de los seguros de los vehículos de motor se ha reducido por la facilidad con la que se recuperan los vehículos robados (al menos, en comparación con la situación previa).

El entonces alcalde de Bogotá, Gustavo Petro, aprobó un decreto en 2014 (Decreto 341 de 15 de agosto) que ponía a disposición de la policía nacional colombiana todas las videocámaras existentes en la ciudad, con lo cual la policía veía multiplicado por decreto el número de cámaras a su disposición. No ha quedado claro el éxito de esta iniciativa, tanto por la fórmula legal utilizada como por la capacidad del destinatario del control de las cámaras para hacerla realmente efectiva. La policía pasaba de disponer de 280 cámaras a tener 4.870 (Guillén, 2016). En todo caso, esta iniciativa de la alcaldía pone sobre la mesa lo que es una necesidad: disponer de redes al alcance de la policía que integren toda la información videográfica existente para obtener los máximos resultados.

A escala más reducida, en otras ciudades también se han empezado a crear pequeñas y medianas redes que buscan compartir la información obtenida de varias fuentes, tanto públicas como privadas. En la ciudad de Turín había un proyecto en marcha y en Bar-

celona se habían hecho pasos en esta dirección para problemáticas relacionadas con el orden público.

Es muy importante, sin embargo, que no nos dejamos deslumbrar por todas estas «maravillas» tecnológicas y recordemos que, del mismo modo que pueden ser de gran ayuda para mantener la seguridad y prevenir la delincuencia, pueden ser una fuente de abusos y violaciones de derechos fundamentales a una escala sin precedentes. Es necesario, pues, seguir aplicando todas las cautelas y garantías que hasta ahora hemos aplicado e, incluso, mejorarlas para que puedan seguir el paso de las innovaciones tecnológicas y no queden obsoletas para su finalidad: garantizar que las nuevas tecnologías no acaben reduciendo o suprimiendo los espacios de libertad y de goce de los derechos fundamentales. Estaría bien imaginarse qué podría haber pasado si regímenes como los dirigidos por Hitler y Stalin hubieran dispuesto de todo este armamento tecnológico.

Bibliografía

British Security Industry Association (2013). *The Picture is not clear. How many surveillance cameras in the UK? A study by the BSIR*. <https://www.bsia.co.uk/portals/4/publications/195-cctv-stats-preview-copy.pdf>

Cerezo, A. (2013). «CCTV and crime displacement: A quasi-experimental evaluation». En: *European Journal of Criminology* (vol. 10, núm. 2, pág. 222-236).

Cerezo, A.; Díez-Ripollés, J. L. (2010). *Videocámaras y prevención de la delincuencia en lugares públicos*. Valencia: Tirant lo Blanch.

Cohen L. E.; Felson, M. (1979). «Social Change and Crime Rate Trends: A Routine Activity Approach». En: *American Sociological Review* (vol. 44, pág. 588-608).

European Forum for Urban Security (EFUS) (2010). *Citizens. Cities and Video Surveillance Towards a democratic and responsible use of CCTV*. Montreuil.

European Forum for Urban Security (EFUS) (2016). *Experiencias europeas en materia de videovigilancia*.

Farrar, T. (2013). *Self-awareness to being watched and socially desirably behaviour: A field experiment on the effect of body worn cameras on police use of force*. PoliceFoundation.

Goold, B. J. (2004). *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Nueva York: Oxford University Press.

Guillén, F. (1997). «Breve resumen y comentario de la Ley Orgánica 4/1997, de 4 de agosto, por la cual se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos». En: *Revista Catalana de Seguridad Pública* (núm. 1, pág. 171-182). Escuela de Policía de Cataluña, Mollet del Vallès.

Guillén, F. (2012). *Policía y seguridad*. Bellaterra: Servicio de Publicaciones de la UAB.

Guillén, F. (2015). *Modelos de policía y seguridad*. Tesis doctoral defendida en la Universidad de Barcelona el 5 de mayo de 2015.

Guillén, F. (2016). *Modelos de policía. Hacia un modelo de seguridad plural*. Barcelona: Bosch editor.

Guillén, F. (2018). *Desencuentros entre la policía y el público. Factores de riesgo y estrategias de gestión*. Barcelona: Bosch editor.

International Center for the Prevention of Crime (ICPC) (2009). *Assessing CCTV as an effective safety and management tool for crime-solving, prevention and reduction*. Montreal.

Klauser, F. (2004). *A Comparison of the Impact of Protective and Preservative Video Surveillance on Urban Territoriality: the Case of Switzerland*. Surveillance and Society.

Menichelli, F. (2014). «Technology, context, users: a conceptual model of CCTV». A: *Policing: An International Journal of Police Strategies & Management* (vol. 37, núm. 2, pág. 389-403).

Nobili, G. G. (2009). «La videosorveglianza come strumento di prevenzione». A: *Il contributo della ricerca socio-criminologica alle politiche di sicurezza urbana* (pág. 99-106). Génova: Briganti.

Piza, E. (2012). *Identifying the best context for CCTV Camera Deployment. An analysis of micro-level features*. Tesis doctoral presentada en la universidad de Rutgers, Nueva Jersey. <https://pdfs.semanticscholar.org/bcd2/232ad171dde3e4ac2c6e1e682b4fd063838d.pdf>

Poyner, B. (1988). «Video Cameras and Bus Vandalism». A: *Journal of Security Administration* (vol. 2, núm. 11, pág. 44-51).

Silverman, E. B. (2001). *NYPD Battles Crime: Innovative Strategies in Policing*. Boston: Northeastern University Press.

Vanier, C.; d'Arbois de Jubainville, H. (2018). «Unsafe feeling on French public transport: Anxiety-provoking situations and avoidance strategies». En: Barabás, A. T. *The dimensions of insecurity in urban areas* (pág. 145-167). Budapest: National Institute of Criminology.

Varona, G. (2012). *Estudio exploratorio sobre los efectos del uso policial de la videovigilancia en lugares públicos. Propuesta criminológica de indicadores sobre su adecuación y proporcionalidad*. Oñati: Instituto Vasco de Criminología.

Welsh, B.; Farrington, D. (2002). *Crime prevention effects of closed circuit television: A systematic review* (Research Study núm. 25). Londres: Home Office.

Welsh, B.; Farrington, D. (2007). *Closed-circuit television surveillance and crime prevention: A systematic review*. Estocolmo: National Council for Crime Prevention.