11750/02/ES
WP 89

Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara

Adoptado el 11 de febrero de 2004

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Visto el artículo 29, así como la letra a) del apartado 1 y el apartado 3 del artículo 30 de dicha Directiva,

Visto su reglamento interno, y, en particular, sus artículos 12 y 14,

HA ADOPTADO EL PRESENTE DICTAMEN:

1. INTRODUCCIÓN

Durante los últimos años, en Europa, los organismos públicos y privados han recurrido cada vez con más frecuencia a los sistemas de captación de imagen. Esta circunstancia ha suscitado un animado debate tanto en el ámbito comunitario como en los diferentes Estados miembros, 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, a partir de la incorporación de la Directiva 95/46/CE en la legislación nacional, 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 miniaturización aumentan de manera considerable las oportunidades que ofrecen los dispositivos de grabación de imagen y sonido, lo que también tiene que ver con su despliegue tanto en las intranets como en Internet.

Además de las operaciones de tratamiento de datos en el contexto laboral, que ya abordó el Grupo en un documento detallado, «Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral[2]», todos los ciudadanos pueden apreciar fácilmente la creciente proliferación de técnicas de vigilancia por videocámara. Por otro lado, hay una tendencia creciente a la interconexión de sistemas de vigilancia por videocámara.

Un análisis no exhaustivo de las principales aplicaciones muestra que la vigilancia por videocámara puede servir para fines bastante diferentes[3], que, sin embargo, pueden agruparse en varias áreas principales:

---

1 DO L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

2 WP 48, adoptado el 13 de septiembre de 2001, disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

3 Se han instalado diferentes sistemas de vigilancia por videocámara:

1) protección de las personas físicas;

2) protección de la propiedad;

3) interés público;

4) detección, prevención y control de delitos;

5) puesta a disposición de pruebas;

6) otros intereses legítimos.

Algunos requisitos también se refieren a la instalación de videocámaras y dispositivos similares.

En algunos casos, la utilización de un sistema de grabación de imagen puede ser, en realidad, obligatoria, de conformidad con disposiciones específicas de los Estados miembros (ha ocurrido, por ejemplo, en algunos casinos) o se realiza con un fin al que los familiares de los interesados conceden especial importancia (por ejemplo, en relación con la búsqueda de personas desaparecidas). Por otra parte, también se pueden citar ejemplos peculiares del uso de tales dispositivos (en particular, relativos a terceros países), como los casos en los que se han utilizado sistemas de reconocimiento fisonómico para impedir la bigamia o en los que una autoridad policial local ha decidido hacer públicas imágenes relativas a lo dura que es la vida en prisión para los presos, sin su consentimiento.

Por consiguiente, 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 medidas pertinentes. A veces, esto es debido a las ventajas económicas que conceden, en su mayoría, los organismos públicos, así como

---

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;
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 rodado, con vistas a controlar el tráfico 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 los colegios y en relación con los casos de menores importunados;
e) en el interior de los centros sanitarios, durante una operación o con vistas, por ejemplo, a dispensar 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 tráfico 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 el interior de las comunidades de vecinos y en zonas adyacentes, tanto por motivos de seguridad como para disponer de pruebas en caso de que se cometan delitos;
j) con fines 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 y salas de baile, en los que se graba a los clientes y visitantes a intervalos regulares sin advertirles.

a las propuestas de mejores condiciones en materia de seguros derivadas de la utilización de equipos de vigilancia por videocámara.

Se da también un efecto psicológico relacionado con la vigilancia por videocámara, según el cual la opinión pública a veces considera este tipo de vigilancia, con o sin razón, una «herramienta inestimable» en su utilización para la detección de delitos.

Así pues, se trata de un sector múltiple, en continua evolución, en el que ya hay varias técnicas disponibles.

El objetivo del presente documento de trabajo consiste en realizar un análisis inicial partiendo de la existencia de normativas parcialmente diferentes, así como de la presencia de disposiciones excesivamente detalladas en la legislación nacional de los diferentes Estados miembros, lo que requiere un enfoque más sistemático y armonizado.

El presente documento se refiere a la vigilancia destinada al control a distancia de acontecimientos, situaciones y sucesos, pero no tiene en cuenta directamente otros supuestos en los que determinados acontecimientos se divulgan de manera ocasional o tendenciosa en relación con la transparencia de la actividad de autoridades locales o instancias parlamentarias, por ejemplo.

