99

Regulación jurídica de la videovigilancia

Julio Téllez Valdés

DERECHO CONSTITUCIONAL

Septiembre de 2007

15 pesos

CONTENIDO

INTRODUCCIÓN

En el año de 2003, tuve la oportunidad de que me publicaran en el libro *Derecho de Internet & Telecomunicaciones*, editado por la Facultad de Derecho Universidad de Los Andes en Colombia y publicado por Legis, una colaboración de 19 páginas intitulada *"Regulación Jurídica de la Videovigilancia"* , tema poco desarrollado a nivel mundial (prácticamente desconocido en América Latina) y a pesar de que en la medida de lo posible lo he seguido fomentando sobretodo a nivel de conferencias, me pareció conveniente escribir un libro sobre el particular.

En este documento, que espero resulte de interés, trataré de retomar algunos de los puntos en el artículo referido en el párrafo anterior, con la consecuente ampliación y actualización. Abordaré la temática bajo cuatro ejes fundamentales: el doctrinario, el legislativo, el jurisprudencial así como las fuentes de información consultables al respecto. Cabe destacar que por la misma novedad del tema, buena parte del contenido de esta investigación se sustentará en una serie de documentos extranjeros que me di a la labor de recopilar y que los he ubicado en el rubro de Anexos.

Admito que la elaboración de éste documento no fue una labor fácil, sobretodo considerando la complejidad del tema y la poca literatura en habla hispana al respecto, sin embargo, espero que lo aquí escrito pueda motivar a que personas e instituciones, se sientan atraídos por este tópico que como veremos en líneas posteriores, alcanza en ocasiones niveles de honda preocupación, más allá de los innegables beneficios que pueda conllevar el uso de la videovigilancia.

Este estudio lo enmarco dentro de la necesaria reglamentación legal de la llamada *Sociedad de la Información*, la cual tanto se soslaya a pesar de su indubitable importancia. Agradezco al Instituto de Investigaciones Jurídicas de la UNAM (México), al cual me honro en pertenecer, la oportunidad de dar a conocer este documento.

I. Origen y evolucion

Aunque se remonta a la década de los sesentas, el periodo de crecimiento de los circuitos cerrados de televisión (CCTV) data de finales de la década de los ochentas, por temor al terrorismo, la delincuencia y el vandalismo. Los sistemas de videovigilancia se están extendiendo cada vez más en la sociedad moderna. Es común ver estas cámaras (algunas solamente de utilería con dificultad de percibirlo a simple vista) instaladas en centros comerciales, bancos, estaciones de metro y de tren, aeropuertos y edificios del gobierno. El objetivo de estos sistemas es la monitorización de las acciones de las personas y los vehículos que están dentro de una zona de interés.

Sin embargo, en la mayoría de casos sólo se utilizan como sistemas de almacenamiento de imágenes que sirven como herramienta forense después de que el hecho haya ocurrido. Normalmente, es necesaria la presencia de un operador humano que monitorice todas las imágenes para poder actuar en tiempo real avisando a los oficiales de seguridad de que puede haber un acto anormal.

Es clara la necesidad de un sistema automático de monitorización ya que en muchas ocasiones no es posible controlar todas las cámaras del sistema de vídeo vigilancia porque no se dispone de suficientes recursos humanos. Además, un operador humano que esté observando un conjunto de cámaras de forma continua, es habitual que se aburra rápidamente y pierda la concentración.

II. Aspectos técnicos

Desde el punto de vista técnico, un sistema automático de videovigilancia incluye tareas de localización de objetos, seguimiento visual, clasificación de objetos y reconocimiento de actividades y acciones humanas. Estas tareas se pueden abordar utilizando técnicas de visión por computador, reconocimiento de patrones e inteligencia artificial. La localización implica la detección de los objetos en la escena de interés, que deben ser clasificados para conocer su tipo, por ejemplo, personas o coches. Una vez localizados, el módulo de seguimiento visual se encarga de mantener sus trayectorias a lo largo del tiempo. Finalmente, los módulos de reconocimiento de actividades y de acciones se encargan de realizar una descripción simbólica de lo que está ocurriendo en la escena.

La mayor dificultad de una aplicación de videovigilancia automática es la diversidad de escenarios y de condiciones que tienen los sistemas de adquisición utilizados. Podemos encontrar sistemas con una o varias cámaras, que pueden ser estáticas o móviles, y diferentes tipos de sensores, por ejemplo, cámaras en blanco y negro, color o infrarrojas.

III. Biometría

Casi todos los nuevos sistemas de identidad también usan algún tipo de dato “biométrico” o trazos corporales: las huellas dactilares, el escaneado del iris, la topografía facial y el escaneado de las manos se usan en diferentes pasaportes y sistemas de carné de identidad. Con frecuencia se nos presentan los datos biométricos como métodos infalibles. La idea es que la precisión se in-

crementará y se reducirá el fraude. Es posible olvidar o perder números de identificación personal (NIP) o contraseñas, pero el cuerpo humano proporciona un vínculo constante y directo entre un registro y la persona. Desde los atentados del 11 de septiembre se han fomentado especialmente en los EE.UU., y este país ejerce presión para la adopción de estándares comunes en los pasaportes biométricos.

Los sistemas de acceso biométricos (mediante el uso de voz y el escaneado de la mano, en particular) ahora son habituales para entrar en numerosos edificios de oficinas o propiedades de empresas privadas así como en algunos aeropuertos .La identificación del rostro y otros sistemas de circuito cerrado de televisión biométricos todavía no funcionan correctamente en exteriores o en calles atestadas de gente que camina rápidamente. No obstante, se está realizando una inversión considerable para su mejora.

IV. Localización, seguimiento y control electrónico

La vigilancia consiste cada vez más en hacer un seguimiento de las personas, mediante GIS (Sistemas de Información Geográfica), GPS (Sistemas de Posicionamiento Global, chips RFID (identificación por radiofrecuencia), y tarjetas inteligentes de identificación, transpondedores o señales de radio emitidas por teléfonos móviles u ordenadores portátiles.

Tanto el GPS como la RFID se consideran cada vez más como soluciones para la aplicación de la ley y la gestión del personal. El seguimiento electrónico también se ha introducido como una condición para otorgar la libertad condicional y se colocaron dispositivos electrónicos de seguimiento que les permitía vivir en sus domicilios a la espera de sus juicios, en vez de permanecer en prisión preventiva. También se somete a los delincuentes que salen de prisión a un seguimiento electrónico como una condición de su puesta en libertad condicional. Estos sistemas ya se comenzaron a utilizar en México y son conocidos como “brazaletes electrónicos.

V. El caso específico de la RFID

La llamada RFID (RADIO FREQUENCY IDENTIFICATION) o IDENTIFICACIÓN POR RADIOFRECUENCIA en español, es un método de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas o tags RFID. Una etiqueta RFID es un dispositivo pequeño, como una calcomanía, que puede ser adherida o incorporada a un producto, animal o persona. Las etiquetas RFID contienen antenas para permitir recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Las etiquetas RFID de baja frecuencia se utilizan comúnmente para la identificación de animales, como llave de automóviles con sistema antirrobo, etc. En los Estados Unidos se utilizan dos frecuencias para RFID: 125 kHz (el estándar original) y 134,5 kHz (el estándar internacional). Las etiquetas RFID de alta frecuencia se utilizan en bibliotecas y seguimiento de libros, seguimiento de productos, control de acceso en edificios, seguimiento de equipaje en aerolíneas, seguimiento de artículos de ropa y últimamente en pacientes de centros hospitalarios para hacer un seguimiento de su historia clínica. Sólo es necesario acercar estas insignias a un lector para autenticar al portador.

No hay ninguna corporación pública global que regule las frecuencias usadas para RFID. En principio, cada país puede fijar sus propias reglas. La organización EPC Global surgida en 2003 inicio una campaña de estandarización mundial de la identificación por radio frecuencia.

Las principales corporaciones que actualmente regulan la asignación de las frecuencias para RFID son:

- EE.UU.: FCC (Comisión Federal de Comunicaciones)
- Canadá: DOC (Departamento de la Comunicación)
- Europa: ERO, CEPT, ETSI y administraciones nacionales.
- Japón: MPHPT (Ministerio de Administración Pública, Gobernación, Correos y Telecomunicaciones)
- China: Ministerio de la Industria de Información
- Australia: Autoridad Australiana de la Comunicación
- Nueva Zelanda: Ministerio de Desarrollo Económico

Las etiquetas RFID de baja frecuencia (LF: 125 - 134 kHz y 140 - 148.5 kHz) y de alta frecuencia (HF: 13.56 MHz) se pueden utilizar de forma global sin necesidad de licencia. La ultra alta frecuencia (UHF: 868 - 928 MHz) no puede ser empleada en forma general, ya que no hay un estándar de uso. En Norteamérica, la frecuencia ultraelevada se puede utilizar sin licencia para frecuencias entre 908 - 928 MHz, pero hay restricciones en la energía de transmisión. En Europa la ultra alta frecuencia está analizándose para un eventual uso entre los 865.6 - 867.6 MHz. Su uso es sin licencia sólo para el rango de 869.40 - 869.65 MHz, pero existen restricciones en la energía de transmisión. El estándar UHF norteamericano (908-928 MHz) no es aceptado en Francia ya que interfiere con sus bandas militares. En China y Japón no hay regulación para el uso de la ultra alta frecuencia. Cada aplicación de UHF en estos países necesita de una licencia, que debe ser solicitada a las autoridades locales, y puede ser revocada. En Australia y Nueva Zelanda, el rango es de 918 - 926 MHz para uso sin licencia, pero hay restricciones en la energía de transmisión.

El uso de la tecnología RFID ha causado una gran polémica e incluso boicots de productos “etiquetados”. Las cuatro razones principales por las que RFID resulta preocupante en lo que a privacidad se refiere son:

- El comprador de un artículo desconoce la presencia de la etiqueta y es incapaz de eliminarla.
- La etiqueta puede ser leída a cierta distancia sin conocimiento por parte del individuo.
- Si un artículo etiquetado es pagado mediante tarjeta de crédito o conjuntamente con el uso de una tarjeta de cliente frecuente, entonces sería posible enlazar la ID única de ese artículo con la identidad del comprador.
- El sistema de etiquetas EPCGlobal crea, o pretende crear, números de serie globales únicos para todos los productos, aunque esto cree problemas de privacidad y sea totalmente innecesario en la mayoría de las aplicaciones.

La mayoría de las preocupaciones giran alrededor del hecho de que las etiquetas RFID puestas en los productos siguen siendo funcionales incluso después de que se hayan comprado los productos y se hayan llevado a casa, y esto puede utilizarse para vigilancia, y otros propósitos ajenos a las funciones de inventario en la cadena de suministro. Aunque la intención es emplear etiquetas RFID de corta distancia, éstas pueden ser "seguidas" a grandes distancias por cualquier persona con una antena de alto rango, permitiendo de forma potencial que el contenido de una casa pueda ser explorado desde una cierta distancia. Incluso un escaneado de rango corto es preocupante si todos los artículos detectados aparecen en una base de datos cada vez que una persona pasa un lector, o si se hace de forma malintencionada a través de *scaners* portátiles por ejemplo. Con números de serie RFID permanentes, un artículo proporciona información inesperada sobre una persona incluso después de su eliminación; por ejemplo, los artículos que se revenden, o se regalan, pueden permitir trazar la red social de una persona.

La primera aplicación en seres humanos a los que se ha implantado chips RFID ha sido en los EE.UU. en personas de edad avanzada que sufren enfermedades degenerativas. Los investigadores y entusiastas de la tecnología también se han aplicado autoimplantes desde hace varios años, y al menos una cadena de discotecas en España ofrece a sus clientes la oportunidad de que sus chips implantados les permitan evitar el manejo de dinero en efectivo y tener privilegios de acceso o incluso su uso para control de empleados en oficinas públicas o incluso en empresas. En la actualidad se está debatiendo seriamente la posibilidad de que todo mundo lleve un implante.

