Ciudadanos, ciudades y vídeovigilancia

Hacia una utilización democrática y responsable de la vídeovigilancia

Esta publicación es el resultado de la colaboración de todos los socios en el proyecto «Ciudadanos, ciudades y vídeovigilancia". Fue publicado por el Foro Europeo para la Seguridad Urbana, Roxana Calfa y Sperber Sebastian y Nathalie Bourgeois.

Traducción: Helga Birkle, Jara Campelo, Charlotte Combe, Elsner Kerstin, Nathalie Elson, Gianfranca Gabbai, John Tyler Tuttle, Maria Pia Falcone.

Gráficos: Pete Jeffs, Marie Aumont

Impreso en junio de 2010
por STIPA -Montreuil
NºISBN : 2-913181-37-6
NºEAN No.: 9782913181373

Foro Europeo para la Seguridad Urbana
10 rue des Montiboeufs, París, Francia
Tel: + 33 (0) 1 40 64 49 00
Fax: + 33 (0) 1 40 64 49 10
www.efus.eu
contact@efus.eu

El proyecto «Ciudadanos, ciudades y vídeovigilancia" con esta publicación, fue posible gracias al financiamiento de la Comisión Europea / Dirección General de Justicia, Libertad y Seguridad / Programa sobre los derechos fundamentales y la ciudadanía.

Sin embargo, refleja sólo la opinión de los autores. La Comisión Europea no se hace responsable ni por su contenido, ni por lo que se podría hacer con la información que contiene.

Agradecimientos
Este proyecto y la publicación no habrían sido posible sin la participación de los representantes de los socios del proyecto, las ciudades, las regiones y las autoridades policiales. Les agradecemos calurosamente por tener este proyecto en vivo.
También damos las gracias en particular a los expertos por sus importantes contribuciones en este libro, los anfitriones de las distintas reuniones, visitas de estudio y de la conferencia final, así como todos aquellos que tuvimos el placer de conocer y escuchar durante todo el proyecto.

Socios:
Catherine Schlitz, Christian Beaupere, Guy Geraerts, Serge Lodrini (Lieja, Bélgica); Bertrand Binctin, Christophe Bois (Le Havre, Francia), Charles Gautier, Dominique Talledec, Eric Fossembas (Saint-Herblain, Francia) ; Rossella Selmini, Gian Guido Nobili (Region Emilia Romaña, Italia), Francesco Scidone, Maria Pia Verdona, Marcelo Sasso, Marco Morelli (Génova, Italia), Giorgio Vigo (Véneto región, Italia), Ahmed Aboutaleb, Ineke Nierstrazs, Afke Besselink, Niels Witterholt, Nienke Riemersma, Wilco Mastenbroek, Linda Ouwerling, Ciska Scheidel (Rotterdam, Países Bajos), Manuel Ayala Garcia, Juan-

Jose Ferrer Planells, Tomas Paris (Ibiza, España), Christopher Ambler, Roger Fox (Policía de Sussex, Reino Unido), Andrew Bayes, James Farrell (Policía Metropolitana de Londres, Reino Unido).
Socios asociados: Stanislav Jaburek, Lenka Stepankova (Brno, República Checa), Béla Danielisz, Gabor Gulyas, Zoltan Nemeth, Krisztina Szego (Budapest, Hungría).

Expertos:
Benjamin Goold (Universidad de Oxford Reino Unido/Universidad de Columbia Británica, Canadá), Jeroen Van Den Hoven (Universidad Tecnológica de Delft, Países Bajos), Laurent Lim (CNIL, Francia), Maye Seck (Foro Francés para la Seguridad Urbana, Francia), Peter Squires (Universidad de Brighton, Reino Unido), Eric Töpfer (Universidad Técnica de Berlín, Alemania).

Otros participantes/personalidades encontradas:
Alessandra Risso, Gianluca Saba, Yuri Piccione, Rinaldo Sironi, Valerio Piazzi, Piero Anchini, Amerigo Alunno, Dario Messina, Furio Truzz (Génova, Italia), Graeme Gerrad, Brian Watkinson, Dave Hinton, Ken Crawley, Mick Neville, Isabella Sankey, (Londres/Brighton, Reino Unido), Isabelle Mercier, Didier Delorme, Emmanuel Magne, Georges Passini, Louis-Jean Despres, Mr. Pareja, Jacques Signourel, Patrick Aujogue, Thierry Dussauze, Jacques Comby (Lyon, Francia), József Schmidt, Attila Cserép, Richárd Schranz, Péter Rózsas, Endre Szabo, Tivadar Hüttl, Tomáš Koníček, Klára Svobodová (Budapest, Hungría), R.V. de Mulder, Laurie Bush, Zsuzsanna Belényessy, Sylvie Murengerantwari, Caroline Atas (Rotterdam, Países Bajos).

Índice

Editorial

Las ciudades son cada vez más densas y multiplican las ofertas de movilidad educativas y culturales que recurren a una multiplicidad de equipamientos cada vez más complejos, con elevados costes de funcionamiento. Los flujos de circulación se entrecruzan, el show off de la oferta comercial se extiende ante la vista y el apetito del público. La vigilancia humana las 24 horas resulta imposible por el coste, aunque el desarrollo de la electrónica en la capitalización de la información y su intercambio, en el suministro de instrumentos preventivos o disuasivos, alientan a la multiplicación de las cámaras instaladas en los espacios dedicados al transporte, a las reuniones multitudinarias, a los lugares de exposición de mercancías o de objetos de gran valor económico. La prevención de incidentes técnicos es predominante en la instalación de cámaras, cuyas imágenes se observan en directo pero cada vez más son analizadas por software. La preservación de la integridad de los equipamientos es la segunda prioridad de estas instalaciones. La mala utilización y el deterioro intencional requieren una intervención rápida en ciertos equipos cuyo funcionamiento puede afectar a miles de personas. Compensar la reducción de la plantilla que se ocupa del funcionamiento de un equipamiento es la

tercera motivación de estas instalaciones. Este conjunto de motivos hace que nuestras ciudades sean consumidoras de imágenes de vigilancia. Los usuarios de estas imágenes pertenecen tanto a la esfera privada como a la esfera pública.

Sin embargo, apareció un cuarto motivo que ha dado al debate un sesgo político. Gracias a las cámaras se pueden detener a delincuentes que operan en la vía pública y en los espacios públicos. Este motivo surgió de una observación negativa que se ha hecho sobre la eficiencia de la policía, ya que aumentar el porcentaje de elucidación reduciría al mismo tiempo las veleidades que pudieran tener los delincuentes de pasar al acto. Este axioma de una criminología de tendencia liberal sienta el principio según el cual si se incrementa en el delincuente la certeza de que le cogerán, renunciará a su acción criminal. Por eso, en los textos oficiales aparece un doble argumento: las cámaras de vídeo contribuyen a prevenir la delincuencia y sirven para detener a los delincuentes. Quizá, quizá... ¿pero esta política vale realmente la pena? Los estudios no muestran claramente una disminución de la delincuencia; registran arrestos en algunos casos criminales que justifican una investigación más detallada, pero el efecto masivo que se esperaba no se ha observado. Observación que está bajo el signo de la inquietud. En efecto, para lograr al menos el segundo objetivo, más que el primero, hay que poner cámaras de vídeo en todas partes ya que los crímenes se reparten bastante homogéneamente en el territorio urbano. A partir de ese umbral, que consiste en saturar el espacio público con cámaras, pasamos a una sociedad de desconfianza, de restricción de las libertades. Lo que da pie al debate.

¿Qué precio estamos dispuestos a pagar por una sociedad que hace de la seguridad un valor absoluto?

Se acaba de publicar un informe parlamentario francés como una respuesta a una serie de catástrofes naturales. Su principal conclusión es interrogarse sobre la necesidad de reintroducir una cultura del riesgo entre los ciudadanos. El triunfalismo de la tecnología ha erradicado de la consciencia del ciudadano la noción de riesgo. ¿Qué podemos hacer para decirle que, a pesar de la tecnología, debe saber que sigue en situación de riesgo? ¿No es, acaso, la misma pregunta que habría que hacerse sobre la delincuencia? No existe una sociedad segura, sin delincuencia, y cualquier medio que, supuestamente, elimine todo riesgo, debería ser rechazado por los ciudadanos responsables.

Saturar el espacio público con múltiples cámaras vulnera nuestro derecho al anonimato. Es un deber de las autoridades públicas justificar que se levante este anonimato. La Convención Europea de los Derechos Humanos nos invita a esta política, pero nos parece indispensable que se indiquen con precisión las modalidades de utilización de las cámaras y de las imágenes. Tal es el objeto del trabajo efectuado por técnicos y expertos, bajo la égida del Foro.

Michel Marcus
Director ejecutivo del Foro Europeo para la Seguridad Urbana

Introducción

La vídeovigilancia se está utilizando cada vez más

La primera década del siglo XX comenzó bajo el signo de un acontecimiento que dejó su impronta en las mentes y en la forma de encarar la seguridad. Los atentados del 11 de septiembre de 2001 han impuesto la seguridad como prioridad de la agenda mundial. Desde entonces, se ha ido desplegando en todos los niveles una plétora de medios que se consideran útiles en la lucha contra el terrorismo, entre los cuales se cuenta la vídeovigilancia. Sin embargo, ha quedado un poco de lado el interrogante sobre su eficacia, la adecuación entre los objetivos que se buscan y los instrumentos que se emplean, al igual que su impacto en las libertades, especialmente a largo plazo.

Se habían cometido otros atentados terroristas antes de 2001, pero no habían alcanzado esa dimensión global que todos los medios de comunicación han destacado. No es una casualidad si el Reino Unido, el país europeo que lo ha utilizado de forma regular y prolongada, es el que más ha buscado desarrollar todas las respuestas posibles, tanto en prevención como en resistencia.

La respuesta tecnológica de cara a una creciente demanda de seguridad por parte de los ciudadanos ha encontrado su justificación en los acontecimientos del 11 de septiembre de 2001, al igual que en los del 11 de marzo de 2004 en Madrid y del 7 de junio de 2005 en Londres. Desde entonces, la utilización de la tecnología no ha dejado de ir creciendo en todos los demás países europeos.

Ahora bien, como las imágenes impresionantes presentadas apenas unas horas después del atentado de

Londres, en las que se muestra de qué modo llegaron al lugar del crimen los presuntos terroristas, la intervención en 2008 del responsable de la vídeovigilancia de Londres calificándola de fiasco dieron la vuelta al mundo. Cuando pasó la emoción vinculada a los acontecimientos, había que interrogarse sobre la pertinencia de la utilización de la tecnología en acciones de prevención, su eficacia, y también las ventajas e inconvenientes resultantes de su uso.

Estos interrogantes no han perdido actualidad, sobre todo en los países que piensan incentivar la vídeovigilancia, como es el caso de Francia que ha optado por ella en 2008, o bien en los países que están muy avanzados en la utilización de esta tecnología, como es el caso del Reino Unido. Desde hace 25 años, en el Reino Unido se ha observado un desarrollo exponencial de estas tecnologías, y este país es hoy un líder mundial en el uso de la vídeovigilancia. No obstante, desde hace unos años, muchas voces se han elevado para cuestionar la pertinencia de la política de "vídeovigilancia total" y para sacar algunas conclusiones de la experiencia hasta ahora acumulada. Los británicos están llevando a cabo una reflexión sobre sus sistemas y sobre el modo de utilizarlos[1]. Así, el nuevo Viceprimer Ministro, Nick Clegg, ha anunciado recientemente que el gobierno prepararía una nueva ley de protección de los derechos fundamentales. En una conferencia de prensa del 19 de mayo de 2010 declaró: *"Este gobierno pondrá un término a esta cultura de intrusión en la vida privada de sus ciudadanos. Es inaceptable que personas que respetan la ley sean tratadas como si tuvieran algo que esconder... La vídeovigilancia será objeto de leyes específicas..."*[2].

Estos interrogantes son tanto más de actualidad para las ciudades europeas que la tecnología participa en la elaboración de políticas locales y regionales de se-

guridad. Los electos locales deben responder a la vez al pedido de mayor seguridad por parte de los habitantes y justificar los instrumentos de control que se han de instalar, con una óptica de transparencia y en un ejercicio democrático decisión política. Admitiendo que la tecnología sea la respuesta más adecuada de los Estados para luchar contra amenazas como el terrorismo, ¿qué pasa con la prevención de la criminalidad a nivel local? La mayor parte de las ciudades y regiones europeas se ven enfrentadas a diario a la delincuencia, que no tiene unos efectos tan espectaculares como los de un ataque terrorista, pero que no obstante cuestiona la vida en comunidad en un territorio determinado y puede resultar negativa para el desarrollo sostenible de ese lugar. Por lo tanto, las ciudades y territorios debe evaluar todo instrumento que pudiera ayudarles a garantizar la seguridad de sus ciudadanos y no pueden ignorar las potenciales ventajas de la tecnología.

Aunque, por cierto, los ciudadanos confieren a los electos un mandato por el cual éstos deben garantizar la seguridad de todos, también les conceden su confianza en el sentido de que las políticas de seguridad no deben aplicarse en detrimento del respeto de los derechos y libertades garantizados por la ley. Esta confianza también supone que las autoridades asumen la responsabilidad de sus orientaciones y hacen una utilización transparente de los instrumentos empleados para garantizar la seguridad.

¿Derecho a la seguridad, derecho a la protección de su vida privada? ¿Hay alguna prioridad? ¿Uno se impone al otro? En teoría, los ciudadanos deberían poder gozar de ambos derechos sin tener que optar por uno de ellos. Ambos van juntos en una sociedad democrá-

[1] Estrategia nacional sobre la vídeovigilancia , 2008
[2] DEPUTY PRIME MINISTER – SPEECH AND Q&A – 19/05/2010, London

tica y están garantizados del mismo modo tanto por los marcos legislativos nacionales como por los textos internacionales como El Convenio Europeo de Derechos Humanos firmado en 1950 bajo los auspicios del Consejo de Europa, y la Carta de los Derechos Fundamentales de la Unión Europea (2000). Pero en los hechos, la conciliación entre seguridad y libertades está lejos de ser algo obvio. La libertad es un derecho "débil" que se relativiza fácilmente de cara a la problemática de la inseguridad. La vídeovigilancia es una tecnología que suscita muchos interrogantes. ¿Qué se puede filmar? ¿Hay un derecho a la vida privada en el espacio público? Y en caso afirmativo, ¿cómo proteger este derecho? ¿Cómo evitar la discriminación de algunos grupos y cómo poner las ventajas de esta herramienta de vigilancia a disposición de toda la población? ¿Cómo hacer para que la vídeovigilancia funcione y cuándo recurrir a otros instrumentos? ¿Cuándo resulta eficaz en una relación costes-beneficios? ¿Cómo proteger los datos personales y cómo no producirlos inútilmente? ¿Cómo utilizar la vídeovigilancia con los ciudadanos como herramienta para prevenir la criminalidad y garantizar la tranquilidad pública?

Reflexión e intercambio de experiencias sobre la utilización de la vídeovigilancia, respetando y protegiendo las libertades individuales

Para responder a todos estos interrogantes e identificar las buenas prácticas se ha desarrollado este proyecto europeo "Ciudadanos, Ciudades y Vídeovigilancia". Esta reflexión se ha podido desarrollar gracias a la participación de diez participantes, a saber, las ciudades del Havre y de Saint-Herblain (Francia), Rotterdam (Países Bajos), Lieja (Bélgica), Ibiza (España), Génova, las regiones de Véneto y de Emilia-Romana (Italia), las policías de Londres y de Sussex (Reino Unido), al igual que una serie de expertos eu-

ropeos. El proyecto ha tenido el apoyo económico de la Comisión Europea (programa "Derechos Fundamentales y Ciudadanía").
El proyecto buscaba dar a las ciudades los conocimientos y las herramientas necesarias para desarrollar una política de seguridad integrada en la cual las realidades sociales y las libertades se tienen en cuente del mismo modo que la tranquilidad pública.
Para responder a los retos que plantea la vídeovigilancia en cuanto a los derechos y libertades, los participantes han establecido el objetivo específico de profundizar el tema fundamental de la responsabilidad del electo local, que debe encontrar un equilibrio entre la seguridad que piden los ciudadanos y las orientaciones estratégicas que le permiten dar una respuesta democrática.

Como lo indica el título del proyecto, los ciudadanos son el centro de las políticas locales. A este título había que prestar una singular atención a los ciudadanos, para tenerlos muy presentes a la hora de instalar o evaluar los dispositivos de vídeovigilancia. En efecto, en la medida en que estos dispositivos están ante todo al servicio de los ciudadanos, éstos no sólo deberían ser consultados sobre lo que esperan y sobre cuáles son sus necesidades en el ámbito de la seguridad, sino también estar perfectamente informados acerca del funcionamiento, los costes y los beneficios de estas nuevas herramientas. Los participantes han analizado cómo tener en cuenta estos interrogantes en todas las etapas de aplicación de un proyecto de vídeovigilancia, desde la instalación y el funcionamiento hasta su evaluación, y han debatido y propuesto soluciones alternativas complementarias.

Además, esta cooperación entre las ciudades, las regiones, las policías municipales y regionales, tenía la ambición de formular una *Carta para el Uso Demo-*

crático de la Vídeovigilancia, es decir, concretar el gran respeto que se tiene por los derechos fundamentales. En definitiva, el objetivo es aplicar esta Carta y definir un sello que identifica a las ciudades que respetan sus principios y sus recomendaciones.
Subyace a esta iniciativa conjunta la idea de establecer un lenguaje compartido sobre la vídeovigilancia en Europa, accesible y comprensible para todos. Se trata de una iniciativa para garantizar la transparencia de los procesos de decisión política.

Las ciudades ayudan a las ciudades…
La metodología del proyecto está fundada en la misión fundamental del Foro Europeo de Seguridad Urbana: *"Las ciudades ayudan a las ciudades"*. Las ciudades, las regiones y las autoridades policiales desean mejorar sus respectivos sistemas, compartiendo experiencias de unos y otros para sacar conclusiones. Este diálogo se ha ido completando con las contribuciones de diferentes expertos, como el Foro Francés de Seguridad Urbana y una serie de profesores de grandes universidades y altos funcionarios, que han ido enriqueciendo la reflexión y han entablado un vínculo entre la investigación y la práctica. Se han analizado las experiencias de cada participante aplicando un esquema de lectura, y este diálogo en el cual se intercambiaron prácticas y conocimientos, se han ido concretando en la *Carta para el Uso Democrático de la Vídeovigilancia.*

…para crear en el marco de una cooperación europea una Carta para el Uso Democrático de la Vídeovigilancia.
Desde la primera reunión que dio origen al proyecto, que se llevó a cabo en París en abril de 2009, se vio la riqueza de las experiencias de unos y otros, y la diversidad de situaciones entre los diferentes participantes. Ante todo, por la diversidad técnica, con dife-

rencias notables tanto por la cantidad de cámaras (¡de 4 a 60.000!), y por el tipo de cámara y sus capacidades funcionales, como por la cobertura geográfica. Diversidad también de los contextos políticos: ¿qué autoridades pueden decidir la instalación de las cámaras en el espacio público, quiénes pueden ser los administradores, qué personas están autorizadas a comunicar la información y quiénes son los destinatarios, qué marco legal, qué clase de debates sobre la vídeovigilancia a nivel nacional y local (véase parte III de esta publicación)? Diversidad, asimismo, en cuanto a la comprensión y a la percepción de la vídeovigilancia por parte de los ciudadanos de las ciudades participantes en este proyecto: ciudadanos favorables en algunas, desconfianza y reservas en otros, lo que induce diferentes niveles de debate público sobre la utilización de las cámaras y la protección de los derechos fundamentales. Diversidad de situaciones y de legislaciones, igualmente, que han hecho patente la dificultad de ponerse de acuerdo sobre el campo de aplicación del proyecto: ¿vídeovigilancia en el espacio público únicamente? ¿Cómo tratar los espacios semipúblicos, es decir, los espacios privados destinados a un uso público? Se optó por centrarse en la problemática del espacio público, en el cual todos los participantes son competentes, sin dejar totalmente de lado los sistemas de vídeovigilancia del espacio semipúblico, que representan una parte muy importante de los sistemas existentes, y para los cuales las conclusiones de este proyecto también podrían ser una fuente de inspiración.

El primer objetivo del proyecto era tener una visión de conjunto sobre la utilización de la vídeovigilancia y de las medidas que se adoptan para proteger la vida privada de los ciudadanos. Los esquemas de lectura aplicados a las políticas desarrolladas por los participantes a este proyecto han mostrado de qué modo la protección de los datos estaba integrada en las dife-

rentes fases de la vida de un sistema de vídeovigilancia, a saber, el análisis de las necesidades, la instalación, administración y evaluación de estos sistemas.
Para completar esta visión de conjunto y tener una comprensión global de la problemática, los participantes de este proyecto han gozado, desde el primer seminario de trabajo que se llevó a cabo en la ciudad del Havre el 3 y el 4 de junio de 2009, de la experiencia de los expertos oriundos de los diferentes sectores, jurídico, político/sociológico, técnico, filosófico, al igual que de la aportación de los representantes de ONG orientadas a la protección de los derechos humanos y de las asociaciones de policía.

Los expertos y profesionales estaban de acuerdo con los principales retos que representa la vídeovigilancia en el espacio público, que serían los siguientes:
➤ Por una parte, buscar un modo de preservar los códigos sociales sobre la intimidad o confidencialidad en el espacio público, en el marco de vídeovigilancia. Esta temática ha sido desarrollada en este caso por Benjamin Goold. También está presente en la jurisprudencia de la Corte Europea de Derechos Humanos de Estrasburgo (Francia), sobre las denuncias contra los "paparazzi".
➤ Por otra parte, encontrar un equilibrio adecuado en cuanto a la relación costes-beneficios, entre el precio que la gente está dispuesta a pagar renunciando hasta cierto punto a su intimidad, y los beneficios que se obtienen con una mayor seguridad. Esto significaría que las decisiones se tomarían en total consciencia y en perfecto conocimiento de las consecuencias.
➤ La intrusión en su intimidad no es percibida por el ciudadano como algo muy importante. No obstante, a final de cuentas, la suma de cada pequeña intrusión en la vida privada de un ciudadano puede cobrar proporciones considerables, y esta tendencia se incre-

menta exponencialmente con cada desarrollo tecnológico. La protección de la vida privada en el espacio público concierne a la autoridad política y los respectivos actores deberían participar en esta política. Por lo tanto, había que tener en consideración la protección de los datos y de las libertades individuales en cada nivel de utilización de la vídeovigilancia.

Una segunda etapa del proyecto ha permitido ver detalladamente la utilización de la vídeovigilancia, a través de una serie de visitas *in-situ* organizadas por tres participantes en este proyecto: la ciudad de Génova (Italia), la policía metropolitana de Londres y la policía de Sussex (Reino Unido) y Lyon (Francia), ciudad asociada al proyecto.
Con estas visitas se han obtenido conocimientos detallados acerca de la utilización de la vídeovigilancia, se ha visto en el terreno la administración de un sistema de vigilancia y se ha dialogado con diferentes interlocutores sobre la problemática y las ventajas que presenta esta tecnología.
- En la visita de estudio a Londres y a Brighton se ha obtenido información sobre la experiencia inglesa en la vídeovigilancia, integrada como un instrumento de investigación de criminología, al igual que sobre los debates actuales en el Reino Unido y su impacto en la vida privada. Esta información se ha obtenido en el marco de los encuentros con expertos que trabajan para el gobierno en la lucha antiterrorista y militantes de ONG como Liberty.
- La visita a Génova ha ilustrado la realidad de una ciudad italiana en la que operan varios sistemas de vídeovigilancia, bajo la dirección de instituciones diferentes. Aquí, el reto consiste en compartir la información: ¿hasta dónde y en qué condiciones?
- La visita a Lyon ha permitido comprender la política de una ciudad que había completado su sistema de vídeovigilancia con una Carta de Ética, y que había

instaurado un Colegio de Ética, responsable de supervisar el sistema.

En estas visitas de estudio también se ha visto que las ciudades y las regiones utilizan la vídeovigilancia de modo diferente, respecto a sus respectivos objetivos, y de qué modo varían los protocolos de gestión, la comunicación, la relación entre las cámaras públicas y privadas, y la actitud de los ciudadanos que va del apoyo a la oposición. Se ha visto claramente que el impacto de la vídeovigilancia varía según la clase y la dimensión de los espacios vigilados, el tipo de delito, la asociación o no de esta tecnología con otras medidas de prevención.
Estas visitas también han permitido identificar una serie de dispositivos y de medidas que se aplican para garantizar la protección de la vida privada de los ciudadanos, entre otras cosas, el establecimiento de parámetros específicos para las cámaras, la formación de los operadores sobre el marco legal que rige la protección de los datos, las Cartas de "buena utilización" a través de las cuales las ciudades se comprometen a respetar los derechos fundamentales, y los sistemas independientes de supervisión.
El enfoque de los expertos, las visitas de sitios, los encuentros con los profesionales locales, los esquemas de lectura que describen el modo operatorio de los participantes han servido como base para los debates de los dos seminarios de trabajo que se llevaron a cabo en Budapest, el 2 y 3 de diciembre de 2009, y en Bolonia, el 11 y 12 de marzo de 2010.
El seminario de Budapest ha sido una buena oportunidad para incluir en el proyecto los modos de trabajo de Europa Central, con visitas a la ciudad de Budapest y contribuciones del ombudsman sobre la protección de los datos y de las ONG húngaras, al igual que las contribuciones de la ciudad de Brno (República Checa) y del Ministerio del Interior checo. El seminario tam-

bién ha sido la ocasión de ilustrar la dificultad de encontrar un lenguaje compartido que refleje la problemática variada que se observa en Europa, superando las diferencias políticas para lograr un denominador común que no sea simplemente un acuerdo sobre el menor común denominador de los participantes. Por ejemplo, la idea de una Carta "Ética", muy aceptada en Francia, no ha sido unánimemente admitida en el resto de Europa. La solución de una Carta para el "Uso Democrático" de la Vídeovigilancia, reflejaba mejor el espíritu del proyecto que sitúa a los ciudadanos en el centro de la política local, para una aplicación democrática del poder que la representatividad ha conferido a los electos. También se ha debatido ampliamente las nociones de "videoprotección" o de "vídeovigilancia".

También se ha debatido la idea de crear un label correspondiente a la aplicación de la Carta, sello destinado a las ciudades que apliquen los principios en ella contenidos. En este punto, no se llegó a una opinión unánime, ya que unos veían en este label la continuación lógica del trabajo necesario para aplicar la Carta, mientras que otros eran más reservados respecto a la idea de someterse a una auditoría para poder exhibir ese label. Dicho lo cual, inicialmente no se había pensado que en el marco de este proyecto se llegara a desarrollar un label de esta clase, sino sólo un estudio de factibilidad del mismo.

El seminario de Bolonia ha servido para identificar los principios clave de la Carta que se deben aplicar a cada fase de la vida del sistema. El principal reto era encontrar los principios independientes, aunque complementarios, que, en su conjunto, caracterizan una utilización democrática de la vídeovigilancia.

Asimismo, se ha propuesta una iniciativa destinada a la creación de un lenguaje único sobre la vídeovigilancia en Europa: crear un sistema unificado de señalización, estandarizado, que pueda comunicar un

mensaje claro y completo a cualquier ciudadano de Europa. Se llevaron a cabo varios debates para determinar cuál sería la información indispensable que debiera incluir esta señalización, teniendo en cuenta lo que ya existe en las ciudades y países representados en el proyecto.

La definición de los siete principios en torno de los cuales se ha estructurado la *Carta para el Uso Democrático de la Vídeovigilancia*, al igual que los comentarios explicativos que los acompañan, han sido redactados por los participantes como fruto de un trabajo conjunto, en un último seminario que se llevó a cabo en París el 9 de abril de 2010.

La conferencia final del proyecto, que se realizó en la ciudad de Rotterdam el 27 y 28 de mayo de 2010, ha marcado el término de 18 meses de trabajo de los participantes y el reconocimiento de la responsabilidad de los electos en lo referente a la utilización de la vídeovigilancia. Como primeros firmantes de la Carta, los alcaldes de Rotterdam, Ahmed Aboutaleb, y de Saint-Herblain, Charles Gautier que también es senador y Presidente del Foro Francés de Seguridad Urbana, han afirmado con vehemencia que los electos locales son responsables de cara a los ciudadanos de las herramientas que eligen para llevar a cabo su política, y que también les incumbe una obligación de transparencia. Además, los dos Concejales Municipales invitaron a las demás ciudades europeas a firmar la Carta. Esta publicación refleja así este largo trabajo, a través del cual los diez participantes europeos en este proyecto han compartido los puntos de vista de los expertos oriundos de los diferentes países de Europa, han dialogado sobre las diferentes prácticas que han experimentado las ciudades, han debatido la problemática y los retos que presenta la vídeovigilancia en relación con la vida privada y, finalmente, han formulado conjuntamente una serie de respuestas posibles.

Parte I

El desafío: Conciliar el uso de la vídeovigilancia y las libertades individuales

Vídeovigilancia y derechos humanos

Benjamin J. Goold
Universidad de Columbia Británica (Cánada) /
Universidad de Oxford (Reino Unido)

En los últimos veinte años, la utilización de cámaras de vídeovigilancia se ha vuelto cada vez más frecuente en Europa. A pesar de que algunos países, como Francia, Alemania, Holanda e Italia tardaron más en adoptar esta iniciativa que lideró el Reino Unido, los sistemas de vídeovigilancia están ahora instalados en pueblos y ciudades de todo el continente. De hecho, la vigilancia del espacio público es hoy un hecho ineludible para un número creciente de europeos. A pesar de que el público concede un apoyo considerable a la utilización de la vídeovigilancia, la difusión de esta tecnología tiene serias consecuencias en las libertades civiles y en la relación entre los ciudadanos y el Estado. En particular, las cámaras de vídeovigilancia representan una amenaza nada desdeñable para la vida privada y para el ejercicio de derechos tales como la libertad de expresión y la libertad de asociación. En consecuencia, es vital que los responsables de la gestión y la operación de estos sistemas de vigilancia sean plenamente conscientes del peligro que representa la vigilancia del espacio público y que hagan todos los esfuerzos necesarios para garantizar que la vídeovigilancia no constituya una amenaza para los derechos humanos fundamentales.

Este capítulo hace una breve presentación general de las consecuencias que puede tener la vídeovigilancia en los derechos humanos, y procura ser una ayuda para los responsables y los operadores de estos sistemas para desarrollar políticas y modos de trabajo en la vigilancia del espacio público que sean coherentes

con un compromiso a favor de la protección de los derechos de los individuos y del respeto de las libertades civiles.

Vídeovigilancia y privacidad

Todos necesitamos cierto nivel de privacidad, sin la cual sería imposible la dignidad, desarrollar relaciones que tengan sentido con los demás, o sencillamente disfrutar estando solo con sus propios pensamientos. La privacidad es crucial para desarrollar su propia identidad porque nos quita el temor de estar constantemente bajo observación y juzgados por quienes nos rodean, y deja en nuestras manos el control de cómo y cuándo compartir la información sobre nosotros mismos con los demás.[3] Por estas razones, la mayor parte de los países reconoce al menos algunas reglas básicas de privacidad, y limita la capacidad de los individuos, de las organizaciones privadas y del Estado a recopilar información sobre la vida privada de la gente, o a efectuar un seguimiento de lo que hacen sin informarles o sin su consentimiento.[4]

Es importante reconocer que el derecho a la privacidad no desaparece en cuanto salimos de nuestros hogares. Aunque ninguna persona sensata puede imaginar que tendrá el mismo nivel de privacidad en la calle que en la sala de su casa, la mayor parte de nosotros pensamos poder tener cierto nivel de privacidad y anonimato cuando realizamos nuestras actividades en la vía pública. De hecho, una de las grandes ventajas de vivir en una ciudad es la capacidad de "perderse" en la multitud, libre de las exigencias de su familia, sus amigos y sus colegas. En parte, es precisamente esta promesa de anonimato y libertad lo que atrae a mucha gente a las calles de los pueblos y ciudades. Del mismo modo, aunque pocos piensan que pueden ir con un amigo a un restaurante o a un bar y estar totalmente protegidos de cualquier seguimiento posible, existen sólidas

convenciones sociales que nos ayudan a gozar de un razonable nivel de privacidad en esas circunstancias. Mientras que en ninguna otra parte como en los espacios que son obviamente privados, como la casa o el coche, esperamos tener tal nivel de privacidad, es obvio que también tenemos derecho a cierta privacidad en el espacio público.[5]

Ahora bien, por su propia naturaleza, la vídeovigilancia del espacio público socava este derecho. Exponiéndonos a una vigilancia constante cada vez que caminamos por la calle, las cámaras nos despojan de la posibilidad de conservar nuestro anonimato y nos hacen visibles ante el ojo atento del Estado. Mientras que renunciamos a buena parte de nuestra privacidad cada vez que nos encontramos en el espacio público, todavía no existe un medio por el cual los usuarios de la vídeovigilancia puedan indicar que otras personas nos están observando en el espacio público. Ser observado por una cámara, que posiblemente también conserve una copia de la grabación, es diferente a ser observado por una persona. En el primer caso, la observación es típicamente más prolongada, más intensa e íntimamente vinculada al poder el Estado. Dado que no vemos ni podemos interrogar a la persona que se encuentra

[3] Para una presentación general de las diferentes teorías acerca de la privacidad, véase: Solove, D.J. (2002), "Conceptualizing Privacy", *California Law Review* 90: 1087-1155; Solove, D.J. (2009) *Understanding Privacy* (Harvard University Press: Cambridge, Mass.); y Nissenbaum, H. (2010), *Privacy in Context* (Stanford University Press: Stanford, California).

[4] Una de las afirmaciones más claras sobre este derecho se halla en el Artículo 8 del Convenio Europeo de Derechos Humanos, donde se afirma que: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia."

[5] Véase: Goold, B.J. (2002), "Privacy Rights and Public Spaces: CCTV and the Problem of the 'Unobservable Observer'", *Criminal Justice Ethics* 21(1) invierno/primavera; y Goold, B.J. (2008) "The Difference between Lonely Old Ladies and CCTV: A Response to Jesper Ryberg", *Res Publica* (marzo).

detrás de la cámara, es difícil para nosotros saber cómo responder a este seguimiento o decidir qué podemos hacer al respecto. Dado que no sabemos qué imágenes captadas por las cámaras se conservarán o quién tiene acceso a ellas, no podemos estar seguros de que no sean malinterpretadas o utilizadas de modo inaceptable. Como ha observado el filósofo y criminólogo Andrew von Hirsch, ser observado a través de un sistema de vídeovigilancia "es como desarrollar nuestras actividades en un lugar con un cristal de espejo, por lo cual mientras que uno sabe que nos están observando detrás del espejo, no necesariamente sabemos quiénes son o qué están buscando los que están del otro lado."[6]

Aparte de la obvia intrusión que esto representa, la sensación de incertidumbre que inducen las cámaras de vídeovigilancia plantea una gran amenaza a nuestra experiencia de la privacidad en el espacio público. De cara a las expectativas que genera la vídeovigilancia, es razonable esperar que algunas personas sientan una aguda pérdida de privacidad y modifiquen su forma de actuar, no porque crean que estén haciendo algo malo, sino porque no desean llamar la atención de la policía o correr el riesgo de que sus acciones sean malinterpretadas. Esto es singularmente cierto con los jóvenes y los miembros de algunas minorías, que ya de por sí se podían sentir injustamente perseguidos por la policía y las autoridades locales. Así, Giovanni Buttarelli, Supervisor Adjunto Europeo de Protección de Datos, afirma lo siguiente:

"Ser observado cambia el modo de comportarse. Por cierto, cuando somos observados muchos de nosotros censuramos lo que decimos o lo que hacemos y ciertamente tal es el efecto de una vigilancia continua y generalizada. Saber que cada movimiento y que cada gesto está controlado por una cámara puede tener un impacto psicológico y cambiar nuestro comportamiento, lo cual

constituye una intrusión en nuestra privacidad."[7]

¿De qué modo, tanto los operadores como los administradores de los sistemas de vídeovigilancia pueden garantizar que la vigilancia del espacio público no socava fundamentalmente el derecho a la privacidad, ni cambia negativamente el modo en que la gente disfruta ese espacio? Ante todo, es esencial que cada sistema sea utilizado conforme a las restricciones que imponen las leyes nacionales y locales, y que se hagan todos los esfuerzos necesarios para evitar abusos en la utilización de las cámaras o que se vulnere la seguridad. En segundo lugar, las cámaras sólo deben ser utilizadas para los objetivos inicialmente previstos, cuando se tomó la decisión de este tipo de sistemas: se debe así evitar el fenómeno de *"function creep"* (desvío gradual de la función inicial). Finalmente, se deben operar los sistemas de modo abierto y transparente, y quienes son sus operadores directos deben responder directamente al público. Aunque inevitablemente la instalación de cámaras de vigilancia en el espacio público tenga consecuencias negativas en la vida privada de la gente, garantizando que se cumplan los pasos mencionados anteriormente los operadores y administradores de la vídeovigilancia pueden disminuir la pérdida de privacidad y garantizar una vigilancia lícita y adecuada al mismo tiempo.

---

[6] von Hirsch, A. (2000), "The Ethics of Public Television Surveillance" in von Hirsch, A., Garland, D. and Wakefield, A. (eds.) *Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing: Oxford)

[7] "Restricciones legales – Vigilancia y derechos fundamentales", Discurso de Giovanni Buttarelli, Supervisor Adjunto Europeo de Protección de Datos, en el Palacio de Justicia, Viena, 19 de junio de 2009 (se lo pueden consultar en: www.edps.europa.eu/.../site/.../09-06-19_Vienna_surveillance_EN.pdf)

Vídeovigilancia, libertad de expresión y libertad de asociación

Aunque resulte evidente que las cámaras de vídeovigilancia tienen serias consecuencias en la vida privada de las personas, la utilización de tecnologías de vigilancia en el espacio público por parte de la policía y de los gobiernos locales pueden asimismo socavar otro derecho humano fundamental. La vídeovigilancia, en particular, tiene la capacidad de desalentar a la gente en cuanto al ejercicio de la libertad de expresión y de la libertad de asociación en lugares públicos. Ambos derechos son esenciales a la idea de autogobierno democrático y deben ser protegidos, garantizando a los individuos la libertad de organizarse políticamente, de criticar las decisiones que tomen las autoridades electas, y de obligar al gobierno a rendir cuentas. Si los ciudadanos saben que pueden ser filmados cada vez que participan a una manifestación pública o a una marcha de protesta, hay un verdadero peligro que la presencia de cámaras de vídeovigilancia pueda tener efectos negativos substanciales en esos derechos, conduciendo eventualmente a una reducción de la libertad política y de la participación democrática.[8] Este punto ha sido reconocido recientemente por el Departamento de Seguridad Interior de Estados Unidos, en una evaluación privada de los sistemas de vídeovigilancia operados por el Ministerio de Aduanas y de Inmigración de Estados Unidos

Las cámaras pueden suministrar al gobierno grabaciones sobre lo que los individuos dicen, hacen y leen en el espacio público, por ejemplo, identificando a los individuos que participan en determinada manifestación pública o la asociación de una personas con otras. Esta situación puede desalentar las libertades constitucionalmente garantizadas de libre expresión y asociación."[9]

Dado que esta tecnología podría constituir una amenaza a la libertad de expresión y de asociación, es importante que la vídeovigilancia sólo se emplee para prevenir el crimen y promover la seguridad pública, y en ningún caso con el fin de recoger información sobre las opiniones políticas o las actividades de los ciudadanos. Cuando, por ejemplo, la policía utilice la vídeovigilancia para hacer un seguimiento de una marcha de protesta con el fin de mantener el orden público o prevenir la violencia, deben ser tener cuidado de no conservar imágenes de individuos, a menos que estén destinadas a ser utilizadas en una investigación criminal. Del mismo modo, cuando se registren imágenes de una persona con el fin de acusarlo por un delito penal, esas imágenes no deben comunicarse ulteriormente a los servicios de seguridad u a otras agencias que hacen cumplir la ley, a menos que existan razones de peso para hacerlo.