A partir de ahí, cada operador podrá ampliar lo indicado aquí, tanto en relación con su sector correspondiente como en lo relativo a los avances tecnológicos futuros que el Grupo pretende investigar.

Asimismo, los principios que se incluyen en el presente documento se refieren a la captación de imágenes, si es posible combinadas con sonido o con datos biométricos, como huellas dactilares[4].

Dichos principios también podrán tenerse en cuenta, en los casos concretos en los que sea aplicable, en relación con el tratamiento de datos personales que no haya sido realizado con equipos de vídeo, sino mediante otros tipos de vigilancia, como control remoto (es el caso, por ejemplo, de los sistemas GPS por satélite).

El primer objetivo del presente documento es atraer la atención hacia la amplia gama de criterios que existen para evaluar la legalidad y la conveniencia de instalar sistemas individuales de vigilancia por videocámara.

No obstante, también se han tenido en cuenta los siguientes aspectos:

a) Conviene que las instituciones pertinentes de los Estados miembros evalúen la vigilancia por videocámara desde un punto de vista general y con vistas a impulsar un enfoque globalmente selectivo, además de sistemático, para este asunto. La proliferación excesiva de sistemas de captación de imagen en zonas públicas y privadas no deberá traducirse en la imposición de restricciones injustificadas a los derechos y libertades fundamentales de los ciudadanos; de lo contrario, los ciudadanos podrían verse obligados a someterse a procedimientos

[4] El Grupo tratará la cuestión más general de la aplicación de la Directiva 95/46/CE a los datos biométricos en un documento independiente.

desproporcionados de recogida de datos que permitirían su identificación masiva en diversos lugares públicos y privados.

b) Las tendencias relativas a la evolución de las técnicas de vigilancia por videocámara podrían evaluarse de manera provechosa para evitar que el desarrollo de aplicaciones informáticas basadas tanto en el reconocimiento fisonómico como en el estudio y el pronóstico del comportamiento humano reproducido conduzca de manera involuntaria a una vigilancia dinámico-preventiva, en contraposición con la vigilancia estática convencional, cuyo objetivo suele ser la documentación de acontecimientos específicos y de sus autores. Esta nueva forma de vigilancia está basada en la captación automatizada de los rasgos faciales de personas físicas y de su conducta «anormal» asociada a la disponibilidad de señales y avisos automatizados, lo que probablemente acarree riesgos de discriminación.

2. INSTRUMENTOS JURÍDICOS INTERNACIONALES

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

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

b) Convenio nº 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 95/46/CE, a las actividades del primer pilar (véase más adelante). 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 recogida y el 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.

c) Carta de los Derechos Fundamentales de la Unión Europea

La Carta de los Derechos Fundamentales de la Unión Europea estipula, en su artículo 7, la protección de la vida privada y familiar, del domicilio y de las comunicaciones y en su artículo 8, la protección de los datos de carácter personal.

3. LA VIGILANCIA EN EL MARCO DE LA DIRECTIVA 95/46/CE

La Directiva 95/46/CE (de aquí en adelante «la Directiva») hace hincapié de manera expresa en las características específicas del tratamiento de la información personal incluida en los datos de sonido e imagen y se refiere a ellas expresamente en varios puntos.

Dicha Directiva garantiza la protección del derecho a la intimidad y la vida privada, así como la gama más amplia de protección de datos personales en lo que respecta a las libertades y los derechos fundamentales de las personas físicas (apartado 1 del artículo 1).

Una parte considerable de la información recogida mediante la vigilancia por videocámara se refiere a personas identificadas o identificables, que han sido filmadas mientras se encontraban en un lugar público o abierto al público. Es muy posible que la persona que se encuentra de paso se espere disfrutar de un menor grado de intimidad, pero lo que no se espera es verse totalmente desprovisto de sus derechos y libertades en lo que se refiere a su propia esfera e imagen.

También cabe tener en cuenta aquí el derecho a la libre circulación de las personas que se encuentran en el territorio de un Estado de manera legal, lo que se contempla en el artículo 2 del Protocolo Adicional nº 4 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

Dicha libertad de circulación sólo puede estar sujeta a restricciones necesarias en una sociedad democrática y proporcionales a la consecución de fines específicos. Los interesados tienen derecho a ejercer su derecho a la libre circulación sin verse sometidos a un condicionamiento psicológico excesivo en cuanto a sus movimientos y su conducta y sin ser objeto de un control detallado, como la posibilidad de que se sigan sus movimientos o se disparen «alarmas» basadas en programas informáticos que «interpretan» de manera automática la conducta supuestamente sospechosa de un individuo, sin ningún tipo de intervención humana, a causa de la utilización desproporcionada de la vigilancia por videocámara por parte de varias entidades en diversos lugares públicos o abiertos al público.