VI. Regulación jurídica de la RFID

El uso de la RFID ha suscitado un animado debate entre los juristas, y actualmente hay dos vertientes respecto a su necesaria regulación jurídica: por un lado tenemos quienes consideran que debe ser legislado bajo la perspectiva penal y mas específicamente contextualizarla bajo los Tratados o Convenios de Cibercriminalidad, dado su inevitable matiz internacional y por el otro lado tenemos quiénes consideran que debe ser reglamentado bajo los lineamientos de los ordenamientos legales en materia de protección de datos. Lo cierto es que es un tema de novísima actualidad y que requiere de un análisis más pormenorizado que desafortunadamente no tenemos la oportunidad de desarrollar ahora, pero que esperamos hacerlo en un futuro inmediato.

VII. Convergencia y vigilancia "omnipresente"

Cada vez más sistemas se diseñan con estos flujos de datos en mente. La interoperabilidad es inherente y existe una creciente convergencia de tecnologías de vigilancia. Esto significa que pueden surgir productos nuevos de forma totalmente imprevista y desordenada. Por ejemplo, en la actualidad existe una gran presión para encontrar carnés de identidad que resulten efectivos para diversas finalidades: cruce de fronteras, control de fraude, acceso a información gubernamental y tal vez comercial (alquiler de videos) así como también semicomercial (bibliotecas). Esto otorga un poder inmenso a los archivos cuya información es esencial en las oportunidades vitales de cada persona a aquellos que controlan las bases de datos de identidad.

Las tecnologías se encuentran en su punto álgido cuando se convierten en omnipresentes, se dan por sentadas y resultan mayoritariamente invisibles. Cada vez más, nos enfrentamos a diversos "puntos de tránsito" que debemos atravesar durante nuestra vida cotidiana, que implican tanto aspectos electrónicos como físicos estrechamente relacionados: una combinación de circuitos cerrados de televisión, datos biométricos, bases de datos y tecnologías de seguimiento. La vigilancia está cada vez más presente en todas partes y a todas horas: es omnipresente.

VIII. Dispositivos técnicos de protección

Es posible que se produzcan algunas respuestas tecnológicas a la vigilancia: algunas de las llamadas tecnologías para la mejora de la privacidad (en inglés, privacy-enhancing technologies, PET) podrían ayudar a frenar el crecimiento de la vigilancia tecnológica y se debería fomentar su uso cuando sea apropiado. No obstante, ni el mal funcionamiento de las mismas ni las PET deben significar que la respuesta es simplemente "mejores tecnologías". Cuanto mayor sea la dependencia por parte de Estados, organizaciones, individuos y sociedad en general de la tecnología de la vigilancia, más se producirá una "dependencia" que evitará la consideración de otras opciones para lograr los mismos objetivos así como un vacío de conocimiento que incrementará nuestra dependencia en competencias fuera del sistema democrático. Por ejemplo, con la introducción de los documentos de identidad, la dependencia de los mismos por parte del gobierno para que proporcionen tanto conocimientos tecnológicos como comerciales se incrementará inevitablemente

IX. Caracteristicas de la videovigilancia

Como lo menciono en mi artículo ya referido al inicio de esta obra, las entidades públicas y los particulares recurren con mayor frecuencia al uso de los sistemas de "captación de imágenes" para diversos fines. Si bien esta actividad es legítima si se realiza bajo determinadas condiciones, su uso inadecuado genera riesgos que pueden afectar derechos fundamentales. Hasta ahora ha sido poco el debate acerca de los límites que debe tener la videovigilancia con miras a proteger ciertos derechos y libertades en una sociedad democrática.

Durante los últimos años, los organismos públicos, los privados e incluso los particulares, han recurrido cada vez con más frecuencia a los sistemas de captación de imagen. Esta circunstancia ha suscitado un animado debate en el ámbito internacional, a fin de determinar los requisitos y los límites relativos a la instalación de equipos destinados a la vigilancia por videocámara, así como las garantías necesarias para los interesados.

La experiencia vivida en los últimos años ha puesto de manifiesto la gran proliferación de sistemas de circuito cerrado, cámaras y otras herramientas más sofisticadas que se utilizan en los sectores más variados.

Asimismo, el desarrollo de la tecnología disponible, la digitalización y la miniaturizacion aumentan de manera considerable las oportunidades que ofrecen los dispositivos de grabación de imagen y sonido, que también tiene que ver con su despliegue tanto en las intranets como en Internet.

Cada vez es más frecuente el uso de la videovigilancia, y su uso sigue siendo fuente de dudas y conflictos legales. La instalación de cámaras de vigilancia en calles y avenidas, establecimientos comerciales, centros de trabajo y casas y departamentos residenciales, es una práctica que no cuenta con una regulación clara en casi ningún país.

Para la policía, las empresas y algunos particulares es un sistema ideal. Permite controlar de forma inadvertida la actividad de los ciudadanos (conductores o transeúntes), clientes, trabajadores, visitas, etc. y averiguar si realiza o pretende cometer alguna conducta desleal o fraudulenta, y obrar en consecuencia.

Cabe mencionar que cada vez es más frecuente que las grabaciones a través de las videocámaras las realicen conjuntamente la policía y otras autoridades públicas o entidades privadas (bancos, asociaciones deportivas, empresas de transporte, etc.). A pesar de que el uso de estas tecnologías por parte de estos organismos reporta enormes beneficios, también da lugar a una cierta confusión respecto al papel y a las responsabilidades individuales sobre las tareas que estos realizan.

X. Seguridad pública y videovigilancia

El principal motivo que incita a los organismos públicos al emplazamiento de las videocámaras, es la preservación de la seguridad pública, es decir, que la sensación de inseguridad de los lugares frecuentados por los ciudadanos, los recursos económicos limitados por parte de las autoridades en el combate a la delincuencia y las medidas preventivas insuficientes tomadas para proteger los bienes y las personas, hacen “necesario” recurrir a la llamada videovigilancia y de esta manera, de manera enunciativa y no limitativa:

- proteger las personas contra la delincuencia;
- asegurar los espacios considerados propicios a las agresiones, a la violencia, a los intrusos o a las personas indeseables, especialmente los estacionamientos y lugares geográficamente criminógenos;
- ofrecer un espacio sano y seguro a los niños, jóvenes, mujeres y trabajadores;
- proteger los equipos e inmuebles;
- atenuar los costos asociados al vandalismo y el mantenimiento de las primas de seguro a un nivel aceptable;
- disuadir las intrusiones para disminuir el número de delitos;
- prevenir accidentes o en su caso atención rápida de las víctimas;
- prevenir suicidios, desafortunadamente cada vez más frecuentes, especialmente entre los jóvenes.

XI. Espacios públicos y privados

La frontera entre un espacio público y uno privado ha sido objeto de numerosos comentarios, pues el efecto de la vigilancia sobre los derechos fundamentales difiere entre ambos lugares. Es necesario circunscribir y y puntualizar la noción de "lugar público", en el contexto de la videovigilancia efectuado por organismos públicos.

Respecto, la videovigilancia de trabajadores, esto constituye un caso muy interesante respecto a si dichas personas al exterior de su lugar de trabajo y especialmente en los lugares públicos puede presentar un alcance a la vida privada.

Algunos de las variables que han sido examinadas para valorar el respeto de un alcance mínimo al derecho a la vida privada respecto al uso de estas tecnologías son:

- intervenir sólo en último recurso;
- no existir ninguno otro método alternativo;
- apoyarse en motivos precisos, graves y concordantes;
- referirse a una situación particular;
- una necesidad legítima e importante de asegurar el orden público.

El recurrir a la videovigilancia debe responder a una necesidad legítima e importante de asegurar el orden público y de cuidar la seguridad del Estado, de las personas y de los lugares, para evitar precisamente atentados en contra de la integridad física, bienes o derechos de las mismas y, preservar así la relación de confianza entre el ciudadano y el Estado.

XII. Clasificación de la videovigilancia

La videovigilancia se suele clasificar de la siguiente forma:

a) videovigilancia en espacios públicos;

b) videovigilancia en lugares privados, domiciliarios y no domiciliarios (un garage, un almacén, etc.), y

c) videovigilancia en espacios intermedios (comercios y demás lugares privados abiertos al público).

Según los tipos de espacios, se distinguen tres clases de captación videográfica/microfónica:

a) cámaras o micrófonos instalados en la vía pública y demás espacios de esta naturaleza;

b) cámaras o micrófonos en lugares privados, domiciliarios o no domiciliarios, y

c) cámaras o micrófonos en espacios intermedios, esto es, espacios privados que por decisión de su titular se encuentran abiertos al público (ej., un establecimiento comercial).

XIII. Algunos ejemplos de videovigilancia

Un análisis enunciativo de las principales aplicaciones, muestra que la vigilancia por videocámara puede servir para fines muy diversos, que, sin embargo, pueden agruparse en algunos de los siguientes casos:

a) En el interior o en las proximidades de edificios públicos o abiertos al público como museos, lugares de culto o monumentos, a fin de evitar delitos o actos vandálicos de importancia menor;

Cabe mencionar en este caso, que si bien la vigilancia por videocámara parece estar en cierto modo justificada en determinadas circunstancias, también se dan casos en los que se recurre a la protección mediante videocámaras de manera impulsiva, sin considerar adecuadamente los requisitos y las medidas pertinentes. A veces, esto es debido a las ventajas económicas que conceden, en su mayoría, los organismos públicos, así como a las propuestas de mejores condiciones en materia de seguros, derivadas de la utilización de equipos de vigilancia por videocámara;

b) En el interior de estadios y otras instalaciones deportivas, en particular cuando se celebran determinados acontecimientos;

c) En el sector del transporte y en relación con el tráfico vehicular, con vistas a controlar el tránsito en carreteras y autopistas, a fin de detectar los excesos de velocidad o las violaciones del código de circulación en los centros urbanos, así como para controlar los subterráneos que dan acceso a las líneas del metro, vigilar las gasolineras y el interior de los taxis;

d) A fin de evitar o detectar conductas ilícitas en los alrededores de las escuelas y en relación con los casos de menores;

e) En el interior de los hospitales, durante una operación o con vistas, por ejemplo a realizar cuidados a distancia o vigilar a los pacientes que se encuentran en unidades de cuidados intensivos o en áreas destinadas a pacientes gravemente enfermos o en cuarentena;

f) En aeropuertos, a bordo de barcos o cerca de las fronteras, para controlar el tránsito ilegal de extranjeros o para facilitar la búsqueda de menores u otras personas desaparecidas;

g) Por parte de detectives privados;

h) En el interior y en las proximidades de supermercados y tiendas, en particular cuando venden artículos de lujo, con vistas a disponer de pruebas en caso de que se cometan delitos, así como para la comercialización de la mercancía o el establecimiento del perfil de los consumidores;

i) En colonias y casas particulares, tanto por motivos de seguridad como para disponer de pruebas en caso de que se cometan delitos;

j) Con propósitos periodísticos y publicitarios, que se prolongan en línea mediante cámaras web o cámaras virtuales que se utilizan con fines promocionales y publicitarios para el turismo, así como en relación con complejos turísticos, bares y discotecas, en los que se graba a los clientes y visitantes a intervalos regulares, sin advertirles.

XIV. Necesidad de regulación

Es necesario reglamentar la videovigilancia para mantener sus efectos negativos bajo control y hacerla compatible con el tipo de sociedad y democracia que deseamos. El exigir la realización de evaluaciones acerca del impacto de nuevos proyectos sobre la privacidad y la vigilancia contribuiría a la conciencia pública y al debate, y añadiría una dimensión importante a los sistemas legales aplicables. Existen muchas leyes y códigos de conducta para la protección de la privacidad (desafortunadamente México no se puede preciar mucho de ello). También existen tecnologías que proporcionan cierta protección. Existen agencias reguladoras dedicadas que aplican la ley, que ayudan con las quejas de las personas y tratan de influir sobre las políticas gubernamentales y los avances empresariales. Existen los grupos de presión y los medios de comunicación que nos alertan de los peligros de la vigilancia. Pero el poder y la eficacia de esos mecanismos reglamentarios es cuestionable; necesitan ser reconsiderados y mejorados. En cualquier caso, mientras que la protección de la privacidad es parte de la historia, no supone la historia completa. La mayoría de las personas deben comprender el significado de la videovigilancia y participar en decidir qué se debe hacer al respecto. Pero no es suficiente con que su reglamentación se realice únicamente en un país o incluso en un grupo de países como es el caso de la Unión Europea. Los flujos de información que forman parte de la videovigilancia son ciertamente globales; como también lo son los movimientos y actividades que se mantienen bajo vigilancia. Existe la necesidad de una reglamentación más integrada y más global para enfrentarse a esos desafíos.