Además de estas restricciones, la policía y demás usuarios de los sistemas de vídeovigilancia del espacio público deben hacer todo lo necesario para que la gente esté perfectamente informada del propósito, las operaciones y las normativas que rigen el sistema. Para evitar que la vigilancia tenga efectos nefastos, no basta con restringir la utilización de la vídeovigilancia y adoptar medidas de protección de la privacidad robustas. El público también debe tener confianza en que no se abusará de los sistemas y que a largo plazo tampoco se los empleará con fines políticos. Esto reviste singular importancia en países que

[8] Como ha argumentado Keith Boone, la privacidad es "vital para una sociedad democrática [porque] respalda la libertad de votar, de participar en debates políticos, y de asociarse libremente, fuera de la mirada de los ojos públicos y sin temor a represalias." Por consiguiente, si los sistemas de vigilancia constituyen una amenaza para la privacidad, también constituyen una amenaza para la libertad política. Véase Boone, C. K. (1983), "Privacy and Community", Social Theory and Practice 9(1): 8.

han tenido una reciente transición hacia un sistema democrático, países en los cuales el recuerdo de la represión política debe ser probablemente vivaz. Es muy difícil lograr que la gente tenga confianza en la policía y en el gobierno, una confianza que se pierde con facilidad, y no es difícil concebir cómo un uso indebido de la vídeovigilancia con fines políticos o cualquier otro fin ilegítimo, podría socavar esa confianza.

Reconciliar la seguridad policial y material con los derechos

"Existen circunstancias en las que es legítimo y necesario sacrificar hasta cierto punto la privacidad y otros derechos fundamentales, en aras de la seguridad. Nuestra sociedad debe ser capaz de defenderse a sí misma del mejor modo contra las amenazas. No obstante, el peso de la prueba siempre debe estar del lado de quienes declaran que tales sacrificios son necesarios y que todas las medidas propuestas son instrumentos eficaces para proteger la sociedad."
Giovanni Buttarelli, Supervisor Adjunto Europeo de Protección de Datos,
Viena, junio de 2009[10]

Uno de los interrogantes más difíciles a los que debe responder la sociedad se refiere a cuál es el mejor modo de conciliar el ansia de mayor seguridad policial y material de la gente con la necesidad de respetar y proteger los derechos de las personas. A pesar de que las cámaras de vídeovigilancia el espacio público, como las calles y el centro de la ciudad, pueden cumplir un papel fundamental en la reducción del crimen y del desorden, también pueden constituir una seria amenaza de los derechos políticos y de los individuos. Por lo tanto, es vital que la policía y demás usuarios de los sistemas de vídeovigilancia tengan muy presente las siguientes afirmaciones

cuando participen en cualquier clase de vigilancia del área pública:

➤ *La vídeovigilancia infringe inevitablemente el derecho de los individuos a la privacidad.*
Por lo tanto, la policía y los gobiernos locales deben garantizar que pueden dar una justificación convincente y legítima del uso de cámaras en el espacio público, y que desarrollen sistemas de control y rindan cuentas de que buscan minimizar los efectos negativos de la vigilancia en la vida privada.

➤ *La vídeovigilancia constituye una amenaza significativa al ejercicio de la libertad política.*
Dado que la vigilancia de las áreas y eventos públicos tiene el potencial de socavar considerablemente la capacidad y el deseo en los individuos de ejercer sus derechos de libertad de expresión y de asociación, la vídeovigilancia nunca se debe usar con el fin de recopilar información sobre las actividades políticas o la afiliación de los ciudadanos. Los usuarios de los sistemas de vídeovigilancia debe ser capaces de garantizar que las cámaras no se usarán con fines políticos o para desalentar la realización de protestas o asambleas públicas.

[9] Departamento de Seguridad Interior de Estados Unidos, Privacy Impact Assessment for the Livewave vigilancia por vídeo System (17 de septiembre de 2009). Este punto también ha sido analizado por Buttarelli, que afirma lo siguiente: "La vigilancia por vídeo puede desalentar comportamientos legítimos tales como protestas políticas en apoyo de causas impopulares. Los participantes tienen tradicionalmente el derecho a participar anónimamente en asambleas pacíficas, sin ser identificados ni sufrir repercusiones ulteriores. Esto está cambiando fundamentalmente." Véase: "Restricciones legales – Vigilancia y derechos fundamentales", Discurso de Giovanni Buttarelli, Supervisor Adjunto Europeo de Protección de Datos, en el Palacio de Justicia, Viena, 19 de junio de 2009, p. 8.
[10] "Restricciones Legales – Vigilancia y Derechos Fundamentales", Discurso de Giovanni Buttarelli, Supervisor Adjunto Europeo de Protección de Datos, en el Palacio de Justicia, Viena, 19 de junio de 2009, p.4 (se lo pueden consultar en: www.edps.europa.eu/... /site/.../09-06-19_Vienna_surveillance_EN.pdf).

➤ *El público debe tener confianza en que los usuarios de los sistemas de vídeovigilancia respetan sus derechos.* Quizás lo más importante de todo, el público debe tener confianza en que los usuarios de los sistemas de vídeovigilancia respetan sus derechos, suministrando las pruebas necesarias para consolidar esa confianza. Aun cuando la vídeovigilancia no se use indebidamente, si la gente piensa que sus derechos son vulnerados entonces la presencia de cámaras socavará la confianza en la policía y en el gobierno. No basta con que los usuarios de los sistemas de vídeovigilancia respeten los derechos de las personas, sino que la gente debe tener confianza en que también se comprometen a proteger la vida privada y respetar el derecho de libre expresión y de asociación.

El uso de sistemas de vídeovigilancia en áreas públicas requiere obligatoriamente que la policía y otros organismos públicos se confronten a una de las tensiones más fundamentales de las sociedades democráticas modernas: se trata de la pugna entre la exigencia de seguridad y nuestro compromiso compartido de protección de los derechos de las personas. Para reconciliar con éxito estos dos objetivos antitéticos, la policía y demás organismos de control deben reconocer que incumbe al Estado justificar por qué autoriza la observación de los ciudadanos, y que no incumbe a los ciudadanos explicar por qué no desean ser observados. En la medida en que se olvida esta verdad fundamental, sólo es cuestión de tiempo hasta que los sistemas de vigilancia amenacen los derechos.

Los sistemas de vídeovigilancia: lecciones útiles de una cultura de la vigilancia

Peter Squires, *Universidad de Brighton (Reino Unido)*

El avance de la vídeovigilancia en el Reino Unido constituye una oportunidad de aprendizaje inestimable para otras sociedades, aunque a ojos de algunos incluso una afirmación como esta podría ser un punto de vista excesivamente controvertido. Aunque, como la profesora Marianne L. Gras señaló ya en su trabajo *The Legal Regulation of CCTV in Europe* [La regulación legal de los sistemas de vídeovigilancia en Europa], publicado en el 2004, el Reino Unido se ha situado incuestionablemente a la cabeza de Europa en lo tocante a la *envergadura* de sus inversiones en vídeovigilancia, otros comentaristas no se muestran igualmente convencidos de que los mecanismos nacionales de supervisión legal y política hayan avanzado al mismo ritmo y ni siquiera de que el modelo del Reino Unido deba convertirse en un ejemplo a imitar.

Durante las últimas dos décadas, el Gobierno británico ha liderado las *inversiones* en sistemas de vídeovigilancia a escala mundial. Como afirman sin disimulo representantes del Ministerio del Interior del Reino Unido, «en muchos sentidos, puede decirse que hemos estado a la cabeza del planeta desde el momento en que se introdujeron, en los años setenta, hasta el auge que la instalación y el uso de este tipo de sistemas experimentaron en los noventa». Solo entre los años 1999 y 2003, las autoridades locales del país recibieron un total de 170 millones de libras esterlinas (aproximadamente 200 millones de euros según el tipo de cambio del 2010) en financiación para equipos de vídeovigilancia tras el oportuno concurso público. Esta abundancia de fondos conllevó que en los centros históricos y otros espacios

públicos de toda Gran Bretaña se instalasen más de 680 sistemas de vídeovigilancia.

El rápido despliegue de una tecnología aún poco contrastada hizo que se cometieran numerosos errores, algo que quizá resulta comprensible; a menudo, las lecciones sobre lo que podía o no lograrse con la vídeovigilancia se aprendieron con mucha lentitud, y en ocasiones por las malas. En el 2004, Benjamin Goold, profesor asociado de la Facultad de Derecho de la Universidad de Columbia Británica y ex profesor de Oxford, llegó a decir que si bien el Gobierno estaba dispuesto a sufragar el desarrollo de nuevos sistemas de vídeovigilancia en numerosas ciudades británicas, «aparentemente no tiene demasiado interés en comprobar si realmente funcionan». En consecuencia, la vídeovigilancia creció a gran velocidad en el entorno británico, o al menos bastante más de lo razonable si se tiene en cuenta la falta de pruebas de su eficacia o repercusión, dado que, aparentemente, el uso de sistemas de vídeovigilancia parecía ejercer tan solo un efecto mínimo sobre los índices de criminalidad de las zonas en las que se habían implantado. A pesar de ello, al final acabaron por imponerse unas expectativas en absoluto realistas, impulsadas en parte por una nefasta alianza entre entusiásticos emprendedores policiales, agentes comerciales del sector de la seguridad y ciudadanos atemorizados, de que la vídeovigilancia podía resolver muchos de los problemas de delincuencia y desorden a los que nos enfrentamos en los espacios públicos.

Como concluyó un estudio del Ministerio del Interior llevado a cabo en el 2005:

«Los sucesivos gobiernos exageraron las bondades [de la vídeovigilancia] como respuesta ideal al problema del crimen. Pocos de los que deseaban hacerse con una porción de los fondos disponibles consideraron necesario demostrar la eficacia de la vídeovigilancia, y sin embargo, casi nunca estuvo del todo claro por qué esta constituía

la mejor arma para luchar contra el crimen en circunstancias particulares».

En un momento como el actual, en que otros países empiezan a incrementar la cuantía de las inversiones destinadas a sistemas de vídeovigilancia, la experiencia británica puede servir para extraer lecciones útiles, y contribuir así a mejorar significativamente el proceso de transferencia de políticas, evitar errores, desarrollar mejores prácticas, aclarar puntos problemáticos e incluso ahorrar dinero. También puede hacer realidad algo que hasta ahora había sido una promesa: el desarrollo de políticas «basadas en la evidencia». En un ámbito de la formulación de políticas que llega hasta el epicentro de las cuestiones de la seguridad y el poder del Estado enfrentadas a la privacidad y los derechos individuales del ciudadano, los diferentes aspectos que rodean la gestión, el gobierno y la supervisión de los sistemas de vídeovigilancia en el Reino Unido pueden ofrecer una base útil para que otras sociedades planifiquen mejor sus propias políticas en la materia. Ahora que el Foro Europeo para la Seguridad Urbana (EFUS) avanza hacia la elaboración de un código ético y de buenas prácticas sobre sistemas de vídeovigilancia, la experiencia británica constituye una valiosa fuente de la que sacar lecciones provechosas. Y en un sentido más amplio, también viene a confirmar una verdad incómoda de las políticas de ley y orden, dado que, como apuntó David Garland en su libro *The culture of control* (2001) [La cultura del control], «no se adoptan estrategias de control del crimen [...] porque, como todo el mundo sabe, con ellas se resuelven los problemas».

Las políticas y estrategias se eligen a menudo porque son políticamente oportunas, populares, baratas o congruentes con las prioridades establecidas o porque están amparadas por los intereses dominantes. Como subraya Stephen Savage (profesor de Criminología y director del Instituto de Estudios de Justicia Penal de la Universidad de Portsmouth), una buena parte de las po-

líticas de ley y orden diseñadas en los años noventa tuvo como principales motores la ideología y la política antes que la investigación. También sería plausible pensar que los diferentes concursos públicos organizados por el Ministerio del Interior desde los noventa para promover la instalación de sistemas de vídeovigilancia —y la forma que aquellos adoptaron, consistente en licitaciones para la captación de recursos basadas en asociaciones público-privadas— aspiraban no solo a impulsar las alianzas orientadas a la prevención del crimen en el ámbito local, sino también a financiar la vídeovigilancia en sí misma. Incluso podría argumentarse que la industria británica de la vídeovigilancia fue la gran beneficiada de una combinación de circunstancias única y de su propia publicidad, ingeniosa y muy lograda. Convendría hacer las cosas de una forma muy distinta si se nos presenta una segunda ocasión.

En un momento en que las amenazas que parecen representar el crimen, la violencia, el desorden y el terrorismo generan nuevas necesidades en materia de seguridad, y en que las empresas del sector están detectando mercados todavía por explotar y muy lucrativos, la comunidad investigadora debería hacer dos cosas:

asegurarse de que las medidas de prevención del crimen adoptadas se traduzcan realmente en los beneficios anunciados en cuanto a reducción del crimen,

velar por que dichas medidas no acaben convirtiéndose en una vía económicamente costosa de intensificar una política de ley y orden ya de por sí muy tensa y a menudo disfuncional, por ejemplo dotando a la policía de poderes aún mayores frente a los derechos de los ciudadanos; reforzando las fronteras sociales problemáticas entre los «ciudadanos (presuntamente) inocentes» y «los demás»; demonizando a la juventud y a otros colectivos «visibles»; subvencionando la seguridad de las clases acomodadas y redistribuyendo (esto es, desplazando) los riesgos vinculados al crimen hacia segmentos de población ya de por sí vulnerables, y facilitando la aparición de

un orden público más reacio a asumir riesgos y, por ende, menos dispuesto a rendir cuentas.

El escritor y comentarista social francés Loic Wacquant ha catalogado las tendencias de este tipo registradas en los EE.UU. a lo largo de la última década y advierte sobre el peligro de que los europeos sigan su estela y traten de combatir los problemas vinculados al crimen y el desorden recurriendo únicamente a la justicia penal y a las medidas de seguridad. En este sentido, observa que «cualquier política que pretenda abordar incluso los delitos más violentos solo con los medios de la justicia penal está condenada al fracaso… y a agravar el mal que supuestamente debía curar».

Por ello, la adopción de la vídeovigilancia según el modelo aplicado en el Reino Unido, que más bien parece una búsqueda de la panacea universal acompañada de una oleada populista pero mal informada de apoyo público, no representa un camino que uno aconsejaría a otros países seguir necesariamente o a ciegas. Y ello no se debe tanto a que la tecnología simplemente no haya dado los frutos anunciados (muchos de estos, de todos modos, eran de por sí exagerados, poco realistas e irrazonables), sino más bien al hecho de que la implantación de la vídeovigilancia da por sentado, sin que lo esté, otras muchas preguntas en torno al cumplimiento de la ley y las prácticas de mantenimiento del orden, aspectos todos ellos que requieren un estudio serio si se pretende que este recurso tecnológico se integre eficazmente en las infraestructuras de la justicia penal y la seguridad.

Fuera del Reino Unido, la ciudadanía y las autoridades políticas pueden responder a estas preguntas de formas muy distintas, y tal vez prefieran utilizar las cámaras de vídeovigilancia para solucionar otros problemas. Ahí radica, en cierto sentido, el quid de la cuestión: lo que deberíamos preguntarnos no es tanto «¿para qué pueden servirnos las cámaras de vídeovigilancia?», sino más bien «¿qué problemas queremos abordar y cómo puede ayudarnos en ello la vídeovigilancia?».

Perspectivas en torno al mantenimiento del orden

En el año 2007, al admitir que aún había un «debate» abierto sobre «hasta qué punto es eficaz la vídeovigilancia para reducir y prevenir el crimen», el Ministerio del Interior y la Asociación de Jefes de Policía (ACPO) del Reino Unido fueron lo suficientemente francos como para reconocer que, aun cuando la vídeovigilancia ha supuesto una contribución destacada a «la protección del público y una ayuda para la policía», ello había sido posible «*a pesar de que* los sistemas de vídeovigilancia se estaban desarrollando de una manera poco sistemática, con escasa regulación, control o dirección estratégica, un enfoque que no ha permitido maximizar el potencial de nuestra infraestructura de vídeovigilancia». Esta «falta de visión coordinada en torno al desarrollo de la vídeovigilancia», según el informe, «plantea riesgos significativos en lo tocante a la compatibilidad de sistemas, el coste del acceso a las imágenes y la posible pérdida de eficacia operativa».

Sin embargo, y como ya hemos señalado previamente, bajo estas cuestiones fundamentalmente operativas (utilidad, impacto y eficacia) subyacen otras muchas relacionadas con temas tales como la democracia, los derechos, la ciudadanía, la supervisión, la rendición de cuentas y el resarcimiento, todos los cuales afectan a la confianza pública y a la fe en las fuerzas de mantenimiento del orden. Las sociedades que desarrollen sistemas propios de vídeovigilancia también tienen que abordar estos aspectos, y no solo los de orden técnico.

De todos modos, y a pesar de la buena disposición demostrada por la policía a la hora de encajar unas críticas que la comunidad científica, investigadora y evaluadora había estado reiterando durante casi una década o más, la respuesta no ha comportado el desmontaje de ninguno de los complejos sistemas de vídeovigilancia actualmente instalados. Más bien podría decirse que se ha presentado una «estrategia nacional» para corregir los fallos de la «exponencial y altamente irregular»

expansión que la vídeovigilancia ha experimentado durante los últimos años. Evidentemente, no sería la primera vez que los responsables de formular políticas en materia de justicia penal reclaman «más y mejor» de algo para subsanar los supuestos fallos de una dosis previa y aparentemente insuficiente de la misma solución.

Tal vez no deba extrañarnos, por tanto, que la Asociación Británica de Empresas de Seguridad no quiera saber nada del asunto, y que su portavoz incluso haya apuntado que si el crecimiento de los sistemas de vídeovigilancia se produjo de forma irregular, los errores de fondo había que buscarlos en los cuerpos policiales, que no habían sabido aprovechar todo el potencial de sus propios sistemas. Parece que, como ocurre en otros ámbitos de la justicia penal, se impone una desagradable tendencia al pensamiento circular. Sean cuales sean los problemas asociados a la vídeovigilancia, la solución que se plantea es más vídeovigilancia, y tanto las fuerzas del orden como las empresas del sector de la seguridad parecen estar totalmente de acuerdo en este punto tan simple. La clave, sin embargo, y esa es la lección que deberían extraer otras sociedades, consiste precisamente en tratar de reflexionar sobre el tema fuera de los estrechos límites de esta caja, incluso yendo más allá de este punto de vista que sienta la cámara de vídeovigilancia.

En fechas todavía más recientes, otra voz procedente de las fuerzas de mantenimiento del orden se ha hecho oír para proclamar su apoyo entusiasta a la vídeovigilancia. En su controvertido libro de memorias, publicado con el título *The Terrorist Hunters* [Cazadores de terroristas], Andy Hayman, antiguo subcomisario de la policía londinense, escribió sobre la significativa aportación que, a su entender, estaban suponiendo las tecnologías de vídeovigilancia para mantener el orden en el mundo contemporáneo: «A pesar de la preocupación de los grupos de defensa de las libertades civiles, la sociedad de la vigilancia con cámaras, los dispositivos de escucha y las

bases de datos que graban nuestras comunicaciones telefónicas y mensajes de correo electrónico, las fichas de antecedentes penales y sanciones de tráfico y todo aquello que se nos ocurra merece la pena cuando se trata de atrapar a delincuentes y terroristas».

Este breve comentario, con los puntos que menciona explícitamente y los que calla, entronca con una buena parte de los temas que llegan hasta el mismísimo núcleo de muchas de las preguntas planteadas en torno al papel de la vídeovigilancia en una gestión eficaz de la seguridad pública.

En primer lugar, Hayman destaca la aportación de las tecnologías de vigilancia «a pesar de la preocupación de los grupos de defensa de las libertades civiles», como si necesariamente tuviera que haber siempre una contradicción intrínseca entre el mantenimiento del orden y la libertad. Sin embargo, no existe ninguna razón por la que tenga que ser forzosamente así, aunque este debate nos retrotrae a la época en que se crearon los primeros cuerpos policiales uniformados en Londres. Como subrayó en su día Robert Peel, fundador de la policía londinense en el año 1829, «la libertad no consiste en que tu casa sea asaltada por bandas de ladrones organizadas y en dejar cada noche las principales calles de Londres en manos de vagabundos y mujeres borrachas. Una vigilancia bien establecida, correctamente gestionada y eficazmente supervisada permite mejorar la seguridad de bienes y personas y también la libertad».

Hayman, sin embargo, alude asimismo a unas tecnologías de vigilancia *distintas de las cámaras*, argumentando que todo este ámbito de la gestión de la seguridad y el mantenimiento del orden ha cambiado con gran celeridad a lo largo de los últimos años, hasta el punto de que las implicaciones sociales, la legislación y los principios de gobernanza no siempre han sabido evolucionar al mismo ritmo que el potencial de las herramientas tecnológicas. Y no obstante, cuando esas tecnologías se

utilizan de una forma que nunca fue la originalmente pretendida, corremos el riesgo de que se produzca una especie de «cambio de rumbo de la misión» que, a su vez, comporte inversiones costosas e inadecuadas y la adopción de supuestas soluciones («parches tecnológicos») de nula eficacia, lo cual se traduciría en el lógico escepticismo y desilusión cuando el sistema no arrojase los resultados previstos.

Es indudable que algunos de estos problemas se han dado ya en conexión con el uso de la vídeovigilancia en el Reino Unido, como ejemplifican los que se plantearon durante la investigación de los atentados suicidas del 2005 en Londres «en relación con la falta de integración [del sistema], la calidad de las imágenes y las dificultades asociadas a la hora de recuperar material filmado con tecnología digital», según ha reconocido la propia ACPO. Es más, al menos un estudio ha concluido que la mejora del alumbrado en las vías públicas podría tener un efecto preventivo mayor en los índices de criminalidad que la vídeovigilancia (Farrington y Welsh, 2002), aparte del hecho de que iluminar calles y plazas resulta mucho más barato.

Análogamente, Hayman habla de emplear tecnologías de vigilancia para «*atrapar* a criminales y terroristas», cuando en el Reino Unido la implantación masiva de sistemas de vídeovigilancia en espacios públicos estuvo basada en el potencial que las cámaras ofrecían para la prevención del crimen. Al operar desde el paradigma de la *prevención situacional del delito*, se asumía que la vídeovigilancia disuadiría a los delincuentes de sus propósitos criminales por el mero hecho de hacerlos visibles e identificables y de llevar a unas zonas relativamente desprotegidas el principio de la «tutela» extraído de la teoría de la actividad rutinaria.

Ambos enfoques sugerían la existencia de algún tipo de conexión entre vigilancia y *elección racional*, es decir, que el hecho de saberse observado y grabado en una cinta de vídeo influiría en el comportamiento de los

delincuentes y los disuadiría de su propósito de delinquir. En la práctica, sin embargo, se demostró que la vídeovigilancia ejercía una influencia relativamente limitada en ciertos tipos de delitos, como por ejemplo la violencia interpersonal (quizá por los efectos del alcohol). Lo cierto es que, de casi todos los programas de evaluación creados al objeto de monitorizar la eficacia real de las cámaras de vídeovigilancia para la reducción de la delincuencia en el centro urbano, pocos iban más allá de valorar meramente el efecto de estas herramientas tecnológicas sobre la tendencia general de los índices de criminalidad. Aún más escasos eran los estudios que profundizaban lo suficiente como para analizar la vídeovigilancia en relación con la gestión de incidencias, la obtención de pruebas, la preparación del caso y las acciones judiciales subsiguientes, aun cuando los propios agentes de policía se daban cuenta de que precisamente en estos aspectos se situaban algunas de las principales ventajas de los sistemas de vídeovigilancia.

Un último tema relacionado con el comentario de Hayman es el que afecta a lo que podríamos denominar *óptica policial.* Los más fervientes partidarios de la vídeovigilancia son a menudo los propios policías, y cuando se les ofrece la oportunidad de utilizar una nueva tecnología de control del crimen es lógico que sientan un vivo interés por probarla. Sin embargo, la policía no es necesariamente el organismo mejor dotado para realizar un análisis del problema, y en el Reino Unido la vídeovigilancia se ha asemejado durante mucho tiempo a «una cura en busca de una enfermedad que sanar». Es posible que ciertos comentaristas hayan tenido la intuición clara de que la vídeovigilancia llegaría a influir —y, de hecho, *debería* hacerlo— en los índices de criminalidad, pero hasta la fecha escasean las pruebas que acrediten su eficacia.

Algunas voces escépticas han argumentado que los mandos policiales podrían adoptar la vídeovigilancia para ahorrar recursos mediante la reducción de las

frecuencias de patrullaje en ciertas zonas. En otros momentos se ha puesto en tela de juicio el ejercicio de presiones y la comercialización de la vídeovigilancia por parte de representantes del sector de la seguridad. La comercialización por intereses adquiridos, en efecto, puede haber generado expectativas escasamente realistas sobre lo que podían ofrecer las cámaras de seguridad.

Ante estos dos grupos de intereses potencialmente adquiridos, los argumentos a favor de una evaluación independiente de los programas de vídeovigilancia parecen incontrovertibles. Ello no obstante, las primeras evaluaciones realizadas se limitaron en muchos casos a una simple cuestión de *impacto* en términos de reducción del crimen. El papel potencialmente mucho más trascendental que las tecnologías de vídeovigilancia podrían desempeñar en un extenso abanico de actividades de mantenimiento del orden quedó relegado así a un segundo término, tal vez por falta de amplitud de miras. Pero a la hora de estudiar los sistemas de vídeovigilancia del futuro, y también si lo que se pretende es modernizarlos y desarrollarlos, hay que prestar la atención debida a todos estos temas: y es que, como han reconocido el Ministerio del Interior y la ACPO, los equipos de vídeovigilancia podrían tener que estar preparados para asumir una mayor *variedad* de funciones en un futuro.

Desde el propio equipo de estudios de vídeovigilancia de la ACPO también se han dejado oír quejas en cuanto a que «la calidad de las imágenes grabadas con este tipo de sistemas varía considerablemente», y los casos de los que se tiene conocimiento parecen indicar que «más de un 80% del material filmado mediante cámaras de vídeovigilancia que se entrega a la policía está lejos de resultar idóneo, especialmente si debe utilizarse para fines de identificación primaria».

En lo que a vídeovigilancia atañe, finalmente, las cuestiones de la supervisión por parte de la sociedad civil, la rendición pública de cuentas y el control independiente

revisten una importancia equivalente a la que poseen en otros muchos ámbitos del mantenimiento del orden de las sociedades contemporáneas. Esto no solo es relevante para garantizar la comprensión de los objetivos de la vídeovigilancia por parte del gran público, sino que también contribuye a definir su aceptabilidad y, al incrementar la confianza pública, mejora la eficacia de los sistemas de mantenimiento del orden. Esta es una vertiente de la cuestión que a menudo se deja de lado, como evidencia incluso el reciente documento estratégico sobre vídeovigilancia aprobado por el Ministerio del Interior británico. Aunque el documento reconoce la necesidad de establecer nexos de colaboración entre los distintos departamentos de la Administración, la importancia de los diferentes interlocutores y partes interesadas del ámbito local, y la necesidad de lograr un buen gobierno y supervisión de los planes de vídeovigilancia, se muestra poco elocuente a la hora de detallar los mecanismos locales de rendición de cuentas a los que podrían estar sometidos tales sistemas de vigilancia.

Cierto es que alude a los procesos *nacionales* de inspección y supervisión, como los que llevan a cabo las comisiones de Información y Vigilancia del Reino Unido, pero, en contrapartida, elude toda referencia a los mecanismos locales, aunque habría muchos buenos ejemplos o modelos que podrían tomarse como punto de partida. Y a la inversa, este podría ser un ámbito en el que culturas políticas distintas o tradiciones opuestas en materia de mantenimiento del orden aportarían soluciones alternativas de indudable interés. Al fin y al cabo, de lo que se trata aquí no es de imponer una única solución universal para todas las culturas europeas, sino más bien de sacar a debate una serie de cuestiones que, como demuestra la experiencia, tienen su importancia a la hora de plantearse la vídeovigilancia como opción.

Tal como ya apuntó Gras, algunas tradiciones culturales —por ejemplo, Alemania, Francia, Holanda y Suecia— podrían reivindicar regímenes normativos más estrictos

que los aplicados en el Reino Unido. En la ponencia que ofreció durante el congreso del EFUS, por su parte, Riches señaló que, en el Reino Unido, la vídeovigilancia se desarrolló de una forma esencialmente pragmática, sin prestar demasiada atención a los temas del control y la rendición de cuentas hasta que los sistemas ya estaban instalados y en servicio.

CONCLUSIONES FINALES

Análisis de problemas e implementación

Si tomamos todos estos temas en su conjunto, podemos extraer algunas lecciones importantes de las experiencias disponibles en el Reino Unido en cuanto a instalación y uso de sistemas de vídeovigilancia. En primer lugar, merece la pena destacar la conclusión un tanto sorprendente a la que llegaron Martin Gill y Angela Spriggs en un estudio elaborado en el 2005 por encargo del Ministerio del Interior británico:

«Sería fácil concluir [...] que la vídeovigilancia no es eficaz: la mayoría de los sistemas analizados no redujo los índices de criminalidad, e incluso en aquellos casos en que sí se registró dicha reducción, esta no se debió fundamentalmente al uso de este tipo de dispositivos; los sistemas de vídeovigilancia, además, tampoco aumentaron la sensación de seguridad de los ciudadanos, y menos aún sirvieron para modificar su comportamiento».

Ante semejante conclusión, uno no puede por menos que preguntarse por qué los sistemas de vídeovigilancia llegaron a popularizarse hasta el punto en que lo hicieron en el Reino Unido. Dejando a un lado las cuestiones políticas, hay que tener en cuenta otros aspectos relacionados con la implementación de la vídeovigilancia que los responsables de seguridad y la policía, en particular, a menudo han tardado demasiado en reconocer y abordar en consecuencia. Como ya pusieron de relieve Gill y Spriggs, sugerir que la vídeovigilancia es un fracaso

resulta igual de engañoso que escuchar las voces excesivamente triunfalistas que desde el sector de las empresas de seguridad trompetean su éxito incuestionable.

Para formarnos una imagen más rica en matices y basada en las evidencias, debemos tener en cuenta diferentes aspectos y analizar una serie de factores.

Los índices de criminalidad *por sí solos* no constituyen necesariamente un buen indicador de los problemas de delincuencia y desorden y de los temores y preocupaciones que afectan a una zona concreta, ni tampoco de la calidad y la opinión de la población acerca de la seguridad en su entorno más inmediato. Por ello, toda iniciativa orientada a la prevención del crimen y al mantenimiento del orden debe tener en cuenta este complejo entramado de factores.

En todo caso, hay que tomar en consideración la variedad y la complejidad de las funciones y los objetivos que debe cumplir un sistema de vídeovigilancia: el desarrollo de inteligencia, la obtención de pruebas, la gestión de incidencias y el mantenimiento del orden. La reducción del delito situacional, ya sea mediante la prevención o por la vía de la disuasión, no es el único resultado posible, y es básico tener claros los diferentes objetivos a cubrir. Tal como el Ministerio del Interior recalcó en su estudio sobre la implementación de proyectos de vídeovigilancia del año 2003: «A la hora de plantearse qué tipo de mecanismos van a utilizarse para la prevención del crimen, es crucial saber definir claramente los problemas de la zona y ser muy preciso en cuanto a las posibilidades que un sistema de vídeovigilancia ofrece para su resolución. Si no existe un buen encaje entre unos y otras, la vídeovigilancia no es la solución apropiada».

Los sistemas de vídeovigilancia, finalmente, deben integrarse en las iniciativas de mantenimiento del orden y de gestión del delito previamente existentes. Ello podría comportar la necesidad de modificar otros procesos relacionados también con el mantenimiento del orden. Sin

duda, era muy poco realista imaginar que los sistemas de vídeovigilancia ejercerían un efecto continuado por sí solos. Análogamente, las prioridades en materia de mantenimiento del orden tenían que haberse fijado en función de los problemas que exigían una solución, y no estar motivadas por suposiciones apriorísticas sobre la necesidad de instalar cámaras de seguridad.

En 1999, el servicio de asesoramiento del Ministerio del Interior para las asociaciones especializadas en el desarrollo de la vídeovigilancia ya insistía en que toda solicitud de financiación debía especificar «los criterios para identificar un mecanismo de prevención del crimen apropiado». Es decir, que todas las propuestas de instalación de sistemas de vídeovigilancia tenían que apoyarse en la acreditación de unos «principios de reducción del crimen teóricamente sólidos que sugiriesen mecanismos causales plausibles a partir de los cuales [el sistema de vídeovigilancia] pudiera acometer el problema de delincuencia o desorden planteado en el contexto actual».

En su informe final, sin embargo, Gill y Spriggs señalaban que, aun cuando los proyectos de vídeovigilancia tuvieran objetivos claramente perceptibles «que debían detallarse en la documentación presentada al concurso», estos «a menudo no regían el proyecto en su conjunto [...] y raramente estaban integrados en la práctica cotidiana». Así que, aun cuando las solicitudes de financiación sí contenían una justificación y un análisis de los problemas a resolver, estos a menudo quedaban relegados al olvido en cuanto se obtenían los fondos solicitados.

Reducción del crimen y consecuencias para la seguridad colectiva

Al aseverar que «hay un debate abierto sobre hasta qué punto es eficaz la vídeovigilancia para reducir y prevenir el crimen», el documento *Estrategia nacional sobre vídeovigilancia* emitido en el 2007 por el Ministerio del

Interior trataba precisamente de alentar ese mismo debate, algo que no debería extrañarnos demasiado. De hecho, la suma de las evidencias obtenidas a partir de las investigaciones y evaluaciones llevadas a cabo, y que es una combinación de resultados bastante heterogéneos, poco espectaculares y en algunos casos incluso decepcionantes o escasamente fiables, compone una historia francamente interesante.

Muchas evaluaciones de sistemas de vídeovigilancia locales se llevaron a cabo en el Reino Unido siguiendo la estela de las sucesivas oleadas de instalación de equipos de este tipo, aunque no siempre estuvieron avaladas por una metodología rigurosa y a menudo se limitaron a meras valoraciones de *impacto*. En un buen número de casos, además, se realizaron tan a corto plazo que no permitían obtener pruebas fiables de una posible influencia sobre patrones y tendencias de criminalidad. Dicho esto, sin embargo, también hay que reconocer que con el tiempo empezaron a surgir proyectos comparativos y/o de mayor envergadura, y que poco a poco se fue perfilando un cuadro cada vez más nítido de las experiencias de evaluación acumuladas.

En el año 2002, Brandon Welsh y David Farrington llevaron a cabo, para el estudio de investigación del Ministerio del Interior, un examen de 46 proyectos de evaluación de vídeovigilancia procedentes de todo el mundo.

Los resultados fueron más bien variados: si en la mitad de los estudios examinados «se observó un efecto positivo sobre la criminalidad», en cinco se constató un impacto «no deseable» y en otros cinco no se detectó ningún tipo de efecto significativo. En líneas generales, los programas de vídeovigilancia del Reino Unido arrojaron un abanico de repercusiones más amplio que los implantados en Norteamérica. Es más, la vídeovigilancia demostró «no influir en los delitos violentos, pero [...] sí tener un efecto positivo apreciable sobre los delitos contra los vehículos» y los cometidos en aparcamientos de coches. «En el centro de la ciudad y en complejos de

viviendas de protección oficial», finalmente, «se demostró que la vídeovigilancia comportaba una mínima reducción de la criminalidad de aproximadamente el dos por ciento en las zonas ensayadas frente a las de control».

Al tiempo que destacaban que los «estudios de vigilancia» constituían todavía un ámbito de trabajo relativamente nuevo, los autores insinuaban la necesidad de seguir investigando tanto sobre las condiciones óptimas para garantizar la eficacia de los sistemas de vídeovigilancia como sobre mecanismos que pudieran ofrecer resultados positivos; parecía obvio, así pues, que si se pretendía cosechar unos frutos óptimos, primero había que definir un paquete de intervenciones apropiado. Welsh y Farrington concluían, con cierto optimismo, que «la vídeovigilancia reduce el crimen en una pequeña proporción», y acababan formulando una recomendación: «En el futuro, los sistemas de vídeovigilancia deberían implantarse con sumo cuidado en entornos diferentes, e incorporar planes de evaluación de alta calidad con periodos de seguimiento prolongados en el tiempo. A fin de cuentas, una visión de la prevención del crimen basada en la evidencia y que utilice los recursos científicos más avanzados es la que ofrece la fórmula más sólida para construir una sociedad segura».

Conclusiones como las que acabamos de exponer en torno a los efectos de la vídeovigilancia se han visto confirmadas por otros muchos estudios similares, y especialmente por el ambicioso estudio de ámbito nacional elaborado por Gill y Spriggs en el año 2005. Estos autores también concluyeron que la vídeovigilancia parecía resultar escasamente eficaz para reducir la criminalidad en los centros urbanos y en zonas residenciales, y que, en contrapartida, conseguía los mejores resultados en espacios relativamente limitados y con un acceso controlado (hospitales, aparcamientos de coches, centros comerciales, etc.). Asimismo, influía escasamente en los delitos relacionados con el consumo de al-

cohol y los actos de violencia no deliberados, mientras que arrojaba mejores resultados en delitos con un mayor grado de premeditación.

Al igual que en otros estudios, también señalaron la presencia de un «efecto halo» (es decir, la reducción de la criminalidad en áreas colindantes) y un desplazamiento de los delitos. Las características técnicas de cada sistema concreto parecían ejercer una influencia marginal, ya fuera en positivo o en negativo, sobre la eficacia del mismo, pero carente de relevancia en términos generales.

Finalmente, las encuestas realizadas al público en todas las áreas cubiertas por los sistemas de vídeovigilancia estudiados pusieron de manifiesto la escasez de indicios de que se hubieran producido cambios significativos en el comportamiento de los sujetos o bien en los niveles de temor o preocupación por la delincuencia.

Gill y Spriggs concluían en su trabajo que «de acuerdo con las evidencias aportadas en este informe, la vídeovigilancia no puede considerarse un éxito; además de tener un coste económico muy elevado, no ha aportado los beneficios previstos». Sin embargo, también subrayaban el hecho de que se estaban extrayendo lecciones valiosas y de que la tecnología mejora día tras día a pasos agigantados gracias a la introducción de nuevos sistemas biométricos y de reconocimiento del comportamiento, unos sistemas «inteligentes», proactivos y «basados en eventos» que ofrecen nuevas oportunidades en materia de gestión de la seguridad... aunque, al mismo tiempo, también plantean unos retos y amenazas desconocidos hasta la fecha.

Ante todo, su conclusión «basada en la evidencia» constituye una advertencia frente a la tentación de lanzarse a la búsqueda de soluciones técnicas. La vídeovigilancia no es más que una herramienta, y en aquellos casos en que se ha percibido que había fallado, a menudo se ha debido a que las expectativas depositadas en ella eran demasiado ambiciosas o a que se utilizó en es-

pacios poco apropiados para solucionar problemas igualmente inadecuados. En estos supuestos, es posible que la vídeovigilancia se haya planificado mal o puesto en práctica de forma incorrecta, y también cabe la posibilidad de que no se haya integrado eficazmente con el resto de las estrategias de seguridad y sistemas de mantenimiento del orden colectivos.

Según Kevin Haggarty, un criminólogo canadiense que escribe sobre temas de vigilancia, tal vez uno de los mitos más seductores que debamos cuestionarnos sea la suposición, aparentemente tranquilizadora, de que existen «soluciones de vigilancia» para afrontar problemas sociales. Lo que el Ministerio del Interior calificaba en el 2007 de «búsqueda [...] de la panacea de la vídeovigilancia» podría ser en vano. Y es que este tipo de «soluciones» seguirá generando en el futuro, sin duda alguna, otros problemas y dilemas que habrá que plantearse.

En este apartado, los temas a tratar podrían ser, entre otros, la cuestión de quién es el más beneficiado por el amparo que brinda la vigilancia protectora: en los centros de las ciudades británicas, los sectorescomerciales con tiendas de categoría fueron los primeros grandes beneficiarios de este tipo de medidas, en contraposición a las zonas residenciales, los parques infantiles y las escuelas. Y no es que representasen necesariamente la máxima prioridad en la agenda municipal de seguridad o bien que fuesen las áreas más necesitadas: lo que ocurría es que la naturaleza de los sistemas de financiación aplicados en los primeros programas hacía que fueran precisamente los ocupantes de estas zonas los que más fácilmente podían permitirse afrontar los costes de una inversión basada en financiación mixta. Llegados a este punto, surge otro tema relacionado con la desigualdad: ¿a quién enfocan mayoritariamente las cámaras?, o, dicho de otra manera, ¿quiénes son los que más a menudo están *bajo vigilancia*? Y es que

todo proceso de vigilancia lleva asociados temas éticos y sociales de gran calado.