El carácter específico y sensible del tratamiento de datos constituidos por imagen y sonido relativos a personas físicas se pone de relieve en los primeros considerandos de la Directiva. Además de las consideraciones que se harán más adelante en cuanto al ámbito de aplicación, los considerandos mencionados y los artículos pertinentes de la Directiva aclaran lo siguiente:

a) en principio, la Directiva es aplicable a este asunto en vista también de la importancia del desarrollo de las técnicas utilizadas para captar, manejar y utilizar en cualquier otro modo la categoría específica de datos personales obtenidos de esta forma (véase el considerando 14);

b) los principios de protección de la Directiva también son aplicables a cualquier información (incluso la que esté constituida por imagen y sonido) relativa a una persona identificada o identificable, teniendo en cuenta el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra

persona para identificar a aquella (véanse la letra a) del artículo 2 y el considerando 26).

Además de las referencias específicas mencionadas, es obvio que la Directiva es plenamente aplicable en el marco de sus disposiciones individuales relativas, en concreto, a:

1) *Calidad de los datos*. Las imágenes serán tratadas de manera leal y lícita, y se destinarán a fines determinados, explícitos y legítimos. Se utilizarán de conformidad con el principio según el cual los datos deberán ser adecuados, pertinentes y no excesivos, y no serán tratadas posteriormente de manera incompatible con dichos fines; se conservarán durante un período limitado, etc. (véase el artículo 6).
2) *Principios relativos a la legitimación del tratamiento de datos*. En base a estos principios, es necesario que el tratamiento de datos personales mediante vigilancia por videocámara esté fundamentado en al menos uno de los requisitos mencionados en el artículo 7 (consentimiento inequívoco, necesidad de obligaciones contractuales, de cumplimiento de una obligación jurídica, de protección del interés vital del interesado, de cumplimiento de una misión de interés público o inherente al ejercicio del poder público, equilibrio de intereses, etc.).
3) Tratamiento de *categorías especiales de datos*, sujeto a las garantías aplicables al uso de datos sensibles o datos relativos a infracciones en el marco de la vigilancia por videocámara (con arreglo al artículo 8).
4) *Información* que se facilitará al interesado (véanse los artículos 10 y 11).
5) *Derechos del interesado*, en concreto el derecho de acceso y el derecho de oposición al tratamiento por razones legítimas (véase el artículo 12 y la letra a) del artículo 14).
6) Garantías aplicables en relación con *las decisiones individuales automatizadas* (véase el artículo 15).
7) *Seguridad* de las operaciones de tratamiento (véase el artículo 17).
8) *Notificación de las operaciones de tratamiento* (véanse los artículos 18 y 19).
9) *Controles previos* de las operaciones de tratamiento que puedan presentar riesgos específicos para los derechos y libertades del interesado (véase el artículo 20).
10) *Transferencia de datos a terceros países* (artículo 25 y siguientes).

El carácter específico y sensible del tratamiento de datos constituidos por imagen y sonido se reconoce finalmente en el último artículo de la Directiva, a través del cual la Comisión se compromete a estudiar, en particular, la aplicación de la directiva a dicho

asunto y a presentar las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información (véase el artículo 33).

4. DISPOSICIONES NACIONALES APLICABLES A LA VIGILANCIA POR VIDEOCÁMARA

En varios Estados miembros ya se han realizado estudios de casos relativos a la vigilancia por videocámara, basados tanto en disposiciones constitucionales[5] como en legislación específica o en resoluciones y otras decisiones emitidas por las autoridades nacionales competentes[6].

En algunos países también existen disposiciones específicas aplicables independientemente del hecho de que la vigilancia por videocámara pueda implicar el tratamiento de datos personales. Con arreglo a dicha normativa, la instalación y el despliegue de circuitos cerrados de televisión y equipos de vigilancia similares deberán ser autorizados previamente por una autoridad administrativa (que podrá estar representada, parcialmente o a todos los efectos, por la autoridad nacional de protección de datos). Dicha normativa podrá diferir en función de la naturaleza pública o privada de la entidad responsable de manejar el equipo en cuestión.