Es necesario una política pública de seguridad de la información con un marco de gestión asociada a la videovigilancia, a manera de ejemplo, tenemos aquella inspirada en el régimen francés, dirigida a organismos públicos y a empresas privadas, para autorizar previamente la instalación de cámaras de vigilancia, especialmente en el rubro de:

- protección de los equipos y de los inmuebles públicos;
- salvaguarda de las instalaciones estratégicas en materia de seguridad del Estado y la defensa nacional;
- prevención sobre la seguridad de los bienes y de las personas en los lugares con riesgo de acciones delictivas;
- regulación del tráfico de carreteras.

XV. Aspectos legales

El campo de estudio legal sobre el tema de por si limitado, generalmente se circunscribe sólo a la utilización de la videovigilancia por los organismos públicos en los lugares públicos. Desafortunadamente, el análisis jurídico respecto al uso de la videovigilancia en las empresas particulares, ambientes laborales, de salud y carcelario está normalmente excluido y por tanto propiciando un mayor vacío legal.

El constitucionalista español Ricardo Martín Morales, nos señala que la vigilancia por medio de cámaras y/o de micrófonos tiene como finalidad la prevención de conductas ilícitas o en su caso la prevención de riesgos. Cuando se utiliza una videocámara, no para prevenir, sino para investigar a posteriori y obtener pruebas relacionadas con delitos ya cometidos o recabar

información sobre cuestiones específicas de carácter laboral, matrimonial, etc., no cabe hablar, en sentido estricto, de videovigilancia, sino simplemente de evidencias o pruebas videográficas. Es verdad que la distinción no siempre resulta fácil, porque es tras la comisión de un delito cuando a veces se toma la decisión de establecer un sistema de videovigilancia, no tanto para obtener pruebas y procurar su esclarecimiento, cuanto para prevenir que se cometa otro en el futuro, aunque al final terminen obteniéndose esas fuentes de prueba.

Debe desarrollarse un marco legislativo que responda eficazmente a la amenaza para la vida privada que eventualmente puede constituir la videovigilancia, colmando los vacíos legales y cerrando la puerta a los abusos. La adopción de directrices es insuficiente. La videovigilancia necesita un marco jurídico que acote el uso de la videovigilancia.

Las normas legislativas deben comprender consignas claras en cuanto al estatuto de las personas quienes tendrán acceso a la información, incluyendo lo referente a la reproducción de la información, con las precisiones en cuanto al lugar y plazo de conservación y el nombramiento de personas responsables de la aplicación de la Ley (en España, como veremos posteriormente existen Comisiones de Videovigilancia para estar atentos a la debida aplicación de las leyes en la materia).

Es igualmente necesario incluir en la legislación, disposiciones mediante las cuales se aclare que el uso de las videocámaras y/o micrófonos no puede servir a otros fines más que los específicamente autorizados.

XVI. Protección de los datos personales

Las imágenes y la voz de una persona, registradas en el marco de actividades de la videovigilancia, son consideradas como informaciones a carácter personal en cuanto que son un medio de identificación de las personas.

La legitimidad del registro de datos personales para un objeto determinado no significa por mucho que puedan ser utilizadas para otros fines. El carácter confidencial de las informaciones nominativas constituye por tanto un un aspecto muy importante a considerar dentro en el empleo de las videocámaras. De aquí que sea menester un adecuado equilibrio entre el derecho de utilizar las cámaras de vigilancia y el respeto de la vida privada mediante la adopción y aplicación de normas adecuadas.

Por otro lado, la protección de la vida privada tiene como principal marco de referencia a las personas en sí mismas y no tanto los lugares donde se encuentran. Una persona que va de compras a un centro comercial no goza habitualmente de la misma intimidad que en su casa. Las nociones de interés particular y de interés público son pues indisociables, el ser humano es ante todo un ser social y la noción de vida privada no reviste ningún sentido si el individuo no puede encontrar la paz en sociedad. Así, los intereses colectivos deben ser tomados igualmente en cuenta respecto al uso de las cámaras de vigilancia.

XVII. INFORME EPIC

En su Informe Anual (2005) sobre Privacidad y Derechos Humanos, el *Electronic Privacy Information Center*, conocido más comúnmente bajo las siglas EPIC, nos menciona que muchas de la actividades relacionadas con la privacidad y la vigilancia son el resultado de la necesidad de los gobiernos por incrementar la seguridad después de los eventos de carácter terrorista acaecidos en los últimos años en Asia, Europa, Estados Unidos y Oriente Medio. Muchos países del mundo han perseguido cambios reguladores y legislativos para dotar a sus gobiernos con la capacidad de incrementar la vigilancia sobre los ciudadanos. Algunas de estas medidas incluyen la incorporación de nuevos sistemas de identificación y la vigilancia de las comunicaciones. Al mismo tiempo que se potencian estos sistemas técnicos, diferentes agentes trabajan sin descanso para debilitar las políticas de protección de datos. A esta intensificación en la obtención de información tanto de fuentes privadas como públicas se une la mayor dispersión de dicha información en un conjunto más amplio de agencias del orden público.

De manera global, la mayoría de los gobiernos ha seguido trabajando en políticas que legitiman el uso de la vigilancia masiva para combatir el terrorismo. Una de las mayores tendencias ha sido la puesta en funcionamiento de medidas que garantizan la identificación de individuos en tránsito entre países. Muchos países han seguido la pauta marcada por Estados Unidos incorporando información biométrica en diferentes distintos documentos oficiales y empleando sistemas más avanzados para estudiar los perfiles de los viajantes. Como resultado, nuevas tecnologías como el escáner de iris, el reconocimiento facial, las etiquetas de radiofrecuencia o el reconocimiento digital de huellas dactilares están (o están en vía de ser) implementados. Estos sistemas, que inicialmente estaban diseñados para mantener la información de los extranjeros viviendo en un país, han sido progresivamente extendidos para controlar y vigilar a otros grupos sociales.

Los gobiernos no sólo se han limitado a la puesta en marcha de medidas tradicionales de vigilancia para responder directamente contra el terrorismo. A la vigilancia tradicional se han incluido nuevos aliados tecnológicos como el uso de tecnología biométrica, tarjetas inteligentes, y la explotación de los datos de todo tipo de bases de datos, incluidas las de información media. Al amparo de garantizar la seguridad pública, se han financiado sistemas de videovigilancia aún más avanzados en lugares públicos, redes de transporte y aduanas.

Es más común que en años anteriores la implementación gubernamental de tarjetas inteligentes o “smart cards” en un amplio abanico de aplicaciones y documentos oficiales incluyendo: pasaportes, licencias para conducir o la identificación electrónica en sistemas de régimen fiscal, bancario o de salud. Muchos de estos nuevos documentos contienen información de carácter biométrico que permiten su uso con nuevos servicios gubernamentales en la red. Es importante mencionar que en la mayoría de los casos estos sistemas se han implementado inicialmente en grupos reducidos de población, como refugiados o inmigrantes ilegales, pero existen planes para su puesta en marcha con toda la ciudadanía. Muchas de las críticas a estos sistemas es la falta de protecciones legislativas en muchos países y los riegos potenciales a nuevos tipos de robo de identidad.

Es notable el crecimiento en el uso de ADN y las bases de datos con información médica. No sólo ha crecido su uso sino también su finalidad: se tratan más tipos de delitos con un grupo más amplio de individuos y con la ampliación de la retención de dichos datos. Las bases de datos también se han empleado con una finalidad diferente a su diseño inicial. Su propósito inicial se

ha extendido a su uso para seguridad nacional, investigación médica o el seguimiento de gastos en el área de la salud. Es preocupante la falta de simples mecanismos para controlar como son realizados los test genéticos y como se emplean después los resultados. Son comunes las críticas que cuestionan su legalidad y constitucionalidad y la poca o ninguna información pública al respecto.

Algunos de los países estudiados han implementado medidas drásticas de censura como mecanismo de control de la población, desde la intercepción del correo electrónico o las búsquedas de los usuarios en Internet hasta los SMSs, el teléfono o el fax. Estas medidas se han implementado no sólo ha nivel individual y privado pero también en accesos públicos como cibercafés.

Estas amenazas no solo están presentes en el sector público, sino que compañías privadas practican la vigilancia incorporando tecnologías como cámaras de vigilancia y las etiquetas de radio frecuencia o RFIDs. Las RFID que inicialmente se usaban en el seguimiento de productos y en el control de almacenes ahora se usan en servicios públicos como librerías o incorporadas a nuevos sistema de pago. Es común encontrar empresas promoviendo esta tecnología y su capacidad de seguir a las personas, como prisioneros u otros grupos minoritarios e incluso como mecanismo de seguimiento del personal en las empresas y en zonas de alta seguridad.

Aunque las etiquetas de radiofrecuencia pueden dar lugar a grandes avances en ciertos campos de aplicación, los riesgos son mucho mayores cuando la tecnología se introduce para controlar a los consumidores, y a las organizaciones civiles y políticas.

Conscientes de su peligro, legisladores y agencias de protección de datos están abordando sus implicaciones en la privacidad. En este campo destacan las numerosas campañas de sensibilización promovidas por organizaciones defensoras de la privacidad.

Aunque el crecimiento de videovigilancia es progresivo, muy pocos países han reaccionado adecuadamente con medidas legales para evitar los abusos que trae aparejado.

XVIII. Informe sobre la sociedad de la vigilancia de septiembre de 2006

En junio de 2006, el Comisario de Información del Reino Unido encargó a la Red de Estudios sobre la Vigilancia (Surveillance Studies Network) la elaboración de un INFORME SOBRE LA SOCIEDAD DE LA VIGILANCIA, mismo que se presentó en septiembre de 2006 y que consta de tres secciones: en la primera, se presentan los componentes básicos de la sociedad de la vigilancia: sus definiciones, temas y repercusiones, en la segunda, se muestra cómo funciona la sociedad de la vigilancia y en la tercera, se examinan algunos de los retos que plantea la sociedad de la vigilancia en el ámbito normativo. Por la importancia que consideramos puede representar para nuestro amable lector, me permito presentar el Resumen Ejecutivo de dicho Informe en los Anexos de esta obra.

XIX. Instrumentos jurídicos internacionales

a) Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales

El artículo 8o del Convenio garantiza la protección del derecho a la intimidad.

b) Convenio N° 108/1981 del Consejo de Europa relativo a la protección de las personas físicas en lo que respecta al tratamiento automático de datos personales

El ámbito de aplicación de este Convenio no se limita, como la Directiva 95/40/CE, a las actividades del primer pilar. Las actividades de vigilancia por videocámara que implican el tratamiento de datos personales entran en el ámbito de aplicación de este Convenio. El comité consultivo creado en virtud de este Convenio ha establecido que las voces y la imagen se considerarán datos personales cuando aporten información sobre una persona y la hagan identificable, incluso indirectamente.