Estas cuestiones éticas también afectan a la definición de los problemas de seguridad y criminalidad que intentamos resolver, así como al diseño, seguimiento e integración de los sistemas desarrollados. Además, repercuten en los procesos de supervisión, control, evaluación, rendición de cuentas y resarcimiento que deben formar parte de toda estrategia eficaz de seguridad colectiva. Si estos temas no reciben la atención necesaria desde el primer momento, con toda probabilidad acabarán surgiendo problemas que minimizarán la eficacia del propio sistema. Por más sofisticado que sea un sistema desde el punto de vista técnico, su eficacia estará siempre en función de aquellos que lo utilicen, y únicamente conseguirá incrementar el nivel de seguridad colectiva si satisface las necesidades y proporciona tranquilidad a los ciudadanos a los que pretende dar servicio.

Como ya afirmaron Gill y Spriggs: «De la vídeovigilancia no debe esperarse demasiado. Es más que una simple solución técnica; exige la intervención del ser humano para funcionar con el máximo nivel de eficiencia y los problemas que ayuda a resolver son complejos. [Puede] contribuir a reducir los índices de criminalidad y dar mayor sensación de seguridad a la población y, al mismo tiempo, tiene la capacidad de generar otros beneficios. Para que ello sea posible, sin embargo, se necesita una mayor conciencia de que reducir y prevenir el crimen no es tarea fácil y de que una solución mal planificada difícilmente va a funcionar, por mucho dinero que invirtamos en ella».

REMARQUE : esta es una versión abreviada del documento elaborado por el profesor Squires. La versión completa se puede consultar en línea a través de la siguiente página web: http://www.brighton.ac.uk/sass/contact/details.php?uid=pas1

BIBLIOGRAFÍA

Armitage, R. 2002 *To CCTV or not to CCTV?* London, Nacro.

Brown, B. 1995 *CCTV in Town Centres: Three Case Studies, Crime Prevention and Detection Series,* no.73. London: HMSO. Deane, A. and Sharpe, D. 2009 Big Brother is watching: A comprehensive analysis of the number of CCTV cameras controlled by local authorities in Britain in 2009. London, www.bigbrotherwatch.org.uk

Clarke, R.V. 1995 Situational crime prevention. In M. Tonry and D.P. Farrington (eds.), *Building a Safer Society: Strategic Approaches to Crime Prevention*: Vol. 19. *Crime and Justice: A Review of Research* (pp. 91-150). Chicago, Illinois: University of Chicago Press.

Clarke, R. V. and M. Felson (Eds.) (1993). *Routine Activity and Rational Choice. Advances in Criminological Theory*, Vol 5. New Brunswick, NJ: Transaction Books.

Crawford, A. 1998 Crime Prevention and Community Safety: Politics, Policies and Practices. London, Longman.

Farrington, D.P. and Welsh, B.W. 2002. *Effects of improved street lighting on crime: a systematic approach,* Home Office Research Study 251.

Felson, M. 1998 *Crime and Everyday Life*, Second Edition. Thousand Oaks, CA: Pine Forge Press.

Gras, M.L. 2004 The Legal Regulation of CCTV in Europe. *Surveillance & Society* CCTV Special (eds. C.

Norris, M. McCahill and Wood) 2(2/3): 216-229

Garland. D. 2001 *The Culture of Control,* Oxford, Oxford University Press.

Gill M. and Spriggs, A. 2005 *Assessing the Impact of CCTV.* Home Office Research Study No. 292. London: Home Office Development and Statistics Directorate.

Gill M. et al., 2003 *National Evaluation of CCTV: Early Findings on Scheme Implementation – Effective Practice Guide*. Scarman Centre National Evaluation Team, London, Home Office Development and Practice Report No. 7.

Haggarty, K. D. 2009 'Ten thousand times larger' – Anticipating the expansion of surveillance, in B. Goold and D. Neyland (eds) *New Directions in Surveillance and Privacy*. Cullompton, Willan Publishing.
TV Evaluation Team

Hayman, A. 2009 The Terrorist Hunters: The ultimate inside story of Britain's fight against terror, (with M. Gilmore). London, Bantam Press.

Home Office/Association of Chief Police Officers (ACPO) 2007 *National CCTV Strategy. London*, Home Office.
Hope, T. 2001, Crime victimisation and inequality in risk society, in R. Matthews and J. Pitts (ed.) *Crime, Disorder and Community Safety*. London, Routledge

Honess, T. and Charman, E., 1992, *'Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Police Research Group Crime Prevention Unit, 35, London: Home Office Police Department.

ICO (Information Commissioner's Office) 2008 CCTV *Code of Practice: Revised Edition*. ICO Office, Wilmslow: www.ico.gov.uk

Loader, I. 2008 Evidence to the House of Lords Select Committee on the Constitution: *Surveillance, Citizens and the State*. May 14th 2008.

Norris, C., Moran, J., and Armstrong, G., 1998 Surveillance, *Closed Circuit Television and Social Control,* Aldershot: Ashgate.

Norris, C., and Armstrong, G., 1999 *The Maximum Surveillance Society: The Rise of CCTV*. Oxford, Berg Publishers.

Riches, J. 2006 CCTV: Does it work? EFUS: Zaragoza Conference. http://zaragoza2006.fesu.org/IMG/pdf/CCTV_PresentationJames_RICHES.pdf

Shearing, C. 2000 Exclusion From Public Space. in Ethical and Social Perspectives on Situational Crime Prevention. (eds) A. von Hirsch, D. Garland and A. Wakefield. Oxford, Hart Publishing, 2000.
Short, E. and Ditton, J. 1998 «Seen and Now Heard: Talking to the Targets of Open Street CCTV», *British Journal of Criminology*, 38/3: 404-428.

Skinns, D. 1998 «Crime Reduction, Diffusion and Displacement: Evaluating the Effectiveness of CCTV», in C. Norris, J. Moran, and G. Armstrong (eds.): *Surveillance, Closed Circuit Television and Social Control, Aldershot: Ashgate.*

Squires, P. 2006 Introduction: Asking Questions of Community Safety, in Squires, (ed.) *Community Safety: Critical Perspectives on Policy and Practice*. Bristol, The Policy Press.

Squires, P. and Measor, L. (1996a). *CCTV Surveillance and Crime Prevention in Brighton: Half-Yearly Analysis.*

Brighton: Health and Social Policy Research Centre, University of Brighton.

Squires, P. and Measor, L. (1996b). *CCTV Surveillance and Crime Prevention in Brighton: Follow-up Analysis.* Brighton: Health and Social Policy Research Centre, University of Brighton.

Surveillance Studies Network, 2007 Evidence to the House of Lords Select Committee on the Constitution: *Surveillance, Citizens and the State*. 28th November 2007.

Von Hirsch, A. 2000 The Ethics of Public Television Surveillance, in Ethical and Social Perspectives on Situational Crime Prevention. (Eds) A. von Hirsch, D. Garland and A. Wakefield. Oxford, Hart Publishing.
Wacquant, L. 2009 Punishing the Poor: The Neo-Liberal Government of Social Insecurity, Duke University Press.

Welsh, B. and Farrington, D. 2002 *Crime Prevention Effects of Closed Circuit Television: A Systematic Review, Home Office Research Study*, No.252, London: HMSO.

«Privacy by design» o la protección de los datos personales desde el diseño: el caso de la vídeovigilancia

Por Jeroen van den Hoven
Universidad de Tecnología de Delft (Países Bajos)

➤ Defiendo el principio de la protección de los datos personales (con el método conocido como *«Privacy by design»*) desde el diseño mismo de las aplicaciones de vídeovigilancia que se emplean para mantener el orden y la seguridad. Este método permite superar las profundas controversias ideológicas, políticas y filosóficas que atañen a la naturaleza y la importancia de la protección de los datos personales. La protección de los datos desde el diseño cobra una gran importancia en las políticas de protección de datos y de ingeniería de software. La Unión Europea impulsa esta idea como una nueva norma en sus *Líneas directrices de vídeovigilancia del CEDP* (Bruselas, 17 de marzo de 2010, p. 10):

"La protección de los datos y de la vida privada debería estar incluida entre las especificaciones correspondientes al diseño mismo de la tecnología que utilizan las instituciones, al igual que a sus modos de aplicación".

Hay que privilegiar este enfoque, pero para que esta idea funcione se requieren dos condiciones:

➤1 – Debemos considerar que los métodos de *Privacy by Design* o de *Privacy Enhancing* (que garantizan la confidencialidad de la vida privada) forman parte de un enfoque global de la innovación técnica. Se suele aludir a este enfoque con el término *Value*

Sensitive Design o Design for Values (diseño en el que se tienen en cuenta los valores éticos). Este enfoque requiere una metodología particular con el fin de evitar las improvisaciones en cuanto al desarrollo de software que pudiera favorecer una falta de transparencia y de responsabilidad.

➤2 - *Privacy by Design* sólo puede tener éxito si los valores morales subyacentes a la protección de datos personales son claros y si obtenemos una explicación detallada de las justificaciones morales referentes a la protección de esos mismos datos. En efecto, todas las decisiones que se toman en la etapa de concepción, por ínfimas que sean, deberán justificarse sobre la base de consideraciones morales claras y convincentes.

La protección de la confidencialidad de la vida privada es un tema central en el debate actual, en la mayoría de los países, entre los liberales y los comunitaristas, ya que afecta el equilibrio entre los derechos individuales, los bienes colectivos y los intereses de la comunidad. En lo referente a la vida privada, este debate opone quienes argumentan que es menester proteger la confidencialidad de la vida privada de los individuos limitando el acceso a la información personal, y quienes piensan que es necesario ampliar este acceso en beneficio de la comunidad. Algunos piensan que se trata de una oposición artificial, aunque subsiste cierta tensión en varios casos de violación de la vida privada, por ejemplo cuando se llevan a cabo acciones policiales secretas en Internet, cuando se divulgan expedientes médicos debido al seguro de salud o de investigaciones epidemiológicas, cuando se intercambia información entre diferentes bases de datos para detectar fraudes a la seguridad social, cuando se pide información a quienes suministran acceso a Internet sobre el com-

portamiento en línea de determinados usuarios en casos de justicia penal, o incluso cuando se utiliza la vídeovigilancia en lugares públicos para prevenir acciones criminales.

El filósofo político Michael Walzer hace una observación pertinente en estos términos: "El liberalismo está roído por los problemas que plantean los aprovechadores, personas que siguen gozando las ventajas que procura pertenecer a una categoría o que confiere una determinada identidad, a la vez que han dejado de participar en las actividades que dan lugar a dichos beneficios. En cambio, el comunitarismo es el anhelo de una sociedad sin aprovechadores"1. Los comunitaristas consideran que estas técnicas de información son medios para lograr esta sociedad sin aprovechadores.

La vida privada también ha sido tema de buen número de debates filosóficos (Nissenbaum 2004; Roessler 2005; Decew 1997, van den Hoven 2009) y muchos autores han presentado su punto de vista sobre la definición de la vida privada. Diferentes explicaciones conceptuales y filosóficas ofrecen respuestas diferentes a la pregunta sobre qué es la vida privada y qué razones se invocan para defender su importancia. Desafortunadamente, no se ha llegado a ningún consenso y parece improbable obtenerlo un día.
El concepto actual según el cual la vida privada es algo completamente obsoleto se añade a esta controversia: "Nada de lo que haga está cubierto por el anonimato; pase pues a otra cosa". Debido a la tecnología moderna, la vida privada es algo que pertenece al pasado, situación que deberíamos finalmente aceptar.

Muchos conceptos sirven de base a la idea de vida privada. Su significado exacto no ha sido comprendido de modo cabal, como tampoco lo han sido el

modo en que la afectan la tecnología, el desarrollo de software y de sistemas. Por razones prácticas, como la formulación y la preparación de leyes, al igual que las políticas y la tecnología, los malentendidos en el plano de la concepción y la confusión sobre la naturaleza y la importancia de la vida privada conducen a una indecisión práctica, a un alargamiento de los plazos, a una mayor ineficacia, a mayores costes y a fracasos de proyectos en el ámbito de las TIC.
Es necesario hoy "reconstruir" el concepto de vida privada para progresar y solucionar los problemas urgentes que debemos enfrentar día tras días, sin enredarse en debates interminables.

El papel principal que se concede al concepto de *vida privada* al debatir asuntos morales relativos a la protección de los datos personales oscurece la búsqueda de soluciones prácticas. Nos quedamos así bloqueados en una profunda controversia, sin solución, sobre la naturaleza del Sí mismo y de la Comunidad, que opone a liberales y comunitaristas. Como no es nada sencillo tomar partido por uno u otro, sugiero que abordemos el problema desde otro punto de vista, planteándonos sencillamente la pregunta siguiente: ¿Por qué deberíamos proteger los datos personales? ¿Qué razones morales nos empujan a hacerlo? ¿Podemos pensar que deberíamos protegerlos del mismo modo que protegemos, digamos, los reactores nucleares, los manuscritos medievales, los bebés o las reservas de aves? En cada uno de estos casos, tenemos buenas razones para restringir el acceso, limitar las horas de visita, estipular un comportamiento adecuado, indicar las personas que están autorizadas a acercarse y de qué modo pueden hacerlo. En cada ejemplo, la protección cobra una forma diferente y responde a una lógica diferente. ¿Cuál sería una buena razón moral de proteger los datos personales y qué tipo de razón podría justificar

que se limite el derecho de los demás a consultar esos datos?

Las razones morales por las cuales deberíamos inquietarnos en lo referente a nuestros datos personales son las mismas razones que justifican que limitemos el acceso a nuestros datos y su utilización a terceros. Se trata de las razones siguientes:

Primero, la protección de los individuos cuyos datos personales están a disposición del público. En una sociedad de la información, las personas corren el riesgo de perjudicarse cuando y debido a que sus datos personales están a disposición del público. Desearíamos evitar que se utilicen los datos personales contra sus propietarios.

La segunda razón se refiere a la equidad en el mercado de los datos personales. Protegemos los datos personales y tenemos leyes para ello, porque muchos desearían consultar esos datos fácilmente y a bajo coste. Muchas personas y organismos tienen buenas razones para esconder al público el valor comercial de los datos personales al igual que la utilización que se pueda hacer de ellos. Los contratos que se ofrecen a los clientes garantizando una reserva sobre sus datos personales, como es el caso de las tarjetas de fidelidad, son a menudo injustos. Los regímenes de protección de los datos deberían garantizar acuerdos equitativos y proteger a los ciudadanos contra los abusos e incumplimientos de los contratos.

La tercera razón se refiere a la justa utilización de la información. Los datos individuales tienen, por así decir, un "hábitat natural". La información se reúne e intercambia en situaciones claramente definidas y en manos de grupos específicos como los médicos, la policía, los responsables de recursos humanos, los abogados, etc. No es adecuado comunicar esta información de un ámbito social a otro, por ejemplo, si la información pasa de la esfera médica a la esfera comercial o incluso de la esfera familiar a la esfera

política. Estas esferas deben permanecer separadas unas de otras.

Finalmente, la última razón es que cada individuo tiene derecho a su autonomía moral y al control de la forma de presentarse. La gente desea ser identificada con las personas con las cuales también ella se identifica. Desean que los vean como la persona que piensan ser. Esto requiere discreción y cierta selección de la información personal que revelan. También implica la protección de los datos personales y que se respete la soberanía de cada individuo sobre su propia información personal.

Value Sensitive Design y Privacy by Design (concepción que tiene en cuenta los valores éticos)

La integración de la seguridad y de la confidencialidad de la vida privada en la concepción, ya sea en arquitectura o en ingeniería, no es una idea nueva. Ya desde el siglo 18, el filósofo Jeremy Bentham había imaginado lo que pensaba que sería la arquitectura ideal de las prisiones. Decía: "La moral reformada, la salud preservada, la industria tonificada, la instrucción difundida, las cargas públicas aligeradas, la economía fortalecida – el Nudo Gordiano de las leyes sobre los pobres no cortado sino desecho – ¡todo ello gracias a una simple idea arquitectónica! Su idea era que la seguridad y el control de los prisioneros mejorarían considerablemente con el concepto de una prisión en forma de domo, a la que denominaba "Panóptico". El balcón de observación de los guardias se hallaría así en el centro, a partir del cual podrían observar a los prisioneros que se situarían alrededor. Tal ha sido uno de los primero ejemplos de integración de los conceptos en una concepción. En la actualidad, la incorporación de los valores éticos al concebir cualquier tecnología se denomina concepción o

diseño ético *(Value Sensitive Design o VSD)*. La *Privacy by Design* es una de las aplicaciones del *Value Sensitive Design* (concepción o diseño ético).

La concepción ética *(Value Sensitive Design)* integra los valores morales en la concepción de los objetos y de los sistemas técnicos, considerando la concepción desde un punto de vista ético y a través de investigaciones sobre la forma en la cual los valores morales (por ejemplo, libertad, igualdad, confianza, autonomía, vida privada y justicia) pueden ser favorecidos o frenados por la misma concepción (Friedman 1997; Friedman 2005). La concepción ética *(Value Sensitive Design)* se concentra *esencial y específicamente* en los valores *morales*, mientras que la concepción tradicional se concentra más bien en las exigencias de funcionamiento como la velocidad, la eficacia, la capacidad de almacenamiento o la facilidad de utilización. Aunque el desarrollo de una tecnología amigable pueda tener como efecto secundario un incremento de confianza o una sensación de autonomía por parte del usuario, en la concepción ética *(Value Sensitive Design)*, la integración de los valores morales en la concepción es un objetivo principal, más que un subproducto. La concepción ética *(Value Sensitive Design)* también es "una forma de trabajar éticamente con el fin de integrar los valores morales a la concepción, a la investigación y al desarrollo tecnológicos", como he dicho anteriormente (van den Hoven 2005: 4).
La concepción ética (VSD) sólo puede aplciarse en el ámbito de la protección de los datos, si llegamos a describir claramente los valores morales que deben ser integrados al diseñar un sistema y el modo de traducirlas en "exigencias no operativas". La etapa siguiente consiste en detallar estas exigencias en un conjunto de funciones sumamente claras y precisas que se deben asignar al sistema. Pero esta metodo-

logía todavía no existe y el peligro es que con la evolución de la tecnología los sistemas se vuelvan aún más opacos de lo que ya son.

La concepción ética (VSD) busca conciliar valores diferentes y opuestos en el diseño de ingeniería o en casos de innovación (van den Hoven 2008b). Se la puede aplicar directamente a los valores opuestos que están en juego en el debate sobre la vídeovigilancia: la seguridad y la vida privada.

En nuestra sociedad, concedemos importancia a la confidencialidad de la vida privada pero, paralelamente, cobra importancia la seguridad y la disponibilidad de la información sobre los ciudadanos. Esta tensión se ilustra en los debates sobre la vídeovigilancia de los lugares públicos. O bien aceptamos trocar nuestra vida privada contra la seguridad instalando las cámaras en todas partes, o bien nos negamos a hacerlo en nombre de la confidencialidad de la vida privada y, en consecuencia, aceptamos un menor nivel de seguridad. Con los sistemas inteligentes de vídeovigilancia podemos tener el oro y el moro, ya que su arquitectura inteligente incluye la función de vigilancia con unos sistemas que limitan el caudal y la disponibilidad de la información registrada.

La primera generación de cámaras de vídeovigilancia ofrece relativamente poca seguridad. Las imágenes son borrosas y violan la vida privada de los transeúntes porque registran sus desplazamientos. La segunda generación es de mucha mejor calidad y ofrece así mayor seguridad. Pero, precisamente, dado que la calidad de las imágenes es muy buena resulta que son mucho más invasivas. Ahora, la tercera generación de "sistemas con cámaras inteligentes" registra únicamente los eventos sospechosos y están esquipadas con una función integrada que bloquea la grabación de imágenes dentro de las casas privadas. Esta es la solución tecnológica perfecta a nuestro di-

lema moral. Por ejemplo, la policía de Rotterdam está ya empleando estos sistemas inteligentes, equipados con un software que impide que los usuarios puedan filmar el interior de las casas privadas.
Los parámetros tecnológicos de estos sistemas inteligentes pueden ser configurados de forma sumamente precisa, ofreciendo así todas las ventajas y todas las funciones de una vídeovigilancia de vanguardia, sin violar ninguna norma de protección de los datos personales. Mientras que los sistemas anteriores estaban basados en "todo o nada", ahora contamos con una tecnología con la cual podemos decidir quién consulta los registros, en qué condiciones se almacenan las imágenes, de qué modo se pueden utilizar las grabaciones y en qué condiciones se las puede incorporar a otras bases de datos.
Un rasgo que comparten muchas tecnologías "inteligentes" e innovadoras es que permiten combinar valores o preferencias que antes era irreconciliables. Por ejemplo, las tecnologías medioambientales inteligentes combinan el crecimiento económico y el desarrollo sostenible. Las bombas "inteligentes" alcanzan el enemigo sin hacer víctimas civiles.

Protección de los datos personales en el diseño del sistema: una innovación moral

Parece legítimo afirmar que, dado que la sociedad tiene la obligación moral de garantizar la confidencialidad de la vida privada de sus ciudadanos, garantizando a la vez la seguridad en todos los lugares públicos, también tiene la obligación moral de hacer lo necesario para satisfacer estas dos obligaciones. Estamos moralmente obligados a proseguir la investigación y las innovaciones a partir del modelo de *Privacy by Design*, una tecnología que combina seguridad y confidencialidad de la vida privada.
Esta orientación requiere un ajuste muy preciso de la

tecnología y una reflexión detallada sobre la justificación moral de la protección de los datos. Además, exige una metodología sistémica para vincular ambas cosas: la tecnología y nuestros valores morales.

Bibliografía

Batya Friedman e.a. Value Sensitive Design: Theories and Methods. Technical Reports, Department of Computer Science and Engineering, Universidad de Washington, 2002. Informe del 02-12-01. http://www.urbanism.org/papers/vsd-theory-methods-tr.pdf

Jeroen van den Hoven & John Weckert, Tecnología de la Información y Filosofía Moral. Cambridge University Press, 2009.

Vídeovigilancia urbana en Europa: ¿Una decisión política?

Eric Töpfer, Universidad Técnica de Berlín

La vídeovigilancia urbana se convirtió en tema de discusión por primera vez en 1997, cuando fue seleccionado como uno de los temas clave de la conferencia europea sobre "Prevención del crimen: hacia un nivel europeo", organizada por la Presidencia holandesa de la Unión Europea en Noordwijk (Países Bajos). La declaración de clausura de esta conferencia expresó, en particular, que:

"Las cámaras, como una herramienta para prevenir el crimen, son en general un modo nuevo y rentable de infundir confianza a los ciudadanos que se sienten inquietos por su seguridad, porque disuaden la criminalidad y suministran un elemento de apoyo al ministerio fiscal. [No obstante], los sistemas de vídeovigilancia o circuitos cerrados de televisión (closed circuit television - CCTV) sólo deben ser usados [dentro del marco de trabajo] de una política más amplia, local y/o nacional, de prevención del crimen [...] y deben estar en manos de personal entrenado [...]. El público debe ser advertido de que se emplean estos sistemas y se debe preservar la privacidad."[11]

Estos eran los comienzos de la vídeovigilancia. Tres años antes, en 1994, el Departamento del Interior de Gran Bretaña inició una verdadera "revolución de la cámara de vigilancia", financiando una serie de *Retos*

[11]Recomendaciones de la conferencia europea sobre "Prevención del crimen: hacia un nivel europeo", Noordwijk, 11–14 de mayo de 1997. En: European Journal on Criminal Policy and Research, Vol. 5, Nº 3 (Septiembre de 1997), pp. 65-70 (66).

de la Ciudad (City Challenge Competitions) con un primer tramo de 2 millones de libras. En Francia, el Parlamento votó en 1995 la así llamada *Ley Pasqua*, que autorizaba explícitamente la instalación de sistemas de vídeovigilancia en una serie de áreas "calientes" de las principales ciudades de Francia. Esta iniciativa se produjo después de la controvertida instalación, dos años antes, de 96 cámaras de vigilancia en el suburbio parisino de Levallois-Perret.[13] En la República Checa, el gobierno comenzó a financiar las iniciativas locales de prevención del crimen en 1996, que incluían, entre otras cosas, la instalación de sistemas de vídeovigilancia. El mismo año y siguiendo el ejemplo checo, el departamento de policía local de Leipzig instaló una cámara en el centro de la ciudad, la primera cámara que se haya instalado nunca en Alemania.[14] En Holanda, el primer sistema comenzó a instalarse en 1998, sólo un año después de la conferencia sobre la prevención del crimen de Noordwijk, cuando el Consejo Municipal de Ede decidió instalar 12 cámaras para controlar, durante la noche, una zona que se encuentra cerca de la estación central de trenes.[15]

En referencia a la conferencia de Noordwijk, la delegación francesa inició un debate, a finales de 1998, sobre la vídeovigilancia en el "Police Cooperation Working Party" (PCWP), un grupo de trabajo del Consejo de la Unión Europea. El informe del PCWP concluye que "las autoridades locales recurren poco a los sistemas de vídeo, excepto en el Reino Unido y en Finlandia", y afirma que el mismo PCWP "podría promover el desarrollo de tales sistemas".[16]

¿Buscando ubiquidad?

La vídeovigilancia o la "televisión industrial", como se la denominó inicialmente, es un antiguo sistema

de difusión de televisión. Pero durante varias décadas, la utilización de cámaras de vídeovigilancia se limitó a la supervisión y ordenación del tránsito, o bien de modo ocasional, a la vigilancia de la multitud en asuntos de primordial importancia como las investigaciones criminales. El uso permanente de sistemas de vídeovigilancia del espacio público era una excepción. En el Reino Unido, por ejemplo, los sistemas de vídeovigilancia sólo se habían instalado en unas pocas áreas de interés nacional como Westminster y Whitehall, donde la red de cámaras había sido instalada por la Policía Metropolitana de Londres como consecuencia de los disturbios políticos que se produjeron a finales de los años 60.[17]
Actualmente, 13 años después de la conferencia sobre la prevención del crimen en Holanda, que obviamente dio comienzo a un proceso de transferencia internacional de políticas, se han instalado ya sistemas de vídeovigilancia en miles de ciudades y

[11] Recomendaciones de la conferencia europea sobre "Prevención del crimen: hacia un nivel europeo", Noordwijk, 11–14 de mayo de 1997. En: *European Journal on Criminal Policy and Research*, Vol. 5, Nº 3 (Septiembre de 1997), pp. 65-70 (66).

[12] Norris, C. y otros (2004): The growth of CCTV. A global perspective on the international diffusion of video surveillance in publicly accessible space. En: *Surveillance & Society,* Vol. 2, Nº 2/3, pp. 110-135 (111).

[13] Töpfer, E. & Helten, F. (2005): Marianne und ihre Großen Brüder. Videoüberwachung à la Française. En: *Bürgerrechte & Polizei* /CILIP, Nº. 81, pp. 48-55.

[14] Müller, R. (1997): Pilotprojekt zur Videoüberwachung von Kriminalitätsschwerpunkten in der Leipziger Innenstadt. En: *Die Polizei,* Vol. 88, Nº. 3, pp. 77-82.

[15] Gemeente Ede (2000): *Ogen in de nacht. Eindevaluatie cameratoezicht Ede*. Agosto de 2000. Sitio Internet: http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/bestuurlijk-handhaven/cameratoezicht/1_ede_effectevaluatiex2000.pdf.

[16] Consejo de la Unión Europea: Doc. 5045/99, 12 de enero de 1999.

[17] Williams, C. (2003): Police surveillance and the emergence of CCTV in the 1960s. En: CCTV, ed. por M. Gill, Leicester: Perpetuity Press, pp. 9-22.

pueblos de Europa. Como Steve Graham, profesor de geografía humana de la Universidad de Durham (GB) y uno de los mejores estudiosos especializado en los fenómenos de ciberciudad, anticipó en 1999 que la vídeovigilancia se habría convertido en la "quinta empresa de servicio público" de la vida urbana moderna, después del agua, el gas, la electricidad y las telecomunicaciones.[18]

El desarrollo de los sistemas abiertos de vídeovigilancia del espacio público, entendiendo que la vigilancia de áreas urbanas públicas las 24 horas y los 7 días de la semana, con la expresa finalidad de controlar la criminalidad y mantener el orden público, comenzó en los años 80. Tres factores principales explican este "boom" de los sistemas de vídeovigilancia en las ciudades europeas:

➤ La aparición de un nuevo paradigma en nuestras políticas de justicia criminal, por el cual el enfoque tradicional, que concebía el crimen como un desvío fundamentalmente individual, ha sido reemplazado por la idea de observar bien determinados grupos y lugares, que se consideran "criminógenos". De ahí que el riesgo puede ser evaluado, prevenido y encarado gracias a los métodos actuariales.

➤ El declive de la industria, como base de la economía urbana, y el auge del consumismo y de los servicios, junto con el surgimiento del "marketing de lugares" *(place marketing)* o la "identidad de la ciudad" *(city branding)*. Actualmente, se considera que la seguridad policial y material son elementos claves de la atracción de una ciudad, en la competición global por la inversión y la actividad económica.

➤ La tendencia a la descentralización por la cual los ayuntamientos han debido hacerse cargo del control

de la criminalidad local y del orden urbano. Muchos países han dado un mandato explícito a los ayuntamientos para instalar cámaras de vigilancia en su territorio, con el fin de luchar contra el crimen.[19]

La diversidad de los sistemas de control por vídeo en el espacio público en Europa

Dejando de lado los factores globales que acabamos de mencionar, también es importante tener en cuenta las características propias de cada país europeo, sus contextos socioeconómicos diferentes, sus sistemas institucionales y la experiencia que tienen con el crimen. Como afirma el sociólogo canadiense David Lyon:

"Es verdad que existen algunas semejanzas estructurales y problemas similares que enfrentan (tarde) los Estados modernos, pueden conllevar a la utilización de técnicas similares en diferentes lugares. [...] También es cierto que los contextos culturales, políticos y sociales, tanto locales como regionales, percibirán la vídeovigilancia de diferente modo. [...] La mera existencia de nuevas tecnologías está lejos de ser una razón suficiente, en estos contextos, para utilizarla."[20]

---

[18] Graham, S. (1999): Towards the fifth utility? On the extension and normalisation of CCTV. In: Surveillance, *Closed Circuit Television and Social Control*, ed. por C. Norris y otros Aldershot: Ashgate, pp. 89-112.

[19] Para una discusión teórica detallada, véase McCahill, M. (1998): Beyond Foucault. Towards a contemporary theory of surveillance. En: Surveillance, *Closed Circuit Television and social control,* ed. por C. Norris y otros, Aldershot: Ashgate, pp. 41-65.

[20] Lyon, D. (2004): Globalizing surveillance. Comparative and sociological perspectives. In: *International Sociology,* Vol. 19, Nº 2, pp. 135-149 (141-142).

[21] *Tageblatt. Zeitung für Luxemburg,* 12 de diciembre de 2007.

En el Gran Ducado de Luxemburgo, el primer sistema de vídeovigilancia del espacio público, fue instalado en 2007, 13 años después que Gran Bretaña lanzara su primer *City Challenge Competition.*[21] En Noruega, sólo hay un sistema instalado, con seis cámaras operadas por la policía local de Oslo, la capital, que fue instalado en 1999.[22]

En contraste, en el Reino Unido se considera que hay de 40.000 a 50.000 cámaras instaladas en el espacio público, en más de 500 ciudades.[23] En Francia, más de 500 municipios cuentan con unas 20.000 cámaras en total, la mayor parte en ciudades grandes. Además, el Ministro del Interior francés anunció en 2009 que el número de cámaras en el país se multiplicaría por tres.[24] En los Países Bajos, un quinto de los 443 cuerpos de gobierno local usan sistemas de vídeovigilancia del espacio público, con un total de unas 4.000 cámaras.[25] En Europa Oriental, se sabe que Polonia, la República Checa, Hungría y los países bálticos utilizan cientos de cámaras en sus principales ciudades.

Los países del sur de Europa tienen diferentes posiciones respecto a la vídeovigilancia. Portugal y España son más reacios. Grecia instaló unas 1.200 cámaras para los Juegos Olímpicos de 2004, una iniciativa que generó una protesta generalizada por parte de la población. No obstante, se dejaron instaladas unas 200 cámaras después de los Juegos.[26] En contraste, cientos de ciudades italianas *(communi)* usan actualmente estos sistemas de vídeovigilancia.

En Alemania, donde la Conferencia de los Ministros del Interior ha apoyado en 2000 la utilización de sistemas de vídeovigilancia como una "herramienta adecuada para apoyar el trabajo de la policía", hay en la actualidad menos de 200 cámaras operativas en unas 30 ó 40 ciudades.[27] En Austria, donde el primer sistema se instaló en 1994 en los alrededores de la estación de trenes de Villach, una iniciativa de nivel federal ha acelerado la instalación de sistemas de vídeovigilancia a partir de

2005. Después de una enmienda del Acta Policial de Seguridad, el Ministerio del Interior anunció la expansión de las áreas públicas sometidas a vigilancia.
En 2006, cinco ciudades austríacas han instalado sistemas de vídeovigilancia en 11 áreas públicas, y se han registrado pedidos para instalar esta clase de sistemas en 17 nuevos lugares.[28]
En Dinamarca, el gobierno ha presentado un nuevo conjunto de medidas destinadas a reforzar la seguridad, que incluye, por primera vez, la autorización oficial de instalar sistemas de vídeovigilancia en áreas públicas.[29]
Esta breve presentación general muestra que el uso de sistemas de vídeovigilancia en Europa varía de un país a otro. También varía en las mismas ciudades, ya que algunas áreas están cubiertas por una densa red de

---

[22] W Winge, S. & Knutsson, J. (2003): An evaluation of the CCTV scheme at Oslo Central Railway Station. En: CCTV, ed. por M. Gill, Leicester: Perpetuity Press, pp. 127-140.

[23] Williams, K. S. & Johnstone, C. (2000): The politics of the selective gaze. Closed Circuit Television and the policing of public space. En: *Crime, Law and Social Change,* Vol. 34, Nº 2, pp. 183-210.

[24] *France Soir,* 16 de febrero de 2009.

[25] Dekkers, S. y otros (2007): *Evaluatie Cameratoezicht op Openbare Plaatsen. Éénmeting. Eindrapport.* Regioplan publicatienr. 1515. Ámsterdam, mayo de 2007, p.IV.

[26] Samatas, M. (2007): Security and surveillance in the Athens 2004 Olympics. Some lessons from a troubled story. En: *International Criminal Justice Review,* Vol. 17, Nº 3, pp. 220-238.

[27] Figures updated from Töpfer, E. (2005): Polizeiliche Videoüberwachung des öffentlichen Raums. Entwicklung und Perspektiven. En: *Datenschutz Nachrichten,* Vol. 28, Nº 2, pp. 5-9.

[28] *Salzburger Nachrichten,* 4 de febrero de 2006.

[29] *heise online,* 4 de noviembre de 2005

centenares de cámaras, mientras que otras áreas urbanas sólo están cubiertas por sistemas mucho más modestos de menos de una docena de cámaras.

Apoyo y regulación

El sistema de vídeovigilancia cuenta con el apoyo de los principales partidos políticos al igual que del público general, como lo muestran con regularidad las encuestas de opinión. No obstante, el nivel de apoyo varía en función de la localización y la extensión de la vigilancia. Según muestra un estudio que se llevó a cabo en 2003 en cinco capitales europeas, el 90% de la gente interrogada en Londres se declaraba favorable a la instalación de sistemas de vídeovigilancia del espacio público, mientras que en Viena, sólo el 25% compartía esa misma opinión.[30] En Gran Bretaña, siguiendo el caso Bulger en 1993, se logró un amplio consenso en torno de la idea de que los sistemas de vídeovigilancia pueden constituir la "bala de plata" mágica contra los demonios del crimen. De hecho, las imágenes que muestran a dos niños de 10 años de edad secuestrando en un centro comercial a un párvulo de 2 años de edad, James Bulger, cuyo cuerpo mutilado fue encontrado dos días después en una vía de ferrocarril no lejos de allí, fueron difundidas durante varias semanas en los principales canales de televisión. El caso suscitó un trauma nacional, mientras que a la vez se ofrecía una promisoria "solución tecnológica" que previniera en el futuro esta clase de eventos tan horribles.[31]

No obstante, los sistemas de vídeovigilancia al estilo británico son vistos por muchos países de Europa continental como una suerte de *"Big Brother"* de la vigilancia. Por ejemplo, en Alemania el ex Ministro del Interior Federal, Otto Schily, estaba a favor de los sistemas de vídeovigilancia del espacio público cuando era un tema de interés político al final de los 90, pero también puso sus reparos contra una política de "vigilancia general", argumentando que constituiría una

violación desproporcionada de los derechos fundamentales.[32] En cierto modo, estas actitudes se ven reflejadas en la normativa legal que rige la vídeovigilancia del espacio público. En Gran Bretaña, la temprana expansión de estos sistemas se produjo en ausencia de regulaciones, ya que el Acta de Protección de Datos del Reino Unido, de 1984, sólo se aplica al procesamiento digital de datos y deja de lado los sistemas analógicos que se instalaron en los albores de la vídeovigilancia. Lo que es más, el Acta sobre el Orden Público y la Justicia Criminal, de 1994, autoriza explícitamente la instalación de "equipos para registrar imágenes visuales de eventos en cualquier lugar del país", que están exentos de pagar licencias costosas del sistema por cable, como indicaba en cambio el Acta de Telecomunicaciones. El marco regulatorio sólo cambió con la implementación de la Directiva sobre la Protección de Datos de la Unión Europea, a través de la modernización del Acta de Protección de Datos de 1998, y la incorporación, en 2000, del Convenio Europeo de Derechos Humanos en el Acta de Derechos Humanos nacional.

Contrariamente a Gran Bretaña, muchos países europeos han considerado desde el comienzo que los sistemas de vídeovigilancia del espacio público constituyen una violación de los derechos fundamentales. En Francia, una corte administrativa de Marsella invalidó en 1990 los planes del Consejo de Aviñón de instalar una red de 93 cámaras, considerando que los registros

---

[30] Hempel, L. & Töpfer, E. (2004): CCTV *in Europe. Final report of the Urbaneye Project.* Zentrum Technik und Gesellschaft, TU Berlin. (Urbaneye Working Paper Nº 15), p. 44. Sitio Internet: http://www.urbaneye.net/results/ue_wp15.pdf.

[31] McGrath, J. (2004): *Loving Big Brother. Surveillance culture and performance space*, London: Routledge.

[32] Discurso en el Parlamento Federal, 9 de noviembre de 2000. Plenarprotokoll 14/130.

eventuales de las imágenes constituirían una violación desproporcionada de la privacidad. Los sistemas de vídeovigilancia del espacio público y el registro de las filmaciones se autorizaron recién en 1995, a través de las Leyes Pasqua, que recomiendan tales sistemas en lugares donde existe un "elevado riesgo de ser agredido o robado".[33]

En la República Federal de Alemania, la Decisión sobre Datos Personales *(Census Decision)* de 1983, de la Corte Constitucional Federal, desarrolla el concepto de un "derecho de autodeterminación respecto a la información personal" *(right to informational self-determination)*, declarando ilegal toda recopilación de datos personales que no cuente con un consentimiento informado, excepto cuando se lo hace en función del "interés general predominante", en consonancia con el principio de proporcionalidad y fundándose en bases legales claras. En efecto, los sistemas de vídeovigilancia en el espacio público, en Alemania, suelen estar regulados por la policía regional y limitados a los, así llamados, "puntos de alta criminalidad" *(crime hot spots)*. Muchos otros países muestran enfoques legales similares, que limitan la utilización de los sistemas de vídeovigilancia del espacio público a determinadas áreas, delimitadas con mayor o menor claridad. No obstante, en países como Hungría y Noruega, la legislación sobre la protección de datos es el punto de referencia legal por antonomasia. Otro tanto sucede hoy en Gran Bretaña. Algunas de estas actas de protección de datos se ocupan explícitamente de los sistemas de vídeovigilancia del espacio público, mientas que otras sólo mencionan la vídeovigilancia en términos generales. En Gran Bretaña, por ejemplo, el primer "Código de Prácticas sobre Sistemas de Vídeovigilancia del Espacio Público" surgió en 2000 del *Information Commissioner* [suerte de Ombudsman de la Información]. [34]

Organización y supervisión

La organización de sistemas de vídeovigilancia del espacio público en los países europeos varía en función de sus respectivos marcos legales. En algunos países, la vigilancia del espacio público queda exclusivamente en manos de la policía, que es el organismo que posee, mantiene y opera los sistemas de vigilancia. En el caso de Alemania, donde las fuerzas policiales de los Länder están a cargo de estos sistemas, aunque a veces comparten información con la Policía Federal y con otros departamentos locales que se ocupan del orden público. En Austria, estos sistemas están en manos de la Policía Federal. En Noruega, el sistema de vídeovigilancia de Oslo está en manos de la policía nacional. En otros países estos sistemas están principalmente en manos de las autoridades locales. Por ejemplo, en Gran Bretaña se estima que un 80% de los sistemas de vídeovigilancia del espacio público son propiedad y están operados por los ayuntamientos.[35]

Los sistemas de vídeovigilancia suelen ser operados por la policía local o municipal, en los países que cuentan con una policía local. La mayor parte de las veces, estos sistemas son operados por civiles, en colaboración con la policía municipal, regional y/o nacional.