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

XX. SITUACION LEGISLATIVA INTERNACIONAL

En varios paises, la videovigilancia no ha sido objeto de legislación específica en la actualidad, sin embargo, las autoridades de protección de datos, fundamentalmente de los paises europeos, han estado trabajando para garantizar la aplicación adecuada de las disposiciones generales sobre la materia, en particular a través de dictámenes, directrices o códigos de conducta. A continuación presentaremos una breve relación de aquellos países que disponen de alguna disposición normativa en materia de videovigilancia, no sin antes comentar que actualmente en la Unión Europea tenemos dos bloques de países que han abordado de manera distinta esta problemática, por un lado tenemos a Francia, Suecia e incluso en España en donde existen disposiciones específicas que regulan el uso de la videovigilancia, independientemente de que pueda implicar el tratamiento de datos personales. Y por el otro lado tenemos a aquellos países en donde la instalación y el despliegue de circuitos cerrados de televisión y equipos de vigilancia son autorizados previamente por una autoridad administrativa que puede estar representada parcial o totalmente por la autoridad nacional de protección de datos y que por tanto, no consideran necesario a una legislación específica al respecto, tal es el caso de Gran Bretaña, Italia, Bélgica, Luxemburgo y Alemania, en donde las autoridades de protección de datos garantizan la aplicación adecuada de las disposiciones generales de protección de datos a través de dictámenes, directivas o códigos de conducta. Aquí una relación sucinta:

1. *Alemania*

- Letra b de la sección 6 de la Ley Federal de Datos de 2001 que reglamenta el uso de la videovigilancia por parte de entidades privadas y autoridades federales como la policía y los servicios de inteligencia.

- Disposiciones varias en la materia a nivel de los 16 estados o bunder sobre el uso de la videovigilancia en las entidades privadas y autoridades federales como la policía y los servicios de inteligencia
- Secciones 26 y 27 de la Ley Federal de la Policía Fronteriza

2. *Bélgica*

- Dictámenes de la autoridad de protección de datos, en concreto, el Dictamen 34/99, de 13 de diciembre de 1999, relativo al tratamiento de imágenes, en particular a través de la utilización de sistemas de vigilancia par videocámara;
- Dictamen 3/2000, de Io de enero de 2000, relativo a la utilización de sistemas de vigilancia por videocámara en la entrada de los edificios de departamentos.

3. *Dinamarca*

- Texto refundido de la Ley N° 76, de primero de febrero de 2000, relativa a la prohibición de la vigilancia por videocámara y que prohibe el monitoreo de calles públicas, caminos, plazas públicas y otros lugares, sin embargo existen algunas excepciones.
- Resolución de la autoridad de protección de datos, de 3 de junio de 2002, relativa a la vigilancia por videocámara por parte de un gran grupo de supermercados y transmisión en directo desde un *pub* a través de Internet.
- Resolución de la autoridad de protección de datos de primero de julio de 2003 relativa al uso de la videovigilancia en los transportes públicos, todo esto en concordancia con la ley danesa de protección de datos
- Resolución de la autoridad de protección de datos de 13 de noviembre, que restringe el uso de la videovigilancia por parte de autoridades públicas

4. *Francia*

- Ley 78-17, de 6 de enero de 1978, relativa a la informática, los archivos y las libertades (Comisión nacional francesa de informática y libertades, CNIL).
- Recomendación 94-056 de la autoridad protección de datos, de 21 de junio de 1994.
- Ley específica relativa a la vigilancia por videocámara para la seguridad pública en zonas públicas: Ley 95-73, de 21 de enero de 1995, sobre seguridad (modificada por la Orden 2000-910, de 19 de septiembre de 2000).
- Decreto 96-920, de 17 de octubre de 1990 y Circular, de 22 de octubre de 1996, sobre la aplicación de la Ley 95-73.

5. *Grecia*

- Resolución de la autoridad de protección de datos de 28 de enero de 2000 sobre el metro de Atenas.

6. *Holanda*

- Informe de la autoridad de protección de datos publicado en 1997, que contiene las directrices para la vigilancia por videocámara, en particular para la protección de las personas físicas y la propiedad en lugares públicos.

Recientemente, la Cámara Baja aprobó un proyecto de Ley por el que se ampliará el alcance del delito de grabar imágenes de lugares abiertos al público sin informar al mismo.

En breve se transmitirá al Parlamento un proyecto de Ley por el que se atribuirán competencias explícitas a los ayuntamientos para utilizar sistemas de vigilancia por videocámara en determinadas condiciones.

7. *Hungria*

- Recomendación de 20 de diciembre de 2000 de la autoridad de protección de datos en materia de aplicación de la ley en la materia.

8. *Irlanda*

- Estudio de casos N° 14/1996 (utilización de circuitos cerrados de televisión)

9. *Islandia*

- Sección 4 de la Ley N° 77/2000

10. *Italia*

- Sección 20 del Decreto legislativo N° 407, de 28 de diciembre de 2001 (relativa a la adopción de códigos de conducta).
- Resoluciones de la autoridad italiana de protección de datos: N° 2, de 1º. de abril de 2002 (relativa al fomento de la adopción de códigos de conducta de 28 de septiembre de 2001 (relativa a las técnicas biométricas y de reconocimiento fisonómico aplicadas por los bancos) y de 29 de noviembre de 2000 (el llamado "decálogo de la vigilancia por videocámara").
- Decreto presidencial N° 250, de 22 de junio de 1999 (por el que se regula el acceso de vehículos a los centros urbanos y a las zonas de acceso restringido).

- Decreto N° 433, de 14 de noviembre de 1992, y Ley N° 4/1993 (relativa a museos, bibliotecas públicas y archivos).
- Decreto legislativo N° 45, de 4 de febrero de 2000 (barcos de pasajeros en rutas nacionales).
- Sección 4 de la Ley N° 300, de 2o de mayo de 1970 (el llamado Estatuto de los trabajadores).

11. *Luxemburgo*

- Artículos I0 y 11 de la Ley de 2 de agosto de 2002, relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales.

12. *Noruega*

- Capítulo VII de la Ley de Protección de Datos del 14 de Abril de 2000.

13. *Nueva Zelanda*

- Directiva referente a las cámaras de vigilancia de circuito cerrado en los lugares públicos derivada de la Ley sobre la protección de las informaciones personales.

Las principales características de esta Directiva son:

— se aplica a las cámaras de circuito cerrado instaladas para un período largo en los lugares públicos con miras a prevenir la delincuencia;

— una consulta pública es necesaria antes de tomar la decisión de instalar las videocámaras de vigilancia. Los sitios de instalación deben ser elegidos en acuerdo con las autoridades y los sectores involucrados. Son restringidos a los lugares públicos identificados con alto índice de criminalidad;

— el período de operación es limitado a las horas reconocidas como especialmente peligrosas;

— hay revisión de las operaciones cada seis meses para asegurarse de la necesidad de la videovigilancia y de la elección de los sitios.

14. *Portugal*

- Decreto ley N° 231/98, de 22 de julio de 1998 (relativo a la actividad privada en materia de seguridad y a los sistemas de autoprotección).
- Ley N° 38/98, de 4 de agosto de 1998 (relativa a las medidas que deberán adoptarse en caso de violencia relacionada con eventos deportivos).
- Decreto Ley N° 203/01, de 28 de septiembre de 2001 (relativo a las discotecas).

- Decreto ley N° 94/2002, de 12 de abril de 2002 (eventos deportivos).

15. *Reino Unido*

- Código Profesional 2000 sobre circuitos cerrados de televisión (Delegado de Información) con matizaciones de la Data Protection Act de 1998 y específicamente de la sección 51 (3) (b)
- Sección 163 de la Ley de Justicia Criminal y Orden Público de 1994 que regula los poderes de las autoridades locales en materia de videovigilancia.

Es importante mencionar que en la actualidad es probable que el número de videocámaras en la Gran Bretaña se aproxime a las 4.2 millones, una por cada 14 personas y que por tanto, un mismo individuo puede ser grabado por más de 300 cámaras al día. Se calcula que durante los últimos diez años, se han invertido unos 500 millones de libras esterlinas del erario público en la infraestructura de cámaras de CCTV, aunque un estudio del Ministerio del Interior llegó a la conclusión de que "los programas de uso de CCTV que se han evaluado han tenido un resultado general limitado respecto los niveles de delincuencia".

La lista de lugares monitoreada por CCTV es interminable. Los centros urbanos de la mayor parte de Gran Bretaña están bajo la vigilancia, así como autopistas, hospitales, escuelas, bancos, museos, centros comerciales, instalaciones deportivas, autobuses urbanos, metro, estaciones del ferrocarril y aeropuertos por mencionar sólo algunos lugares. Las cámaras de CCTV son operadas por la policía, los servicios de seguridad agencias gubernamentales nacionales y locales así como instituciones y sociedades privadas.

Por otro lado, no sólo Gran Bretaña es el líder del mundo en videovigilar a sus ciudadanos (quiénes por cierto son los que menos renuencia tienen a este respecto a nivel mundial quizás por los riesgos de terrorismo más que la delincuencia en sí misma), ya que la base de datos de ADN iniciada en 1995, proyecta tener 3.7 millones de registros para abril 2007, convirtiéndose en la base de datos de ADN más grande del mundo.

16. *Suecia*

- Ley 1998/150 sobre vigilancia general por videocámaras
- Ley 1995/1500 sobre vigilancia secreta por videocámara (en investigación de delitos).

En este país, aunque la vigilancia general por videocámara requiere, en principio, autorización de la junta administrativa municipal, existen varias excepciones, por ejemplo, en lo relativo a la vigilancia de oficinas de correos, bancos y tiendas. La vigilancia secreta por videocámara debe contar con la autorización de un tribunal. A fin de preservar intereses públicos, el Ministro de Justicia puede apelar una sentencia de la junta administrativa municipal dictada de conformidad con la Ley sobre vigilancia general por videocámara. Se considera que la grabación de imágenes utilizando cámaras digitales constituye tratamiento de datos personales en el sentido contemplado en la ley sueca sobre datos personales y, en consecuencia, entra en el marco de la supervisión por parte de la autoridad de protección de datos. En la actualidad, un comité de investigación está analizando la utilización de vigilancia por videocámara desde una perspectiva de

prevención criminal. Entre otras cosas, dicho comité evaluará la Ley sobre vigilancia general por videocámara a fin de verificar si es necesario introducir modificaciones. Así mismo, el comité de investigación analizará el ámbito de aplicación de la ley sueca de datos personales en lo que respecta a la vigilancia por videocámara y la posible necesidad de establecer normas específicas relativas al tratamiento de datos personales en relación con la vigilancia por videocámara.

17. Suiza

- Recomendación del Delegado Federal

XXI. El caso particular de España

Debido a la cercanía especial que tenemos la mayoría de los latinoamericanos con este entrañable país, he decidido dedicarle un espacio especial al estudio de la regulación jurídica de la videovigilancia.

Los principales ordenamientos aplicables sobre el tema en este país son los siguientes (a mayor abundamiento el texto completo de muchos de estos documentos pueden encontrarse en la sección de Anexos de esta obra) :

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter PersonaL *(BOE núm. 298 de 14 de diciembre de 1999)*
- Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana *(BOE núm. 46 de 26 de febrero de 1992)*
- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos (BOE núm. 186 de 5 de agosto de 1997)
- Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado (BOE núm.63 de 14 de marzo de 1986)
- Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la Intimidad Personal y a la propia imagen *(BOE núm 115 de 14 de mayo de 1982)*
- Real Decreto 596/1999, de 16 de abril, por el que se aprueba el Reglamento de desarrollo y ejecución de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos (BOE núm. 93 de 19 de abril de 1999)
- Real Decreto 1247/1998, de 19 de junio, por el que se modifica el Real Decreto 769/1993, de 21 de mayo, por el que aprueba el reglamento para la prevención de la violencia en los espectáculos deportivos (BOE núm. 152 de 26 de junio de 1998)
- Real Decreto 769/1993, de 21 de mayo, por el que se aprueba el Reglamento para la prevención de la violencia en los espectáculos deportivos (BOE núm. 146 de 19 de junio de 1993)

- Decreto 134/1999, de 18 de mayo, de regulación de la videovigilancia por parte de la policía de la Generalidad y de las policías locales *(Diario Oficial de la Generalitat de Catalunya núm. 2892, de 19 de mayo; corrección de errores en el Diario Oficial de la Generalitat de Catalunya núm. 2988, de 5 de octubre de 1999)*
- Decreto 168/1998, de 21 de julio, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la policía del País Vasco en lugares públicos regulado en la Ley orgánica 4/1997, de 4 de agosto *(Boletín Oficial del País Vasco núm. 142 de 29 de julio de 1998)*
- Orden de 2 de mayo de 2006, del Consejero de Interior, por la que se publica la modificación de la composición de la comisión de videovigilancia y libertades creada por el decreto 168/1998, de 21 de julio, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la policía del País Vasco en lugares públicos *(Boletín Oficial del País Vasco nº 96 de 23 de mayo de 2006)*
- Corrección de errores de la Orden de 10 de febrero de 2006, del Consejero de Interior, por la que se modifica y publica la composición de la Comisión de Videovigilancia y Libertades creada por el Decreto 168/1998, de 21 de julio, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la policía del País Vasco en lugares públicos *(B.O.P.V. num 54 de 17 de marzo de 2006)*
- Orden de 10 de febrero de 2006, del Consejero de Interior, por la que se modifica y publica la composición de la Comisión de Videovigilancia y Libertades creada por el Decreto 168/1998, de 21 de julio, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la policía del País Vasco en lugares públicos (B.O.P.V. *num. 47 de 8 de marzo de 2006)*
- Orden de 22 de diciembre de 1998 por la que se regulan las unidades de control organizativo para la prevención de la violencia en los espectáculos deportivos *(BOE núm. 309 de 26 de diciembre de 1998)*
- Orden de 9 de noviembre de 1998, del Consejero de Interior, por la que se hace publica la constitución de la Comisión de Videovigilancia y Libertades creada por el Decreto 168/1998, de 21 de julio, por el que se desarrolla el régimen de autorización y utilización de videocámaras por la Policía del País Vasco en lugares públicos (*Boletín Oficial del País Vasco núm. 231 de 3 de diciembre de 1998)*
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras *(BOE núm. 296 de 12 de diciembre de 2006)*

A manera ejemplificativa podemos decir que en España y específicamente en Madrid, el Metro dispone hoy en día de 3,447 cámaras de vigilancia que se encargan de controlar 192 estaciones (sólo se graban imágenes en 87), 278 vestíbulos, 1 223 escaleras mecánicas y 253 ascensores de que consta la red. Para mediados de 2007 se pretende que el número de videocámaras se incremente a las 4,500. Hasta ahora, el 45% de las imágenes que captan esas videocámaras son enviadas en tiempo real al centro de seguridad que el Metro tiene en la estación Alto del Arenal. Por otro lado solo en la nueva terminal (la 4) del aeropuerto de Barajas hay 4,500 cámaras. Al igual que Inglaterra, el uso de estos sistemas no es tanto para prevenir la delincuencia genérica

sino el terrorismo tanto interno como externo como los lamentables sucesos del 11 de marzo de 2004. Como hemos percibido, este país dispone de una amplia regulación referido al uso de estos sistemas de videovigilancia, además de algunas sentencias interesantes que pueden ser consultadas en los Anexos de este libro.

A nivel doctrinario tenemos algunas obras interesantes sobre el tema y que vienen referenciadas en el rubro de fuentes de información consultables, sin embargo, a mi modo particular queda destacar lo esgrimido por Imma Garrós y Fuente en su tesis doctoral en catalán intitulada *La videovigilacia y el control de las garantías constitucionales* (también referenciada), presentada en 2005, en donde aborda puntos relevantes sobre el régimen jurídico de la vigilancia, tales como el equilibrio entre seguridad y libertad (La vigilancia como instrumento de prevención del delito y como forma de control social, la ley orgánica 4/1997, de 4 de agosto de 1997 sobre la utilización de videocámaras, la regulación legislativa y desarrollo reglamentario , el respeto a los derechos fundamentales como límite a la intervención pública de las fuerzas y cuerpos de seguridad , la regulación de las videocámaras en el ámbito de la seguridad privada, la prueba videográfica en el proceso penal y administrativo: validez y límites, un estudio de Derecho Comparado, así como la aplicación práctica de la videovigilancia , señalando que el objetivo de dicho estudio consiste básicamente al hacer un análisis sobre un fenómeno emergente actualmente en nuestra sociedad cómo es la utilización de videocámaras. Concretamente, la videovigilancia y el control de las garantías constitucionales. Mencionando que la violencia en la calle y la progresiva inseguridad ciudadana ha llevado a las fuerzas policiales e incluso a muchos establecimientos públicos y privados a la necesidad de emplear medios de prevención y controles cada vez más sofisticados. A pesar de este interés, la utilización de estos medios tecnológicos tan adelantados de vigilancia a la calle ha causado perplejidad e impotencia por parte de la ciudadanía por la afectación tan directa que estos causan sobre los derechos fundamentales. Si bien a nivel teórico este problema parece haberse resuelto con la existencia de una serie de garantías legales desarrolladas en España, a nivel práctico existen conceptos jurídicos indeterminados y que producen vacíos legales que no dan respuesta a una serie de conflictos que se presentan.

A nivel normativo, cabe destacar la Instrucción 1/2006, de 8 de noviembre de 2006, de la Agencia Española de Protección de Datos (AEPD) publicada en el Boletín Oficial de España (BOE) el 12 de diciembre de 2006 y con fe de erratas publicadas en el BOE del 3 de enero de 2007, mediante la cual se regula el tratamiento de imágenes de personas físicas identificadas o identificables con fines de vigilancia, a través de sistemas de cámaras y videocámaras.

Dicha Instrucción, tiene como objetivo lograr una regulación concreta y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de sistemas de cámaras y videocámaras con fines de vigilancia, debido al incremento que últimamente están experimentando las instalaciones de estos dispositivos. Asimismo, se ha pretendido dar solución a algunas de las cuestiones que se han planteado en la AEPD en lo relativo al tratamiento de las imágenes tales como la forma de ejercitar los derechos de los ciudadanos, o la necesidad de cumplir con el deber de informar.

La Instrucción establece consignas varias en materia de grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con ellas. Por el contrario, se excluyen de la Instrucción los datos personales grabados para uso doméstico y el trata-

miento de imágenes por parte de las Fuerzas y Cuerpos de Seguridad, que está regulado por la Ley Orgánica 4/97, de 4 de agosto de 1997.

Entre los principales exigencias establecidas por la Instrucción para la captación y el tratamiento de imágenes mediante Videovigilancia destacan las siguientes:

— Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en la Ley Orgánica de Protección de Datos (LOPD). A tal fin deberán colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados.

Según se establece en la Instrucción el contenido y el diseño del distintivo informativo deberá de incluir una referencia a la "LEY ORGANICA 15/1999, DE PROTECCIÓN DE DATOS", incluirá una mención a la finalidad para la que se tratan los datos ("ZONA VIDEOVIGILADA"), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos de las personas en materia de Protección de Datos.

— Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

— Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida.

— Las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

— La creación de un fichero (archivo) de imágenes de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General.

La Instrucción adecua los tratamientos de datos personales con fines de videovigilancia a la LOPD. A manera de recapitulación, es importante señalar que la videovigilancia en España se encuentra también regulada en la Ley Orgánica 4/97 de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y la Ley 23/1992, de 30 de julio, de Seguridad Privada y en sus reglamentos de desarrollo aprobados por los Reales Decretos 596/1999, de 16 de abril 2364/1994, de 9 de diciembre, respectivamente.

XXII. Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la proteccion de las personas fisicas en lo que respecta al tratamiento de datos personales a la libre circulacion de estos datos respecto a la vigilancia por videocámaras y tratamiento de datos personales

El punto 16 de los considerandos de dicha Directiva señala que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están compren-

didos en el ámbito de aplicación de dicho documento, cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario, por lo que el artículo 29 instituyó la creación de un Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, a quien se les encomendo elaborar documentos de trabajo relativos al tratamiento de datos personales mediante vigilancia por videocámara.

A la luz de las diversas situaciones mencionadas, el Grupo considero necesario llamar la atención sobre el hecho de que la Directiva 95/46/CE es aplicable al tratamiento total o parcialmente automatizado de datos personales, incluidos los constituidos por imagen y sonido captados mediante circuito cerrado de televisión y otros sistemas de vigilancia por videocámara, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un archivo.

Los datos relativos a personas físicas identificadas o identificables, constituidos por imagen y sonido, son datos personales:

a) Incluso si las imágenes se utilizan en el marco de un sistema de circuito cerrado, y aunque no estén asociadas a los datos personales del interesado;

b) Incluso si no se refieren a personas cuyos rostros hayan sido filmados, aunque contengan otra información, como, por ejemplo, números de matrícula o números de identificación personal (NIP) captados durante la vigilancia de cajeros automáticos;

c) Independientemente del método utilizado para el tratamiento (por ejemplo, sistemas de video fijos o móviles, como receptores de imagen portátiles, o imágenes en color o en blanco y negro), la técnica (dispositivos de cable o fibra óptica), el tipo de equipo (fijo, móvil o portátil), las características de la captación de imágenes (es decir, continua, por oposición a discontinua, lo que ocurre, por ejemplo, cuando la captación de la imagen sólo se realiza en caso de que no se respete el limite de velocidad y no tiene nada que ver con la grabación de imágenes realizada de manera totalmente fortuita y poco sistemática) y las herramientas de comunicación utilizadas (por ejemplo, la conexión con un centro o el envío de imágenes a terminales remotos).

A efectos de la Directiva, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o incluso de la aplicación, en el caso individual, de técnicas o dispositivos específicos.

Por lo tanto, una de las primeras precauciones que deberá tomar el responsable del tratamiento es verificar si la vigilancia por videocámara implica el tratamiento de datos personales relacionados con personas identificables. En ese caso, la Directiva es aplicable, independientemente de las disposiciones nacionales en las que se requiera, además, autorización por motivos de seguridad pública.

Este puede ser el caso, por ejemplo, cuando se trate de equipos colocados a la entrada o en el interior de un banco, cuando dichos equipos permitan identificar a los clientes; por el contrario, en determinadas circunstancias, la Directiva dejará de ser aplicable cuando se trate de imágenes captadas durante un reconocimiento aéreo, que no puedan ser ampliadas de manera ventajosa o no incluyan información relativa a personas físicas (como puede ocurrir cuando las

imágenes se recogen para identificar manantiales o zonas de vertido de residuos), o en el caso de imágenes de barrido del tránsito en las autopistas.

XXIII. Vigilancia por videocámara en el contexto laboral

El multicitado Grupo, en su Dictamen N° 812001 sobre el tratamiento de datos personales en el contexto laboral, adoptado el 13 de septiembre de 2001, y en su Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, adoptado el 29 de mayo de 2002, puso de relieve, de manera mas general, algunos principios destinados a proteger los derechos, las libertades y la dignidad de los interesados, en el contexto laboral.

Además de las consideraciones realizadas en los documentos mencionados más arriba, en la medida en que sean realmente aplicables a la vigilancia por videocámara, conviene señalar que los sistemas de vigilancia por videocámara cuyo objetivo directo es controlar, desde una situación remota, la calidad y la cantidad de las actividades laborales y, por lo tanto, implican el tratamiento de datos personales en este contexto, por regla general no deberán estar permitidos.

La situación es diferente en lo que se refiere a los sistemas de vigilancia por videocámara que se utilizan, sujetos a las garantías adecuadas, para cumplir requisitos de producción y seguridad laboral, que también implican el control remoto (aunque sea indirectamente).

La experiencia ha puesto de manifiesto, además, que la vigilancia no deberá abarcar lugares reservados al uso privado de los empleados o no estén destinados a la realización de tareas de trabajo (como servicios, duchas, vestuarios o zonas de descanso); que las imágenes recogidas exclusivamente para proteger la propiedad o detectar, evitar y controlar infracciones graves no deberán utilizarse para acusar a un empleado de una falta disciplinaria menor; y que deberá permitirse siempre a los empleados que utilicen para su defensa el contenido de las imágenes captadas.