También hay ejemplos de colaboración entre el

---

[33] Sección 10 de la Ley Nº 95-73 del 21 de enero de 1995, sobre la orientación y la programación relativa a la seguridad.

[34] Podrá consultar una versión revisada en: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf.

[35] *CCTV Image*, Nº 25 (febrero de 2008), pp. 5-6.

[36] Töpfer, E. (2008): Videoüberwachung in Europa. Entwicklung, Perspektiven und Probleme. En: *Informatik und Gesellschaft. Verflechtungen und Perspektiven*, ed. por H.-J. Kreowski, Münster: LIT Verlag, pp. 61-82 (65-66).

sector público y el sector privado. Por ejemplo en Vilnius, capital de Lituania, una compañía de seguridad privada está a cargo de la sala de control.[36] En el Reino Unido, la primera ola de sistemas de vídeovigilancia solían resultar de la colaboración entre los miembros de la comunidad de comerciantes, y en muchos casos, se establecía una estrecha red entre la sala de control del sistema de vídeovigilancia público y un sistema de "Vídeovigilancia de las tiendas" privado.[37] En el Reino Unido también hubo iniciativas destinadas a obtener el asentimiento de la gente, como el experimento realizado hace unos años en el área londinense de Shoreditch, donde los residentes locales podían recibir imágenes del sistema de vídeovigilancia en su televisión personal.[38]

Parte de esta diversidad organizativa se debe al régimen de supervisión y de concesión de licencias propio a cada país. En muchos países, los sistemas de vídeovigilancia del espacio público están bajo la supervisión de las autoridades de protección de datos, que son quienes suelen estar autorizadas a inspeccionar los sistemas de vídeovigilancia, denunciar malas prácticas y recomendar mejoras en la gestión de los datos. No obstante, algunos países no incluyen a los sistemas de vídeovigilancia entre las áreas de responsabilidad de las autoridades de protección de datos. Tal es el caso de Austria, por ejemplo, en donde el Representante de la Protección Legal *(Rechtsschutzbeauftragter)* del Ministerio Federal del Interior tiene la autoridad para controlar los sistemas de vídeovigilancia, pero sus recomendaciones no son obligatorias. En Francia, la Autoridad Nacional de Protección de Datos (CNIL en su sigla francesa) ha sido eludida por la "Ley Pasqua", que creó nuevos organismos en cada distrito, denominados Comisiones Provinciales de Vídeovigilancia (Commissions Départementale de Vidéosurveillance - CDV). Presidida por un juez, la Comisión analiza

cada proyecto de vídeovigilancia y sus miembros votan a favor o en contra. No obstante, la decisión final queda en manos del Prefecto, que es el representante del gobierno central *(nacional)* en la provincia *(département).* La mayor parte de las veces, el Prefecto sigue las recomendaciones que sugiere la Comisión.

Enfoque global versus local

El coste es un factor clave que determina la dimensión del sistema de vídeovigilancia. Como cabe esperar, la expansión de estos sistemas es más limitada en países donde sólo los policías debidamente entrenados están autorizados a controlar las imágenes de las cámaras en la sala de control, en comparación con los países que emplean personal civil mal pago.

En algunos países, el gobierno central ha hecho inversiones significativas para vigilar el espacio público, como es el caso del Reino Unido, donde el Ministerio del Interior concedió fondos en cuatro oportunidades, entre 1994 y 1998, para llevar a cabo los City Challenge Competitions, por un total de 85 millones de libras, es decir, el 75% del presupuesto total de prevención del crimen. Después de 1998, el partido *New Labour* siguió la misma política e invirtió unos 170 millones en su Iniciativa de Vídeovigilancia, hasta 2002.[39]

Otros países que han hecho inversiones públicas significativas han sido la República Checa, donde el

[37] Coleman, R. (2004): *Reclaiming the streets. Surveillance, social control and the city,* Cullompton: Willan Publishing.

[38] *Guardian*, 11 de enero de 2006.

[39] Töpfer, Eric (2007): Entgrenzte Raumkontrolle? Videoüberwachung im Neoliberalismus. In: *Kontrollierte Urbanität. Zur Neoliberalisierung städtischer Sicherheitspolitik*, ed. por V. Eick y otros, Bielefeld: transcripción, pp. 193-226 (204-206)

presupuesto del gobierno para la prevención del crimen incluye una partida significativa para los sistemas de vídeovigilancia, al igual que Italia y Alemania, donde los gobiernos regionales han apoyado la vídeovigilancia.

Los gobiernos nacionales y/o regionales de Europa han alentado la instalación de sistemas de vídeovigilancia, no sólo estableciendo reglas legales y suministrando recursos financieros, sino también definiendo cómo utilizarlos. En varios países, el gobierno central ha sentado una serie de pautas destinadas a las autoridades locales, con el fin de evitar que permanentemente se "reinvente la rueda" en el plano local. El folleto producido por el Ministerio del Interior del Reino Unido, titulado *CCTV: Looking Out For You* [Sistemas de vídeovigilancia: estamos cuidándole], publicado en 1994, puede ser mencionado como uno de los primeros ejemplos, aunque estaba destinado más bien a fines promocionales que de guía. Más avanzada es la guía titulada *Handreiking Cameratoezicht,* producida por el gobierno holandés en 2000, y distribuida a todos los ayuntamientos del país. Este folleto presenta un resumen de las experiencias con los sistemas de vídeovigilancia del espacio público en Holanda y en otros países, suministrando información sobre los aspectos técnicos de la vídeovigilancia e incluyendo herramientas prácticas como una lista de elementos que se deben tener presentes para instalar estos sistemas y un CD con información adicional.[40] El gobierno de Bélgica ha hecho algo similar, suministrando directrices, consejos y promoviendo el intercambio de experiencias.

En el Reino Unido, la expansión de los sistemas de vídeovigilancia y su eficacia contra el crimen han suscitado una crítica creciente en los últimos años, especialmente desde la publicación, en 2005, de la evaluación nacional efectuada por el Ministerio del Interior y la Asociación de Jefes de Policía publicada

en 2007 con el título "Estrategia de Vídeovigilancia Nacional" *(National CCTV Strategy).* Este documento destaca 44 recomendaciones para instaurar "potenciales mejoras". Entre otras cosas, recomienda la estandarización de todos los aspectos de la vídeovigilancia, la creación de una red de imágenes de vídeovigilancia, tanto en vivo como registradas, el entrenamiento del personal, y una mayor sinergia entre los diferentes actores involucrados en la gestión de la vídeovigilancia. Además, pide que se incremente el poder del *Information Commissioner* [suerte de Ombudsman de la Información] para garantizar la conformidad de los sistemas con el Acta de Protección de Datos. La estrategia está respaldada por el Comité del programa de estrategia nacional de vídeovigilancia, que asesora sobre las recomendaciones que se deben tomar y coordina las actividades futuras.[41]

Francia está avanzando en la misma dirección, dado que su gobierno está trabajando actualmente en una estrategia nacional de vídeovigilancia.

La mayor parte de los demás países europeos están lejos de diseñar esta clase de enfoque estratégico, dejando el desarrollo de la vídeovigilancia en manos de las iniciativas locales.

¿Decisión política o impulso tecnológico?

Como hemos visto, el panorama europeo de la vídeovigilancia en zonas urbanas se caracteriza por una enorme diversidad en términos de apoyo político, regulaciones legales, organización, regímenes de pro-

[40] Las líneas directrices se actualizan con regularidad. La versión actual se puede consultar en: http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/bestuurlijk-handhaven/cameratoezicht/handreiking_cameratoezicht_mei_2009.pdf.

[41] Gerrard, G. y otros (2007): *National CCTV Strategy*. London: Home Office.

tección de datos y estrategias nacionales. La evolución de la vídeovigilancia del espacio público varía en función del marco institucional de cada país, de los recursos financieros disponibles y, por último pero no menos importante, del consenso que prevalezca entre la gente.

No obstante, en Europa el verdadero motor del desarrollo se encuentra a nivel local. Los electos, los políticos locales y la policía impulsan o impiden el desarrollo de los sistemas de vídeovigilancia del espacio público en función de sus respectivos puntos de vista, intereses e intenciones.

¿Pero hasta qué punto la política, en lugar de la tecnología, influye en la evolución de los sistemas de vídeovigilancia del espacio público? Las cámaras de vigilancia han sido utilizadas para controlar el espacio público desde hace más de 50 años. En los años 90, se produjo una expansión masiva de estos sistemas de vídeovigilancia, que han sido promovidos como una herramienta eficaz para luchar contra el crimen. Al mismo tiempo, los estudios que evalúan estos sistemas cuestionan su eficacia como "bala de plata" contra el crimen. Actualmente, el énfasis que se pone en los debates públicos cuando se trata de justificar los sistemas de vídeovigilancia, ha pasado de la prevención del crimen a la investigación criminal, y estos sistemas se presentan como una herramienta muy valiosa para buscar evidencias una vez que se ha cometido un crimen.

En la actualidad, los sistemas de vídeovigilancia del espacio público no se limitan a la prevención del crimen. Una vez que están instalados, estos sistemas pueden ser utilizados para controlar delitos menores como arrojar basura o aparcar el coche en sitios no autorizados, o incluso observar el personal municipal que trabaja en el espacio público. Pero también se los puede utilizar para controlar eventos públicos de gran envergadura o emergencias graves.

Está surgiendo una nueva tendencia con la constitución de redes de lo que antes eran sistemas "discretos". La policía y otras fuerzas del orden piden acceder en tiempo real a las imágenes de vídeovigilancia de los sistemas de transporte urbano, por ejemplo, o bien otros grandes organismos públicos y privados. Actualmente, el espacio público está cubierto por una intrincada red de sistemas de vídeovigilancia.[42]

En un esfuerzo por asimilar el creciente número de imágenes, los algoritmos de vigilancia están asumiendo el trabajo que antes se hacía con métodos tradicionales, lo que implica que las decisiones cruciales queda en manos de las cajas negras de la tecnología biométrica, de patrones de reconocimiento automático y de sistemas de toma de decisiones basados en GIS. Dado que tanto a los ciudadanos como a los responsables les resulta cada vez más difícil entender la forma y la función actual de las redes de sistemas de vídeovigilancia del espacio público semiautomáticas, la actual tendencia plantea serios interrogantes en cuanto a la transparencia y la responsabilidad o rendición de cuentas democrática de los actuales sistemas de vigilancia urbana.

El desarrollo y la evolución de los sistemas de vídeovigilancia del espacio público en Europa han alcanzado un punto donde se hace urgente que discutamos, desarrollemos e implementemos principios compartidos para utilizarlos.

---

[42] El término ha sido tomado de McCahill, M. (2002): *The surveillance web. The rise of visual surveillance in an English city,* Cullompton, Devon, UK: Willan Publishing.

Marco jurídico de la vídeovigilancia en Europa

Laurent Lim, Asesor jurídico, Comisión Nacional de la Informática y de las Libertades de Francia (CNIL)

➤ Las cámaras de vigilancia se emplean hoy en todo el mundo, de modo más o menos masivo, para controlar el espacio público y privado. Acompañando el movimiento tecnológico general que facilita cada vez más la captación de imágenes, los sistemas de vídeovigilancia se perfeccionan y evolucionan rápidamente.

De este modo, las herramientas de vídeovigilancia proponen hoy la transmisión de las imágenes por Internet (Vídeo por IP), interfaces de gestión que se integran al entorno ofimático, una calidad de imagen y unas capacidades de almacenamiento cada vez mayores. También existen diversas clases de software destinados a comunicar alertas a partir de una lectura *"inteligente"* de imágenes, software que debería seguir avanzando hacia posibilidades de análisis más importantes, en particular con la utilización de imágenes de vídeo sumadas a otras tecnologías (reconocimiento sonoro, reconocimiento facial).

Estas evoluciones futuras, la diversificación del uso, al igual que la madurez del mercado de la vídeovigilancia, constituyen un nuevo reto para las normas jurídicas europeas y nacionales, que deben enmarcar específicamente la utilización de la vídeovigilancia o tratan de modo general la protección de los datos de carácter personal.

Aunque las instituciones europeas han encuadrado bastante pronto la recopilación y la utilización de datos de carácter personal, los primeros instru-

mentos que deben enmarcarlos específicamente han aparecido recientemente.

A nivel nacional, la legislación de los Estados miembros de la Unión Europea, aunque establecen reglas y condiciones diferentes, autorizan la utilización de la vídeovigilancia.

En Europa, se plantea el tema de la conformidad de la utilización de los sistemas de vídeovigilancia con la directiva sobre la protección de los datos, y veremos que existen respuestas legislativas muy variadas sobre la forma de enmarcar jurídicamente estos sistemas. Hay que destacar que la ley no es necesariamente el único instrumento jurídico para enmarcar la vídeovigilancia: se deben tener en cuenta la jurisprudencia, las resoluciones, resoluciones y recomendaciones de las instituciones europeas o nacionales, al igual que las autoridades de protección de los datos. Por último, los códigos de buenas prácticas o las cartas deontológicas o éticas constituyen herramientas sumamente útiles de autorregulación.

I. MARCO JURÍDICO EUROPEO

A nivel europeo se han adoptado algunos principios fundamentales en materia de protección de derechos y libertades fundamentales, al igual que en materia de protección de datos de carácter personal. Estos textos también conciernen el tratamiento de datos realizado en el marco de operaciones de vídeovigilancia.

A. Garantías fundamentales de los textos del Consejo de Europa

El Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales, que el Consejo de Europa adoptó en Roma el 4 de noviembre de 1950,

en su artículo 8, afirma el derecho a la intimidad de la vida privada y familiar, del domicilio y de la correspondencia.

Este Convenio ha sido completado con el Protocolo A dicional Nº4, del 16 de septiembre de 1963, que en su artículo 2 garantiza la libertad de circulación de todo aquel que se encuentre en situación regular en el territorio de un Estado.
Por lo demás, el Convenio Nº108/1981 del Consejo de Europa sobre la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, del 28 de enero de 1981, ha sido ratificado por 40 Estados europeos y constituye el primer instrumento internacional cuyo objetivo es sentar las normas mínimas destinadas a proteger a las personas de los abusos susceptibles de producirse durante la recolección y el tratamiento de los datos de carácter personal.
Este Convenio de aplica a los sectores público y privado, y contiene una serie de principios generales que se aplican a la recopilación, el tratamiento y la comunicación de datos de carácter personal a través de las nuevas tecnologías de la información.
Las actividades de vídeovigilancia entran en su ámbito de aplicación, en la medida en que implican el tratamiento de los datos de carácter personal, según lo define la Convención Nº 108, y en donde el Comité de Consulta establecido por este Convenio ha estimado que las voces y las imágenes deben ser consideradas como datos de carácter personal cuando suministran información sobre una persona haciéndola identificable, incluso indirectamente.
Estos principios se interesan en el carácter lícito y leal de la recopilación y del tratamiento automatizado de los datos personales, el principio que rige su grabación y registro para determinadas finalidades que deben ser legítimas, la no utilización de los datos con fines incompatibles al destino de estas imágenes, la limitación de la

conservación de estas imágenes a un plazo estrictamente necesario, el carácter adecuado y no excesivo del sistemas respecto a las finalidades que se persiguen, al igual que la pertinencia de los datos y la obligación de actualizarlos. El Convenio proscribe el tratamiento de datos "sensibles" (relativos a las características raciales, a las opiniones políticas, a la salud, a la religión, a la vida sexual), y garantiza, asimismo, el derecho que tienen las personas de conocer la información sobre ellas almacenada y de exigir, en su defecto, las rectificaciones del caso.

La Corte Europea de Derechos Humanos (o Tribunal Europeo de Derechos Humanos) ha tenido la oportunidad de indicar los límites de estas garantías en materia de vídeovigilancia. Ha declarado así que la revelación y la publicación en los medios de comunicación, en el marco de campañas de lucha contra el crimen, de imágenes obtenidas con sistemas de vídeovigilancia de la vía pública, y a espaldas de la persona filmada, constituyen una violación del artículo 8.[43]

Para responder a la necesidad de sentar un marco jurídico más específico para las operaciones de vídeovigilancia, y después de haber observado *"con inquietud que las leyes nacionales están lejos de ser homogéneas en la materia"*, la Asamblea Parlamentaria del Consejo de Europa ha adoptado el 25 de enero de 2008 la resolución Nº1604, por la cual pide formalmente a los Estados miembros del Consejo de Europa que apliquen conjuntamente los *"principio directivos para la protección de las personas respecto a la recopilación y el tratamiento de datos a través de la vídeovigilancia"*.

[43] Fallo de la Cámara 28/01/2003 Peck contra el Reino Unido App. 44647/98

Se trata de doce principios que retoman y aplican a la vídeovigilancia los principios que los instrumentos del Consejo de Europa ha afirmado, insistiendo singularmente en la necesidad de varias condiciones: una utilización pertinente, adecuada y no excesiva respecto a la finalidad que se persigue; evitar que los datos recopilados sean indexados, comparados y conservados sin necesidad; no efectuar una vídeovigilancia si el tratamiento de los datos de carácter personal puede producir una discriminación contra algunos individuos o grupos de individuos, únicamente en razón de su opinión política, de sus convicciones religiosas, de su salud, de su vida sexual, de sus características raciales o étnicas; informar claramente y de forma adecuada a las personas, indicando la finalidad del sistema y la identidad de los responsables; garantizar el ejercicio del derecho de consultar sus imágenes y grabaciones; al igual que garantizar la seguridad y la integridad de las imágenes a través de toda medida técnica y organizativa necesaria.

El Consejo de Europa incita a sus miembros a prever en su legislación nacional las disposiciones que definen las restricciones técnicas destinadas a limitar la instalación de estos equipos en función del lugar que se deba vigilar, las zonas privadas que se deben excluir del ámbito de la vídeovigilancia, exigiendo la utilización de un software adecuado, la codificación criptográfica de los vídeos, al igual que la creación de vías de actuación jurídica en caso de que se alegue una utilización abusiva de la vídeovigilancia.

Hay que destacar que la Asamblea Parlamentaria considera que es necesario que una señalización y un texto de acompañamiento uniformizados se adopten lo antes posible y sean utilizados por los Estados miembros. Con vistas a los progresos técnicos constantes en lo referente a la vídeovigilancia, destaca la necesidad de proseguir la reflexión en el futuro sobre el tema de la vídeovigilancia.

B. Otros textos europeos

Entre los demás textos europeos que pueden aplicarse a las actividades de vídeovigilancia, hay que citar la Carta de Derechos Fundamentales de la Unión Europea. Esta proclamación solemne, adoptada el 7 de diciembre de 2000 por la Unión Europea, ha sido mencionada en el Tratado de Lisboa del 13 de diciembre de 2007, que entró en vigor el 1 de diciembre de 2009, en el artículo sobre los derechos fundamentales. Esta proclamación está destinada a conferir a la Carta un valor jurídicamente obligatorio (bajo las fuertes restricciones de algunos países: Polonia y Reino Unido, al igual que la República Checa).

El artículo 7 de la Carta prevé así que *"Toda persona tiene derecho a que se respete su vida privada y familiar, su domicilio y sus comunicaciones".*
Además, el artículo 8 garantiza que *"Toda persona tiene derecho a la protección de los datos de carácter personal que le incumben"*. Indica, además, que *"estos datos deben ser tratados lealmente, con fines determinados, y sobre la base del consentimiento de la persona respectiva, o en virtud de otro fundamento legítimo previsto por la ley", que "toda persona tiene derecho de consultar los datos registrados que le conciernen y obtener su eventual rectificación" y que "el respeto de estas reglas está sometido al control por parte de una autoridad independiente".*

Asimismo, hay que indicar que el Supervisor Europeo de Protección de Datos (CEPD)[44], que es competente para supervisar los tratamientos de datos de carácter personal y que llevan a cabo las instituciones europeas, ha publicado el 17 de marzo de 2010 un conjunto de líneas directrices sobre la vídeovigilancia, destinadas a las instituciones y organismos europeos.

Estas líneas directrices detalladas, elaboradas al término de un proceso de consulta, incluyen una serie de recomendaciones prácticas. De hecho, destacan el concepto de *"privacy by design"*, según el cual las medidas técnicas de precaución que permiten proteger mejor los datos de carácter personal y la vida privada de las personas filmadas, debe estar incorporadas, desde la etapa de diseño, en las características tecnológicas de los sistemas de vigilancia.

C. La Directiva 95/46/CE del Parlamento Europeo y del Consejo Europeo, del 24 de octubre de 1995, relativa a la protección de personas físicas respecto al tratamiento de los datos de carácter personal y a la libre circulación de estos datos

Esta Directiva constituye el instrumento jurídico que ha adoptado la Unión Europea para establecer los principios de protección de los datos de carácter personal de los ciudadanos europeos. Sobre la base de este texto, los Estados miembros han adoptado sus respectivas legislaciones nacionales sobre la protección de datos.

En principio, la Directiva se puede aplicar a los sistemas de vídeovigilancia, dado que se aplica a toda información, incluyendo la información en forma de sonido e imágenes, referente a una persona identificada o identificable, teniendo en cuenta todos los medios que pueden ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona con el fin de identificar dicha persona.

En efecto, las imágenes y sonidos referentes a personas físicas identificadas o identificables, se consideran como datos de carácter personal, aun cuando las imágenes sean utilizadas en el marco de la vídeovigilancia, e incluso si no están asociadas a los datos de identidad de la persona; incluso si no corresponde a personas cuyo rostro ha sido filmado, y aunque

contenga otra clase de información (por ejemplo, el número de la placa con la matrícula de su vehículo).
No obstante, la vídeovigilancia de los lugares públicos sólo concierne parcialmente a la Directiva 95/46, en la medida en que no es aplicable al tratamiento de los datos en forma de sonidos y de imágenes, con una finalidad de seguridad pública, defensa, seguridad del Estado, para el ejercicio de actividades del Estado en el ámbito del derecho penal, o para otras actividades que no entren en el ámbito de aplicación del derecho comunitario.
Por lo demás, la Directiva no se puede aplicar al tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.
A nivel europeo, el grupo de autoridades nacionales de protección de datos (conocido como *"Grupo del Artículo 29"* o "G29") ha precisado en una resolución de 2004[45] la interpretación de las disposiciones de la Directiva Nº 95/46.
Esta resolución destaca la necesidad de que las instituciones respectivas de los Estados miembros lleven a cabo una evaluación general de la vídeovigilancia para *"evitar que una proliferación excesiva de los sistemas de adquisición de imágenes en lugares públicos y privados no implique una restricción injustificada de los derechos y libertades fundamentales de los ciudadanos"*, que volviera a los ciudadanos "*masivamente identificables en muchos lugares públicos y privados*". También destaca la necesidad de llevar a cabo una evaluación de la evolución de las técnicas de vídeovigilancia, con el fin de evitar que el desarrollo de software de reconocimiento del rostro de las personas y de la detección/previsión del comportamiento *"no conlleve el paso masivo e inconsiderado hacia una vigilancia de tipo dinámico-preventiva"*.
Estos dos mensajes siguen siendo de actualidad, de

[44] Véase el sitio web www.edps.europa.eu
[45] Resolución del G29 Nº WP 89, del 11 de febrero de 2004

suerte que la definición de herramientas y métodos lo más fiables posible para evaluar la eficacia de la vídeovigilancia sigue siendo crucial e indispensable.

II. LEGISLACIONES NACIONALES

A. La diversidad de los sistemas de regulación

En diferentes Estados miembros, existen casos de estudio en materia de vídeovigilancia, que se fundan en normas constitucionales o en disposiciones legislativas específicas, de prescripciones y demás decisiones que emanan de las autoridades nacionales competentes.

En algunos países, también existen disposiciones específicas que se aplican independientemente del hecho de que la vídeovigilancia supone o no el tratamiento de datos de carácter personal. Estas disposiciones también prevén que la instalación y la utilización de un sistema de vídeovigilancia estén sometidas a autorizaciones previas por parte de una autoridad administrativa, que puede estar representada total o parcialmente por la autoridad nacional que se ocupa de la protección de los datos de carácter personal. Las reglas pueden variar según la naturaleza pública o privada de la persona responsable del funcionamiento de la instalación.

En otros países, la vídeovigilancia no ha sido objeto de disposiciones legales específicas. Sin embargo, en algunos casos las autoridades que se ocupan de la protección de datos de carácter personal han podido cumplir su cometido a través de resoluciones, líneas directrices o códigos de conducta (Reino Unido, Italia), que garantizan una aplicación adecuada de las disposiciones generales de protección de datos.

La resolución del G 29 del 11 de febrero de 2004, citada anteriormente, incluye un cuadro recapitula-

tivo de las principales fuentes jurídicas nacionales en materia de vídeovigilancia conocidas en los diferentes Estados miembros al día de su adopción.

ADVERTENCIA: Este cuadro, que se transcribe más abajo a título de información, no puede considerarse exhaustivo tratándose de los eventuales textos nuevos que habrían podido producirse después del 11 de febrero de 2004.

Alemania
Artículo 6, punto B de la Ley Federal de 2000
Artículo 25 de la ley sobre protección de fronteras.
Otras normativas en materia de la vídeovigilancia que ejerce la policía en las legislaciones correspondientes de los Länder.

Bélgica
Resolución de la autoridad que se ocupa de la protección de datos, especialmente la resolución de iniciativa 34/99, del 13 de diciembre de 1999, relativa al tratamiento de las imágenes efectuada especialmente a través de los sistemas de vídeovigilancia.
Resolución de iniciativa 3/2000, del 10 de enero de 2000, relativa a la utilización de sistemas de vídeovigilancia en las entradas de edificios de apartamentos.
Ley del 21 de marzo de 2007 sobre la instalación y utilización de cámaras de vigilancia.

Dinamarca
Ley de síntesis Nº 76 del 1 de febrero de 2002, relativa a la prohibición de la vídeovigilancia. Esta ley prohíbe en términos generales que organismos privados puedan ejercer una vídeovigilancia de la vía pública, de los parques y de cualquier otra zona equivalente de libre circulación, incluyendo, no obstante, algunas derogaciones a esta prohibición.
Decisión de la autoridad que se ocupa de la protección de los datos, del 3 de junio de 2002, sobre la

vídeovigilancia por parte de un gran grupo de supermercados y transmisión directa a Internet a partir de un café.
Decisión de la autoridad que se ocupa de la protección de los datos, del 1 de julio de 2003, según la cual la vídeovigilancia ejercida por una sociedad privada de transporte público debe ser adaptada y conforme a las disposiciones de la ley sobre la protección de datos.
Decisión de la autoridad que se ocupa de la protección de los datos, del 13 de noviembre de 2003, imponiendo algunas restricciones a la vídeovigilancia que ejercen las autoridades públicas.
En junio de 20007, se han adoptado dos leyes en materia de vídeovigilancia: la primera concede a las empresas privadas el poder de llevar a cabo una vigilancia de las zonas de las que son propietarias, sin obligación de declaración previa a la autoridad que se ocupa de la protección de los datos. La segunda ley confiere a los servicios de la policía mayores poderes para poder imponer a sus administraciones o a organismos privados, la instalación y utilización de sistemas de vídeovigilancia.

España
Ley Orgánica Nº 4/1997 (vídeovigilancia por parte de las fuerzas y cuerpos de seguridad en lugares públicos)
Real Decreto Nº 596/1999 de aplicación de la ley Nº 4/1997

Finlandia
En Finlandia no existe una legislación especial en materia de vídeovigilancia, sino disposiciones que emanan de un gran número de textos legislativos diferentes y que se aplican a la vídeovigilancia al igual que a otros sistemas técnicos de vigilancia, de observación y de control.

El mediador para la protección de los datos ha presentado una resolución sobre el registro o grabación de las conversaciones telefónicas por parte de los servicios a los clientes y en el ámbito del trabajo (números de expediente 1061/45/2000 y 525/45/2000).

Francia

Ley Nº 78-17 del 6 de enero de 1978 relativa a la informática, los archivos y las libertades (CNIL).
Ley Nº 95-73 del 21 de enero de 1995 relativa a la seguridad (modificada), decreto Nº 96-926 del 17 de octubre de 1996 (modificada) y circular del 22 de octubre de 1996 (modificada) sobre la aplicación de la Ley Nº 95-73 enmarca, con un régimen específico de autorizaciones de la Prefectura, la instalación y utilización de sistemas de vídeovigilancia destinados a la seguridad en lugares públicos.
La Comisión Nacional de Informática y Libertades (CNIL), autoridad responsable de la protección de los datos, ha publicado una Guía con las recomendaciones concernientes a la vídeovigilancia en el lugar de trabajo.

Grecia
Carta Nº390 del 28 de enero de 2000 sobre la instalación de un sistema de televisión en circuito cerrado en el Metro de Atenas.
Directiva Nº1122 del 26 de septiembre de 2000 sobre la televisión en circuito cerrado.
Decisión Nº84/2002 relativa a los sistemas de televisión en circuito cerrado en los hoteles.

Irlanda
Ley sobre la protección de los datos de 1998 y de 2003. Estudio de caso Nº 14/1996 (utilización de la vídeovigilancia o CCTV)

Italia

Artículo 34 del Código de Protección de Datos de Carácter Personal (D.lg. Nº196, del 30 de junio de 2003, sobre la adopción del Código de Conducta).
Decisión de la autoridad de control (Garante) Nº 2, del 10 de abril de 2002 (promoción del Código de Conducta); 28 de septiembre de 2001 (técnicas biométricas y reconocimiento del rostro en los bancos) y del 29 de noviembre de 2000 ("decálogo" sobre la vídeovigilancia) d.P.R. del 22 de junio de 1999, Nº 250 (acceso de los vehículos al centro histórico y a las zonas de circulación limitada).
D.l. del 14 de noviembre de 1992, Nº 433 y l. n. 4/1993 (museos, bibliotecas y archivos del Estado)
D.lg. del 4 de febrero de 2000, Nº 45 (buques destinados a viajes nacionales)
Artículo 4 l., del 20 de mayo de 1970, Nº 300 (situación de los trabajadores)

Luxemburgo

Artículos 10 y 11 de la ley del 02.0802002 relativa a la protección de las personas respecto al tratamiento de datos de carácter personal.

Países Bajos

El informe de la autoridad que se ocupa de la protección de datos, publicado en 1997, contiene las líneas directrices sobre la vídeovigilancia, en relación con la protección de las personas y los bienes en los lugares públicos.
Investigación sobre la vídeovigilancia en todos los municipios neerlandeses en 2003.
Modificación del código penal en vigor a partir del 1 de enero de 2004, que amplía el ámbito de aplicación de la infracción que consiste en fotografiar los lugares accesibles al público sin informar a las personas.

Portugal
Decreto-Ley 231/98, del 22 de julio de 1998 (actividades privadas de seguridad y sistemas de autoprotección)
Ley 38/98, del 4 de agosto de 1998 (medida que se debe adoptar en caso de violencia asociada a eventos deportivos)
Decreto-Ley 263/01, del 28 de septiembre de 2001 (discotecas)
Decreto-Ley 94/2002, del 12 de abril de 2002 (eventos deportivos)

Reino Unido
CCTV Code of practice (Information Commissioner) revisado en 2008

Suecia
La vídeovigilancia ha sido específicamente reglamentada por la ley (1998:150) relativa a la vídeovigilancia general, y por la ley (1995:1506) sobre la vídeovigilancia secreta (en investigaciones criminales).
La vigilancia general por vídeo requiere en principio la autorización de una administración regional, aunque haya una serie de excepciones por ejemplo en lo referente a la vigilancia de las oficinas de correo, los bancos y las tiendas. La vigilancia secreta por vídeo debe estar autorizada por una corte. El Ministro de Justicia puede apelar una decisión de la Comisión Administrativa Regional.
La grabación y registro de vídeo de cámaras numéricas se considera un tratamiento de datos de carácter personal y, por lo tanto, se encuentra bajo la supervisión de la autoridad responsable de proteger los datos, en la medida en que no ha sido específicamente reglamentada por la ley relativa a la vigilancia general por vídeo.
Una comisión de investigación ha publicado en 2002 un informe sobre la vídeovigilancia (SOU 2002:110).

Los demás instrumentos que merecen ser mencionados conciernen a Islandia (artículo 4, Ley Nº 77/2000), Noruega (título VII, Ley Nº 31 del 14 de abril de 2000), Suiza (recomendación del Responsable Federal) y Hungría (recomendación DPA del 20 de diciembre de 2000).

B. ¿Hacia una legislación europea específica?

Esta diversidad de legislaciones, combinada con los rápidos avances tecnológicos de los sistemas, confirma la pertinencia de un enfoque jurídico más armonizado. Varios trabajos recientes a nivel europeo se inscriben, en efecto, en esta óptica y recomiendan que se refuerce la legislación europea y nacional.

En su informe del 7 de mayo de 2010 sobre el papel de las autoridades de protección de datos en Europa[46], la Agencia Europea de Derechos Fundamentales indica que el desarrollo de sistemas de vídeovigilancia es un punto inquietante que requiere una acción urgente: *"La vídeovigilancia de los lugares públicos se ha difundido ampliamente, pero en cambio no se ha actualizado el marco legislativo. El informe muestra, por ejemplo, que en los hechos las cámaras de vídeovigilancia suelen no haber sido declaradas y/o no están sometidas a ningún control en algunos Estados miembros"*.

El informe indica así que en Austria, la amplia mayoría de las cámaras no han sido declaradas (escapando al control de la autoridad de protección de datos), y que en Alemania se han denunciado algunos casos de vídeovigilancia a espaldas de los trabajadores. Recuerda que en Grecia, se negó el acceso a los locales de policía donde se estaban tratando los datos a la autoridad de protección de datos y que en el Reino Unido existen pocas restric-

ciones sobre la utilización de cámaras en el espacio público, siendo que en este Estado miembro hay más cámaras que en ningún otro lado del mundo.
La agencia de derechos fundamentales estima así que, sin dejar de lado las características técnicas intrínsecas de los datos sonoros y visuales, al igual que el impacto potencial importante que pueden tener en los individuos, en el futuro habría que considerar la instauración de un instrumento legislativo europeo específico.

Por último, el Consejo de Europa en su proyecto de recomendación sobre la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, en el marco de los tratamientos de *"profiler"* adoptada el 15 de junio de 2010[47], observa que la recolección y el tratamiento de los datos para constituir perfiles pueden utilizar diferentes tipos de datos, como los que *"provienen de los sistemas de vídeovigilancia"*.
En ausencia de iniciativa legislativa europea destinada a encuadrar de modo específico las operaciones de vídeovigilancia, los actores pueden apoyarse en las resoluciones o recomendaciones sectoriales de las autoridades nacionales de protección de datos.
Con el fin de contar con un mejor marco jurídico y la utilización más coherentes posible de su sistema de vídeovigilancia, algunos han elaborado una Carta Ética sentando en ella las reglas de buena conducta y de buena gestión. En esta óptica se inscribe la Carta que ha propuesto el Foro Europeo de Seguridad Urbana, en el marco del proyecto "Ciudadanos, Ciudades y Vídeovigilancia".

[46] Se puede consultar en el sitio web de la Agencia Europea de Derechos Fundamentales: http://fra.europa.eu/
[47] Se puede consultar en el sitio web del Consejo de Europa: http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp

Parte II

Hacia una Carta por una utilización democrática de la vídeovigilancia en las ciudades europeas

« Pido a los electos que estudien y firmen la Carta por una utilización democrática de la vídeovigilancia »

Entrevista a Charles Gautier, senador y alcalde de Saint-Herblain, Presidente del Foro Francés de Seguridad Urbana

➤ **Es usted uno de los primeros que ha firmado, junto con el alcalde de Rotterdam, la nueva Carta por una utilización democrática de la vídeovigilancia. ¿Por qué esta Carta?**

Charles Gautier : Esta Carta es el fruto de un trabajo realizado a escala europea por un conjunto de ciudades y actores involucrados en la vídeovigilancia. Desde hace unos quince años, la vídeovigilancia en ámbito urbano ha tenido un enorme desarrollo en Europa, aunque existan diferencias significativas de un país a otro, tanto por la densidad de las redes instaladas como en lo referente a la legislación y las formas de control. Actualmente, hemos llegado a un punto en donde se ha vuelto necesario reflexionar entre todos sobre esta tecnología que no es anodina, ya que *de facto* produce una injerencia en la vida privada de los ciudadanos, que son filmados sin saberlo en las calles de nuestras ciudades.

El EFUS *(European Forum for Urban Safety)* ha lanzado pues un proyecto europeo en torno de este tema, en el cual el Foro Francés se ha desempeñado como experto, con el objetivo de debatir entre todos cuáles serían las consecuencias políticas y sociales de la vídeovigilancia en el ámbito urbano. ¿Cómo utilizar esta tecnología? ¿Qué marco legal y político aplicar? ¿Cómo garantizar las libertades? ¿Quién controla? ¿Quién vigila? ¿A quién se vigila? ¿Qué experiencias realizadas en tal o cual ciudad o país

pueden aplicarse en otras partes? ¿Qué lecciones se pueden sacar de las "malas" experiencias?
La Carta por una Utilización Democrática de la Vídeovigilancia retoma los temas clave en los cuales hemos trabajado y, sobre todo, presenta una serie de principios fundadores para, como indica su título, una utilización democrática de la vídeovigilancia que respete las libertades fundamentales de los ciudadanos.

¿A quién se dirige la Carta y para qué sirve?
Ante todo hay que indicar que esta Carta no es de ningún modo un documento reglamentario que impondría una serie de directivas a las ciudades europeas. Ha sido pensada y redactada por las mismas ciudades para aclarar una serie de ideas compartidas. Por lo tanto, se trata de una herramienta que está a disposición de las ciudades para ayudarlas a definir el lugar que incumbe a la vídeovigilancia en sus respectivas políticas de seguridad urbana, por una parte, y por otra, para definir las modalidades prácticas de su utilización. Es, por así decir, una suerte de guía y también una declaración de principios.

¿En calidad de qué participa usted en este proyecto?
Ante todo, como senador y alcalde de Saint-Herblain, una de las diez ciudades que participan en este proyecto. Saint-Herblain es una ciudad de 45.000 habitantes, que se encuentra en la aglomeración de Nantes, en el Loira Atlántico, al noroeste de Francia. Nantes y su extrarradio suman unos 500.000 habitantes. Saint-Herlain ha instalado las primeras cámaras de vídeovigilancia en 1999 y actualmente cuenta con 18 cámaras. Como alcalde, tengo una política clara: conciliar la exigencia de seguridad de los ciudadanos con el respeto de las libertades individuales. El desarrollo de nuestro sistema de vídeovigilancia se hace en función de esa decisión estratégica.

También participo en este proyecto en mi calidad de senador ya que, junto con el senador Jean-Patrick Courtois, he elaborado un informe sobre la vídeovigilancia, destinado al Senado. Nuestras recomendaciones se sitúan en la misma línea que los principios definidos en el proyecto europeo *Ciudadanos, ciudades y vídeovigilancia*. Por último, he participado en este proyecto en mi calidad de Presidente del Foro Francés, en el cual también hemos llevado a cabo una serie de reflexiones en torno de este tema con los electos.

¿La vídeovigilancia es un tema importante para los electos en Francia?