Deberá facilitarse información a los empleados y a cualquier otra persona que trabaje en el lugar. Esta información incluirá la identidad del responsable del tratamiento y el objetivo de la vigilancia, así como otra información necesaria para garantizar que el tratamiento es justo en lo que respecta al interesado, por ejemplo, en qué casos las grabaciones van a ser examinadas por la dirección de la empresa, el período de grabación y cuando ésta se revelará a las autoridades judiciales. En el contexto laboral, la información facilitada en forma de símbolo, por ejemplo, no se considerara suficiente.

XXIV. Situación en México

Como nos dice Jacob Bañuelos en su artículo *Videovigilancia en la Sociedad Panóptica Contemporánea*, la grabación y clasificación de imágenes videográficas en espacios públicos o privados no está legislada en México. La videovigilancia es una práctica que debería estar legislada, ya que grabar, clasificar y almacenar imágenes de personas en espacios públicos y privados sin su autorización puede llegar a vulnerar derechos de las personas. Las imágenes tomadas por cámaras administradas por el Estado , en un sistema de vigilancia panóptico que se implementa cada día con más énfasis en las sociedades modernas, no están a disposición de cualquier ciuda-

dano, se consideran información clasificada de seguridad pública o seguridad nacional, y en algunas sociedades como la nuestra, insistimos, no está regulada, no hay un control sobre el que vigila, sobre sus implicaciones morales, sobre el uso que se hace del material grabado y sobre el papel del ciudadano en este proceso de vigilancia, que incluso corre el riesgo de convertirse en material de vigilancia como espectáculo (como es el caso por ejemplo de los videos que se venden en la calle, grabados “subrepticiamente” en los llamados hoteles y moteles de paso).

El concepto de seguridad en nuestros días pasa necesariamente por el de videovigilancia o televigilancia, cuyos términos son ambivalentes, y sus alcances juegan con una doble moral, con un halo de conveniencia benefactora y con otro de represión y control. Su implementación se ha acentuado desde los acontecimientos del 11 de septiembre de 2001 en los EUA. La inseguridad se entiende como la consecuencia de todo desorden social y económico: es argumento político, ético, económico, moral, y cultural para justificar la intervención de los poderes gubernamentales, mediáticos y financieros, en la esfera del espacio público y la vida privada.

La experiencia de ser vigilado, adquiere diversos términos: videogilancia, "vigilancia universal", televigilancia, telepresencia o videopresencia, videoscopía, o maquinaria de la visión, es decir: "todos aquellos aspectos en los que se manifiesta la gran escalada sociológica de las máquinas de visión electrónicas" como lo señala Eugeni Bonet.

Por otro lado, como nos señala Nelson Arteaga en su artículo Vigilancia y Control Social de la Violencia en México, los sistemas electrónicos de vigilancia han tenido una expansión significativa en los últimos veinte años. Esto ha representado un cambio en las formas de organización social, en la medida en que dichos sistemas presentan dos caras: el cuidado y el control social. Por un lado se busca reducir los riesgos; por el otro, la administración de la población. En dicho documento examina, el caso de un municipio urbano de la ciudad de México, el de Huixquilucan, Estado de México, cómo la definición de un campo de problematización alrededor de la violencia por parte de autoridades locales, sectores privados y sociales, constituye una orquestación de relaciones de poder que determina la organización de un dispositivo electrónico de vigilancia que institucionaliza una cierta lógica de exclusión social y cultural.

Dicho sistema fue puesto en funcionamiento el 10 de septiembre de 2004 por el entonces Presidente Municipal David Korenfeld, dicho sistema considerado de alta seguridad con equipo de tecnología avanzada fue denominado Sistema Municipal de Tecnología Policiaca (SMTP) e inicialmente integrado por :

- 43 cámaras estratégicamente colocadas en todo el territorio municipal.
- Botones de enlace ciudadano.
- Patrullas equipadas con localizador satelital (GPS) .
- Módulo de videovigilancia.
- Módulo de Enlace Ciudadano
- Módulo GPS para ubicación de las patrullas.
- Módulo de Autoridades Municipales.

Las cámaras, son de alta resolución, con un movimiento de giro horizontal de 360º y otro más vertical de 180º. La transmisión del vídeo es inalámbrica vía microondas.

Ciertamente nos dice Arteaga, la decisión de instalar videocámaras representa la apertura de varios retos. El primero es en gran medida de carácter financiero (en este caso el costo del proyecto fue calculado con un costo de 100 millones de pesos pagaderos en el transcurso de tres años) ; pero no solo eso, se debe definir cómo instalarlas, qué vigilar y dónde vigilar , ya que las videocámaras, por muchas que se instalen, no pueden estar vigilando la totalidad de un espacio geográfico amplio al mismo tiempo.

Para definir cómo instalar las videocámaras en dicho Municipio, se recurrió a la elaboración y análisis de mapas e índices delictivos, accesos y puntos de confluencia en el espacio municipal y de factibilidad de mantenimiento a las videocámaras, así como la definición de las llamadas "líneas de vista" (rangos espaciales que tendrían que cubrir cada videocámara). Una vez con estos criterios de distribución se organizó una recopilación de información "ciudadana" (llamadas así por las propias autoridades municipales y de la empresa de seguridad pública) a través del uso de encuestas, entrevistas y diálogos con los "líderes sociales" para definir dónde y qué vigilar, ajustando así la orientación de las cámaras y el establecimiento de su "línea de vista". De hecho, este tipo de consultas se realiza regularmente para realizar algún tipo de acomodo de las videocámaras y responder así a las necesidades de seguridad pública.

Por otro lado tenemos que en la ciudad de México, a partir de octubre de 2006 en la Delegación Política Álvaro Obregón, se inicio un sistema de videovigilancia con 23 cámaras y a las cuales se les pretende sumar 16 cámaras más con una inversión de 73 millones de pesos. Por otro lado , a fines de 2006 se anunció que la Secretaría de Seguridad Pública del DF y la Delegación Política Miguel Hidalgo alistan un sistema de videovigilancia para una colonia de clase media-alta conocida como Polanco , con una inversión aproximada de 70 millones de pesos, mediante la instalación de 25 cámaras de seguridad, que se ubicaran en las zonas y avenidas más importantes de dicha zona de las cuales hasta el momento seis cámaras ya se encuentran instaladas y cuentan con un sistema de fibra óptica que permitirá la conexión de hasta 64 terminales más. Este sistema de seguridad estará operado por personal de la Policía capitalina, desde una base de radiooperaciones en un edificio ubicado a un costado del Parque Lincoln. Otra Delegación que actualmente dispone de sistemas de videovigilancia es la Gustavo A. Madero, fundamentalmente para el cuidado del peregrinar hacia la Basílica de Guadalupe.

En el llamado Sistema de Transporte Colectivo del DF más conocido como Metro, con el propósito de inhibir la comisión de delitos se pretenden colocar 1,600 cámaras de videovigilancia en andenes, vías, áreas de transbordo, talleres de mantenimiento, subestaciones eléctricas y almacenes, así como un sistema de telecomunicaciones de voz, datos e imágenes, para contar con información en tiempo real de llegadas y salidas de trenes, uso de telefonía celular y computadoras en sus instalaciones.

Cabe mencionar que a finales de 2006, el jefe de Gobierno, Marcelo Ebrard, ofreció convertir al DF en la ciudad "más vigilada de todo el planeta" con videocámaras y anunció que solicitará apoyo económico a la Cámara de Diputados para este programa a través de la licitación para la compra de cuatro mil cámaras de videos que serán colocadas en diversos puntos de la ciudad a partir del próximo año 2007.

De acuerdo con un Informe de la Secretaría de Seguridad Pública del Distrito Federal "la tecnología en cámaras de videovigilancia avanza a gran velocidad; hoy en día, estos aparatos cumplen con especificaciones inimaginables, como la detección de movimiento e incidentes, y

(serán) una herramienta poderosa para combatir la delincuencia", "son capaces de resistir condiciones climatológicas extremas, además de que son a prueba de vandalismo o explosiones; pueden observar de día y de noche con alta sensibilidad a la luz, en un rango de la frecuencia de infrarrojo", se lee. Las videocámaras, que serán instaladas en postes abatibles en zonas estratégicas de la ciudad, brindarán a las autoridades policiacas imágenes en tiempo real; permitiendo a los policías intervenir de inmediato en caso de emergencia. El funcionamiento de estas videocámaras estará regido por un Centro de Control, Comando, Comunicaciones y Cómputo (C4) y forma parte de un proyecto del Sistema Nacional de Seguridad Pública.

Por otro lado tenemos el caso del estado mexicano de San Luis Potosí , el cual dispone de 30 cámaras robóticas que giran 360 grados y suben y bajan 90 grados para poder ampliar la vigilancia en avenidas transitadas, centros comerciales, bancos, plazas y sitios públicos, así como sistemas de videograbación, todo esto con una inversión de 7 millones de pesos

Cabe mencionar que los bancos de México invirtieron en los últimos 4 años 190 millones de dólares en sistemas de videovigilancia para prevenir asaltos contra sus sucursales, aunque en algunos casos tuvieron pocos resultados.

Sin embargo, a pesar de todas estas declaraciones bienitencionadas y en algunos casos enormes cantidades de dinero, poco se habla de la regulación jurídica que necesariamente implica el uso de estos sistemas de videovigilancia (y no olvidemos el uso de los llamados “brazaletes electrónicos” y del valor probatorio de las evidencias videográficas) y no es de extrañarnos, considerando la prácticamente nula “cultura jurídica” en cuanto a la protección de datos personales. Como hemos podido percatarnos, en la mayoría de los países en donde se han instalado estos sistemas de videocámaras , usualmente van aparejados al desarrollo y puesta en vigor, de ordenamientos específicos que que reglamentan el adecuado funcionamiento de esta nueva modalidad de vigilancia, sin embargo la pregunta es si las autoridades mexicanas, llamese federales, estatales o municipales así como los organismos privados involucrados tienen la sensibilidad y voluntad de que se legisle el tema de la videovigilancia. No olvidemos que no bastaría con tener leyes adecuadas al respecto sino quererlas y saberlas aplicar por parte de las autoridades, solo así podremos hablar de un verdadero cambio, al menos en cuanto a la credibilidad de nuestras de por si desacreditadas instituciones jurídicas.

XXV. Consideraciones finales

1. La utilización de la videovigilancia presupone una cierta intrusión en la vida privada y, si ésta no es controlada, constituye una seria amenaza al respeto de la vida privada.

2. La vigilancia sin motivo válido constituye una grave amenaza a la vida privada. Esta amenaza es todavía más grande cuando el registro es permanente.

3. El deseo de mejorar la seguridad no debe violar el derecho a la vida privada.

4. Las entidades públicas deben comprobar si existen soluciones alternas no “invasivas” a la privacidad de las personas en materia de seguridad pública y privada

5. La videovigilancia es “justificable” en los lugares donde han habido actos delictivos reiterados en zonas determinadas.

6. El advenimiento de un acontecimiento deleznable y condenable, pero aislado como los actos terroristas, no deben necesariamente servir de aval para adoptar y generalizar un conjunto de reglas en detrimento de las personas.

7. La Administración Pública en sus distintos niveles, debe conciliar no sólo su misión de servicio con la noción de eficacia, sino también con el respeto de los valores fundamentales de los ciudadanos.

8. La utilización de la videovigilancia, con fines de la preservación de la seguridad pública, la defensa y la seguridad del Estado, puede ser inicialmente aceptada. Sin embargo, debe tratarse de un riesgo real, concreto e importante.

9. Los dos principales motivos que justifican la utilización de la videovigilancia son la prevención del crimen y el sentimiento de inseguridad manifestada por la población.

10. La videovigilancia es empleada desde hace más de 28 años por ciertos organismos públicos y mayoritariamente operado bajo su responsabilidad directa por lo que no debemos considerarlo necesariamente reciente, aunque si con un crecimiento exponencial.

11. La consulta pública respecto al uso de la videovigilancia por parte del Estado, adolece usualmente la presencia de representantes de universidades, de asociaciones de consumidores y de los ciudadanos en general.

12. En ocasiones, el impacto real de la instalación de las videocámaras no es razonablemente medido y por tanto derivan en ocasiones en resultados no necesariamente convincentes, como por ejemplo la disminución de la criminalidad.

13. La finalidad respecto al uso de la videovigilancia puede ser desvirtuado fácilmente, derivando en propósitos contrarios a los propósitos iniciales.

14. La informática, los nuevos sistemas sofisticados como el RFID y la videovigilancia permiten un control sobre la localización de los individuos.

15. Los datos obtenidos por estos sistemas, pueden permitir categorizar, diferenciar y jerarquizar diferentes grupos sociales.

16. El estudio del comportamiento humano por medio del registro de las imágenes debe ser evitado: la utilización de cámaras no puede servir para identificar las características racial, religiosa, política o sindical de los individuos.

17. La utilización de la videovigilancia debe ser sometida a una aprobación que debe ser a la vez, simple, flexible y eficaz.

18. La adopción de reglas uniformes, obligatorias, actuales e inmediatas debe tener como eje rector el hacer públicas y transparentes las acciones de los organismos en materia de videovigilancia;

19. La utilización de las cámaras de vigilancia a nivel público y privado debe sustentarse en un régimen jurídico suficientemente claro y provisto de sanciones ejemplares para quienes lo contravengan.

20. Es necesario que los lugares videovigilados cuenten con señalizaciones visibles para quiénes vayan a ser motivo de vigilancia por este medio.

21. De manera enunciativa y no limitativa, el horario de uso de las videocámaras, en algunos casos podría limitarse a los días y horas en que habitualmente se cometen más ilícitos

22. El manejo del material grabado por las videocámaras de videovigilancia debe estar a cargo de personas sensatas y responsables que conozcan los alcances legales del uso inadecuado de dicho material.

23. Las imágenes que se obtengan, deben ser adecuadas, pertinentes y no excesivas, no pudiendo ser objeto de un uso ulterior ajeno a aquellos que consigne la ley.

24. Los videoregistros no pueden ser objeto de una asociación de imágenes y de los datos biométricos, especialmente por medio de software de consulta automática de imágenes o de reconocimiento facial, ni ser vinculados a otros registros, ni constituir un banco de datos o ser comunicados a terceros.

25. Las protecciones acordadas por las leyes se circunscriben a las personas y no los lugares. El factor determinante de análisis es la expectativa del individuo al respeto de la vida privada.

26. Desafortunadamente, en la mayoría de los casos, el personal que emplea las cámaras de vigilancia no reciben una formación específica sobre las cuestiones relativas a la preservación de la vida privada.

27. En ocasiones, las personas son normalmente indiferente a la videovigilancia, muchas veces por desconocimiento. Sin embargo hay países como Inglaterra en donde el índice de aceptación de estas tecnologías es significativo por parte de la ciudadanía.

28. La evaluación del respeto de la vida privada debe tener en cuenta si la videovigilancia se realiza por medio de cámaras fijas, rotativas o móviles, por circuito cerrado o automatizado, con terminal única o una central de difusión de las imágenes con vigilancia y conexión a distancia.

29. Los ángulos de visión, es decir la posibilidad de ampliar o “congelar” las imágenes, así como la conexión con una central, deben estar debidamente justificadas.

30. La accesibilidad de un espacio común, de una calle o de un área abierta a toda persona, la ausencia de coacción para llegar y la expectativa de considerar el lugar como privado son los principales criterios para determinar del carácter público de un lugar.

31. Un lugar “privado” es aquel en donde una persona espera estar razonablemente ajena a una intrusión o una vigilancia fortuita u hostil.

32. En el caso de México (y por supuesto extensible a muchos otros países) es urgente una adecuada regulación jurídica de la videovigilancia a efecto de evitar excesos que contravengan los derechos fundamentales que toda persona debe tener.

XXVI. FUENTES DE INFORMACION CONSULTABLES Y EN SU CASO CONSULTADAS

1. *Bibliohemerografía en castellano*

Arteaga Botello, N., Vigilancia y Control Social de la Violencia en México, Capítulo Criminológico Vol. 34, Nº 1, Enero-Marzo 2006, 33 - 54

Arzoz Santiesteban, X., «Videovigilancia y derechos fundamentales: análisis de la constitucionalidad de la Ley Orgánica 4/1997», Revista Española de Derecho Constitucional, núm. 64, 2002.

Bañuelos Capistran, J., Videovigilancia en la Sociedad Panóptica Contemporánea, Revista Electrónica Razón y Palabra, Número 31. ,Febrero-Marzo 2003, ITESM-CEM , México.

Bacigalupo, E., «La regulación del uso de medios técnicos para la interceptación de comunicaciones privadas», Justicia penal y derechos fundamentales, Marcial Pons, Madrid, 2002.

Barcelona Llop, J., «A propósito de la Ley Orgánica 4/1997, de 4 de agosto, llamada de videovigilancia», AA, núm. 13, 1998.

Bauza Martorell, F. J., Régimen Jurídico de la Videovigilancia, Editorial: Marcial Pons , Madrid, 2004 , 142 pp .

Bruno, P., «Intercettazioni di comunicazioni e conversazioni», Digesto delle discipline penalistiche, vol. VII, ed. UTET, Torino, 1993.

Butrón Baliña, P. M., «Utilización de videocámaras en lugares públicos para prevenir la comisión de ilícitos», en VV.AA. (Coord. Martín Morales): El principio constitucional de intervención indiciaria, Grupo Editorial Universitario, Granada, 2000.

Choclán Montalvo, J. A., «La prueba videográfica en el proceso penal: validez y límites», Poder Judicial, núm. 38.

De La Oliva Santos, A., «Sobre la ineficacia de las pruebas ilícitamente obtenidas», Revista Española de Derecho Procesal, núm. 8-9, agosto-septiembre 2003.

De Urbano Castrillo, E. y Torres Morato, M. A., La prueba ilícita penal. Estudio Jurisprudencial, Aranzadi, Navarra, 2003.

Del Moral García, A., «Tratamiento procesal de la prueba ilícita por vulneración de derechos fundamentales», Estudios Jurídicos. Ministerio Fiscal, Tomo V-2001, Ministerio de Justicia. Centro de EstudiosJurídicos de la Administración de Justicia.

Díaz Cabiale, J. A. y Martín Morales, R., La garantía constitucional de la inadmisión de la prueba ilícitamente obtenida, Civitas, Madrid, 2001.

Gálvez Muñoz, L., La ineficacia de la prueba obtenida con violación de derechos fundamentales, Aranzadi, Navarra, 2003.

García De Gabiola, J., «Cámaras ocultas: El derecho a la información vs. los derechos al honor, a la intimidad y propia imagen», E.& J. núm.70, 2003.

Garrós Y Fuente, I., La videovigilacia y el control de las garantías constitucionales, Tesis doctoral , Universidad Autónoma de Barcelona, Facultad de Derecho, Bellaterra, 2005

Gómez Orfanel, G., «Jueces y micrófonos. La experiencia alemana», en JpD, núm. 32, 1998.

———, «Domicilios y escuchas. La reforma constitucional alemana de 1998», en CDP, núm. 3, 1998.

Goñi Sein, J. L., El respeto a la esfera privada del trabajador, Civitas, Madrid, 1998.

Greenberg, Enrique, Videovigilancia en la Via Publica , Madrid, 2001

Gudín Rodríguez-Magariños, F., La lucha contra el terrorismo en la sociedad de la información : los peligros de estrategias antiterroristas desbocadas, Madrid España , 2006, 256 pp.

Jiménez Campo, J., «La garantía constitucional del secreto de las comunicaciones», Revista Española de Derecho Constitucional, núm. 20,1987.

López Barja De Quiroga, J., Las escuchas telefónicas y la prueba ilegalmente obtenida, Akal, Madrid, 1989.

Magro Servet, V., «Consideraciones sobre la nueva ley que regula la utilización de las videocámaras por las fuerzas de seguridad en lugares públicos», en PJ, núm. 47, 1998.

Martín Pallín, J. A., Escuchas telefónicas. Homenaje a Enrique Ruiz Vadillo, Colex, Madrid, 1999.

Martínez García, E., Eficacia de la prueba ilícita en el proceso penal (a la luz de la STC 81/98, de 2 de abril), Tirant lo Blach, Valencia, 2003.

Martín Morales, R., El régimen constitucional del secreto de las comunicaciones, Civitas, Madrid, 1995.

El derecho a la intimidad: grabaciones con videocámaras y microfonía oculta, La Ley, año XXV. Número 6079, 6 de septiembre de 2004

Martínez Martínez, Ricardo, Tecnologias de la Información, Policía y Constitución, Ricard, Editorial Tirant Lo Blanch , Madrid, 2001, 430 pp.

Martínez Ruiz, J., Límites jurídicos de las grabaciones de la imagen y el sonido, Bosch, 2004.

Molina Navarrete, C. y Olarte Encabo, S., «Límites constitucionales a la libertad de empresa y derechos fundamentales inespecíficos del trabajador», Revista de la Facultad de Derecho de la Universidad de Granada, núm. 2 (monográfico Derechos Humanos, Derechos Fundamentales), 1999, págs. 263 y ss.

Montón Redondo, A., «Las interceptaciones telefónicas constitucionalmente correctas», LA LEY, 1995, t. V.

Navajas Ramos, L., «La prueba videográfica en el proceso penal», en Eguzkilore, núm. 12, 1998.

Noya Ferreiro, M. L., La intervención de comunicaciones orales en el proceso penal, Tirant lo Blanch, Valencia, 2000.

Ordoño Artés, C., «Las grabaciones magnetofónicas de las comunicaciones orales directas en el marco del proceso penal», Los derechos humanos. Libro Homenaje al Excmo. Sr. D. Luis Portero García, Granada, 2001.

Peso Navarro, E. *et al*., Los datos de los ciudadanos en los Ayuntamientos, 2004, Madrid, 440 pp.

Rodríguez Coarasa, C., «Algunas proyecciones del derecho constitucional a la intimidad en el ámbito laboral», Revista de Derecho Político, núm. 51, 2001, págs. 183-222.

Rodríguez Ruiz, B., El secreto de las comunicaciones: tecnología e intimidad, Mc-Graw Hill, Madrid, 1998.

Rafols Llach, J., «Autorización judicial para la instalación de aparatos de escucha, transmisión y grabación en lugar cerrado», La prueba en el proceso penal. Cuadernos de Derecho Judicial, CGPJ, Madrid, 1992.

Rives Seva, A. P., La intervención de la comunicaciones en la Jurisprudencia penal, Aranzadi, Navarra, 2000.

Roxin, C., «Comentario a la resolución del Tribunal Supremo Federal alemán sobre las trampas de la escucha» (trad. por De Hoyos Sancho, M.), RPJ, núm. 47, 1997.

Sánchez Barrilao, J. F., Las funciones no jurisdiccionales de los jueces en garantía de derechos, Civitas, Madrid, 2002.

Senés Motilla, C., «Cámaras de control y filmación de las vías públicas, redadas y controles policiales», en Velasco Núñez (dir.), Medidas restrictivas de derechos fundamentales, CGPJ, Madrid, 1996.

Serra Uribe, C. E. Derecho a la Intimidad y Videovigilancia Policial , Editorial Laberinto, Madrid , 2006, 159 pp.

Soto Nieto, F., «La motivación, la proporcionalidad y el control en las intervenciones telefónicas», LA LEY, 1995, t. II.

Tellez Valdes, J. , Regulación Jurídica de la Videovigilancia, en Derecho de Internet & Telecomunicaciones, Ed. Legis , Universidad de Los Andes, pags. 273-291, Bogotá, 2003

VV.AA. (Coord. Martín Morales): El principio constitucional de intervención indiciaria, Grupo Editorial Universitario, Granada, 2000.