Sin ninguna duda, y no sólo porque la vídeovigilancia es un elemento importante de la política de seguridad de las ciudades, sino también porque hay una clara voluntad política a escala nacional. El gobierno ha anunciado que, en el marco de la lucha contra el terrorismo, su objetivo era triplicar, a finales de 2011, el número de cámaras instaladas en Francia, sumando un total de 60.000. Se hacen inversiones importantes en el ámbito de la vídeovigilancia. Así, una buena parte del Fondo Interministerial de Prevención de la Delincuencia está dedicado a su financiación. Las provincias (Départements) también dedican una parte importante de su presupuesto, con no menos de 30 millones de euros de un total de unos 49 millones en 2010.

¿Cuál es la posición del Foro y de los electos franceses sobre este tema?

No tenemos ninguna posición dogmática en nuestra red. Es seguro que muchas colectividades buscan hoy evaluar la eficacia de la protección por vídeo y, sobre todo, conciliar esta tecnología con las libertades fundamentales. Hay muchos debates sobre estos temas. Para resumirlos, digamos que existe un consenso general en torno de cuatro principios

generales:
Primero, la protección por vídeo es una herramienta que se debe emplear en el marco de una política global de prevención de la delincuencia. Es importante tener en cuenta no sólo los aspectos técnicos sino también la organización, los recursos humanos, el coste financiero y la dimensión ética.
En segundo lugar, nos parece fundamental que los ayuntamientos inviertan para formar mejor a los operadores, y no sólo en la utilización técnica de los sistemas sino también en los objetivos de la municipalidad. Los operadores deben conocer la política local de seguridad y de prevención de la delincuencia, al igual que los objetivos del ayuntamiento. También deben conocer la reglamentación en vigor, especialmente en lo referente a la confidencialidad de la vida privada y las libertades individuales.
El tercer principio concierne la importancia de recurrir a un método de evaluación del sistema local de protección por vídeo en función de los objetivos que le han sido asignados. Estos sistemas cuestan caro a las colectividades y por eso nos parece indispensable que cuenten con herramientas de evaluación, especialmente para garantizar una buena coherencia entre el sistema de vídeo y los demás dispositivos locales de seguridad y, de ser necesario, introducir las mejorar necesarias.
Por último, la cuarta idea fuerte es que todo sistema de protección por vídeo debe utilizarse en el marco de la aplicación de reglas éticas. Dos conceptos nos parecen de singular importancia: la utilización transparente de estos sistemas y la "trazabilidad" de la información recogida.

Junto con el ayuntamiento de Rotterdam (Países Bajos), es usted uno de los primeros firmantes de la Carta por una Utilización Democrática de la Vídeovigilancia. ¿Qué novedad aporta esta Carta?

A la fecha no existe ningún texto europeo sobre la vídeovigilancia. Esta Carta es, pues, una novedad fruto de la voluntad de una serie de ciudades europeas de adoptar un marco de referencia. Si los alcaldes han sentido esta necesidad, es porque están directamente a la escucha de las necesidades de los habitantes de las ciudades en lo referente a la seguridad, al igual que de sus temores sobre las injerencias en su vida privada. Por lo tanto, es lo opuesto a un enfoque burocrático que partiera "desde arriba".
Esta Carta nos da, a los electos locales, los criterios de evaluación y las recomendaciones concretas en el marco de las reglamentaciones europeas y nacionales actuales. No es una declaración a favor o en contra de la vídeovigilancia.

Usted ha hecho un llamamiento a sus colegas alcaldes y electos locales europeos para que firmen esta Carta. ¿Qué cambia, concretamente, ser signatario de la Carta?
Llamo a los electos no sólo a firmar sino también a estudiar la *Carta por una Utilización Democrática de la Vídeovigilancia,* porque creo que aborda un tema esencial y urgente.
Actualmente, dada la expansión de los sistemas de vídeovigilancia y su evolución tecnológica, todo alcalde o representante de una colectividad local, incluso relativamente pequeña, debe contar con estos sistemas y, por lo tanto, a tomar una posición al respecto.
Con esta Carta, las autoridades electas que así lo deseen podrán adoptar una serie de principios que garantizan la utilización *democrática* de la vídeovigilancia. Firmar la Carta implica un compromiso público del electo de cara a los ciudadanos de su ciudad o de su colectividad local, comprometiéndose a garantizar las libertades fundamentales.

>>

LA VÍDEOVIGILANCIA EN FRANCIA: CIFRAS CLAVE

➤ Francia cuenta con **396.000** cámaras autorizadas, de las cuales **20.000** en el espacio público (cifras de 2007).

➤ En 2007 se han concedido **9.772** autorizaciones a los operadores públicos y privados (es decir un incremento del 5% respecto a 2006), de los cuales el 86% concierne a sistemas instalados en lugares o centros abiertos al público, y el 14% a sistemas que controlan la vía pública.
Nota: No obstante, estos datos se deben tomar con precaución. Sin duda, se instalan algunos sistemas sin autorización, y pueden ser objeto de una regularización a posteriori. A la inversa, se conceden autorizaciones pero no necesariamente se instalan las cámaras.

➤ **1.522 municipios** franceses (de 36.682 en total, al 1 de enero de 2009, según el Instituto Nacional de Estadística y Estudios Económicos) utilizan al menos un sistema de vídeovigilancia.

LOS FRANCESES SON MUY AMPLIAMENTE FAVORABLES A LA VÍDEOVIGILANCIA

Según un sondeo realizado en 2008, el 71% de la población francesa es favorable a la utilización de la vídeovigilancia en los lugares públicos, contra el 28% que se opone.

A la pregunta, "En términos generales, ¿es usted muy favorable, más bien favorable, más bien desfavorable o muy desfavorable a la presencia de cámaras de vídeovigilancia en los lugares públicos?",

➤ **21 %** se declara muy favorable

➤ **50 %** más bien favorable

➤ **15 %** más bien desfavorable

➤ **13 %** muy desfavorable

➤ **1 %** no sabe

Este sondeo ha sido realizado por la sociedad Ipsos, del 14 al 17 de marzo de 2008, por cuenta de la Comisión Nacional de Informática y Libertades (CNIL), sobre una muestra de 972 personas mayores de 18 años, representativa de la población francesa.

1. ¿Por qué elaborar una Carta?

A través del proyecto *Ciudadanos, Ciudades y Vídeovigilancia,* el Foro Europeo de Seguridad Urbana inició una reflexión y un intercambio de experiencia sobre las formas prácticas que adopta la vídeovigilancia, en una óptica de respeto y protección de las libertades individuales. A través de tres visitas de estudio a Génova (Italia), Londres y Brighton (Reino Unido), y a Lyon (Francia), y de la experiencia en la materia de los diferentes participantes a este proyecto, a través de este trabajo se ha obtenido una visión global de las formas que cobra la vídeovigilancia y los medios que se emplean para garantizar los derechos de los ciudadanos.

¿Qué conclusiones se pueden sacar de este proyecto? ¿Qué enseñanzas se puede extraer de la experiencia acumulada por las ciudades? ¿Qué consejos se pueden dar a las ciudades que participan al EFUS (*European Forum for Urban Safety* - Foro Europeo de Seguridad Urbana) y, en general, a todos los actores a quienes incumbe la vídeovigilancia? ¿Se pueden recomendar buenas prácticas en la materia?

Principios clave para conciliar la vídeovigilancia y la protección de los derechos fundamentales

Desde luego, el proyecto ha identificado diferentes prácticas que los actores han calificado como "buenas" cuando se aplican a un problema determinado y en un contexto específico. Al comienzo del proyecto, los participantes han desarrollado conjuntamente un esquema de lectura para evaluar las diferentes prácticas con los mismos criterios, planteando cada vez las mismas preguntas y los mismos temas: protección de los datos, medidas precautorias que garanticen la vida privada, participación de los

ciudadanos en todas las etapas de un proyecto de vídeovigilancia (concepción, implementación, utilización, evaluación y desarrollo del sistema). No obstante, los participantes han considerado que sería difícil recomendar a todas las ciudades que apliquen tal o cual práctica, pensada e implementada por una ciudad en particular y en función de un contexto específico. En efecto, el proyecto ha mostrado que no existe una buena práctica europea sino que, en cambio, resulta interesante intercambiar múltiples ideas y prácticas para que cada cual determine el camino que habrá de seguir para alcanzar el objetivo que todos buscan, el de la protección de los derechos individuales.

Por lo tanto, primero había que identificar los principios generales en los cuales se fundan las buenas prácticas; después, se analizaron los diferentes retos de la vídeovigilancia y, finalmente, se formularon ideas prácticas para aplicar esos principios teniendo en cuenta los retos previamente identificados.

La idea de una *Carta para el Uso Democrático de la Vídeovigilancia*, que fuere realmente universal y que formule los principios básicos que deberían aplicarse a la vídeovigilancia, ha surgido de una triple reflexión:

1) Principios que se pueden aplicar a la vídeovigilancia en toda Europa

En una reflexión europea sobre la utilización de la vídeovigilancia que respete los derechos fundamentales, es necesario encontrar un común denominador que pueda guiar a los usuarios, más allá de los diferentes contextos institucionales, legales y culturales. No se trata de obtener el común denominador más pequeño, sino que, por el contrario, encontrar los

puntos esenciales en los cuales todos puedan estar de acuerdo, sabiendo que, después, cada cual es enteramente libre de apoyarse en un amplio abanico de opciones para adoptar la o las mejores soluciones para cada país o cada región, en función de cada situación.

2)Principios que puedan aplicarse a todos los retos que presenta la vídeovigilancia

El objeto de la Carta es formular un conjunto de normas que respondan a todos los retos que presenta la vídeovigilancia. Los participantes han buscado pues identificar los principios fundamentales que fundan el derecho a la confidencialidad de la vida privada en todos los aspectos correspondientes a la vídeovigilancia. Estos principios son independientes unos de otros, aunque también son complementarios. Se los puede aplicar en todos los casos donde se recurre a la vídeovigilancia, ya sea al planificar un proyecto, al implementar un sistema, al concebir el modo de utilización, la protección de los datos o la evaluación del sistema y las eventuales modificaciones. En la aplicación de estos principios aparecen las recomendaciones sobre el tipo de acción que se debe realizar. Además, los ejemplos de prácticas y técnicas concretas pueden inspirar la realización de acciones concretas.

3)Principios sostenibles en un contexto de desarrollo tecnológico rápido

La evolución tecnológica y el permanente incremento de la capacidad de los sistemas de vídeovigilancia han constituido un tema clave de los debates sobre la protección de la vida privada. En efecto, los sistemas son cada vez más potentes e inteligentes (reconocimiento automático de los vehículos, de las personas, de los comportamientos, etc.), y están cada

vez más conectados a otros sistemas de información. La vídeovigilancia es sólo un elemento entre otros dentro de la red tecnológica que rige nuestras ciudades, se desarrolla de modo irreversible y lo hace a una velocidad exponencial. Por esta razón, toda recomendación sobre la buena utilización de la vídeovigilancia puede quedar superada muy pronto por la evolución de la realidad tecnológica.
Por otra parte, la evolución de la tecnología ofrece nuevas soluciones a determinados dilemas éticos. Por ejemplo, actualmente existen sistemas que impiden que las cámaras puedan filmar el interior de los espacios privados (véase el artículo de Jeroen van den Hoven). Por ello, las recomendaciones formuladas en la Carta no se refieren a métodos prácticos de utilización de tal o cual técnica, sino a la aplicación de principios de fondo.

No obstante, uno de los objetivos de este trabajo también era suministrar a las ciudades los medios concretos para que pudieran llevar a cabo sus propias políticas. Por esta razón, la Carta presenta una serie de recomendaciones y métodos prácticos a título indicativo.
Es importante indicar que la Carta para el Uso Democrático de la Vídeovigilancia no pretende resumir todos los debates existentes en el marco del proyecto. Además, la Carta no puede ni pretende substituir el diálogo a través del cual se intercambian prácticas concretas y que se llevan a cabo en el marco del proyecto, del cual esta publicación es la narración. La publicación es un complemento de la Carta y constituye un primer paso hacia una guía práctica.

Una Carta europea de las ciudades y las regiones
La elaboración de la Carta no se lleva a cabo únicamente sobre la base de prácticas que se observan en

las ciudades. Desde luego, los debates también se han fundado en las legislaciones nacionales en vigor, los textos europeos y las primeras iniciativas de las Cartas locales que tratan de los derechos individuales.

La iniciativa que impulsa aquí el EFUS *(European Forum for Urban Safety)* no es única en su tipo. Se trata, más bien, de un trabajo complementario que colma un vacío tanto local como europeo. La vídeovigilancia es un fenómeno europeo que concierne a todos los ciudadanos que viven, trabajan y viajan por Europa. Al mismo tiempo, las autoridades locales son responsables de la vídeovigilancia del espacio público. La originalidad de la Carta se observa en el establecimiento de un puente entre las dimensiones local y europea.
En efecto, los textos europeos que tratan de la vídeovigilancia sólo pueden suministrar la opinión y las recomendaciones de los expertos. Por su parte, una Carta de las colectividades locales europeas refleja el compromiso de un conjunto de ciudades y regiones de Europa para aplicar, localmente, los principios que garantizan una utilización democrática de la vídeovigilancia.

Las instituciones europeas tienen un papel importante en la protección de los derechos fundamentales y en la protección de la vida privada: Convención de los Derechos del Hombre, del Consejo de Europa (1950) artículo 8, Carta de los Derechos Fundamentales de la Unión Europea (2001/2009) artículos 7 y 8, y, en la protección de los datos, Convenio 108 de 1981 del Consejo de Europa, Directiva 95/46/CE de la Unión Europea. También se han pronunciado sobre la vídeovigilancia y han formulado recomendaciones muy similares a las de la Carta en el informe del Comité Europeo de Cooperación Jurídica (CDCJ) (2003), en la resolución 4/2004 del Grupo de Trabajo sobre Protección de Datos – Artículo 29 de la Comisión de Venecia

(2007), en la resolución 1604 (2008) de la Asamblea Parlamentaria del Consejo de Europa, y en las líneas directrices sobre la vídeovigilancia del Supervisor Europeo de Protección de Datos (CEPD) (2010).
Aun cuando estos textos muy completos han inspirado profundamente el proyecto, no han explicitado los principios en los cuales se han fundado estas diversas recomendaciones. A pesar de que varios países hayan aprovechado la oportunidad para transponer la directiva 95/46/CE al derecho nacional y legislar también sobre la vídeovigilancia, y aunque los convenios sobre la protección de los derechos fundamentales y la protección de la vida privada atañe al derecho europeo e internacional, por el momento las instituciones europeas no tienen competencia para legislar sobre la vídeovigilancia. Por lo tanto, las instituciones europeas deben contentarse de las orientaciones y las recomendaciones, contando en el hecho de que su mensaje sea escuchado al igual que en la buena voluntad de los interesados. Es precisamente a falta de una reglamentación europea que la Carta del Foro cobra un sentido cabal.

Las legislaciones nacionales que sientan el marco obligatorio dentro del cual se debe utilizar la vídeovigilancia varían mucho de un país a otro (véase el artículo de Laurent Lim en este volumen). Mientras que algunos países tienen una legislación y una reglamentación muy precisas en lo referente a la vídeovigilancia, otros países siguen teniendo una legislación general de protección de la vida privada y de los datos personales. En algunos países, una Carta sobre la vídeovigilancia sería una verdadera novedad. En muchos otros, los principios de la Carta completarán la legislación en vigor, y sobre todo destacarían una voluntad y una inquietud políticas para una utilización responsable de esta tecnología por parte de las autoridades y de los electos territoriales.

El compromiso de las ciudades con la Carta – un complemento importante para la legislación en vigor.[48]

Las Cartas y los códigos deontológicos son modos de regulación informal o de *"soft law"*, ya que no constituyen una legislación oficial. No obstante, sería un error pensar que estas Cartas no son importantes para la regulación interna. Suministrando valores y principios de administración, les incumbe un papel central para crear una cultura organizativa de la vídeovigilancia, poniendo a disposición de los operadores de cámaras y a los responsables, los principios que pueden guiar la toma de decisiones día a día. Además, estos documentos pueden servir como punto de referencia y comparación *(benchmark)* para medir el funcionamiento del sistema y suministrar una base sobre la cual desarrollar procedimientos detallados referentes a la operación y a la gestión de un centro de vídeovigilancia.

Las Cartas también pueden tener una función importante en la comunicación destinada al público. Al dar una explicación clara sobre la razón de ser y los límites de la vídeovigilancia, una Carta puede infundir confianza en la finalidad del sistema y darle al público una serie de criterios para evaluar el buen funcionamiento y el éxito del sistema. En este sentido, pueden suministrar a los ciudadanos un marco claro en el cual expresar sus inquietudes. Por consiguiente, este marco es una ayuda a los ciudadanos, para verificar que los responsables del sistema asuman sus responsabilidades y no superan su mandado "de vigilancia".

En cuanto a la relación entre las Cartas y el poder discrecional del ejecutivo local, es evidente que la importancia de la *"soft law"* depende de las circunstancias y de las necesidades locales. En varias ciudades europeas existe la idea de que las instala-

ciones de vídeovigilancia deberían estar bajo el control directo de los electos locales y que su funcionamiento debería formar parte de su poder discrecional. Evidentemente, como las Cartas no son legalmente obligatorias u oponibles, no pueden substituirse al poder discrecional del ejecutivo. Tampoco pueden ser utilizadas para modificar o interpretar las leyes existentes. No obstante, la adopción de una Carta tendría la ventaja de suministrar una estructura para la utilización discrecional del poder, confiriendo transparencia para utilizar la vídeovigilancia y garantizar que sus objetivos sean bien conocidos y comprendidos por el público. Por último, las Cartas pueden ayudar a los nuevos electos a comprender el funcionamiento y los retos que presenta la vídeovigilancia, garantizando cierto nivel de continuidad operativa y de gestión, después de las elecciones o durante otros períodos de cambio político.

En síntesis, la principal ventaja de las Cartas es su capacidad de crear estilos organizativos y operativos, promover la responsabilidad *(accountability)* y la transparencia, y de este modo hacer que el público general comprenda mejor qué cosa es la vídeovigilancia. Por esta razón, las Cartas pueden constituir un elemento muy útil para las leyes y regulaciones existentes, y ser un contrapeso en la administración de la vídeovigilancia ejercido por el poder ejecutivo discrecional y por la administración. Por estos motivos, varios miembros del EFUS *(European Forum for Urban Safety)* como Lyon y Le Havre tienen ya una Carta, y por lo mismo, la Comisión Nacional de Informática y Libertades (CNIL) de Francia ha acompañado esta iniciativa y ha contribuido a una iniciativa similar con el Grupo Art 29, una iniciativa que el Su-

[48] Benjamin Goold, Universidad de British Columbia/Universidad de Oxford

pervisor Europeo de Protección de Datos (CEPD). Así, los participantes en el proyecto consideran que toda iniciativa orientada a crear una Carta puede interesar no sólo las ciudades y regiones europeas, sino también todos los actores que tienen objetivos similares.

3. Los principios de la Carta

1. Principio de legalidad

El Foro se ha constituido en torno de una convicción – "las ciudades ayudan a las ciudades" – que está presente en todos los proyectos europeos que lleva a cabo. En la reflexión en torno de la temática central del proyecto sobre la vídeovigilancia, cada ciudad participante ha expresado la decidida intención de conocer la experiencia y el contexto de las demás ciudades que participan en el proyecto.

Los proyectos están ante todo determinados por la legislación en vigor. Invocar un principio de legalidad no es una evidencia inicial, ya que queda pendiente la pregunta de si había que hablar de legalidad o más bien de legitimidad.

La legitimidad es tener el derecho de llevar a cabo una acción o de ocupar un cargo. Por ejemplo, los electos obtienen su legitimidad de las elecciones y los policías de una condición específica que les confiere un concurso. La única legitimidad que se aplica en todos los casos es la de la ley. Afirmar el principio de legalidad en lo referente a la vídeovigilancia es afirmar que la primera legitimidad de un sistema de vídeovigilancia debe fundarse en la legislación en vigor.

Estas legislaciones reflejan una mentalidad y revelan orientaciones sociales. También revelan una cultura, una historia y relaciones de fuerza, de equilibrio o de

compromiso entre autoridades y ciudadanos, ciudades y estados, e incluso entre diferentes planos territoriales.

Evidencian relaciones de confianza o desconfianza y son, esencialmente, una herramienta de legitimación de un modo de operar.
Por lo tanto, constituyen una base de trabajo fundamental.

El primer plano en el que se han interesado los diferentes participantes es el nivel comunitario, ya que las legislaciones definen las reglas que se han de ejercer en todos los países de la Unión Europea.

>>

Así, la Carta recuerda que:
La elaboración y el desarrollo de los sistemas de vídeovigilancia sólo pueden realizarse en cumplimiento estricto de la ley las reglamentaciones en vigor, es decir, en aplicación y de conformidad con las exigencias de la ley europea, nacional, regional o local. Su desarrollo también debe hacerse en cumplimiento estricto de las normas referentes a la protección de los datos, de los textos que rigen la escucha de las comunicaciones y las conversaciones, la injerencia ilícita en la vida privada, la protección de la dignidad, la imagen, el domicilio y demás lugares en los cuales existe una protección análoga. También se deben tener en cuenta las normas referentes a la protección de los trabajadores.

¿Cómo se debe aplicar este principio de legalidad?
Esta aplicación supone el conocimiento de los textos en vigor. El reto para los diferentes participantes era destacar estos textos que no conciernen específicamente la vídeovigilancia pero que las ciudades

deberán tener en cuenta al instalar sus sistemas, además de su propia legislación, cuando exista.

➤ L os sistemas de vídeovigilancia deben elaborarse en coherencia con:

1) El derecho europeo e internacional:

➤ El Convenio Europeo para la Salvaguarda de los Derechos Humanos y de las Libertades Fundamentales (CEDH) del Consejo de Europa – 1950;

➤ El Convenio 108 del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal – 1981;

➤ La Carta de los Derechos Fundamentales de la Unión Europea;

➤ - La Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas respecto al tratamiento de los datos de carácter personal y la libre circulación de esos datos.

2) Las reglamentaciones nacionales y locales rigen los sistemas de vídeovigilancia y la protección de los datos de carácter personal;

➤ Evaluar la pertinencia de una instalación de vídeovigilancia respecto a los objetivos para los cuales la Constitución autoriza una limitación del ejercicio de los derechos fundamentales de los ciudadanos.

3) Las diferentes jurisprudencias existentes en la materia

➤ Habida cuenta de las evoluciones tecnológicas, en caso de vacío jurídico sobre un punto específico, la adopción del sistema de vídeovigilancia debe obedecer a los demás principios definidos en la presente Carta.

A través de este principio de legalidad se afirma lo siguiente: el cumplimiento de la reglamentación en vigor es el primer acto de democracia. Las diversas legislaciones, por más diferentes que sean, permiten encuadrar el desarrollo de los sistemas de vídeovigilancia.

Tener en cuenta la legislación en vigor es una prenda de sostenibilidad.
Este principio de legalidad sienta un marco de legitimación, de objetivación de la vídeovigilancia que, como todo marco, debe ser precisado con más precisión.

La legalidad en los hechos

Este principio de legalidad se aplica de modos diferentes a través de Europa. Mientras que en algunos Estados el funcionamiento de la vídeovigilancia está regido por una ley general que concierne la protección de los datos, en otros países como Bélgica, Italia y España, la utilización de esta tecnología está estrictamente delimitada. Por ejemplo, la ley impone en estos países que se apliquen determinados parámetros técnicos al sistema para no filmar las zonas privadas (ventanas y puertas, por ejemplo). La ley también estipula el tiempo durante el cual se podrán conservar los datos personales y hace obligatorio informar al público la identidad de la autoridad responsable de la instalación y la administración del sistema de vigi-

lancia. Sobre este último punto, tanto el sistema italiano como el belga imponen el marco dentro del cual se debe realizar la comunicación destinada a los ciudadanos, exigiendo que todas las ciudades utilicen el mismo cartel de señalización y hagan figurar determinada información que exige la ley.

Otro aspecto importante del principio de legalidad concierne la formación de los operadores de vídeo. Es fundamental que ese personal conozca la legislación en materia de protección de los datos, que es obligatoria en algunos países como por ejemplo el Reino Unido. En otros, como en Francia, esta formación figura habitualmente entre las prescripciones deontológicas que las autoridades públicas dan a los operadores. Por último, en otros países, la formación depende de la voluntad de las autoridades locales.

Un tercer aspecto fundamental del principio de legalidad se refiere a los procedimientos de control independientes de las autoridades públicas. De tal suerte, muchos países han instituido organismos independientes que velan por que las autoridades públicas, que son los usuarios de los sistemas de vídeovigilancia, cumplan cabalmente la ley. Se trata, por ejemplo, de los Comités de Ética en Francia, el "*Garante de la Privacy*" en Italia y la Agencia Española de Protección de Datos (AEPD) que por ejemplo tiene el derecho de infligir sanciones si no se cumplen las disposiciones legales.

La creciente utilización de la vídeovigilancia exige que se adapten las leyes para encuadrar y limitar la injerencia en la vida privada. En este sentido, en el Reino Unido, en 2008 se ha definido un marco estratégico nacional y el gobierno electo en junio de 2010 ha incluido en su programa de acción el tema de la protección de la vida privada respecto a la vídeovigilancia.

Conocer y aplicar la ley es, evidentemente, una obligación *sine qua non,* pero nada impide que las ciudades

tomen medidas que van más allá de las exigencias de la ley para garantizar la confidencialidad de la vida privada y las libertades fundamentales. Recopilar las experiencias y formular recomendaciones al respecto era justamente uno de los objetivos del proyecto que ha dado origen a esta Carta.
La ley no prescribe sino que establece un marco en el cual se puede implementar el sistema. Así, ¿qué elementos de un sistema de vídeovigilancia podemos considerar que son prescriptivos? En otras palabras, ¿cómo aplicar los principios de la Carta para adoptar y/o administrar un sistema de vídeovigilancia?

2. Principio de necesidad

Todos los participantes han podido observar que la vídeovigilancia no es una solución en sí misma, sino una herramienta entre otras de una estrategia global de seguridad. De cara a una evolución tecnológica de los sistemas de vídeovigilancia y la cantidad creciente de ciudades que los utilizan, es importante recordar que la instalación de esta clase de sistema no puede constituir un fin en sí mismo, sino que debe ser un instrumento necesario.

Pero, ¿cómo definir una necesidad de esta clase sin caer en la apología de la vídeovigilancia? ¿Cómo definir un principio de necesidad sin prejuzgar la libertad que le cabe a cada ciudad de definir sus propias orientaciones estratégicas en materia de seguridad, con o sin vídeovigilancia? Por lo demás, ¿se puede decir que la necesidad es, en sí misma, un principio fundamental?

Siempre es delicado decidir instalar un sistema de vídeovigilancia como algo necesario. En efecto, responder a la pregunta de si tal sistema es necesario requiere conocimientos sobre la eficacia de la vídeovigilancia. ¿Cuál es la contribución de la vídeovigilancia a la resolución de una problemática específica? ¿La vídeovigilancia es acaso la

mejor respuesta en tal o cual contexto?
No hay una respuesta sencilla a estos interrogantes, sobre los cuales los participantes a este proyecto han debatido profundamente. Las evaluaciones científicas suministran resultados mitigados, como lo prueban, por ejemplo, los estudios realizados para el Home Office británico (Welsh y Farrington 2002, Gill y Sprigg 2005, Gill y otros 2005). Lo primero que conviene distinguir es la finalidad del sistema: ¿se trata de un dispositivo destinado a evitar la criminalidad o bien de facilitar la investigación *a posteriori*? En cuanto a los efectos que se piensa obtener, pueden variar considerablemente en el tiempo y no son idénticos con toda clase de delitos. La función de *prevención* supone, pues, que el delincuente potencial razone y actúe de modo racional. Pero se sabe perfectamente que muchos delitos se cometen, precisamente, "impulsados por la emoción". Tampoco está garantizada la eficacia de la vídeovigilancia en el ámbito de la investigación del delito, ni su eficacia en la atenuación del sentimiento de inseguridad.

Lo dicho son otras tantas consideraciones que se tienen que tener en cuenta al hablar de necesidad. No se trata de una necesidad en sí misma, sino más bien de una necesidad que debe ser formulada al término de un diagnóstico. Es el razonamiento que desemboca en la decisión de instalar un sistema de vídeovigilancia que resulta necesario.

>>

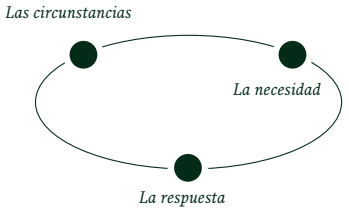
DEFINICIÓN DEL PRINCIPIO EN LA CARTA:
Instalar un sistema de vídeovigilancia no puede constituir, en sí mismo, una exigencia.

La instalación de esta clase de sistemas se debe decidir en función de una necesidad. La necesidad remite a la adecuación entre las circunstancias y una

necesidad, por una parte, y la respuesta que constituye el sistema de vídeovigilancia, por otra. Es determinada necesidad y tales o cuales circunstancias lo que determina que una decisión a favor de esta clase de sistemas sea pertinente y su acción ineluctable. El principio de necesidad exige que aparezca claramente el razonamiento correspondiente a una actuación determinada y que la justifique como corresponde. Este principio de necesidad es lo que respalda la decisión de instalar un sistema de vídeovigilancia. La necesidad cobra así una dimensión prescriptiva. "La necesidad es ley".

¿De qué modo, pues, aplicar este principio de necesidad? A través de este principio se presenta el razonamiento que justifica la instalación del sistema de vídeovigilancia. Este razonamiento se estructura en torno de la identificación de las circunstancias, de la definición de las necesidades y de la necesidad de la respuesta que es la vídeovigilancia.

Tres elementos constituyen este principio de necesidad:



La conjunción de las circunstancias y la necesidad funda la necesidad de la respuesta.

Aquí, la Carta retoma un método de resolución de problemas similar a la que ha utilizado la policía británica en su trabajo de proximidad *(neighborhood policing)*. El

método que se sigue aquí el del procedimiento conocido como «SARA», cuya sigla en inglés significa *scanning* (rever un problema, una situación y las circunstancias correspondientes), *analysis* (analizar las necesidades), *response* (definir una respuesta) y *assessment* (evaluar la respuesta que se ha dado al problema).

La principal ventaja de este enfoque es que permite distinguir el problema que se debe abordar, de los síntomas observados. Si no se realizan las dos primeras fases del "*scanning*" y del "analysis" con rigor suficiente, se puede lograr una respuesta que sólo se ocupe de los síntomas y no del verdadero problema subyacente.
El peligro que presenta la vídeovigilancia es que resulta muy tentador pensar que constituye la respuesta que se busca y que, por ello, ya no es menester seguir todos los pasos de este proceso. La pregunta central ya no es "¿cuál es la mejor respuesta a este problema?", sino "si se desea instalar un sistema de vídeovigilancia, ¿cómo se lo puede justificar?".

El principio de necesidad de la Carta impone un enfoque diferente, que plantea el problema antes que la solución, considerando que según el caso la vídeovigilancia puede o no resultar eficaz. Este enfoque considera que la vídeovigilancia es una respuesta entre muchas otras y también permite relativizar su eficacia respecto a otras herramientas de seguridad urbana.

También es muy importante evaluar el sistema (la cuarta fase del proceso SARA). El principio de necesidad no sólo concierne la decisión de instalar un sistema, sino también cada desarrollo durante toda su "vida útil". La pregunta por la necesidad del sistema es en realidad permanente y se plantea, por ejemplo, cuando se piensa en una ampliación del sistema: ¿es

una inversión necesaria para la seguridad? También se plantea si la situación inicial cambia. Por ejemplo, ¿qué hacer cuando se observa una significativa mejora del nivel de seguridad? ¿La vídeovigilancia sigue siendo entonces necesaria? Aunque fuera irresponsable no tener en cuenta las inversiones realizadas y hay que interrogarse sobre cuáles serían las consecuencias de suprimir el sistema de vídeovigilancia, la opción de retirar las cámaras siempre es una posibilidad.

Así, la ciudad de Rotterdam ha pensado en determinado momento retirar algunas cámaras, después de llevar a cabo un proceso de evaluación. Los habitantes del barrio en donde se retirarían las cámaras se han opuesto porque la presencia de esas cámaras les daba más seguridad. Otras ciudades europeas han tenido la misma experiencia, lo que muestra al mismo tiempo que el principio de participación de los ciudadanos puede resultar más complejo de lo que podría pensarse. En el caso de Rotterdam, se decidió finalmente reducir la cantidad de cámaras instaladas, lo que equivale a dar una respuesta adecuada a una nueva necesidad.

Otro ejemplo interesante es el de la ley del Länd alemán de Bade-Wurtemberg, según la cual sólo se puede considerar que es necesario un sistema de vídeovigilancia si se puede demostrar estadísticamente que una zona determinada resulta singularmente criminógena. En Mannheim, las autoridades locales y la policía debieron desmantelar un sistema de seis cámaras instalado en el centro de la ciudad desde hacía unos cinco años, porque la tasa de criminalidad había disminuido significativamente. Desde que se retiraron las cámaras, la situación permaneció estable, lo que también podría resultar de otras medidas que adoptaron las autoridades locales, por ejemplo, haber modernizado el lugar y el alumbrado público.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

RECOMENDACIONES / MODALIDADES DE ACCIÓN

En este contexto, para la aplicación del principio de necesidad se pueden hacer las recomendaciones siguientes:

Sobre las CIRCUNSTANCIAS

➤ Identificar con precisión la problemática de la seguridad y la prevención de la delincuencia identificada en el territorio de la ciudad efectuando una auditoría o un diagnóstico.

➤ Describir los recursos locales disponibles y los dispositivos existentes que permitan responder a esta situación descrita en el diagnóstico.

Sobre las NECESIDADES

➤ Establecer las necesidades resultantes del diagnóstico y de la descripción de las potencialidades locales. Las necesidades deben indicarse con el mayor detalle posible, ya que a partir de ellas se establecerán los futuros objetivos del proyecto.

➤ Considerar si es posible recurrir a otros medios menos intrusivos para responder a esta problemática.

Sobre la RESPUESTA

➤ Hay que definir los objetivos e identificar los beneficios y los resultados que se espera obtener con el sistema. Estos objetivos deben traducirse en modos de funcionamiento, de suerte que habrá que definir, por ejemplo, qué implicaciones funcionales caben para un

sistema de vídeovigilancia destinado a prevenir la delincuencia.

➤ de modo realista, lograr sus objetivos. El sistema de vídeovigilancia debe estar calibrado para responder con pertinencia y eficacia a las necesidades identificadas.

➤ Las instalaciones de vídeovigilancia sólo se podrán en servicio una vez que todas las demás medidas, menos intrusivas, hayan mostrado que son insuficientes o inaplicables (después de una evaluación pertinente), o bien que el tipo de problema que se debe resolver está fuera del alcance de esos medios. Como sea, la vídeovigilancia sólo debe representar una parte de una respuesta coordinada al problema identificado.

➤ Autorizarse a aplicar un derecho de retirada, de ser necesario. Las ciudades deben poder considerar, basándose en una evaluación, que la vídeovigilancia puede dejar de ser necesaria o bien que se deberían distribuir las cámaras de otro modo.

Una vez que se haya sentado la necesidad del sistema, todavía hay que establecer su dimensión y calibrarlo respecto al razonamiento que se aplica en el marco del principio de necesidad. De este modo, los dispositivos de vídeovigilancia se calibrarán en la justa proporción.

3. Principio de proporcionalidad

La proporcionalidad es un principio que ha sido difícil definir. Se la puede definir como la justa medida, pero ¿cómo evaluarla, en qué momento y respecto a qué? Además, ¿cómo se puede determinar la proporcionalidad fuera de un contexto específico? ¿Cómo prescribir en una Carta Europea lo que es adecuado en tal o cual contexto específico de una ciudad o de una región determinada?

Para los diferentes participantes, después de debatir este principio, lo importante no era definir una norma general, sino más bien insistir en la necesidad de calibrar el sistema de vídeovigilancia en función de cada contexto particular y de circunstancias específicas.

La comparación entre los sistemas de vídeovigilancia se suelen hacer en función de la cantidad de cámaras. Pero no es necesariamente el mejor criterio, ya que el número de cámaras debe corresponder a las necesidades identificadas en la ciudad.

Detrás de este principio de proporcionalidad, está la búsqueda de la justa medida. Un sistema de vídeovigilancia debe aplicarse en coherencia con el razonamiento que se recomienda en el principio de necesidad. Este principio de proporcionalidad también está vinculado al principio de responsabilidad. En efecto, definir un sistema que respete la justa medida es un acto de responsabilidad de las autoridades.

>>

Así:

La elaboración, la instalación, el funcionamiento y el desarrollo de los sistemas de vídeovigilancia deben respetar una justa medida.

La instalación de estos sistemas de

vídeovigilancia debe evaluarse respecto a la problemática a la que se debe responder. La proporcionalidad que se busca es, ante todo, cuestión de adecuación entre los objetivos que se deben lograr y los medios que se emplean para hacerlo. El principio de proporcionalidad está, pues, íntimamente vinculado a la noción de equilibrio, y este equilibrio exige que la vídeovigilancia no sea la única respuesta de seguridad y de prevención de la delincuencia a la que recurra una ciudad.

¿Cómo se debe aplicar este principio de proporcionalidad? Este principio se ejerce en diferentes niveles de la definición y de la aplicación del sistema.

RECOMENDACIONES / MODALIDADES DE ACCIÓN

La proporcionalidad se debe evaluar en cada fase y en cada modalidad del tratamiento de los datos, especialmente cuando se debe definir:

La dimensión de la instalación y la capacidad técnica de las cámaras

➤ La organización técnica y humana debe adaptarse estrictamente a las necesidades. Esto exige que se emplee una tecnología con la cual se puede responder a los objetivos que se buscan, sin rebasarlos. La utilización de un sistema de vídeovigilancia debe estar limitada en el tiempo y en el espacio, es decir, a un momento y en un territorio específico, como respuesta a una necesidad claramente definida. Asignar una nueva función al sistema de vídeovigilancia impone una reflexión sobre la necesidad (Principio I). –
➤ Esta instalación técnica debería integrar

también un sistema de ocultación de las zonas privadas a través de un enmascaramiento dinámico, ya que un sistema de vigilancia del espacio público no puede tener como "efecto secundario" la vigilancia del espacio privado. Se trata de un imperativo que debe tenerse en cuenta cuando se planifica el posicionamiento, la orientación y el tipo de cámaras (fijas o móviles).

La protección de los datos

Las imágenes capturadas a través del sistema de vídeovigilancia constituyen datos de carácter personal y deben ser protegidos del mismo modo que cualquier otro dato personal. Esto exige aplicar reglas estrictas que rigen la grabación, conservación, consulta y supresión eventual de las imágenes. Es importante cerciorarse que los objetivos estén perfectamente adecuados con los puntos siguientes:

➤ La decisión de almacenar o no las imágenes.

➤ Tiempo durante el cual se conservarán eventualmente los datos que, de todos modos, debe ser temporal. El plazo durante el cual se conserven los datos debe limitarse a lo estricto necesario, restringido y definido por los parámetros del sistema.

➤ La protección física y técnica de los datos personales.
Por lo tanto, es necesario definir los protocoles que habilitan el acceso y la transmisión de las imágenes. En estos protocolos se debe incorporar la política *"Privacy by design"*, por la cual la protección de los datos personales se

tiene en cuenta en las etapas iniciales de concepción de los equipos de vídeovigilancia.

➤ Los sistemas de vídeovigilancia deben encontrar su equilibrio y su proporción en una política integrada de seguridad y de prevención de la delincuencia. Son una herramienta para una política de seguridad global y deben estar en coherencia con las demás respuestas que se aplican localmente.

La proporcionalidad en la práctica...

En 1997, la ciudad de Saint-Herblain ha llevado a cabo una auditoría de seguridad antes de instalar un sistema de vídeovigilancia, realizada por un estudio exterior. Paralelamente, la Comisión de Seguridad del Consejo Comunal de Prevención de la Delincuencia (CCPD) llevó a cabo una reflexión sobre los diferentes aspectos de la seguridad en la ciudad de Saint-Herblain. En 1998, esta Comisión entregó su informe al senador-alcalde, quien decidió la creación de varios grupos de trabajo sobre las diferentes temáticas vinculadas a problemas de seguridad. En 1999, se presentó ante el Consejo Municipal la síntesis de los grupos de trabajo. Además, una encuesta de opinión sobre la seguridad, realizada a través de un panel representativo ha mostrado que este tema constituía la primera preocupación de los habitantes de Saint-Herblain.