2. *Bibliohemerografía en otros idiomas*

Colecciones

Ball, K. and Webster, F. (eds.) (2003) The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Era. London: Pluto Press.

Haggerty, K. and Ericson, R. (2006) The New Politics of Surveillance and Visibility, Toronto: University of Toronto Press.

Levin, T. Y., Frohe, U. and Weibel, P. (eds.) (2002) CTRL [Space]: Rhetorics of Surveillance from Bentham to Big Brother. Cambridge, MA and London: MIT Press.

Lyon, D. (ed.) (2003) Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination, London and New York: Routledge.

Lyon, D. and E. Zureik (eds.) (1998) Computers, Surveillance and Privacy. Minneapolis: University of Minnesota Press.

Libros de consulta

Cavoukian, A. and Tapscott, D. (1995) Who Knows? Safeguarding Your Privacy in a Networked World, Toronto: Random House.

Davies, S. (1996) Big Brother: Britain's Web of Surveillance and the New Technological Order, London: Pan Books.

Garfinkel, S. (2001) Database Nation: The Death of Privacy in the 21st Century. Cambridge, MA: O'Reilly.

O'Harrow, R. J. (2005) No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society. New York: Free Press.

Parenti, C. (2003) The Soft Cage: Surveillance in America from Slave Passes to the War on Terror. New York: Basic Books.

Parker, J. (2000) Total Surveillance Investigating the Big Brother world of e-spies, eavesdroppers and CCTV, Piatkus.

Rosen, J. (2004) The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age. New York: Random House.

Whitaker, R. (1999) The End of Privacy: How Total Surveillance is Becoming a Reality. New York: The New Press.

Libros editados por universidades

Bogard, W. (1996) The Simulation of Surveillance: Hypercontrol in Telematic Societies. Cambridge: Cambridge University Press.

Coleman, R. (2004) Reclaiming the Streets: Surveillance, Social Control and the City. Cullompton, UK: Willan.

Dandeker, C. (1990) Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day. Cambridge, MA: Polity Press.

Ericson, R. V. and Haggerty, K.D. (1997) Policing the Risk Society. Toronto: University of Toronto Press.

Foucault, M. (1977) Discipline and Punish: The Birth of the Prison. New York: Pantheon

Garland, D. (2001) The Culture of Control: Crime and Social Order in Contemporary Society. Chicago: University of Chicago Press.

Gilliom, J. (2001) Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy. Chicago: University of Chicago Press.

Lyon, D. (ed.) (2006) Theorizing Surveillance: The Panopticon and Beyond. Cullompton, UK: Willan.

Lyon, D. (2003) Surveillance after September 11. Cambridge: Polity Press.

Lyon, D. (2001) Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press.

Lyon, D. (1994) The Electronic Eye: The Rise of Surveillance Society. Cambridge, MA. Polity Press.

McCahill, M. (2002) The Surveillance Web: The rise of visual surveillance in an English city, Cullompton: Willan.

McGrath, J. (2004) Loving Big Brother: Performance, Privacy and Surveillance Space. London: Routledge.

Marx, G.T. (1988) Undercover: Police Surveillance in America. Berkeley, CA: University of California Press.

Monmonier, M. (2004) Spying with Maps: Surveillance Technologies and the Future of Privacy. Chicago: University of Chicago Press.

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

Rigakos, G. (2002) The New Parapolice: Risk Markets and Commodified Social Control. Toronto: University of Toronto Press.

Rule, J.B. (1974) Private Lives and Public Surveillance: Social Control in the Computer Age, New York, NY: Schocken Books.

Staples, W.G. (2000) Everyday Surveillance: Vigilance and Visibility in Postmodern Life. New York: Rowman and Littlefield.

Staples, W.G. (1997) The Culture of Surveillance: Discipline and Social Control in the United States. New York: St. Martin's Press.

Reporte de expertos

Andreas, P. and Snyder, T. (eds.), The Wall Around the West: State Borders and Immigration Controls in North America and Europe. Lanham MD: Rowman and Littlefield.

Bigo, D. and Guild, E. (eds.) (2005) Controlling Frontiers: Free Movement into and within Europe, Aldershot: Ashgate.

Salter, M. (2003) Rights of Passage: The Passport in International Relations. Boulder, CO. Lynne Rienner.

Torpey, F. (2001) The Invention of the Passport: Surveillance, Citizenship and the State. Cambridge: Cambridge University Press.

Zureik, E. and Salter, M.B. (eds.)(2005) Global Surveillance and Policing: Borders, Security, Identity. Cullompton, UK: Willan.

Ciudadania e identidad

Caplan, J. and Torpey, J. (eds.) (2002) Documenting Individual Identity: The Development of State Practices in the Modern Word, Princeton, NJ: Princeton University Press.

Garton-Ash, T. (1997) The File: A Personal History. London: Harper Collins.

House of Commons Select Committee on Science and Technology (2006) Identity Card Technologies: Scientific Advice, Risk and Evidence,

http://www.parliament.uk/parliamentary_committees/science_and_technology_committee/sag.cfm

Lyon, D. (2004) 'Identity cards: social sorting by database,' OII Internet Issue Brief No. 3 . http://www.oii.ox.ac.uk/research/publications.cfm

Solove, D. (2004) The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press.

Consumo

Elmer, G. (2004). Profiling Machines: Mapping the Personal Information Economy. Cambridge, MA: The MIT Press.

Gandy, O. (1993) The Panoptic Sort: A Political Economy of Personal Information, Boulder, CO: Westview Press.

Lace, S. (ed.) (2005) The Glass Consumer: Life in a Surveillance Society, Bristol: The Policy Press.

Turow, J. (2006) Niche Envy: Marketing Discrimination in the Digital Age. Cambridge MA. MIT Press.

Derecho penal y procuración y administración de justicia

Gill, M. and Spriggs, A. (2005) Assessing the impact of CCTV. London, Home Office Research, Development and Statistics Directorate.

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

Newburn, T. and Hayman, S. (2001) Policing, CCTV, and Social Control: Police Surveillance and Suspects in Custody. Collumpton: Willan Publishing.

Norris, C., McCahill, M. and Wood, D. (eds.) (2004) The Politics of CCTV in Europe and Beyond. Special Issue of Surveillance and Society, 2(2/3), http://www.surveillance-andsociety.org/cctv.htm

Painter, K. and Tilley, N. (1999) Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention. Cullompton: Willan.

Infrastructura y urbanismo

Coaffee, J. (2003) Terrorism, Risk and the City: The Making of a Contemporary Urban Landscape. Aldershot UK: Ashgate.

Graham, S. (ed.) (2004) The Cybercities Reader, London: Routledge.

Graham, S. and Marvin, S. (2001) Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition. London: Routledge.

Institute for the Future (2004) Infrastructure for the New Geography. Menlo Park: California. IFTF.

Kang, J. and Cuff, D. (2005) 'Pervasive Computing: Embedding the Public Sphere, Washington and Lee Law Review 62(1): 93-146.

Medicina

Armstrong, D. (1995) 'The Rise of Surveillance Medicine,' Sociology of Health and Illness, 17(3): 393-404.

Cole, S. (2001) Suspect Identities: A History of Fingerprinting and Criminal Identification, Boston; Harvard University Press.

Nelkin, D. and Tancredi, L. (1994) Dangerous Diagnostics. Chicago: University of Chicago Press.

Laurie, G. (2002) Genetic Privacy: A Challenge to Medico-Legal Norms, Cambridge: Cambridge University Press.

Rose, H. (2001) The Commodification of Bioinformation: The Icelandic Health Sector Database, London: The Wellcome Trust.

Servicios públicos

Bellamy, C. and Taylor, J. (1998) Governing in the Information Age, Buckingham: Open University Press.

Cabinet Office (2005) Transformational Government – Enabled by Technology (Cm 6683), London: Cabinet Office, Available at: http://www.cio.gov.uk/documents/pdf/transgov/trangovstrategy.pdf#search=%22Transformational%20Government%20%E2%80%93%20Enabled%20by%20Technology%20%22

Snellen, I. and van de Donk, W. (eds.) (1998) Public Administration in an Information Age: A Handbook, Amsterdam: IOS Press.

Parton, N. (2006) Safeguarding Childhood: Early intervention and surveillance in later modern society, Basingstoke: Palgrave-Macmillan.

Performance and Innovation Unit, Cabinet Office (2002) Privacy and Data-Sharing: The Way Forward for Public Services, London: Cabinet Office, Available at:

http://www.strategy.gov.uk/downloads/su/privacy/downloads/piudata.pdf#search=%22Privacy%20and%20DataSharing%3A%20The%20Way%20Forward%20for%20Public%20Services%2C%22

Regulacion legal

Bennett, C. (1992) Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Ithaca, NY: Cornell University Press.

Bennett, C. and Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge, MA: MIT Press.

Flaherty, D. (1989) Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States, Chapel Hill, NC: University of North Carolina Press.

Regan, P. (1995) Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: University of North Carolina Press.

Telecomunicaciones

Bamford, J. (2001) Body of Secrets: Anatomy of the Ultra-Secret National Security Agency. New York: Random House.

Keefe, P.R. (2005) Chatter: Dispatches from the Secret World of Global Eavesdropping. New York: Random House

Crampton, J. (2004) The Political Mapping of Cyberspace. Chicago: University of Chicago Press.

A Report on the Surveillance Society: Appendices

Diffie, W. and Landau, S. (1998) Privacy on the Line: The Politics of Wiretapping and Encryption, Cambridge, MA: MIT Press.

Lessig, L. (1999) Code and Other laws of Cyberspace, New York, NY: Basic Books.

Materia laboral

Ball, K.S. (ed.) (2002) Work. Special issue of Surveillance and Society 1(2),

http://www.surveillance-and-society.org/journalv1i2.htm

Frenkel, S. et al. (1999) On the Front Line: The Organization of Work in the Information Economy. Ithaca: Cornell University Press.

McKinlay, A. and Starkey, K. (eds.) (1998) Foucault, Management and Organization Theory: From Panopticon to Technologies of Self. London: Sage.

Stanton, J.M. and Stam, K.R. (2006) The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets-Without Compromising Employee Privacy or Trust. Medford, NJ: Cyberage Books.

Zuboff, S (1988) In the Age of the Smart Machine. New York: Basic Books.

Reportes

ACLU (American Civil Liberties Union) (2004) The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society. Washington DC: ACLU.

http://www.aclu.org/FilesPDFs/surveillance_report.pdf

European Parliament Scientific and Technological Options Assessment Committee (STOA) (1999) Development of Surveillance Technology and the Risk of Abuse of Economic Information (5 Vols), Luxembourg: STOA. Available from:

http://www.europarl.europa.eu/stoa/publications/studies/default_en.htm

SWAMI (2006) Safeguards in a World of Ambient Intelligence: Report on the Final Conference: Brussels March 21-22, 2006, Information Society: Technologies.

http://swami.jrc.es/pages/documents/Deliverable5ReportonConference.pdf#search=%22swami%20report%22

Privacy International / Electronic Privacy Information Center (EPIC) (Annual) Privacy and Human Rights: An International Survey of Privacy Laws and Developments. Available from: http://www.privacyinternational.org/

UrbanEye Project (2001-2004) Working Papers http://www.urbaneye.net/results/results.htm

Cibergrafia

- CASPIAN (Consumers against supermarket privacy and numbering) http://www.nocards.org/
- Roger Clarke's Dataveillance and Information Privacy Home-Page http://www.anu.edu.au/people/Roger.Clarke/
- Electronic Privacy and Information Centre http://www.epic.org/
- Liberty http://www.liberty-human-rights.org.uk/
- New York Surveillance Camera Players http://www.notbored.org/the-scp.html
- Notags.co.uk http://www.notags.co.uk/
- Privacy International http://www.privacyinternational.org/
- Statewatch http://www.statewatch.org/
- The Surveillance Project http://www.queensu.ca/sociology/Surveillance/
- Surveillance and Society http://www.surveillance-and-society.org/
- UrbanEye Project http://www.urbaneye.net/