Con todos estos elementos de diagnóstico, el alcalde lanzó un debate en el Consejo Municipal sobre la aplicación de las propuestas del CCPD, entre las cuales figuraba la vídeovigilancia. En junio de 1999, el Consejo Municipal votó favorablemente la instalación de un sistema en el municipio y la creación de un Comité de Ética para acompañar el desarrollo de este proyecto.

Se ve, pues, que en Saint-Herblain el debate sobre

la vídeovigilancia se ha incorporado a una reflexión global sobre la problemática de la seguridad. Gracias al diagnóstico inicial se ha podido establecer una necesidad y se han hallado los elementos para calibrar todo el dispositivo.
La proporcionalidad se ejerce así tanto para definir la envergadura que debe tener el sistema de vídeovigilancia como integrarlo a una política local de seguridad y de prevención de la delincuencia. La vídeovigilancia forma parte de una política global y tiene una coherencia proporcional con los demás elementos del dispositivo.
En razón de que la instalación del sistema responde a una necesidad y que su despliegue se lleva a cabo en una justa medida, el sistema tendrá una perfecta transparencia.

4. Principio de transparencia
Durante todo el proyecto, una de las principales preguntas de los participantes fue la siguiente: ¿cómo hacer que los sistemas de vídeovigilancia resulten comprensibles para los ciudadanos y garantizar tanto la confidencialidad de su vida privada como sus derechos fundamentales?
La transparencia está directamente vinculada a la información que se comunica a los ciudadanos y en este sentido hay que preguntarse ¿cuál es la información pertinente? ¿Qué nivel de información se debe suministrar a los ciudadanos? ¿Los ciudadanos desean ser informados? En caso afirmativo, ¿sobre qué temas?
El reto que presenta este principio no es tanto afirmar la necesidad de informar a los ciudadanos sino definir el tipo de información que se les debe suministrar y las condiciones de esa información.
Toda autoridad a cargo de un sistema de vídeovigilancia debe tener una política clara y transparente en cuanto al funcionamiento de su sistema.

La transparencia depende estrechamente de la comunicación. Es transparente lo que se ve desde el exterior. Este principio se basa pues en la información que se suministra. Es un principio fundamental ya que si se puede considerar que la vídeovigilancia es una tecnología que restringe las libertades, debe acompañarse siempre con una sólida información destinada al público. Toda información correspondiente al dispositivo debe respetar la legislación en vigor y asumir este principio de transparencia.

RECOMENDACIONES / MODALIDADES DE ACCIÓN

➤ La autoridad que tiene la iniciativa de instalar las cámaras de vídeovigilancia debe informar claramente a los ciudadanos sobre los siguientes puntos:

➤ El proyecto de instalar un sistema de vídeovigilancia.

➤ Los objetivos de esas cámaras.

➤ Los medios que se utilizarán para instalar el sistema.

➤ Las zonas sometidas a una vídeovigilancia. A este efecto, es necesario recurrir a una señalización visible y reconocible con un pictograma.

➤ La identidad, la función y los datos necesarios para ponerse en contacto con las personas a quienes pedir información sobre la vídeovigilancia. Esta información debe figurar en los carteles de señalización de las

zonas que están sometidas a una vídeovigilancia.
➤ Las medidas específicas de protección de las imágenes registradas. Los datos creados con un sistema de vídeovigilancia deben estar protegidos por un acceso restrictivo que incluya una contraseña y sólo se los debe utilizar para los fines previstos, por las personas autorizadas y ser conservadas el tiempo necesario. Toda utilización de estas imágenes grabadas debe ser notificada en un registro actualizado a tal efecto.

➤ Las autoridades que pueden ser destinatarias de estas imágenes registradas.

➤ Los derechos de las personas en lo referente a sus imágenes. En particular, se trata de los derechos siguientes:

Derecho de consultar su imagen sin infringir el derecho de terceros. Este derecho puede ser negado en el caso de investigaciones judiciales o incluso en casos de riesgo vinculados a la seguridad o a la defensa nacional.

Derecho de verificar la supresión de las imágenes que le incumban cuando la fecha límite de conservación de las mismas se haya rebasado.

Esta información debe ser comprensible y estar expresada en un lenguaje claro e inteligible.

➤ La autoridad que está a cargo del sistema deberá informar a los ciudadanos con frecuencia los resultados que obtiene y el logro de los objetivos, recurriendo a los modos de comunicación habituales. Esto implica una formulación clara de los objetivos al comienzo

del proyecto y requiere evaluaciones del dispositivo fundadas en indicadores que serían definidos previamente.
➤ Queda totalmente desaconsejado recurrir a las cámaras ficticias. Esta información falsa puede desacreditar el sistema y comprometer la responsabilidad de sus administradores.

La transparencia en la práctica

Todas las ciudades que participan en el proyecto han establecido un sistema para informar a los ciudadanos sobre su sistema de vídeovigilancia.
Por ejemplo, en Rotterdam, cada vez que se instala una cámara, se invita a todos los actores correspondientes, incluyendo a los ciudadanos, a visitar el centro de control. La experiencia ha mostrado que se aprecia mucho esta política de transparencia y que está dando buenos resultados, ya que el 80% de la población interrogada en una encuesta destinada a evaluar los diferentes dispositivos de seguridad se ha pronunciado a favor de la utilización de cámaras, y sólo el 1,2% estaba en contra, mientras que el resto no manifestó ninguna opinión. La dificultad se presenta cuando se produce un incidente y que no se han registrado imágenes, porque en este caso los habitantes tienen mayores expectativas.
La ciudad de Lyon también ha iniciado una acción a favor de la transparencia a través de su Colegio de Ética y una acción sobre la señalización. En efecto, del 30% al 40% de la población conoce el Colegio. Asimismo, la señalización responde al marco reglamentario y suministra una buena información a los ciudadanos. En cada lugar sometido a la vídeovigilancia, la señalización es muy clara y visible. De este modo, el público está informado que puede dirigir cualquier reclamo al Colegio de Ética.
Además, la Carta de Ética elaborada por la ciudad de Lyon, que retoma los compromisos asumidos por la ciudad a favor de la protección de los derechos de los ciu-

dadanos, se encuentra disponible en el sitio Internet de la ciudad, en el ayuntamiento de cada barrio y en el ayuntamiento central, al igual que en todas las asociaciones miembros del Colegio.

5. Principio de responsabilidad

El principio de responsabilidad debe garantizar que la responsabilidad del sistema esté en manos de una autoridad precisa. Esto implica que sus responsabilidades sean claras y conocidas, y que esta autoridad asume las responsabilidades del sistema.

El derecho de vigilancia del espacio público está reservado a las autoridades que deben ser designadas de modo muy restrictivo. Estas autoridades son responsables de los sistemas instalados en su nombre.

Las autoridades que están a cargo de los sistemas de vídeovigilancia son garantes de una utilización legal y que respete tanto la confidencialidad de la vida privada como las libertades fundamentales de estos sistemas. Deberán asumir su responsabilidad en caso de cometerse una falta o una violación claramente constatada. Las autoridades administrativas antes las cuales se podrá poner en juego esta responsabilidad deben ser claramente identificadas. Las empresas privadas que poseen y administran esta clase de sistemas de vídeovigilancia que registran escenas del espacio público deben adoptar las mismas normas que las autoridades públicas.

Habría que interrogarse sobre qué sería una responsabilidad sin sanción. La vocación de la Carta no es definir sanciones, sino suministrar las herramientas que destaquen las autoridades responsables y destacar prácticas de ciudades que obliguen a los operadores a asumir su responsabilidad.

La elección de electos locales por sufragio universal es la garantía de legitimidad y responsabilidad por excelencia.

El electo debe asumir sus responsabilidades de cara a los electores y, en caso de no asumirla, corre el riesgo de no ser reelecto. No obstante, en la mayor parte de los casos, los electos no son directamente responsables del sistema de vídeovigilancia, especialmente cuando este sistema no sea exclusivamente municipal. En este caso, es más complicado identificar las responsabilidades, razón por la cual el principio de responsabilidad requiere el principio de transparencia.

La responsabilidad no se aplica sólo a la decisión de instalar un sistema de vídeovigilancia, al buen funcionamiento del sistema y al respeto de los demás principios, sino que también se aplica a las diferentes utilizaciones del sistema, que deben responder a los objetivos que se les han asignado. Uno de los riesgos es el fenómeno de *"function creep"* (desvío gradual de la función inicial), es decir, "deslizarse" hacia nuevas funciones que no se habían planificado inicialmente y para las cuales se buscan nuevas justificaciones, o que son posibles gracias a la evolución tecnológica. No se debe invertir la lógica y llegar a utilizar el sistema para algo, sencillamente porque es posible y no porque es realmente necesario (principio 1). Si se asignan nuevas misiones al sistema, se las debe realizar bajo la responsabilidad explícita del operador.

RECOMENDACIONES / MODALIDADES DE ACCIÓN

Por esta razón, la Carta sugiere las recomendaciones y modalidades de acción siguientes:

>>

➤ Hacer públicos los datos para ponerse en contacto con la institución y el servicio responsable. Cada señal que indique una zona en

la cual exista un sistema de vídeovigilancia podrá incluir esta información de contacto.

➤ Afirmar la obligación de confidencialidad que incumbe a los administradores del sistema, ya sea en el marco de un reglamento interior o de un código de deontología destinado a los administradores del sistema. Deberán asumir su responsabilidad en caso de no cumplir con esta obligación.

➤ Recurrir a medidas de seguridad que permitan proteger el acceso a la sala desde la cual se administra el sistema, pero también proteger el acceso a las imágenes registradas. Para ello, se adoptarán medidas técnicas de control al acceso a las imágenes.

➤ Dar a conocer los modos operativos que tendrán las autoridades administrativas responsables de sancionar todo abuso confirmado.

➤ Aplicar un mecanismo adecuado a la difusión de la información necesaria para la comprensión pública de la utilización de los sistemas de vídeovigilancia.

6. Principio de supervisión independiente

Una de las ideas claves para una utilización democrática de la vídeovigilancia es adoptar un sistema de control independiente de los administradores de la vídeovigilancia. Como lo ha resumido el profesor Richard de Mulder, de la Universidad de Rotterdam, en el título de su intervención correspondiente a la conferencia final del proyecto: "Vigilar a los ciudadanos no es un problema. Pero, ¿quién vigila a los vigilantes?" Los ciudadanos deben estar tranquilos porque

los administradores de la vídeovigilancia respetan sus derechos. Por lo tanto, es necesario un control que garantice que los operadores del sistema aplican las reglas y demás principios de la Carta.

La supervisión independiente no necesariamente debe estar en manos de una autoridad de control que tenga la capacidad de aplicar sanciones, al igual que las autoridades públicas que han reglamentado la vídeovigilancia. El concepto de supervisión independiente es a la vez más flexible que el de la autoridad del Estado, y también más exigente. Este concepto refleja la idea de peso y contrapeso ("check and balance") como los federalistas han denominado a este principio, que constituía la base del concepto de separación de poderes, tal como lo ha definido Montesquieu (Trias Política).

La supervisión no necesita una jerarquía pero está fundada en la idea de que la responsabilidad no incumbe a un único actor. El usuario de la vídeovigilancia es, a la vez, observado en su obrar (principio de transparencia) y debe dar cuenta de sus acciones (principio de responsabilidad). Esta supervisión debe ser ejercida por un supervisor independiente de las autoridades que administran el sistema de vídeovigilancia.

El profesor Richard de Mulder explica perfectamente los nuevos poderes que confieren las nuevas tecnologías y el vídeo a quienes los utilizan, lo que presenta un riesgo inédito de desequilibrio de poderes y del sistema de pesos y contrapesos en que se funda la democracia. A su juicio, la solución es instaurar un cuarto poder (además de los poderes ejecutivo, legislativo y judicial),

[49] A veces se considera que los medios de comunicación son el cuarto poder. Sin embargo, para Mulder sólo pueden asumir esa función muy parcialmente, ya que tienen su propia agenda y sus propios intereses, y no se ocupan necesariamente de los retos más importantes para la sociedad.

que sería el de control/vigilancia/supervisión, lo que supone instaurar la *Tetras Política*. Ya existen instituciones que ejercen este "cuarto poder", como por ejemplo la figura del *Ombudsman* (mediador), que puede supervisar el correcto funcionamiento y, más importante aún, intervenir cuando un sistema no marcha como se desea[49]. De Mulder también destaca que es más importante cerciorarse de que existe una figura de control independiente como ésta, más que buscar evitar todo disfuncionamiento posible. Llegado el caso, el supervisor puede intervenir y rectificar un disfuncionamiento. Es en este sentido que la supervisión resulta independiente.

La idea de la supervisión va más allá de la idea de autorización. La supervisión debe aplicarse a largo plazo, a todos los retos que presenta la vídeovigilancia y en todas las fases de un proyecto de vídeovigilancia.

Por esta razón la supervisión independiente se define del siguiente modo:

« Frenos y contrapesos al funcionamiento de los sistemas de vídeovigilancia que deben aplicarse a través de un proceso de control independiente.».

Todo control supone la definición de normas. A través de estas normas, este principio de supervisión independiente permite armonizar las prácticas según lo indicado en la Carta. Este proceso de control independiente puede cobrar varias formas e intervenir en diferentes momentos en el desarrollo de los sistemas. Tiene su papel en la concepción de un sistema

para, por ejemplo, insistir en que la solución propuesta responda al problema o bien, si está en su poder, puede dar luz verde a la vídeovigilancia. Después, puede efectuar un seguimiento de la instalación del sistema y velar, más tarde, por el buen funcionamiento y la correcta utilización del sistema, por la protección de los datos, por la formación de operadores de las cámaras, discutiendo el resultado de la evaluación del sistema para decidir su desarrollo. El "supervisor independiente" puede ser una personalidad cualificada o un órgano específico compuesto por ciudadanos.

Existen muchas formas de organizar esta supervisión independiente. De hecho, en la mayor parte de los casos, la supervisión existe ya de diversos modos. Hay autoridades que conceden la autorización para instalar un sistema de vídeovigilancia. En Francia, por ejemplo, hay una Comisión Provincial que depende del gobierno central. En Italia, la autoridad de protección de los datos es la "*Garante privacy*" a quien incumbe un importante papel en la vídeovigilancia, basándose en una legislación detallada, al igual que en España, en Francia y en Bélgica.
En estas ciudades, el Consejo Municipal es quien, tradicionalmente, asume la función de supervisor y participa en mayor o menor medida en la administración de la vídeovigilancia. El ejemplo del Consejo Municipal también muestra sus límites, ya que suelen ser las mismas mayorías las que deciden y supervisan la vídeovigilancia. Si el alcalde no ha sido electo por sufragio universal y es independiente de la mayoría en el Consejo Municipal, o si la oposición no tiene ese papel de supervisión, la supervisión ya no se puede considerar independiente. Además, sería menester que ese supervisor pueda asumir esa tarea o que, desde el exterior, se le pida que lo haga.

En la multitud de pesos y contrapesos existentes, los participantes del proyecto han identificado dos casos que presentan singular interés pero que se ocupan de la supervisión de forma muy diferente. Por una parte, un Comité de Ética (como es el caso en Lyon o en Le Havre, en Francia), y por otra parte la figura del "visitante independiente" como es al caso en el condado de Sussex, en el Reino Unido.

Comité de Ética (Francia)

El Comité de Ética es una institución que se creó específicamente para supervisar la vídeovigilancia, en las ciudades francesas de Lyon y del Havre, cuya misión específica es velar por las libertades individuales. "Su composición responde a los objetivos de equilibrio, independencia y pluralidad, y está compuesto por diferentes electos de la mayoría y de la oposición, personalidades cualificadas que representan el universo del derecho, de la economía y de la educación, al igual que de representantes de asociaciones de defensa de los derechos humanos. Este Comité debe velar, más allá de las obligaciones legislativas y reglamentarias, por que el sistema de vídeovigilancia instalado por la ciudad no afecte las libertades públicas y privadas fundamentales. Además, debe informar a los ciudadanos acerca de las condiciones de funcionamiento del sistema de vídeovigilancia y recibe sus denuncias" (Art 4.1 de la Carta de Ética de la vídeovigilancia del espacio público de la ciudad de Lyon). La Carta de Ética, como la que ha adoptado la ciudad de Lyon o la que propone el proyecto, puede funcionar como referencia de base para el Comité y regular su funcionamiento. El Comité vela por la aplicación de la Carta de Ética, y para ello elabora un informe anual sobre las condiciones de funcionamiento y el impacto del sistema. En este marco, puede pedirle al alcalde que pida estudios detallados a organismos inde-

pendientes, como la ciudad de Lyon los hace en el mismo momento que se imprimen esta líneas (julio de 2010), con una evaluación global (técnica y sociológica) de su sistema de vídeovigilancia, realizado por la facultad de urbanismo y de ordenación territorial de la universidad de Lyon (profesor Jaques Comby). Por último, el Comité de Ética formula las recomendaciones al alcalde.
En la práctica, los ciudadanos recurren poco a los Comités de Ética de Lyon y del Havre, lo que también puede interpretarse como una prueba de su bien funcionamiento. Los ciudadanos saben que un supervisor independiente vela por la privacidad de la vida privada y supervisa el buen funcionamiento del sistema. Además, puede ocuparse de todo asunto que entre en su ámbito de competencia.

Visitantes Independientes (Reino Unido)
La cooperación sobre la vídeovigilancia del condado de Sussex, en la que participan la policía y las colectividades locales, ha optado por otro modo de supervisión. Se invita a los ciudadanos a que verifiquen por sí mismos el correcto funcionamiento del sistema, controlando su conformidad con el Código de Utilización. Para ello, un grupo de doce ciudadanos ha sido seleccionado de un grupo de voluntarios, para realizar las "verificaciones puntuales" de los locales de vigilancia de la policía y garantizar la conformidad con el Código de Utilización. Además, los visitantes independientes pueden asistir a las reuniones en las que se examinan a las autoridades policiales y consultar los informes anuales.
Las verificaciones pueden efectuarse en todo momento, tanto de día como de noche, sin advertencia previa. La mayor parte del tiempo, dos personas efectúan las visitas. Al principio de su mandato, estos ciudadanos reciben una formación sobre el sistema y el Código de Utilización, para que sepan lo

que deben controlar. Si detectan un problema o si algo les preocupa, lo comunican a las autoridades policiales y a la Dirección de la Vídeovigilancia.
Contrariamente al sistema de Comités de Ética, este dispositivo se aplica principalmente al funcionamiento de la vídeovigilancia. Por esta razón, su trabajo se completa con el de las autoridades policiales y de los electos locales, que trabajan junto a la policía en sus diversas actividades, al igual que en el planeamiento, la administración, la evaluación y el desarrollo del sistema de vídeovigilancia. Este dispositivo es de singular interés por su sencillez, la participación de los ciudadanos (principio 7) y su gran transparencia (principio 4).

Así, para aplicar este principio de supervisión independiente, se pueden hacer las recomendaciones siguientes:
➤ Esta autoridad independiente debe ocuparse de suministrar, después de estudiar los expedientes, las autorizaciones necesarias para instalar los sistemas de vídeovigilancia.
➤ Debe velar por la instalación y la utilización del sistema, de suerte que se ajuste a las reglas y normas definidas.

7. Principio de participación de los ciudadanos
Es sin duda el principio más directamente vinculado a la temática de este proyecto europeo "Ciudadanos, Ciudades y Vídeovigilancia", orientado a tener en cuenta los derechos y libertades de los individuos, y cómo hacer participar a los ciudadanos en la elaboración y la reflexión sobre la instalación de un sistema local de vídeovigilancia.

No es fácil hacer participar a los ciudadanos. ¿Hasta dónde se puede llegar en la intromisión en vida privada de los ciudadanos para garantizar su seguridad? ¿Cómo

hacer participar a los ciudadanos en un sistema que debería garantizar la confidencialidad de la información que produce?
Se debe hacer todo lo posible para favorecer una participación de los ciudadanos en todas las etapas de la vida de un sistema de vídeovigilancia.

El objetivo es dar a los ciudadanos la oportunidad de expresarse a través de diferentes formas de consulta, de participación, de deliberación y de toma compartida de decisiones. Toda nueva instalación o extensión de los sistemas de vídeovigilancia siempre deberá considerar la participación activa de los ciudadanos que viven en esa zona. Cada vez que sea posible se deben prever grupos de discusión y demás medios de participación de los ciudadanos. La participación de los ciudadanos incrementa las oportunidades de éxito.

>>

RECOMENDACIONES / MODALIDADES DE ACCIÓN

➤ Consultar a los ciudadanos sobre la identificación de las necesidades en el marco del diagnóstico previo, por ejemplo a través de encuestas de victimización.

➤ Favorecer la participación inicial de los ciudadanos en la localización de las cámaras, cuando responde a una necesidad. Esta actuación puede realizarse a través de marchas exploratorias.

➤ Buscar la aceptación, por parte de los ciudadanos, de los proyectos de seguridad global organizando, por ejemplo, reuniones públicas de información en las que puedan expresar su adhesión a los proyectos del ayuntamiento.

➤ Favorecer la participación de los ciudadanos para controlar y evaluar el sistema a través de cuestionarios de satisfacción.

➤ Prever un proceso enmarcado y formalizado a través del cual los ciudadanos pueden visitar la sala de control y de administración del sistema de vídeovigilancia, incluso de modo espontáneo. Todo rechazo de tales visitas debe ser justificado (por ejemplo, en razón de que se esté llevando a cabo una investigación judicial). Esta posibilidad debe estar claramente enmarcada para no afectar el derecho de terceros.

➤ Reforzar el compromiso, por parte de las autoridades locales, de adoptar un instrumento que haga posible la participación de los ciudadanos con cierta frecuencia. La creación de una estructura local responsable de velar por la correcta utilización del sistema deberá incluir una activa participación de los ciudadanos en la vida y el desarrollo del sistema.

Principio de participación de los ciudadanos en los hechos

Para las ciudades que participan en este proyecto, este principio era ya una realidad, dado que el proyecto como tal de instalar un sistema de vídeovigilancia era una respuesta a una petición de mayor seguridad por parte de los ciudadanos. Tal ha sido el caso del municipio de Ibiza (España), por ejemplo, que después de analizar las peticiones de los habitantes y cotejar los dispositivos existentes decidió instalar cinco cámaras en zonas donde no había resultado eficaz ningún otro medio.

Otros municipios, como el de Génova, Le Havre o Saint-Herblain, han organizado debates públicos con los habitantes o encuentros con asociaciones de barrio para determinar las necesidades y el mejor

modo de responder a ellas.

En Rotterdam, este principio está incorporado en todas las políticas de la ciudad, incluyendo la política de seguridad. Para garantizar que las políticas propuestas por el ayuntamiento den una respuesta cabal a lo que piden los ciudadanos, cada año el ayuntamiento hace una evaluación de sus dispositivos de seguridad que incluyen el sistema de vídeovigilancia. El alcalde se reserva el derecho de poder instalar y retirar las cámaras en función de las reacciones del público y de los resultados obtenidos.

Este principio no sólo se aplica cuando se debe tomar la decisión de instalar cámaras o para evaluar si la respuesta suministrada por las autoridades ha satisfecho lo que piden los habitantes. También se lo incluye en todas las etapas de la instalación de un instrumento que forma parte de una política de seguridad integrada, es decir, en el funcionamiento mismo del sistema de vídeovigilancia. A través de la consulta de los habitantes, las autoridades pueden elegir el lugar exacto donde instalar una cámara, para dar seguridad a un espacio que se percibe como potencialmente peligroso. Este diálogo permanente consolida en todos la sensación de participar en las decisiones políticas.

En Lieja, se han organizado unas jornadas de "puertas abiertas" en las cuales los habitantes pueden visitar las salas de control, en visitas comentadas por expertos.

En Sussex, el sistema de "visitantes exteriores" ha sido plebiscitado por la población.

Estos son diferentes ejemplos de iniciativas que han tomado las autoridades responsables para asociar a los ciudadanos a las políticas de seguridad.

3. Hacia un lenguaje unificado de la vídeovigilancia en Europa: propuesta de una señalización unificada

¿Cómo avanzar en Europa hacia la creación de un lenguaje compartido sobre la seguridad y la vídeovigilancia? Tal fue uno de los hilos conductores de este proyecto, centrado en la importancia de una comunicación clara y honesta con los ciudadanos. Dada la creciente movilidad de las personas en el territorio europeo, se ha manifestado como una evidencia la necesidad de crear esquemas de referencia compartidos y traducir las políticas públicas en un lenguaje que resulte claramente comprensible para todos. De allí la idea de diseñar una señalización compartida para las ciudades que utilicen cámaras de vigilancia. Esta propuesta también es una respuesta directa a una petición formulada por diferentes organismos europeos. En tal sentido, la Asamblea Parlamentaria del Consejo de Europa, en su resolución 1604 de 2008, ha pedido la creación de una señalización europea, como lo había hecho ya en 2004 el Grupo de Trabajo sobre Protección de Datos – Artículo 29 de la Comisión de Venecia, en su Resolución 4/2004 sobre la vídeovigilancia.

Un primer estudio sobre lo que ya existe ha destacado que se emplean instrumentos de comunicación muy buenos, pero también que hay lagunas y carencias. En algunos países, como Bélgica e Italia, el marco legislativo sobre la señalización es muy preciso, suministrando una estructura clara con todos los detalles que se deben mencionar e imponiendo, incluso, un pictograma estándar. En otros países, la ley prevé que los ciudadanos sean informados cuando se encuentran en una zona que está sometida a la vídeovigilancia, sin dar consignas precisas, y en este caso cada autoridad responsable debe decidir de qué forma habrá de organizar la comunicación. Es más bien en este caso que se han encontrado ejemplos de señalización que no in-

cluyen ningún pictograma, escritas sólo en el idioma del país y, por lo tanto, incomprensibles para un turista, sin información sobre la identidad de la autoridad responsable.
Con vistas de los resultados de esta investigación, se decidió que los participantes a este proyecto piensen en la creación de una señalización unificada y en un pliego de condiciones.
De estas reflexiones se ha llegado a la conclusión de que una señalización europea debería absolutamente ajustarse a lo siguiente:

➤ Contener al mismo tiempo texto e imagen para que pueda ser comprendida por toda persona que no hable el idioma local.
➤ El pictograma debería reflejar la situación tecnológica actual, ya que las ciudades emplean cada vez más las cámaras de vigilancia de tipo "domo", y como son nuevas, los ciudadanos no necesariamente las identifican ni las localizan. Al incluir un pictograma con forma de domo, el proyecto desea no sólo informar a los ciudadanos acerca de la utilización cada vez más frecuente de esta clase de cámaras sino también acerca de la existencia de esta nueva tecnología. La señalización también tiene así un papel pedagógico.
➤ En cuanto al texto, todos los participantes se han puesto de acuerdo con el hecho de que la palabra "vídeo" debe figurar, ya que es idéntica en todos los idiomas europeos.
➤ Otro elemento importante es que aparezca el término "espacio público", ya que es necesario indicar que la política pública de seguridad se aplica al espacio público y no al espacio privado.
➤ También se vio que era importante indicar el objetivo que tiene el sistema de vídeovigilancia, para que los habitantes comprendan claramente el vínculo entre este instrumento y la política local de seguridad.
➤ Las reglas de transparencia de las políticas públicas

exigen que la autoridad responsable de la instalación y del funcionamiento de las cámaras esté claramente indicada, y que se haya previsto al menos un medio directo de consultar o de ponerse en contacto con los responsables (teléfono, sitio Internet).

➤ Por último, el principio de legalidad según el cual la instalación y la gestión de un sistema de vídeovigilancia sólo puede hacerse en estricta aplicación de la ley, también debe estar incluido en la señalización, que debe mencionar asimismo el marco legal en el cual se inscribe el sistema y las disposiciones referentes a la protección de los datos.

¿Qué utilización se debe hacer de la señalización?

En la medida en que la mayor parte de las ciudades cuentan ya con una señalización, los participantes en el proyecto se han preguntado cuál sería el valor añadido de una señalización paneuropea.

En primer lugar, las recomendaciones de la Carta a favor de una señalización que suministra mucha información pueden incitar a las ciudades a modificar y completar sus respectivas señalizaciones.

Además, las recomendaciones pueden suministrar una guía fácil de aplicar en el contexto local, en el caso de las ciudades que todavía no tienen una señalización propia.

En el caso de otras autoridades que financian la instalación de sistemas de vídeovigilancia, como las regiones o los ministerios, los elementos citados anteriormente pueden constituir un pliego de condiciones sobre las comunicaciones.

Last but not least, la utilización de la misma señalización en toda Europa contribuiría a una mayor transparencia de las políticas públicas, lo que es beneficioso para todos los ciudadanos de los países miembros.


VÍDEO
VIGILANCIA
PARA SU
SEGURIDAD
DIRECTIVA 95/46/CE
AUTORIDAD RESPONSABLE
AYUNTAMIENTO DE XXXX
MAS INFORMACIÓN
04 55 55 55 55
WWW.VIDEO-CIUDAD.ES
ESPACIO
PÚBLICO


VÍDEO
VIGILANCIA
PARA SU
SEGURIDAD
DIRECTIVA 95/46/CE
AUTORIDAD RESPONSABLE
AYUNTAMIENTO DE XXXX
MAS INFORMACIÓN
04 55 55 55 55
WWW.VIDEO-CIUDAD.ES
ESPACIO
PÚBLICO

Parte III

Zoom sobre las ciudades: Cómo usan la vídeovigilancia y protegen los derechos fundamentales y las libertades

BOLONIA

NÚMERO DE HABITANTES:
377 258

NÚMERO DE CÁMARAS:
291

AUTORIDAD RESPONSABLE:
La ciudad

Ciudad de Bolonia y región Emilia-Romaña

➤ El proyecto de vídeovigilancia en la ciudad de Bolonia nace del deseo de encontrar soluciones a los problemas prioritarios: el sentimiento de inseguridad, unido a la presencia de bandas de camellos, y la degradación de ciertos espacios públicos en el casco histórico de la ciudad.

En abril del año 2000, el servicio responsable de la seguridad del ayuntamiento de Bolonia realizó una encuesta entre 753 ciudadanos, con el fin de conocer su percepción sobre la inseguridad. Los resultados mostraron que el sentimiento de inseguridad, junto con la criminalidad, era particularmente fuerte en el

centro histórico de la ciudad. Frente a esta situación, la administración decidió implantar un sistema de vídeovigilancia en la zona noreste del casco histórico.

En junio del mismo año, la ciudad de Bolonia presentó este proyecto preliminar de vídeovigilancia a la región Emilia-Romaña, ya que ésta financia regularmente proyectos para la mejora de la seguridad urbana y los espacios públicos en las ciudades, con un interés particular por la recalificación urbana, el alumbrado público y la vigilancia de terroristas a través de las nuevas tecnologías.

Así, la región Emilia-Romaña se hizo cargo del 50% de la financiación de este proyecto de vídeovigilancia, en el marco de un acuerdo del programa firmado en 2002 con la ciudad de Bolonia. El coste total de la instalación fue de 1.829.164, 80 €. El coste de la red de fibra óptica para transmitir las imágenes se eleva a aproximadamente 100.000 € al año, a los que hay que añadir cerca de 50.000 € anuales de mantenimiento.

Además, en 2009 se liberaron 200.000€ (66% financiado por la región Emilia-Romaña y el resto a cargo de la ciudad de Bolonia) para remplazar las cámaras más obsoletas (instaladas en 2000) y mejorar los aspectos tecnológicos del conjunto del sistema. Los costes de instalación se dividieron entre la ciudad y la región, pero los costes operativos y de mantenimiento recaen en su totalidad sobre la ciudad.

En total, se instalaron 291 cámaras, y con la nueva financiación de la región Emilia-Romaña se alcanzarán las 315 antes de finales de 2010.

Las cámaras son analógicas y están dotadas de un sistema de visión nocturna. En 18 casos, se trata de

cámaras "*dome*" (cámaras con una rotación horizontal de 360º con posibilidad de zoom).

El sistema de transmisión de datos es coaxial y analógico. Para la transferencia entre las cámaras y el sistema de grabación se utiliza un cable coaxial, mientras que las centrales operativas de la policía están conectadas a través de fibra óptica. Se espera que gracias a la financiación de la región Emilia-Romaña se pueda conectar todo el conjunto del sistema con fibra óptica.

El "Proyecto del sistema de red integrado de protección y seguridad" se basa en la implantación de tecnologías innovadoras para prevenir y limitar la delincuencia.

Las imágenes de las cámaras colocadas a lo largo de las vías peatonales más frecuentadas y en las paradas de autobús, en el centro de la ciudad, se envían simultáneamente a las estaciones de la prefectura de la policía y a la estación central de la policía municipal. La prefectura de policía puede entonces enviarlas a las autoridades judiciales como pruebas. Tanto la policía local como la nacional pueden ver las imágenes encriptadas y conservarlas durante siete días antes de que sean destruidas.

El operador de la estación de la prefectura o de la policía municipal tiene la posibilidad de:

- Ver las imágenes de todas las cámaras y
- Dirigir las cámaras a distancia.

La policía municipal gestiona la instalación con la ayuda de los técnicos de una empresa privada y la policía nacional; el control de las cámaras recae en la policía nacional, la municipal y los carabinieri (gendarmes).

En la estación de vídeovigilancia de la prefectura de policía se encuentran un inspector de la policía del Estado y dos asistentes durante las 24 horas del día. Uno de los dos asistentes y el inspector han participado en la formación organizada por la ciudad de Bolonia.

La elección de los operadores está regida por la legislación nacional, la cual obliga a que se haga entre los miembros de la policía judicial. En total, hay una decena de operadores que consultan las imágenes, repartidos entre la policía nacional, la municipal y los carabinieri. Las imágenes no pueden enviarse a tiempo real a otros servicios.

Sólo los agentes de la policía judicial tienen acceso a las imágenes grabadas, bajo autorización de los magistrados. Para ver dichas imágenes, hace falta no sólo la autorización sino también la llave de acceso física. Sin embargo, sólo el responsable de la instalación está capacitado para consultar las grabaciones y debe utilizar una llave de acceso específica.

A tiempo real, la función de la policía del Estado es principalmente represiva (tras la alerta activada por las imágenes de las cámaras) pero permite también una forma de "identificación" de las personas sospechosas gracias al uso de los zooms de las cámaras.

La función preventiva está evidentemente vinculada al aumento del riesgo para los delincuentes de cometer un robo o actos incívicos. Una mayor vigilancia del territorio permite transmitir a los ciudadanos el sentimiento de una mayor protección y de la posibilidad de que la policía intervenga más rápidamente.

La red ha sido evaluada antes, durante y después de ponerse en funcionamiento. La evaluación se hizo a

través de las estadísticas de los delitos cometidos, de la denuncia de pequeños robos y actos incívicos, degradaciones urbanas, incivilidades, y de la percepción de la inseguridad.

Sin embargo, es difícil medir el alcance del proyecto de manera precisa puesto que las estadísticas de la criminalidad no vienen lo suficientemente detalladas (sobre todo desde un punto de vista geográfico) y no permiten analizar correctamente su evolución. Por su parte, las fuerzas de la policía se muestran satisfechas ya que perciben la vídeovigilancia como una herramienta eficaz para la identificación de los individuos y para su uso ante la justicia (de ahí el aspecto represivo). El aspecto preventivo sigue estando menos claro: la satisfacción de los ciudadanos es importante, a pesar de que muestra un retroceso con relación a las expectativas expresadas antes de la puesta en marcha de esta red.

En cuanto a los efectos de redirección o localización de la criminalidad ("displacement effects") causados por la colocación de cámaras no son cuantificables, dada la falta de estadísticas fiables.

Gian Guido Nobili

➤ Entre los años 1996 y 2008, el ayuntamiento y la policía local de Brno pusieron en marcha un sistema de vídeovigilancia que se inscribía dentro de los programas de prevención de la criminalidad. Se trata de un sistema de 18 cámaras, en el cual se han invertido 627.000€ (utilizando la tasa de cambio de julio de 2010). Las cámaras cubren principalmente el centro de la ciudad, los espacios alrededor de las estaciones y de las paradas de autobús, y los lugares más frecuentados. Antes de la instalación del sistema el ayuntamiento realizó una serie de investigaciones sobre la seguridad en Brno, lo que incluía encuestas entre la población, análisis socio-demográficos y estadísticas de la policía. Los trabajos preparatorios también incluyeron entrevistas con policías, trabajadores so-

ciales, representantes de ONGs y otros actores que intervienen en el espacio público.

Los objetivos principales que se identificaron para este sistema fueron:
➤ Aumentar el sentimiento de seguridad de los lugares de la ciudad con la tasa de criminalidad más elevada;
➤ Prevenir la criminalidad;
➤ Facilitar la intervención de las fuerzas de la seguridad en caso de delitos en los espacios videovigilados.

Además de este sistema, se instalaron otras 57 cámaras en diferentes distritos de la ciudad, que están gestionadas por la policía y las autoridades del barrio. El coste de este sistema fue de aproximadamente 2.3 millones de euros (utilizando la tasa de cambio de julio de 2010). Estas cámaras vigilan los lugares considerados como problemáticos por la presencia, entre otros, de grupos de personas que sabemos que a menudo están implicados en asuntos criminales. Además, la empresa de transportes públicos de la ciudad utiliza 24 sistemas exteriores y ha equipado 38 vagones de tranvía con cámaras. Por último, el servicio de mantenimiento de las carreteras utiliza 64 cámaras. NI la inversión ni los costes de operación de estos sistemas son publicados en los informes anuales de estas empresas.

La ley checa establece que sólo la policía nacional o la policía municipal pueden gestionar sistemas de vídeovigilancia en el espacio público. Los sistemas se financian con el presupuesto de la ciudad y con subvenciones de programas para la prevención de la criminalidad. El coste de explotación va a cargo de las autoridades policiales y de las empresas de transportes y de mantenimiento de las carreteras. Todos los sis-

temas de vídeovigilancia de Brno están integrados en una red.

Según la reglamentación de la Oficina para la Protección de Datos Personales, que tiene autoridad para sancionar, los operadores privados pueden tener como tarea supervisar ciertos espacios (semipúblicos) como parkings o supermercados, pero su sistema de vídeovigilancia no puede grabar imágenes, y por lo tanto, sus imágenes no pueden ser utilizadas en investigaciones policiales.
Las grabaciones del sistema de vídeovigilancia de la ciudad de Brno y de la policía nacional se conservan durante 20 días para a continuación ser automáticamente borradas por nuevas grabaciones. Sólo la policía nacional tiene acceso a estas imágenes; el equipo está compuesto por 70 agentes responsables de la vigilancia y 3 miembros del departamento de análisis. La policía criminal y la policía de carreteras pueden utilizar las imágenes durante sus investigaciones. Las grabaciones se guardan en una sala especial en el Centro de Comando de la policía nacional, a la que solo tienen acceso agentes autorizados. Estos agentes reciben una formación especial y solo ellos conocen los códigos de acceso a dicha sala.
La legislación de la República Checa en materia de protección de la vida privada se inscribe en el código civil y en la ley sobre la protección de datos. Las autoridades checas aplican también el Código ISO de las buenas prácticas para la gestión de la seguridad de la información (CSN ISO 27 001). Además, existe un reglamento específico dentro de la policía para la gestión de los centros operativos y también hay directivas sobre el tratamiento de la grabación video de la policía nacional. La función que la policía tiene como controladora de la protección de datos personales se le asignó para velar por la correcta aplicación de esta reglamentación.

La tecnología actual no permite visualizar los espacios privados en las cámaras

Hay una carencia importante: la falta de información que se da al público. Las conferencias de prensa son el único medio en el que se anuncia la instalación de nuevas cámaras. Por otra parte, en ciertos lugares problemáticos la ciudad ha obligado a que se coloquen carteles en las calles indicando la presencia de cámaras, para que tengan un efecto preventivo de la delincuencia y acrecentar así el sentimiento de seguridad en la población, a un coste muy poco elevado. Sin embargo, aún no se ha colocado ningún cartel.

Con frecuencia, la ciudad realiza estudios con la población, que tratan sobre su sentimiento de seguridad y su apreciación del sistema de vídeovigilancia. Estos estudios indican que la mayoría de los habitantes no tienen ni idea de donde están colocadas las cámaras, pero a pesar de ello sienten que están más seguros gracias a la vídeovigilancia. En el año 2005, el 4,5% de las personas interrogadas estimaban que la instalación de la vídeovigilancia limitaba la libertad personal. Cuatro años más tarde, esta cifra ha bajado a un 1,9%. Teniendo en cuenta el margen de error habitual en este tipo de estudios, es razonable afirmar que el número de personas que creen que la vídeovigilancia mina su libertad personal es ínfimo.

El sistema de vídeovigilancia de Brno no ha engendrado ningún tipo de debate público u oposición. No ha habido ni protestas públicas ni ninguna otra iniciativa en contra o a favor de la vídeovigilancia. Todos los partidos políticos democráticos representados en la Asamblea Municipal de Brno incluyen en su programa un capítulo sobre la seguridad y la prevención de la criminalidad, y de la totalidad de los miembros del panorama político, todos están a favor de la prevención.

Todas las fases de instalación de la vídeovigilancia se han discutido en el Consejo sobre la Prevención de la Criminalidad de la ciudad, tratadas en el Consejo de la ciudad y por último aprobadas por la Asamblea Municipal de Brno. A nivel nacional, se consultó con el Departamento de Prevención de la Criminalidad del Ministerio del Interior y se aprobó el proyecto en el Comité Nacional para la Prevención de la Criminalidad.

El público no está autorizado a ver las grabaciones de video, tal y como establece la legislación. En los casos de crímenes extremadamente graves, la policía está autorizada a difundir ciertas imágenes a los medios de comunicación, algo de lo que se encarga el Departamento de Información de la policía, ubicado en el barrio general regional de Moravia del sur.

La evaluación del sistema de vídeovigilancia está a cargo de los Departamentos de la Prevención de la Criminalidad del Ministerio del Interior, y se realiza, entre otros, gracias a las informaciones suministradas por la ciudad y por la policía, incluidos los análisis comparativos de la tasa de crímenes y delitos en los lugares videovigilados y en aquellos que no lo son. Es interesante señalar que, efectivamente, la vídeovigilancia ha permitido disminuir los crímenes contra la propiedad. También hay grupos de ladrones de carteras que han abandonado sus lugares de acción habituales para ir a otras zonas menos "atractivas". Por último, los estudios muestran que los ciudadanos se sienten más seguros en los lugares en los que hay cámaras de vigilancia.

Todos estos elementos muestran que el sistema de vídeovigilancia puede considerarse como una herramienta útil en la política de seguridad de la ciudad de Brno. Recomendamos su utilización en una sociedad

funcional y democrática, con la condición de que los datos y las grabaciones estén lo suficientemente protegidos gracias a medios legislativos y técnicos, garantizando los derechos y libertades individuales fundamentales. El riesgo, como siempre que se trabaja con datos sensibles, es el factor humano. De lo que estamos seguros es de que no recomendaríamos la utilización de la vídeovigilancia en una sociedad no democrática donde el chantaje y la extorsión están a la orden del día.

Stanislas Jaburek

La vídeovigilancia en Italia y la experiencia llevada a cabo por el Ayuntamiento de Génova

En Italia somos testigos de una creciente demanda de los ciudadanos en materia de seguridad, a pesar de la disminución, o al menos la relativa estabilización, del número de delitos graves. Los factores que han contribuido a aumentar estas exigencias son esencialmente:

a) la mediatización de los delitos y la búsqueda constante del sensacionalismo, lo que tiene como consecuencia convertir en algo banal los crímenes excepcionalmente espectaculares y aumentar el sentimiento general de inseguridad, bajo los efectos de

un acontecimiento concreto;
b) el miedo ante la diversidad, un desafío al que nos enfrentamos constantemente debido al rápido ritmo y a la evolución continua de los cambios sociales y de los problemas relacionados con la inclusión;
c) la convicción de que deberíamos encontrar un medio para controlar todos los aspectos de nuestro entorno, tanto en sus componentes individuales como colectivos y que, en consecuencia, todo acontecimiento negativo que pudiera pasarnos debería ser imputable a la responsabilidad de alguien, por lo menos desde el punto de vista de la responsabilidad objetiva;
d) el hecho de que "nuestro" comportamiento es una variable independiente y que alguien tiene que hacerse responsable de nuestra seguridad.
Teniendo todo esto en cuenta, las medidas de intervención más solicitadas son:
1) penas más severas ;
2) una policía con más recursos y más poder ;
3) tecnologías de control. Pero a menudo, estas últimas dan respuesta en función de las circunstancias y sólo en un número limitado de casos.

En Italia, el orden y la seguridad públicos son responsabilidad del Estado. La reciente modificación de la legislación ha delegado en los ayuntamientos competencias en materia de seguridad urbana que ejercen a través de ordenanzas y, sobre todo, desarrollando sistemas de vídeovigilancia.
En la ciudad de Génova, las políticas municipales de seguridad urbana comenzaron a desarrollarse a mediados de los años 90, al tiempo que surgía una expectativa cada vez mayor por parte de los habitantes de que la seguridad fuera garantizada no sólo por parte de las instituciones tradicionales (fuerzas del orden y de la autoridad pública) sino también de los alcaldes y los cargos políticos.

Estas políticas de seguridad se concentraron, en una primera fase, en una intervención en el casco histórico de la ciudad y se enmarcaban dentro del programa europeo Urban II, el cual permitió, con el acuerdo de la prefectura de policía, instalar cámaras bajo la responsabilidad de las fuerzas del orden para vigilar un cierto número de lugares problemáticos. Como resultado del *Pacto para la seguridad* firmado por el Ministerio del Interior y la Asociación Nacional de los Municipios Italianos, se firmó en 2007 el pacto "Génova ciudad segura", y es ahí donde se integra el proyecto de vídeovigilancia municipal. El objetivo principal era poner en marcha una herramienta de prevención de la delincuencia con el fin de tranquilizar a los habitantes.

Para identificar los lugares más sensibles de la ciudad que serían objeto de vídeovigilancia, se creyó indispensable implicar a los Ayuntamientos, en calidad de representantes de la población residente en las zonas concernidas. Convencidos de que la identificación de los lugares y la elección de las tecnologías implantadas debían aportar una respuesta real a las necesidades de seguridad de los ciudadanos, realizamos una identificación de los lugares críticos gracias a un sistema de georeferencia que nos permitió decidir dónde instalar las cámaras. A los ciudadanos se les informó de los resultados a través de diversos canales de comunicación.

Actualmente existen sobre el territorio del municipio de Génova tres sistemas de vídeovigilancia. El primero, cuyo objetivo es controlar la fluidez del tráfico, está compuesto por 38 aparatos colocados en las principales arterias. La policía nacional, gracias a su puesto de control central, gestiona por su parte 97 cámaras. Por último, están las primeras 60 cámaras del sistema de vídeovigilancia municipal, instaladas en 2009.
Las líneas directrices para garantizar un desarrollo

adecuado del sistema municipal se encuentran en la ordenanza del Garante para la protección de datos personales, promulgada en abril de 2004, y que enuncia cuatro grandes principios generales:

1-Legalidad
2-Necesidad
3-Proporcionalidad
4-Finalidad

Con el fin de garantizar el respeto de estos principios, se ha creado una Comisión Técnica Específica, compuesta por un representante de la policía local, un representante de la policía nacional y un funcionario experto en vídeovigilancia. Esta Comisión se encarga, dependiendo de las necesidades expresadas por los ciudadanos, de identificar los lugares que deberían estar bajo vídeovigilancia.

Desde un punto de vista legal, el tratamiento de imágenes es en general comparado con el tratamiento de datos personales. Dada la gran diferencia que existe entre la naturaleza de los datos personales contenidos en una imagen, en comparación con la que presenta un soporte papel o informático, se pensó que era necesario alinear las modalidades de tratamiento de imágenes bajo una norma en vigor en materia de protección de la vida privada, con el objetivo de garantizar la protección y los derechos de los ciudadanos.

Para ello, el municipio de Génova ha elaborado un reglamento, actualmente en vía de adopción, el cual:

➤ Enuncia los principios generales que debe respetar la administración municipal en las actividades de vídeovigilancia;

➤ Enumera los objetivos sobre los que la administración puede basarse para efectuar el tratamiento de imágenes;

➤ Delimita situaciones en las cuales es posible recurrir a las medidas de vídeovigilancia;

➤ Identifica las herramientas que pueden ser

utilizadas;
➤ Impone la obligación de trazado de los accesos a los datos grabados;
➤ Define las vías de comunicación con los ciudadanos y fija los períodos durante los cuales se pueden conservar las imágenes, en función de los diferentes objetivos trazados;
➤ Reconoce los derechos de las personas grabadas así como del conjunto de la población y define bajo qué formas pueden ejercerse estos trechos.

El derecho de acceso a las imágenes de las personas grabadas debe estar definido principalmente en relación con los objetivos de los actores públicos en materia de eficacia, eficiencia y economía. Conviene también tener en cuenta la protección de la identidad de terceros. Además, se debe respetar el principio de respuesta a una petición razonable, respetando la obligación de imparcialidad y de buen funcionamiento de la administración pública, tal y como estipula la Constitución italiana.
Dada la importancia de los recursos humanos y financieros necesarios para la puesta en marcha de los sistemas de vídeovigilancia, es indispensable evaluar y verificar su eficacia. El municipio de Génova ha dado un primer paso en este sentido al realizar periódicamente encuestas de satisfacción a sus habitantes. Éstas se hacen con el objetivo de evaluar el impacto de las intervenciones sobre el sentimiento de seguridad de los ciudadanos. A largo plazo, la ciudad también está definiendo una serie de indicadores que permitirán medir el impacto del conjunto de iniciativas tomadas en el marco de su política de seguridad urbana.

Mariapia Verdona

IBIZA

NÚMERO DE HABITANTES:
41 000

NÚMERO DE CÁMARAS:
4

AUTORIDAD RESPONSABLE:
La ciudad

En julio de 2009, la ciudad de Ibiza, capital de la isla balear del mismo nombre, puso en marcha un sistema de vídeovigilancia que forma parte de una serie de medidas tomadas por el ayuntamiento para rehabilitar los barrios del casco histórico, donde existen serios problemas de marginalización y delincuencia. Los diferentes equipos municipales que se han sucedido en el ayuntamiento desde 1987 han invertido un total de 50 millones de euros en la renovación de tres de los barrios más "difíciles" del casco histórico: Sa Penya, La Marina y Dalt Villa, a través de acciones tales como la creación de nuevos espacios culturales, la peatonalización de las calles, mejora de las infraestructuras,...

Paralelamente, el ayuntamiento ha reforzado su polí-

tica de prevención de la delincuencia, aumentando en primer lugar el número de policías de proximidad en estos barrios y, en segundo lugar, iniciando en 2006 un proceso en el gobierno regional para que éste autorizara la instalación de cámaras de video. El dossier de presentación del proyecto incluía datos estadísticos sobre la criminalidad local así como artículos de prensa sobre la delincuencia en el casco histórico. También trataba cuestiones relacionadas con las características técnicas de las cámaras y su posición prevista.
La ciudad de Ibiza (Eivissa en catalán) cuenta con una población permanente de aproximadamente 41.000 habitantes, pero acoge cada año a unos 400.000 turistas. El éxito turístico de Ibiza, uno de los parajes más frecuentados del Mediterráneo y de los lugares legendarios de la "movida" española, tiene un impacto directo sobre la delincuencia, principalmente en el tráfico de drogas, a la que se suman los robos y la gente en estado de ebriedad en las vías públicas. El tráfico de drogas es especialmente importante en el casco histórico de la ciudad de Ibiza, punto neurálgico de la vida nocturna. Según una información publicada en el Diario de Ibiza en junio de 2006, el índice de criminalidad registrado en las islas de Ibiza y Formentera era en esos momentos dos veces superior a la media española (118 "delitos y faltas" por habitante, frente a la media Española de 49,3).

El Ayuntamiento solicitó la autorización para instalar un total de cinco cámaras de video, de las cuales finalmente se colocaron cuatro en junio de 2009. El coste de la instalación fue de 89.600 euros, y el mantenimiento corre a cargo de la diputación.

Protección de datos y respeto de la vida privada
El consejo municipal es responsable de la conservación de las grabaciones, el cual ha delegado esta tarea en la policía municipal, además del uso y destrucción de di-

chas imágenes. Hay un equipo de ocho operadores de video que hacen funcionar las cámaras y que tienen acceso directo a las imágenes. Una vez que éstas están grabadas, sólo hay tres oficiales de policía autorizados a ver las imágenes. No hay ningún otro tipo de transmisión de las imágenes, ni en directo ni en diferido. Sin embargo, se ha dado el caso de que la policía municipal envíe ciertas grabaciones a la policía nacional si consideran que pueden servir de ayuda en sus investigaciones.
Las grabaciones se destruyen tras un período máximo de un mes, salvo si están siendo utilizadas en el marco de una investigación policial sobre un delito grave o durante un proceso judicial en curso.
Cuando se graban actos potencialmente delictivos se envían los videos pertinentes a las autoridades judiciales, en un plazo máximo de 62 horas después de la grabación. Cuando se trata de actos que pueden constituir una "falta administrativa" vinculada a la "seguridad cívica" (según los términos de la ley española), las grabaciones se envían inmediatamente a las autoridades competentes, con el fin de iniciar un proceso penal. En el caso de grabaciones ilegales de imágenes y sonidos, la grabación debe ser destruida inmediatamente, según lo establecido por la Ley Fundamental 4/1997.
En caso de que sea necesario destruir tan solo una parte de la grabación, y siempre y cuando la destrucción total de la misma sea imposible o innecesaria por motivos técnicos o en función de un proceso en curso, la persona responsable de la salvaguarda de las grabaciones deberá distorsionar o bloquear el sonido y las imágenes pertinentes, volviéndolas inutilizables. Esto lo hará con los medios técnicos disponibles a tal efecto.

Información al público
Los habitantes de Ibiza tuvieron conocimiento de la instalación del sistema de vídeovigilancia principalmente a través de una campaña en los medios de comunicación locales. Las autoridades locales también

informaron a la población de los barrios en los que se colocaron las cámaras sobre todas las disposiciones legales sobre la protección de datos personales y los procesos para recurrir en caso de anomalía. Además, los habitantes de los edificios donde se instalaron las cámaras fueron informados personalmente por las personas encargadas de su instalación, quienes pidieron el consentimiento de los vecinos, a pesar de que legalmente esto no fuera obligatorio. Sin embargo, hay que señalar que salvo los habitantes de los inmuebles donde están colocadas las cámaras, el resto de la población de Ibiza no ha sido informado de la posición exacta de los dispositivos.
La puesta en marcha del sistema de vídeovigilancia no provocó ninguna clase de controversia, aunque sí que se registraron algunas protestas sobre el plazo de instalación de las cámaras, que algunos consideraron demasiado largo.

Un balance positivo
Al final del primer año de funcionamiento, el equipo municipal y la policía local juzgan positivos el uso del sistema, ya que ha permitido reducir los actos delictivos y también se ha utilizado durante varias operaciones policiales. Por tanto, la vídeovigilancia constituye un complemento útil para el trabajo que la policía de proximidad realiza en los barrios del casco histórico de Ibiza. De manera general, ésta es también la opinión de la mayoría de la población local.

** « Las Pitiüses duplican la tasa media de delincuencia por habitante de España », Diario de Ibiza, 6 de junio de 2006.*
Manuel Ayala Garcia

EL HAVRE

NÚMERO DE HABITANTES:
180 000

NÚMERO DE CÁMARAS:
90

AUTORIDAD RESPONSABLE:
La ciudad

➤ En La Haya, hemos iniciado una colaboración permanente entre los servicios del Estado (Subprefecto), la Justicia (Procurador de la República, Policía Nacional), el Jefe de la Seguridad Pública del Distrito de La Haya y la Educación Nacional (Inspector de la Academia), quienes se reúnen regularmente cada quince días con el Primer Teniente Alcalde y el Adjunto responsable de la Seguridad y de la Dirección de la Seguridad Municipal, acción que se enmarca en las actividades de la célula restringida del Comité Local de Seguridad y de la Prevención de la Delincuencia « C.L.S.P.D ».

➤ Desde que empezamos a reflexionar sobre la posibilidad de realizar un proyecto de vídeovigilancia, plan-

teamos esta cuestión a nuestros socios para conocer su punto de vista, proceso que se repitió durante cada etapa de la puesta en marcha, de la creación y de la composición de un posible Comité Ético, y seguimos convocando estos encuentros cuando creemos necesario aumentar las zonas vigiladas por cámara.
➤ A veces, a petición de la Policía Nacional, estudiamos y proponemos un aumento de las cámaras en función del número de actos delictivos que se repiten en una zona o barrio.
➤ Por lo tanto, es tan solo tras una reflexión colectiva, y siempre con tiempo, cuando ponemos en funcionamiento cámaras suplementarias y no como respuesta a la petición de un ciudadano, víctima de una mala acción.

Las demandas de cámaras en todos los barrios, hechas por personas particulares, comerciantes o jefes de empresa, son tan numerosas que no podríamos responderlas todas.
Entre 2004 y 2005 se instalaron las tres primeras cámaras en un centro comercial de barrio que se disponía a cerrar debido a la alta tasa de delincuencia que no lográbamos controlar. El Adjunto encargado de la Seguridad informó sobre este proyecto al Consejo Municipal, y recibió a los representantes de todos los medios de comunicación: prensa escrita, radio y televisión, además de a asociaciones como la Liga de los Derechos del Hombre, asociaciones de barrio y a todos los ciudadanos que pidieran cita para informarse sobre el proyecto. Se transmitió el máximo de información posible antes, durante y después de la instalación. Evidentemente se trataba de información precisa, transparente y completa.
Consideramos que la vídeovigilancia urbana es una herramienta al servicio de la política de seguridad y de prevención de la delincuencia en el marco del compromiso local con la seguridad de la Ciudad de

La Haya. Sus objetivos son: prevenir los atentados a las personas y a los bienes, participar del sentimiento de seguridad de las personas y garantizar la seguridad de los edificios municipales y los espacios públicos expuestos.
Esta acción debe conciliarse con el imperativo de respeto de las libertades públicas e individuales, conforme al espíritu de la Ley de Orientación y de Programación de la Seguridad del 21 de enero de 1995 y sus decretos de aplicación.

Precisamente como respuesta a esta inquietud permanente de garantizar a los ciudadanos un nivel máximo de protección, la Ciudad de La Haya ha trabajado para crear el Comité Ético para la vídeovigilancia de los espacios públicos.

Este Comité Ético está compuesto por tres tipos de miembros:
➤3 cargos políticos electos, uno de ellos elegido por la oposición municipal;

➤ 3 personas cualificadas:
• el ex-rector de la Universidad;
• un antiguo Decano del Colegio de Abogados;
• un representante de la Cámara de Comercio;

➤ representantes de Asociaciones :
• el Presidente de la Asociación Aide aux Victimes (Ayuda a las Víctimas);
• el Presidente del Consejo Superior de Senegaleses de La Haya y
• el Presidente de una asociación de trabajadores sociales.

El Comité Ético para la vídeovigilancia de los espacios públicos se encarga de:

➤ Velar por el respeto permanente de las libertades públicas;
➤ Informar a los ciudadanos sobre el funcionamiento del sistema;
➤ Examinar a petición del Alcalde de La Haya todas las demandas de acceso a las imágenes y otros problemas de los ciudadanos;
➤ Dar consejo y recomendaciones al Alcalde sobre el funcionamiento del sistema;
➤ Entregar al Alcalde de La Haya un informe anual sobre el funcionamiento de la vídeovigilancia.

Todas las informaciones y la realidad de su utilidad hacen que hoy en día no constatemos oposición, salvo en contados casos, al funcionamiento de la videoprotección en nuestra ciudad.

Bertrand Binctin

LIEJA

NÚMERO DE HABITANTES:
190 000

NÚMERO DE CÁMARAS:
109

AUTORIDAD RESPONSABLE:
La ciudad

Lieja, ciudad milenaria, ciudad universitaria, metrópolis económica y cultural de la Región Valona, se sitúa en el corazón de una aglomeración urbana de 600.000 habitantes, donde convergen las autopistas transeuropeas y la red de trenes de alta velocidad (TGV) , a 100 km de Bruselas, 25 km de Maastricht y 40 km de Aix-la-Chapelle.

Es una ciudad ardiente, tanto de día como de noche, y prima la convivencia y la hospitalidad. Acoge además numerosos acontecimientos deportivos, festivos y culturales.
Desde el año 2002, el proyecto de renovación de la red de cámaras de vigilancia figuraba entre las propuestas

de acciones prioritarias sometidas a elección por parte de los ciudadanos de Lieja. Esta acción se inscribe en el capítulo "Una ciudad segura" de consulta ciudadana para conocer el proyecto de ciudad que sus habitantes imaginan. El proyecto de vídeovigilancia había sido aprobado por una gran parte de las personas que respondieron a la encuesta.
Desde entonces, y a petición del burgomaestre, los servicios de la zona de la policía local de Lieja instalaron de manera escalonada un total de 109 cámaras de vídeovigilancia, entre los años 2003 y 2008. Desde un punto de vista tecnológico, se trata de cámaras tipo "speed dome" de alta tecnología y alta definición, que permite una rotación de 360º en horizontal y 90º en vertical. El zoom permite leer claramente una matrícula a 150 metros, tanto de noche como de día.

Estas cámaras están programadas según ciertos parámetros, con el objetivo de hacer imposible la visualización de imágenes en lugares privados, pero no están equipadas con un soporte inteligente para la explotación de imágenes, de ahí la importancia de la formación de los operadores, los cuales deben conocer a la perfección tanto el barrio que vigilan como la población habitual de los mismos.
Las cámaras están conectadas con una red a través de un circuito cerrado de fibras ópticas, lo que excluye cualquier riesgo de pirateo. Las imágenes se visualizan en el Centro de Gestión de Acontecimientos, además de en dos comisarías de barrio. Los datos no se comparten ni con otros servicios ni con otras instituciones.

La visualización la efectúan exclusivamente policías experimentados, obligados a respetar el secreto profesional.
Las imágenes se graban y se destruyen siete días más tarde, aunque la ley belga permite que se conserven

durante un mes.
Todos los habitantes pueden solicitar la visualización de imágenes que les conciernan, tras hacer la petición necesaria al gestor del sistema, es decir, al burgomaestre, contra el que es posible presentar un recurso.
Asimismo, el Ministerio Fiscal y el Juez de Instrucción pueden igualmente solicitar imágenes para casos penales.

Los lugares de instalación de las cámaras se han elegido en función de los objetivos asignados al sistema durante su puesta en marcha. Se trata de dar una respuesta de calidad a los tres siguientes tipos de problemáticas:
➤ Problemas de circulación, a través del visionado de los grandes ejes de entrada a la ciudad;
➤ Problemas de orden público, a través del visionado de los lugares recurrentes de manifestación;
➤ Problemas de seguridad y medio ambiente, a través del visionado de ciertas zonas sensibles, como las calles de los barrios con vida nocturna activa.

Se coloca una señalización específica para que se sepa que se está grabando, y en ella se indica quién es el gestor del sistema.

Durante cada una de las cuatro fases de instalación, se envió el dossier correspondiente para la aprobación del consejo municipal, donde se trataron públicamente los temores relativos al respeto de las libertades individuales.
Cada cierto tiempo se hace pública la posición exacta de las cámaras y los objetivos perseguidos con estas acciones a través de comunicados y de conferencias de prensa.
La información para la población se garantiza igualmente a través de contactos con los comités de barrio,

un paso que se dio antes incluso de instalar el sistema y que sigue en pie desde entonces gracias a una evaluación regular. De esta manera, el burgomaestre invita a los participantes a estas reuniones a que expresen abiertamente sus expectativas.

En 2007 se formó una comisión de control local compuesta por representantes de cada uno de los cuatro grupos políticos democráticos representados en el consejo municipal de Lieja, la cual se reúne cada dos o tres meses.

La misión de esta comisión es garantizar la adecuada aplicación de la ley de 2007. Más concretamente, vela por que:

➤ Sólo haya personal policial específicamente formado trabajando con la visualización de imágenes en el centro de "cámaras";
➤ Se respete la vida privada;
➤ Las cámaras estén programadas según parámetros que oculten las zonas particulares de los inmuebles privados;
➤ Se coloquen carteles informativo con la información legal necesaria en las calles donde haya vídeovigilancia;
➤ Las imágenes se conserven debidamente para ser destruidas siete días después.

Regularmente se informa a los consejeros municipales sobre los elementos de evaluación: resultados de los trabajos de la Comisión de Control Local, reuniones de la Comisión Especial de Policía, visitas del Centro de Gestión de Acontecimientos,...

Además, se invita frecuentemente al gran público a que visite el centro, por ejemplo durante la Jornada de Puertas Abiertas de la Policía, las cuales atraen a

numerosas personas.

En cuanto al coste, la instalación de la integridad del sistema representa una cantidad de más de cinco millones de euros. Los gastos de explotación son nulos, ya que la red se basa en la fibra óptica. El presupuesto anual de mantenimiento preventivo es de aproximadamente 100.000€. También hay que contar con los gastos relacionados con la actualización regular del sistema, principalmente la compra de nuevos programas informáticos.

El impacto del sistema se estima positivo en términos de disuasión y de seguridad para la población. Sin embargo, éste no ha sido todavía objeto de una evaluación externa.

En el período de un año, las cámaras han conseguido establecer 54 hechos criminales en flagrante delito y responder positivamente a 58 demandas de investigación policiales.

Catherine Schlitz

Descripción del proyecto de creación de un sistema de vídeovigilancia

La experiencia londinense con la vídeovigilancia es en realidad la experiencia de todo el país, y se trata de un solo proyecto. En primer lugar, explicar que Londres está dividido en 33 zonas administrativas, cada una de ellas equipada con su propio sistema de vídeovigilancia. Además, existen otros proyectos a los que las autoridades públicas tienen acceso y hay numerosos sistemas privados de vídeovigilancia que cubren espacios públicos (cámaras pertenecientes a empresas, que filman las zonas de entrada y de salida).

La utilización de la vídeovigilancia ha aumentado de

manera exponencial a lo largo de los últimos decenios. A principio de los años 60, se colocaban las cámaras para controlar la circulación en las carreteras; en los 70 y los 80, se instalaron en los grandes centros comerciales, donde había una cierta ambigüedad sobre la naturaleza de los espacios. En otros términos, en los grandes centros comerciales se tiene la impresión de que las calles existentes entre las diferentes tiendas pertenecen al espacio público, mientras que en realidad se trata de zonas privadas. La mayoría de estos centros comerciales son patrullados por agentes de seguridad privados, generalmente con un protocolo con la policía local que les permite y les anima a realizar patrullas regulares. Además, la vídeovigilancia se está utilizando desde hace algún tiempo para gestionar los grandes acontecimientos deportivos, sobre todo los partidos de fútbol, donde ha demostrado ser una herramienta eficaz y estratégica para suprimir la violencia en los estadios y sus inmediaciones. Todo ello, combinado con un período prolongado de amenaza real de terrorismo, ha permitido acostumbrar al público británico a la utilización de la vídeovigilancia. Este proceso ha sido tan efectivo que a menudo son las propias comunidades las que piden la instalación de cámaras.

La voluntad de reducir la criminalidad ha sido un factor importante para el desarrollo de proyectos, con el objetivo potencial y complementario de prevenir el terrorismo y dar una alternativa de gran valor a los detectives. La utilización de la vídeovigilancia está en estos momentos tan presente que tenemos tendencia a creer que estamos siendo observados, incluso cuando no es así. En la mayoría de las ciudades de Londres, si no en todas, sus centros están cubiertos por cámaras de vigilancia. No es fácil afirmar con precisión cuántas cámaras hay, aunque se sabe que el Centro de Gestión y de Control de la

policía puede tener acceso a 60.000 cámaras. A título indicativo, sólo en el aeropuerto de Heathrow podemos encontrar 3.000 cámaras.

Cada vez se sostiene con mayor determinación que el uso y la colocación de las cámaras se ha hecho un poco al azar. La tendencia era no tener en cuenta el impacto potencial sobre el desplazamiento de los criminales o los problema de orden público y semejantes, aunque ha habido casos en los que una vez que se ha demostrado que un problema específico había disminuido, las cámaras sí se han quitado o han sido redistribuidas en la zona. Estos problemas son ahora tratados de manera más estructurada gracias al desarrollo de una estrategia nacional para la vídeovigilancia, con los consejos del Ministerio del Interior. Manifiestamente, esta actividad llega después de que la utilización de esta tecnología haya sido bien establecida. Podemos considerar que somos la segunda o incluso la tercera generación que utiliza esta tecnología, ya que las autoridades locales y sus socios modernizan sus sistemas para aprovechar las recientes mejoras en este campo. Por ejemplo, se ha experimentado un cambio de tecnología, yendo de lo analógico a lo digital, y un aumento de la utilización de cámaras dome, que tienen la ventaja de que la gente que está en la zona de grabación no puede saber en qué dirección está enfocando la cámara. Por supuesto, las tecnologías de moda provocan que el deseo de tener el material más novedoso impidan reflexionar racionalmente sobre qué nivel de complejidad tecnológica sería necesario para cada situación particular; presentando un ejemplo más claro, sería lo mismo que si cogiéramos un Ferrari para ir a comprar al supermercado de la esquina. Existe hoy en día un deseo creciente de examinar los beneficios acumulados por este sistema, algo que deriva de los costes considerables con los que se

juega. Sin embargo, parece que la retirada de los sistemas sería una decisión política delicada.

Con la aparición de los sistemas de vídeovigilancia de las autoridades locales, hacia 1985, se presupuso que estos sistemas deberían estar bajo el control de las autoridades locales en lugar de bajo el de la policía. Sin embargo, siempre se previó que la policía tuviera acceso a las cámaras, ya fuera a través de los policías en las salas de control o por las imágenes retransmitidas en directo en las salas de control de la policía, donde también se encuentra el personal capacitado para controlar las cámaras con el fin de vigilar los incidentes específicos. La rápida implantación de relaciones eficaces entre la policía y las autoridades locales ha contribuido a borrar la distinción entre la policía y las autoridades locales en todo lo concerniente al control de la vídeovigilancia. Ahora hay un cierto número de salas de control de vídeovigilancia que están situadas en las salas de control de la policía, y aunque los operadores de la vídeovigilancia son personal que depende de las autoridades locales, los policías tienen acceso constante a las imágenes en directo.

Un cierto número de salas de control de las autoridades locales tienen la función de encargarse de operaciones confidenciales, algo que se logra gracias a la vigilancia desde cámaras aisladas en el banco principal de vigilancia, a espaldas de los operadores y sin su participación. Un ejemplo que ilustre estos casos sería, por ejemplo, una operación antiterrorista en directo o un delito importante. Esta temática sería sin duda interesante para ser tratada en relación con las cuestiones de los derechos del hombre y de la vida privada.

La legislación en este dominio incluye la Ley de

Derechos Humanos (Human Rights Act) así como la Ley de Protección de Datos (Data Protection Act). Hay que señalar que no existe ninguna cláusula legal específica para la vídeovigilancia en el Reino Unido. No obstante, la legislación, incluida la Ley de Protección de Datos, se aplica a todos y no se limita a los organismos públicos. Además, como ya hemos señalado, la estrategia nacional para la vídeovigilancia prevé el desarrollo de un código de conducta que cubra todos los aspectos relacionados con la vídeovigilancia. Por otra parte, el Reino Unido, junto con otros Estados, utiliza tecnologías diversas para proteger los espacios privados de la vigilancia indiscreta. Por ejemplo, los sistemas que pertenecen a las autoridades locales tienen por costumbre oscurecer o difuminar las partes de las imágenes de las cámaras que conciernen a un espacio privado. Un ejemplo sería una propiedad residencial justo al lado de un comercio en una calle principal. Cuando la cámara recorre su perímetro de observación, las zonas privadas se oscurecen automáticamente, aunque hay la posibilidad de anular esta tecnología (con la autoridad competente) en situaciones que así lo exijan. Tales casos se reducen a delitos serios, incluido el terrorismo, y requieren autorizaciones de las más altas esferas.

Todos los lugares bajo vídeovigilancia deben anunciarlo a través de carteles que indiquen la presencia de cámaras, además de la información sobre cómo contactar con los operadores. Sin embargo, parece que las cámaras están tan omnipresentes que dichas señalizaciones son casi ignoradas. Como ya hemos subrayado, el trabajo sobre la estrategia nacional para la utilización de la vídeovigilancia continúa. Los documentos relacionados con ello se pueden encontrar en la web del Ministerio del Interior británico. En el momento de redacción de este

texto, el gobierno de coalición recientemente en el poder había mostrado sus intenciones de aumentar la legislación sobre la vídeovigilancia, lo que afectaría a la puesta en marcha de la estrategia nacional, pero por el momento aún no se han dado a conocer los detalles de la estructura reglamentaria mejorada.

Ya existen códigos de conducta que se aplican a los operadores que vigilan los sistemas, fruto de la base de la formación que reciben. La mayor parte de las salas de control de vídeovigilancia están al mismo tiempo vigiladas por cámaras de vigilancia permanentes, inmejorable ejemplo de "vigilancia de los vigilantes". También existen las prácticas de los "visitantes no iniciados" que acuden a las salas de control de vídeovigilancia. Estos voluntarios de la comunidad tienen derecho a un acceso directo a la zona de detención y tienen la oportunidad de hablar con los prisioneros para establecer las condiciones de su detención. De este mismo modo, los voluntarios pueden estar presentes en las salas de control de vídeovigilancia, de improvisto, con el objetivo de hablar con los operadores y así reforzar la convicción de que los procedimientos establecidos se cumplen al pie de la letra.

En todas las zonas de prestación de este servicio público, se es testigo de una voluntad de implicar más a los ciudadanos en los procesos de toma de decisión. En cuanto al mantenimiento del orden, se materializa de diferentes formas, siendo un ejemplo las comisiones de barrio. Esta iniciativa, que forma parte del enfoque nacional para el mantenimiento del orden en los barrios, agrupa a individuos de una misma comunidad local con el objetivo de establecer sus prioridades en materia de mantenimiento del orden y de enfrentar a la policía local y a sus socios ante sus responsabilidades profesionales y las prio-

ridades de dicha comunidad. Estas organizaciones pueden actuar como catalizador para la instalación de sistemas de vídeovigilancia.

Puesto que la percepción pública en cuanto a los beneficios potenciales de la vídeovigilancia es realmente positiva, tales grupos se convierten en auténticos militantes para proyectos locales. Esto puede en algunos casos provocar una imagen que fuera contra la policía, la cual intentaría atenuar el entusiasmo mostrado hacia la vídeovigilancia haciendo hincapié en que el lugar que ocupa es dentro de un conjunto de medidas que tratan un problema identificado que previamente ha sido correctamente investigado.

Desde hace algunos años, existe una cantidad creciente de opiniones favorables a ser prudentes (en vez de oponerse categóricamente) en todo lo relacionado con la vídeovigilancia. Esta prudencia parece tener su origen tanto en los costes frente a los beneficios como en los atentados a la vida privada. Este fenómeno tiene que ser percibido como una consecuencia de la experiencia de situaciones en las cuales las cámaras han sido colocadas sin reflexión previa o sin los recursos necesarios para responder eficazmente a lo que se grababa; nada disminuye más rápidamente el valor de la vídeovigilancia que la percepción generalizada de que nadie acudirá a la zona donde se está cometiendo un delito a pesar de estar siendo grabado por las cámaras.

Como en todas las actividades de seguridad de la comunidad o de mantenimiento del orden, la tarea de evaluar la eficacia de la vídeovigilancia es compleja. Los cálculos de la pertinencia frente a los objetivos es difícil si los propios objetivos no están claros. Por ejemplo, ¿el término "eficacia" hace alusión a la pre-

vención o a la lucha? ¿Existe un valor intrínseco y mesurable en la percepción de que la vídeovigilancia engendra seguridad? ¿Cómo se pueden separar los efectos de la vídeovigilancia de todas las otras intervenciones que han podido ser puestas en marcha como respuesta a un problema identificado?

Hay ciertas pruebas de que la vídeovigilancia puede reducir la criminalidad y el desorden público, aunque no sea tan seguro que sus efectos sean duraderos en el tiempo. También hay ciertas pruebas de que la vídeovigilancia es eficaz en el contexto de crímenes mayores, como el terrorismo (incluso para los atentados suicidas), quizás más por las limitaciones de las fases de reconocimiento necesarias que preceden al ataque.

Quizás haya más pruebas de que la vídeovigilancia puede dar apoyos de gran valor para los investigadores. Por lo menos, la vídeovigilancia puede facilitar a menudo pruebas irrefutables de conducta o de identificación; también hay que señalar que hay estudios que han demostrado que la existencia de pruebas obtenidas gracias a la vídeovigilancia facilita el que la gente se declare culpable en un alto porcentaje, lo que evita el que se haga un juicio y además permite economizar gastos. De hecho, se ha demostrado que en los casos en los que se utilizan imágenes de vídeovigilancia se dictan sentencias más severas.

En cuanto a la garantía, los resultados vuelven a no estar claros. El uso de la vídeovigilancia está tan expandido que con frecuencia se ignora. Al mismo tiempo, nos podríamos preguntar sobre su tendencia a aumentar el miedo en las zonas donde no se utiliza. La necesidad humana de seguridad es su propio motor, el cual exige cada vez una mayor garantía, ya se trate de un policía en cada esquina o una cámara en cada farola.

Como conclusión, podemos afirmar que la vídeovigilancia es una herramienta de gran valor para el conjunto de la seguridad comunitaria, pero no es una respuesta por sí sola: ésta debe inscribirse dentro de una respuesta estratégica planificada, coherente y bien fundamentada. Su eficacia debe ser establecida teniendo en cuenta los objetivos por los que se ha decidido recurrir a ella, estudiando cada caso de manera específica. Los objetivos podrán variar según el conjunto de los delitos o crímenes, y también de los lugares físicos, y por lo tanto las posibilidades de éxito también variarán de un caso a otro.

Andrew Bayes

LYON

NÚMERO DE HABITANTES:
472 000

NÚMERO DE CÁMARAS:
219

AUTORIDAD RESPONSABLE:
La ciudad

La Comisión Ética para la vídeovigilancia en Lyon

Desde que la ciudad de Lyon comenzó a trabajar en la instalación de un sistema de vídeovigilancia, se decidió poner en marcha una comisión municipal externa, bautizada como la Comisión Ética *(Collège d Étique).* El alcalde de Lyon, presidente natural de esta comisión, delegó esta misión en una personalidad independiente, Jean-Pierre Hoss, Consejero de Estado, quien estuvo al mando del primer mandato de esta Comisión. En el segundo mandato fue sustituido por el Sr. Daniel Chabanol, Consejero de Estado honorario, antiguo presidente de la Corte de Apelaciones de Lyon.

La Comisión se compuso haciendo especial aten-

ción a la diversidad: además de cargos políticos electos de todos los partidos (también de la oposición), hay miembros de la llamada sociedad civil, ya sea representantes de asociaciones, como la liga para los derechos del hombre, o de personalidades cualificadas, como el decano honorario del Colegio de Abogados, y un rector honorario de la Academia de Lyon.

La misión que se le ha confiado oficialmente a la Comisión se articula alrededor de tres ejes principales:
➤ Redactar y mantener al día un cuaderno de responsabilidades de la vídeovigilancia, trabajo realizado bajo la presidencia del Sr. Hoss, pero que ahora hay que retomar para actualizar con los desarrollos legislativos en el campo. El objetivo de este cuaderno de responsabilidades, votado por los cargos electos, es el de definir las modalidades complementarias de captura y utilización de imágenes que aumenten las garantías ofrecidas a los utilizadores del espacio público, respetando siempre las prescripciones legislativas. La reflexión sobre la que se está trabajando ahora, además de sobre la inserción de nuevas normas legislativas, se centra en los derechos de acceso a las imágenes y al uso que se puede hacer de ellas. Por ejemplo, las personas que han sido grabadas, ¿pueden tener derecho a ver esas imágenes que les conciernen? ¿Qué hay que hacer para conseguirlas? ¿Qué autoridades pueden ver las imágenes "a tiempo real"? ¿ Y con qué objetivo? ¿Quién puede acceder a las grabaciones y bajo qué condiciones?

➤ Recibir las reclamaciones presentadas por personas que han sido grabadas, opinar sobre la respuesta que hay que darles y hacer todo tipo de proposiciones con este objetivo. Hay que señalar, y es lógico, que esta actividad se da en muy pocos casos,

ya que es muy raro que se presenten reclamaciones serias por un motivo lógico: si se diera el caso de que una persona fuera grabada en condiciones discutibles (en un espacio privado, por ejemplo, suponiendo un desajuste de los mecanismos que impiden esta práctica), si sus imágenes se conservaran más allá del tiempo legal, o fueran vistas por personas no habilitadas, esta persona no sabría que se ha cometido una falta y por tanto difícilmente podrían denunciar este acto.

➤ Constituir una base de datos sobre las prácticas en materia de vídeovigilancia que se llevan a cabo tanto en Francia como en otros países de Europa. El objetivo en este caso es doble. Por una parte, esos datos deberían permitir responder de la manera más científicamente posible a la cuestión de la utilidad de la vídeovigilancia. Debemos señalar que la ciudad de Lyon lanzó, bajo el seguimiento de la Comisión Ética, un estudio universitario dedicado a esta cuestión: hay un estudiante de doctorado a cargo de esta investigación, dentro de un acuerdo universitario estricto entre las Universidades de Lyon-II y la de Ginebra, que cuenta con el apoyo financiero de la ciudad, y se dan todas las garantías para que esta investigación se desarrolle en la más total independencia universitaria.
Por otra parte, los contactos entablados durante la recogida de datos deberían de acercarnos a la puesta en marcha de una red de ayuntamientos, siendo la idea final el tener una especie de multiplicación de la institución lionesa.

Además del ejercicio de sus competencias, es importante señalar que la existencia de esta Comisión y los intercambios que alimentan sus reuniones tienen como efecto conducir a una reflexión pacífica y tranquila sobre un tema sensible, al tiempo que

apaga debates a menudo fantasmales. Desde luego, esto no quiere decir que un consenso vacío de contenido ocupe el lugar de un necesario debate sobre la sociedad fundamental, ya que en primer lugar no sería deseable y, en segundo lugar, no es éste el caso. En estas reuniones está siempre presente y vigilante la oposición, y la dialéctica que nace entre el entusiasmo de los unos y las restricciones de los otros anima el debate. Esto enriquece la reflexión más de lo que lo harían unas exposiciones sobre estadísticas desde posiciones inamovibles. Y creemos que precisamente es ese el aporte esencial de la existencia de la Comisión Ética.

Emmanuel Magne

ROTTERDAM

NÚMERO DE HABITANTES:
589 615

NÚMERO DE CÁMARAS:
289

AUTORIDAD RESPONSABLE:
La policía

La vídeovigilancia en Rotterdam: cómo mantener un sistema eficaz al mismo tiempo que se gestionan las expectativas

La participación de Rotterdam en el proyecto del FESU sobre las cámaras de vigilancia es coherente con nuestro objetivo de mejorar nuestro sistema de vídeovigilancia. ¿Cuáles son las opciones que aún no utilizamos? ¿Cuál es el equilibrio entre la tecnología y la capacidad de los individuos para reaccionar ante los acontecimientos? ¿Cómo se interpreta el concepto de vida privada en el espacio público? Este artículo examina nuestra experiencia con las cámaras de vigilancia en Rotterdam, las normas que rigen este sis-

tema y los problemas concretos sobre los que Rotterdam está trabajando todavía.

Experiencias

Todas las ciudades intentan controlar la criminalidad y el desorden público. Todas las ciudades investigan para obtener métodos más inteligentes y eficaces para aumentar la seguridad. Todas las ciudades pueden utilizar innovaciones tecnológicas. Rotterdam no es una excepción a ninguna de estas tres afirmaciones: la vídeovigilancia a través de cámaras tiene como objetivo reducir el desorden público y la criminalidad, y aumentar el sentimiento de seguridad de la población.

Las primeras cámaras fueron instaladas en Rotterdam hace diez años. La razón más importante era el campeonato de fútbol del Euro 2000: era importante que se desarrollase sin problemas, lo que significaba poder tener una vista panorámica precisa de la atmósfera y de los acontecimientos al tiempo que estos ocurrían. Así, se instalaron cámaras en el centro de la ciudad con el fin de vigilar la llegada en masa de los hinchas. Ese mismo año, se instalaron también cámaras en Saftlevenkwartier, un barrio cercano a la estación central. En ese caso, el objetivo era el de reducir y prevenir los problemas de violencia y acoso en las calles.

Desde el año 2000, el número de cámaras en los espacios públicos ha ido aumentando regularmente hasta alcanzar la cifra de 300. Además, existen 1.600 cámaras colocadas en la red de transportes públicos (metro, tranvía, bus y estaciones). Estas cámaras pertenecen a compañías de transporte privadas, que las controlan y las vigilan. Cuando se produce un accidente, las imágenes en directo pueden verse desde la sala de vídeovigilancia.

Cada demanda de instalación de una cámara de vigilancia viene acompañada de un informe detallado en el que se describen el número y el tipo de incidentes

que se produce en la zona y se presenta la situación local en materia de seguridad. Cada decisión sobre la instalación de una cámara se examina minuciosamente: las cámaras no se instalan al azar, sino cuando se está realmente convencido de que es una herramienta necesaria para mejorar la seguridad.
Las cámaras de vigilancia no son un remedio contra todo mal, pero en Rotterdam se han convertido en una herramienta de base para garantizar la seguridad y prevenir los delitos contra la violencia y la propiedad privada y pública.
Se ha demostrado que los actos violentos a menudo se producen «sin pensarlo» o bajo la influencia de las drogas y/o el alcohol. Seguramente la presencia de las cámaras no disuade a los delincuentes, pero es de gran utilidad ya que las imágenes grabadas pueden presentarse como pruebas ante los tribunales.
Los delitos contra la propiedad, como por ejemplo los robos de carteras o en los coches, son un caso diferente, dado que son de naturaleza premeditada. Si hay cámaras instaladas en la zona, y la policía actúa inmediatamente después de la infracción, el delincuente intentará no actuar de nuevo en el mismo barrio. Por lo cual, la vídeovigilancia puede reducir el número de incidentes.

Condiciones
Desde su llegada, con frecuencia se pone sobre la mesa la misma cuestión: ¿cómo utilizar la vídeovigilancia de manera ética y democrática? Cuantas más cámaras hay, más importante es tratar estos aspectos adecuadamente.
Según la ley holandesa, son los consejos municipales quienes autorizan la instalación de cámaras de vigilancia. Si el consejo decide favorablemente, puede delegar en el alcalde la autoridad para decidir dónde se colocarán las cámaras. Las decisiones del alcalde son públicas y están abiertas a las objeciones de los vecinos.

Una vez que las cámaras comienzan a grabar imágenes en Rotterdam, éstas dependen de la Ley de Datos de la Policía (Police Data Act), la cual limita estrictamente la utilización y el intercambio de estas imágenes.

Desde sus comienzos, la vídeovigilancia en Rotterdam se basa en un cierto número de principios:
- Todas las cámaras se vigilan 24 horas al día, siete días a la semana;
- Las imágenes se graban siempre, lo que garantiza a los ciudadanos que cualquier incidente será tenido en cuenta;
- Se le debe dar seguimiento a todos los incidentes observados;
- La presencia de cámaras significa una intensificación considerable de la vigilancia en un barrio, no sólo porque la zona esté bajo observación sino también porque cada incidente exige una respuesta de la policía o de los organismos de control.

Aclaración de algunos puntos
Numerosos partidos políticos han trabajado duro para convertir Rotterdam en una ciudad más segura. Nuestros habitantes exigen que el gobierno local garantice una ciudad limpia, correcta y segura. Ven los problemas en sus calles, bajo sus propios ojos, en los lugares donde viven. En consecuencia, es habitual que los consejos locales respondan a las expectativas de los ciudadanos, y las cámaras de vigilancia son una herramienta indispensable para lograr esta tarea.

La inversión que Rotterdam ha hecho es importante. La vídeovigilancia es una tecnología costosa para la que además hay que prever una financiación para el mantenimiento de los equipos y los gastos de personal (los equipos de operadores y el personal responsable de las actividades de seguimiento). En Rot-

terdam, el número de imágenes que una misma persona puede vigilar es limitado, lo que significa que cada vez que se instala una cámara nueva en una zona hace falta contratar nuevo personal, lo que supone un problema cuando se recibe una petición de instalación de una nueva cámara. Al mismo tiempo, el valor de la vídeovigilancia es también importante: incidentes que nunca hubieran sido observados o que antes quedarían sin prueba son ahora objeto de investigación policial. En 2009, el departamento de cámaras de vídeovigilancia grabó 23.700 incidentes, es decir, 65 por día. Debemos continuar los cálculos de los beneficios con respecto al coste. La actitud de los vecinos de Rotterdam ha cambiado a lo largo de estos últimos diez años: al principio, las primeras cámaras fueron acogidas con cierta desconfianza. La gente tenía dudas sobre su eficacia, y además no confiaban en la profesionalidad de los usuarios, temiendo así injerencias en sus vidas privadas.

Sin embargo hoy, diez años más tarde, las actitudes han evolucionado de manera significativa, y parece que los ciudadanos les han cogido aprecio "a sus cámaras". Cada vez más frecuentemente la gente pide que se instalen cámaras de vídeovigilancia en sus barrios. Una encuesta anual ha revelado que hay un nivel muy alto de confianza hacia el sistema de vídeovigilancia y que los ciudadanos lo consideran como una herramienta eficaz.

Conclusión

Las cámaras se han convertido en una característica familiar en los lugares públicos. En Rotterdam, éstas han probado su valor durante acontecimientos importantes, como el Euro 2000, momento en el que se empezó a utilizar la vídeovigilancia. Recientemente, ha demostrado su importancia durante graves motines; gracias a las imágenes de estas cámaras, pu-

dimos detener a numerosos agitadores.
Por lo tanto, nuestra experiencia con la vídeovigilancia es positiva. El marco legal se ha desarrollado para dar respuesta a los problemas vinculados con el derecho civil y a las expectativas del público en materia de seguridad. Hemos puesto en marcha una organización y una estructura de gestión sólidas. Los procedimientos operativos son claros. Debemos proseguir con los esfuerzos para mantener este sistema en el futuro. Sin embargo, también es obvio que nuestra misión está llamada a evolucionar con las nuevas cuestiones que van surgiendo, y al tiempo que el público presenta nuevas expectativas. Tendremos que enfrentarnos a nuevas exigencias. Por otra parte, la crisis económica conlleva importantes reducciones presupuestarias. Nuestro objetivo es controlar el gasto de la vídeovigilancia a la vez que mantenemos nuestro presupuesto. Un desafío ambicioso que requiere una profunda reflexión.

Afke Besselink, Niels Wittersholt

SAINT-HERBLAIN

NÚMERO DE HABITANTES:
43 510

NÚMERO DE CÁMARAS:
18

AUTORIDAD RESPONSABLE:
La ciudad

➤ Saint-Herblain es una ciudad francesa de 45.000 habitantes situada en la primera corona de la aglomeración de Nantes (500.000 habitantes); es la segunda ciudad de esta aglomeración y la tercera del Departamento de Loire Atlantique.

Al principio de su mandato 1996-2002, el Senador y Alcalde, junto con los cargos políticos electos, pusieron en marcha el proyecto de instalación de un sistema de vídeovigilancia, siendo las primeras cámaras instaladas en 1999. La ciudad dispone hoy en día de un sistema compuesto de 18 cámaras. En el año 2000 se puso en marcha el Centro de Supervisión Urbana (CSU), según

lo establecido por un decreto de la Prefectura. Este centro, que en un principio tenía como misión gestionar únicamente el sistema de vídeovigilancia, permite en la actualidad gestionar al mismo tiempo la vídeovigilancia urbana y el dispositivo de televigilancia, y tiende a cobrar cada vez un mayor peso como herramienta global de gestión urbana.
En 1997, se llevó a cabo una auditoría en materia de seguridad a través de una consultora exterior. Paralelamente, la Comisión de Seguridad del Consejo Municipal de Prevención de la Delincuencia (CCPD) tenía la responsabilidad de llevar a cargo una reflexión sobre las cuestiones de seguridad en la ciudad de Saint-Herblain. Esta comisión entregó su informe en 1998 al Senador y Alcalde, quien decidió entonces crear diferentes grupos de trabajo sobre las temáticas relacionadas con la seguridad. En 1999, se presentó la síntesis de éstos en el Consejo Municipal. Paralelamente a este trabajo dentro de la CCPD, una serie de ciudadanos de Saint-Herblain respondieron a un cuestionario sobre la seguridad, que reveló que ésta era su preocupación principal.
Basándose en estos elementos de diagnóstico, el alcalde inició un debate dentro del Consejo Municipal sobre la aplicación de las proposiciones de la CCPD, entre las cuales se encontraba la vídeovigilancia. En junio de 1999, el consejo municipal votó a favor de la instalación de un sistema de vídeovigilancia en el municipio y también de la creación de un Comité Ético para acompañar la puesta en marcha de este proyecto.

La ciudad de Saint-Herblain asignó tres grandes objetivos a su dispositivo de vídeovigilancia:

➤ Garantizar la seguridad en los lugares donde el flujo de bienes y de personas son más importantes para reducir los delitos en las vías públicas;
➤ Completar gracias a medios tecnológicos el dispo-

sitivo de prevención de la delincuencia existente (policía municipal, acciones de prevención en medio escolar);
➤ Tranquilizar a los habitantes y suministrar a los servicios de policía del Estado elementos que permitan explicar los actos delictivos. El objetivo en este caso era doble: acompañar a la policía nacional para que aumente el porcentaje de casos resueltos, muy bajo en ese momento, y conseguir la seguridad de los espacios públicos con vocación familiar, industrial o de grandes multitudes.

El sistema de vídeovigilancia se puso en marcha para aumentar la seguridad de todos los habitantes de Saint-Herblain. Fue concebido como una herramienta suplementaria integrada en la política local de seguridad y prevención de la delincuencia. Para ello, el Centro de Supervisión Urbana de la ciudad se ocupa del sistema de vídeovigilancia y de televigilancia, que garantiza una mayor reacción por parte de los servicios municipales (policía municipal, servicios técnicos, etc.) y de la policía nacional o de la gendarmería. Se trata por tanto de una auténtica herramienta de gestión de la ciudad.
La política municipal en materia de prevención y de seguridad se inició hace más de veinte años. Se inscribe dentro de la preocupación permanente de prevención de las conductas de riesgo y de la delincuencia por parte de los que la cometen por primera vez, considerando que esta etapa es fundamental antes de cualquier otro posicionamiento represivo. Existen diferentes herramientas a través de las que se expresa la voluntad política de prevención, tales como las acciones preventivas dentro de los establecimientos escolares, la prevención situacional, las intervenciones de la policía municipal o la realización de actos reglamentarios municipales relativos con la gestión del espacio público.

A nivel político, es el Teniente Alcalde responsable de la prevención y de la seguridad pública quien está a cargo de organizar el conjunto de acciones preventivas; a nivel administrativo, se encarga la Dirección de la Prevención y la Tranquilidad Pública, compuesta por 40 agentes.

En este contexto, la vídeovigilancia urbana constituye uno de los elementos de la política global de prevención y seguridad. La herramienta fue creada respetando estrictamente los textos por los que se regulan las imágenes. La ciudad deseó hacerlo a través de un proceso transparente, implicando a la población. En consecuencia, se organizaron diversas presentaciones y visitas que permitieron a los ciudadanos apreciar las garantías adoptadas para preservar su vida privada.

El dispositivo puesto en funcionamiento está compuesto de 18 cámaras. El CSU está formado por 14 agentes y un responsable de la explotación del sistema de vídeovigilancia. Hay parámetros digitales que permiten que se respete la prohibición de grabar las propiedades privadas o discernir los rasgos faciales de un individuo. De acuerdo con la reglamentación en vigor, hay carteles instalados en los diferentes accesos por carretera que informan a los ciudadanos de la presencia de cámaras.

Las imágenes de vídeovigilancia de la ciudad se transmiten a tiempo real al Centro de Información y de Mando de la policía nacional.

Las imágenes tan sólo se pueden consultar bajo demanda de los servicios de la policía nacional, teniendo en cuenta las quejas de los ciudadanos, o de las peticiones específicas de los servicios de seguridad del Estado.

Saint-Herblain (Francia)

El sistema de vídeovigilancia ha tenido efectos positivos en la seguridad de los espacios vigilados y la reducción de actos delictivos. Por otra parte, no se ha constatado un desplazamiento de la criminalidad.

La actividad del CSU (vídeovigilancia y televigilancia) se somete a una evaluación anual. Por último añadir que los operadores reciben una formación, impartida por un organismo exterior, sobre la deontología, el contexto, las asociaciones y las responsabilidades existentes en el dominio de la seguridad.

Dominique Talledec

El principio de la vídeovigilancia en el condado de Sussex

El uso del Circuito Cerrado de Televisión (CCTV) en el Condado de Sussex se remonta a 1993, cuando un primer grupo de 15 cámaras fue instalado en las calles de Brighton, de acuerdo con la decisión de la Policía de Sussex y los socios de las autoridades locales para utilizar cámaras con el objetivo de prevenir y reducir la delincuencia y ayudar a efectuar detenciones. A esta primera instalación le siguieron otras, tanto en Brighton como en otras ciudades, pueblos y aldeas, financiadas a medias con fondos de las autoridades locales y con ayudas del gobierno central. Desde el

principio, los CCTV en Sussex se desarrollaron gracias a una estrecha relación de trabajo entre la policía y las autoridades locales, estableciendo turnos de vigilancia en las tres comisarías de policía de Brighton (Haywards Heath, Bognor y Eastbourne), además de abrir cinco salas de vigilancia para las autoridades locales. Paralelamente, se decidió compartir los costes.

Las iniciativas del gobierno central para apoyar el crecimiento de los CCTV se materializaron en la competición CCTV Challenge (Reto CCTV) de 1994 y en el Programa para Reducción de la Delincuencia llevado a cabo entre 1999 y 2003. Además se le dio a esta iniciativa un nuevo apoyo legislativo gracias a la Ley de Criminalidad y Disturbios de 1998, que obliga a las autoridades públicas a trabajar conjuntamente para luchar contra la problemática de la criminalidad y los comportamientos antisociales. Como resultado del mismo, en 2006 había aproximadamente 30 ciudades, pueblos y aldeas en todo el Condado de Sussex con cámaras instaladas, con 17 autoridades locales y una asociación involucrados.

Como resultado, se creó el partenariado Sussex CCTV: una colaboración definida ahora gracias a contratos legales individuales entre la Policía de Sussex y cada autoridad local, fijando los protocolos operativos, roles, responsabilidades y arreglos financieros de cada colaboración individual.

La actualidad de los CCTV en Sussex

Actualmente hay casi 400 cámaras en todo el condado, mezcla de cámaras "*dome*" y cámaras análogas *"pan-tilt-zoom"*, conectadas con varias salas de vigilancia a través de una red de cables de transmisión de fibra. La plataforma de control, vigilancia y

grabación es un sistema recientemente instalado llamado "i-witness", diseñado por Teleste e instalado por BT Redcare. Esta plataforma muestra grabaciones a tiempo real de 25 fotogramas por segundo, grabando imágenes seleccionadas en cada secuencia.

Además, las terminales "cliente" se han colocado en las principales comisarías de policía, permitiendo a los oficiales locales tener acceso inmediato a los videos con fines de investigación.

Este sistema totalmente interconectado permite controlar todas las imágenes de las cámaras "en directo" desde cualquier sala de vigilancia del Condado, además de un acceso inmediato a material histórico en cualquiera de los "clientes" locales.

Beneficios

Un sistema totalmente interconectado como el nuestro presenta una cierta cantidad de beneficios probados:

1. *Continuidad Empresarial:* el sistema es inherentemente elástico. Las cámaras pueden ser utilizadas desde cualquiera de los diferentes puertos de entrada del sistema, garantizando así una continuidad para servir al público.

2. *Ahorro de tiempo para los oficiales:* los miembros de la policía encargados de las investigaciones en las comisarías locales tienen un acceso rápido y sencillo a las imágenes que necesitan para sus investigaciones. Esto ha eliminado los cansados *viajes por todo* el condado para recuperar (con cita previa) las imágenes que necesitaban. El resultado es evidente: ahora los policías pasan más tiempo recorriendo los

vecindarios y garantizando la seguridad de sus poblaciones.

3. *Beneficios medioambientales:* cuantos menos viajes en coche tienen que hacer los policías, mayor es la reducción de las emisiones de carbono, además de ahorrar en gasolina.

4. *Juicios más rápidos:* durante las investigaciones, los sospechosos arrestados se ven enfrentados a pruebas visuales en una etapa previa que cuando no las hay, lo que ayuda a disminuir las liberaciones con fianza, a que las declaraciones sean más rápidas y, por último, se le puede ofrecer un mejor servicio a las víctimas de los delitos.

5. *Seguridad de las imágenes:* la existencia de un acceso protegido por contraseña y sometido a auditoría a través de un sistema de registro de las actividades garantiza un mejor control de los datos sensibles.

Derechos individuales, privacidad y uso de los CCTV en Sussex

El uso adecuado de los CCTV en el Reino Unido está regido por tres documentos clave de la legislación, además de ciertas pautas provenientes de la Oficina de los Inspectores de la Información *(Information Commissioners Office)*. La Ley de Protección de Datos de 1998 establece ocho principios sobre la protección de datos; trata asuntos como el buen procesamiento de los datos, un control adecuado de los mismos, la pertinencia de los datos retenidos y la proporcionalidad en el tiempo de retención de dichos datos. La Ley de Derechos Humanos de 1998, incluida en el derecho del Reino Unido, incluye los principios fundamentales tratados en el Convenio Europeo de los Derechos Humanos, siendo el de-

recho a la privacidad (Art. 8) uno de los más pertinentes cuando se habla de CCTV. La Ley de Regulación de los Poderes Investigadores del año 2000 prevé las reglas para el uso encubierto de las cámaras, con severas penas según el nivel de delito cometido.

En Sussex, todos los operadores reciben una formación para alcanzar los niveles exigidos por la Autoridad de la Seguridad Industrial *(Security Industry Authority).* Esta formación trata sobre las leyes pertinentes y las responsabilidades de los operadores a la hora de utilizar las cámaras, además del respeto a la igualdad y la diversidad. Además, se ha adoptado un Código de Prácticas CCTV en el que se prevén las mejores prácticas relativas al uso operativo y ético de los CCTV. Este código ha sido compartido entre los diferentes socios y en conjunto con los protocolos entre las autoridades locales y la policía, lo que asegura la regularidad y la compatibilidad.

Al mismo tiempo, todo uso de las terminales "cliente" locales está altamente garantizado a través de un programa de formación que asegura el buen uso y tratamiento de las imágenes de video más sensibles. Por último, existen contraseñas individuales para acceder a los sistemas que permiten garantizar el buen uso de los mismos.

La confidencialidad y la responsabilidad del uso policial de los CCTV en Sussex

La responsabilidad para con los habitantes de Sussex se consigue a través de procesos de encuentros de gestión con auditorías con todos los socios de los CCTV y un proceso de vigilancia independiente.

Gestión del Partenariado

El Sussex CCTV Partnership supone un enfoque compartido de la gestión y uso de las cámaras en el espacio público. Las cámaras propiedad de las autoridades locales son operadas por un equipo combinado de miembros de la policía en las comisarías y de autoridades locales en las salas de vigilancia de las autoridades locales. Los costes para mantener el sistema son compartidos entre ambos.

Se organizan encuentros trimestrales entre la Policía CCTV de Sussex y los socios de las autoridades locales donde se tratan temas como los resultados del sistema, desarrollos técnicos, problemas financieros y cualquier otro tema que se prevea que puede surgir en un futuro. A través de estos medios, se controla el uso policial de las cámaras del ayuntamiento

Estamos actualmente desarrollando un proceso común para iniciar la instalación de nuevas cámaras, garantizando así un enfoque coherente por parte del Condado de Sussex.

Vigilancia Independiente

En Sussex estamos convencidos de que la vigilancia independiente es esencial para mantener la confianza pública en el uso de los CCTV. Por ello, ahora se acaba de adoptar un proceso independiente de vigilancia y verificación del uso policial de las cámaras. Las Autoridades de la Policía de Sussex han reclutado a 12 personas del público para llevar a cabo exámenes hechos al azar en las instalaciones de vigilancia de la policía y asegurar así el respeto por las leyes y los Códigos de Buenas Prácticas. Estos exámenes pueden realizarse en cualquier momento del día o de la noche sin aviso previo. Cualquier pro-

blema o preocupación detectado durante los mismos se les hace llegar a las Autoridades Policiales y a la Gestión de los CCTV. Los informes anuales y las reuniones de escrutinio abiertas al público garantizan la transparencia.
Ahora se ha propuesto extrapolar este sistema a las salas de vigilancia de los socios de las autoridades locales.

Es interesante señalar que el trabajo con los socios europeos a través del proyecto del FESU ha confirmado la validez y eficacia de este sistema, y desde el Condado de Sussex consideramos que cualquier otro proceso de este tipo será un elemento clave para eventuales Cartas del Uso de los CCTV.

La Estrategia Nacional de los CCTV y Sussex
La Estrategia Nacional de los CCTV fue publicada por primera vez en Octubre de 2007 y presenta los resultados de un estudio de amplio alcance de los CCTV en Inglaterra y Gales. Aunque en un principio estuvo a cargo de un equipo conjunto del ACPO y el Ministerio del Interior británico, en la actualidad esta estrategia es responsabilidad de un programa llevado a cabo por un equipo de varias agencias con representación de numerosos participantes/ accionistas.

La Estrategia apoya y desarrolla recomendaciones que asegurarán:
1. CCTV bien gestionados y efectivos, teniendo en cuenta el papel de la industria de los CCTV y la visión del público;
2. Mejores prácticas para las relaciones entre las autoridades locales, los operadores de los CCTV, los oficiales de policía y los servicios de emergencia, ofreciendo una mejor protección al público gracias a su capacidad de elemento disuasorio y también a su

importancia durante la investigación del crimen;
3. Mayor calidad en las intervenciones a través de los CCTV y en la presentación de imágenes.

A través de las características arriba citadas, el Sussex CCTV Partnership intenta adoptar e implementar todos y cada uno de estos elementos clave, para así garantizar la compatibilidad con las mejores prácticas adoptadas a nivel nacional.

Christopher Ambler, Roger Fox

La región de Véneto está situada al noreste de Italia y cuenta con casi cinco millones de habitantes, de los cuales un 7% son inmigrantes, en una superficie de 18.400 km2. Es uno de los principales ejes económicos e industriales del país y se sitúa entre las 30 primeras regiones europeas. También es la región italiana que acoge el mayor número de turistas, con un total de 60 millones de visitantes al año. Está dividida en siete provincias y agrupa 581 municipios, de los cuales un 80% tienen menos de 5.000 habitantes.

Según los datos generales sobre el fenómeno de la criminalidad en la región, en los últimos años se ha constatado una clara tendencia a la baja, acompañada

sin embargo de un sentimiento creciente de inseguridad. Esto ha incitado a varias colectividades locales a poner en marcha o a desarrollar políticas de seguridad urbana. Desde el año 2002, la administración regional ha adoptado un texto de ley (La Ley 9/2002) cuyo objetivo es apoyar y promover un conjunto de acciones que garanticen la seguridad urbana. La región desea crear un "sistema", destinado a gestionar de manera coordinada los problemas complejos que se dan en un territorio, en el marco de una colaboración entre los diferentes niveles de gobierno (Estado, región, provincia y municipio) y las fuerzas policiales (nacionales y locales).

Por ello, se invitó a los municipios y provincias a que elaboraran proyectos integrales de seguridad urbana, que posteriormente fueron examinados y financiados por la región. Durante los últimos cinco años (2005-2009), se aprobaron y financiaron 278 proyectos, que están siendo ejecutados en la actualidad. Según los datos administrativos, 131 de estos proyectos incluyen la puesta en marcha de un sistema de vídeovigilancia, lo que representa casi un proyecto de cada dos.

En el año 2007, el Observatorio Regional para la Seguridad, cuya creación está prevista por la ley regional más importante, realizó su primera encuesta con el fin de verificar el número de equipos de vídeovigilancia instalados, y así poder evaluar su utilización. De los 581 municipios, respondieron a la encuesta 215, y los resultados permitieron constatar que la motivación principal para poner en marcha los sistemas de vídeovigilancia fue la financiación recibida por la región. También se constató que la demanda de vídeovigilancia tiende a aumentar.

En cuanto a los equipos escogidos, en más del 70% de los casos se trata de sistemas digitales dotados de

más de tres cámaras. Las cámaras se suelen colocar en parkings públicos, cruces, parques públicos y centros escolares. En aproximadamente un 60% de los casos, somos testigos de un descenso de los fenómenos de pequeña delincuencia y desorden público, según los cálculos de los comandantes de la policía local que han respondido al cuestionario. Sin embargo, hay que subrayar que en el 21% de los casos se ha observado que los comportamientos ilícitos se han desplazado hacia otras zonas que no están dotadas de sistemas de vídeovigilancia.

Existe otro proyecto concreto de instalación de cámaras en los medios de transporte públicos de las capitales de provincia de la región de Venecia. Se trata del sistema de transportes públicos urbanos, el cual aparentemente está expuesto a numerosos factores de riesgo, como actos vandálicos, violencia y crímenes menores, y que además puede ser objeto de atentados terroristas (tal y como mostraron las trágicas experiencias de Londres y Madrid). En consecuencia, se han instalado sistemas de vídeovigilancia en la red de transportes urbanos, así como en las paradas de autobús. En la ciudad de Venecia, se ha prestado especial atención a los embarcaderos de los vaporetti, que vienen a ser "barco-autobuses".

Por lo tanto, la región ha jugado un rol importante en el fomento y coordinación de las instalaciones colocadas y gestionadas por las diferentes colectividades locales o por los departamentos. Esto ha ayudado mucho a desarrollar la utilización y la difusión de la vídeovigilancia en las zonas de fuerte concentración urbana. En conjunto, el balance es más bien positivo, como lo demuestra el aumento exponencial del número de sistemas en funcionamiento.

Basándonos en las actividades y experiencias reali-

zadas dentro del proyecto europeo sobre seguridad urbana, ahora es importante interrogarnos sobre el papel que pueden jugar las administraciones regionales en la gestión de las políticas de seguridad urbana, sobre todo en materia de vídeovigilancia.

Otras regiones italianas ya han imitado el enfoque adoptado por la región de Venecia. Dos de los elementos clave de su política en materia de seguridad urbana son, por una parte, conceder ayudas económicas con el fin de fomentar las inversiones de las colectividades locales, y por la otra, proponer instrumentos de análisis con el fin de identificar, dentro de un proyecto local, los medios más adecuados a adoptar para abordar el tema de la seguridad urbana, teniendo en cuenta que siempre es preferible tratar de resolver los problemas desde el nivel más cercano a la población, es decir, el nivel local.

No obstante, es posible pensar en una segunda fase de este proyecto, por ahora sin desarrollar, durante la cual se podría prever que la región jugará el papel de coordinador, trabajando más estrechamente con los municipios. Esto tendría el objetivo de garantizar una mayor homogeneidad y una mayor sinergia en la aplicación de su política de seguridad, para así evitar el riesgo de aislamiento. Por otro lado, también se podría apoyar a nivel regional la utilización de herramientas complementarias que favorecieran la participación y el control. Esto aún no ha suscitado demasiado interés entre los municipios, que por el momento se han limitado a aplicar estricta y burocráticamente las normas previstas por el organismo nacional encargado de la protección de la vida privada.

En otras palabras, haría falta desarrollar la coordinación entre las colectividades territoriales desde el punto de vista de las tecnologías utilizadas, con el fin

de lograr una mayor eficacia de los medios de vídeovigilancia y obtener intervenciones inmediatas y preventivas (gracias a la utilización de otros bancos de datos disponibles y una mejor organización del servicio). Por ahora, estos sistemas tan sólo son utilizados como soporte técnico de apoyo a las encuestas de la policía.

Sin embargo, las herramientas tecnológicas deben estar apoyadas para poder tener una buena organización de los servicios de policía. En ese sentido, la región de Venecia está realizando un proyecto de reparto territorial en la organización de los servicios de la policía local ("distrettualizzazione"), el cual permite asociar más municipios que se encuentren en aglomeraciones de por lo menos 20.000 habitantes, que correspondan dentro de lo posible con la estructura de la organización de la policía nacional. Esta nueva división territorial permite a los municipios más pequeños beneficiarse de un servicio de policía municipal más completo, en coordinación con la policía nacional, la cual garantiza de este modo intervenciones más rápidas y acciones preventivas. Y es que es el impacto de la vídeovigilancia tan sólo puede ser optimizado a través de actividades de prevención

Paralelamente, hay que aumentar la implicación de los ciudadanos en su comunidad y sensibilizarles más sobre la utilidad de la vídeovigilancia, que a pesar de ser bastante invasiva, es por lo general bien aceptada en Venecia. Es necesario que los ciudadanos estén convencidos de los beneficios de la vigilancia cívica y de la cooperación para luchar contra los fenómenos bastante expandidos de degradación y desorden urbano. La existencia de "redes sociales" civiles es uno de los cimientos de la vida en común, y es también una referencia para las fuerzas del orden.

En este campo, la región puede formular orientaciones reglamentarias (elaboración de leyes y de disposiciones reglamentarias apropiadas) y actuar sobre el plano financiero, orientando las inversiones hacia una mejor integración de las tecnologías según estándares compartidos. La región también se compromete a apoyar a las administraciones locales, dándoles líneas directrices y directivas para ayudarles a poner en marcha los sistemas de seguridad urbana, entre ellos la instalación de sistemas de vídeovigilancia con un enfoque coordinado en asociación con los ciudadanos. Un paso semejante tendría que ayudar a hacer evolucionar el concepto de seguridad y situar la videoprotección como un instrumento entre otros de una política global.

Giorgio Vigo

Conclusión

Hacia una utilización de la vídeovigilancia respetuosa de las libertades individuales

En 2008, más del 50% de la población mundial vivía en las ciudades y se observa una tendencia al aumento de la movilidad entre las diferentes zonas urbanas. Por lo tanto, se observa también una intensificación de los fenómenos urbanos, lo que también repercute en la seguridad. En este contexto, la vigilancia por vídeo es, desde luego, un instrumento tecnológico, pero también ilustra una forma de colaboración social entre las diferentes instituciones y administraciones.

Estos sistemas plantean una serie de retos que este proyecto desea estudiar:

1. La relación entre la vigilancia por vídeo, herramienta tecnológica, y el factor humano que la controla. La tecnología como tal no es un elemento de riesgo, sino el uso que de ella se haga, es decir, el riesgo de que sus potencialidades sean desviadas de su objetivo inicial; por ello, desde la instalación del sistema su utilización debe estar claramente enmarcada, tanto por medidas técnicas como por los compromisos políticos explícitos.

2. Se puede pensar en un sistema de vigilancia por vídeo como en un terminal inteligente, no sólo por la recuperación de las imágenes, sino también por cuanto a la reorganización de los diferentes recursos de la ciudad. Este sistema puede facilitar el trabajo de los agentes de la ciudad, pero requiere respuestas menos genéricas y más adecuadas a las necesidades concretas. De tal suerte, la seguridad podrá tener una mejor visibilidad, fundada en una mejor información a los ciudadanos.

3. Los pocos estudios realizados a la fecha sobre la eficacia de la vigilancia por vídeo han mostrado que los resultados obtenidos con esta tecnología deben correlacionarse con el contexto particular en donde se supone que deben intervenir las cámaras. Esto significa que se tenga en cuenta la naturaleza y la dimensión del territorio vigilado, la población y las necesidades concretas identificadas con una auditoría de seguridad. Expertos y profesionales han reconocido unánimemente que la vigilancia por vídeo no constituye la panacea que pudiera solucionar todos los problemas de seguridad de una ciudad, sino que se la debe considerar como un instrumento entre otros, en el marco de una política global de seguridad. Hay, pues, que buscar un equilibrio entre el uso de las diferentes herramientas que tienen a su disposición quienes deben tomar las decisiones. También es importante no limitarse a usar un único instrumento ya que la verdadera eficacia de una política de seguridad resulta de la complementariedad de las herramientas que se emplean y de la capacidad de dar respuestas coordinadas y adecuadas a cada situación.

4. Buscar más eficacia se refleja asimismo en la posibilidad de incorporar diferentes sistemas de vigilancia por vídeo del espacio público. En algunas ciudades existen vario sistemas administrados por diferentes actores. La posibilidad de de integrar diferentes sistemas, lo que supone una información mejor compartida, no sólo se aplica en el plano local, sino también regional y metropolitano. Esta orientación podría cobrar la forma de unos pactos "transversales" entre gobiernos, regiones y municipios, o bien, de una colaboración entre el sector privado y público cuando se trata de la vigilancia de espacios semipúblicos. Pero para ello hay que definir protocolos precisos y estrictos que indiquen cómo compartir la información para no afectar la confidencialidad de los datos personales y de

la vida privada. Al mismo tiempo, la conjunción de la vigilancia por vídeo con otros sistemas de información y otras bases de datos, que se está volviendo técnicamente posible, es un arma de doble filo. Aunque esta posibilidad aumente la capacidad de vigilancia de los sistemas, el principio de necesidad impone una rigurosa justificación para acumular y correlacionar tanta información sobre los individuos.

Por último, la óptica transversal que se aplica a todos estos temas ha analizado hasta adónde se puede llegar para garantizar la seguridad de los ciudadanos, sin interferir con ello en su vida privada. ¿Existe un derecho a la intimidad en el espacio público? ¿Hasta qué punto? ¿En qué medida el derecho a la seguridad puede afectar otros derechos fundamentales como la libertad de expresión, de asociación y de manifestación?

Todos estos aspectos han sido abordados a través del prisma de los habitantes de las ciudades, en estos 18 meses de cooperación europea. Los participantes han hecho del ciudadano el centro de sus preocupaciones. En efecto, los ciudadanos necesitan sentirse en seguridad en sus hogares, pero no por ello desean que se cuestione su derecho a la protección de la imagen personal. Como garantes del bienestar de los ciudadanos, los responsables políticos deben considerar, pues, este punto como una preocupación constante, poniendo en la balanza los diferentes aspectos involucrados. De un país a otro, de una ciudad a otra, el modo de equilibrar la búsqueda de seguridad y la reivindicación de un derecho al anonimato cambia. Analizando las políticas públicas con vistas a la percepción que tiene la gente, este proyecto tenía el objetivo de reforzar el lugar que ocupan los ciudadanos y la información que se les da, en el marco de la utilización de sistemas de vigilancia por vídeo, con vistas a una indispensable transparencia y al desarrollo de políticas públicas democráticas.

Como usuarios o actores de los servicios públicos, ¿los ciudadanos piden o no que se instalen sistemas de vigilancia por vídeo? ¿Estos sistemas son una respuesta adecuada a los temores expresados? ¿Corresponden al presupuesto disponible? ¿Qué formaciones y medios de control o qué instancias ante las cuales recurrir se pueden considerar?
¿De qué modo expresan los ciudadanos la aceptación o el rechazo de los sistemas de vigilancia por vídeo? ¿De qué modo son informados y cómo participan en las diferentes etapas de implementación de una política de vigilancia por vídeo? ¿De qué modo influyen estos dispositivos en la percepción que tienen los ciudadanos ya en el comportamiento de las víctimas y de los autores potenciales?

Los participantes se han planteado todos estos interrogantes y han intentado dar respuesta, ya sea ilustrando las políticas que desarrollan o bien formulando recomendaciones. El resultado de estos interrogantes y de esta búsqueda de soluciones se ha concretado en *la Carta para una Utilización Democrática de la Vigilancia por Vídeo,* un documento que prueba la decidida voluntad política de las ciudades en esta materia. Estas ciudades se comprometen a utilizar la vigilancia por vídeo de modo tal que respete los derechos fundamentales de los ciudadanos, a través de procesos de decisión que sean perfectamente transparentes y claros.

Para avanzar en este sentido, los primeros firmantes de la Carta, el alcalde de Rotterdam (Países Bajos), el Presidente del Foro Europeo y alcalde de Matosinhos (Portugal), al igual que el Presidente del Foro Francés y alcalde de Saint-Herblain (Francia) invitan a los demás alcaldes a sumarse a esta política franca y decidida.