En otros países, la vigilancia por videocámara no es objeto de legislación específica en la actualidad; sin embargo, las autoridades de protección de datos han estado trabajando para garantizar la aplicación adecuada de las disposiciones generales de protección de datos, en particular a través de dictámenes, directrices o códigos de conducta (que ya han sido adoptados en el Reino Unido y están siendo elaborados en Italia, por ejemplo).

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 por videocámara; el Dictamen 3/2000, de 10 de enero de 2000, relativo a la utilización de sistemas de vigilancia por videocámara en la entrada de los edificios de apartamentos.
Dinamarca	Texto refundido de la Ley nº 76, de 1 de febrero de 2000, relativa a la prohibición de la vigilancia por videocámara. En general, esta Ley prohibe a las entidades privadas la vigilancia por videocámara de calles, carreteras o plazas públicas o de cualquier otra área similar utilizada para el desplazamiento común. Sin embargo, hay varias excepciones a esta

[5] Véase la sentencia 255/2002 del Tribunal Constitucional de Portugal, con arreglo a la cual el Tribunal determinó que «la utilización de dispositivos de vigilancia electrónica y el control de ciudadanos por parte de organismos privados de seguridad constituye un límite o una restricción al derecho a preservar la vida privada, consagrado en el artículo 26 de la Constitución».

[6] Al menos en un país (Bélgica, caso Gaia), el incumplimiento de la legislación relativa a la protección de datos en el marco de la captación de imágenes ha llevado al rechazo de pruebas admisibles ante el Tribunal.

	prohibición. 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 1 de julio de 2003, en la que se establece que la vigilancia por videocámara realizada en medios de transporte público gestionados de manera privada ha de ser proporcionada y cumplir lo dispuesto en la Ley danesa de protección de datos. Resoluciones de la autoridad de protección de datos, de 13 de noviembre de 2003, en virtud de las cuales se establecen determinados límites a la vigilancia por videocámara realizada por autoridades públicas.
Finlandia	En Finlandia no existe legislación especial sobre vigilancia por videocámara, pero existen disposiciones sobre vigilancia por videocámara y otros tipos de vigilancia, observación y control técnicos en muchas leyes diferentes. Con frecuencia se plantean preguntas sobre vigilancia por videocámara y grabación de conversaciones, y hemos tenido varios casos. Por ejemplo, el Defensor del Pueblo en materia de protección de datos ha dado su opinión acerca de la grabación de conversaciones telefónicas en los servicios al consumidor y en el entorno laboral (números de registro 1061/45/2000 y 525/45/2000). Nuestra oficina ha publicado un folleto sobre la intimidad en la vigilancia por videocámara (Asiaa tietosuojasta 4/2001 Yksityisyyden suoja kameravalvonnassa. http://www.tietosuoja.fi/uploads/03wamgvxuybt4ti.rtf).
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 de protección de datos, de 21 de junio de 1994. Directrices de la autoridad de protección de datos relativas a la vigilancia por videocámara en el lugar

	de trabajo: http://www.cnil.fr/thematic/index.htm; sobre otros asuntos (como la cámara *web*)[7]. 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 2000-916, de 19 de septiembre de 2000). Decreto 96-926, de 17 de octubre de 1996 y Circular, de 22 de octubre de 1996, sobre la aplicación de la Ley 95-73.
Grecia	1) Carta nº 390, de 28 de enero de 2000, relativa a la instalación de un circuito cerrado de televisión en el metro de Atenas. 2) Directiva nº 1122, de 26 de septiembre de 2000, sobre los circuitos cerrados de televisión. 3) Decisión nº 84/2002 sobre los circuitos cerrados de televisión en hoteles.
Alemania	Letra b de la sección 6 de la Ley federal de 2001. Sección 25 de la Ley sobre protección en la frontera. Otra normativa sobre vigilancia por videocámara por parte de la policía en las leyes de la policía de los Estados federados. Actualmente se está debatiendo en el Parlamento un proyecto de ley que prohíbe la vigilancia secreta por videocámara.
Irlanda	Ley de protección de datos de 1998 y 2003. Estudio de casos nº 14/1996 (utilización de circuitos cerrados de televisión).
Italia	Sección 134 del Código de protección de datos personales (Decreto legislativo nº 196, de 30 de junio de 2003, en el que se contempla la adopción de un código de conducta). Resoluciones de la autoridad italiana de protección de datos: nº 2, de 10 de abril de 2002 (relativa al fomento de la adopción de códigos de conducta), de 28 de septiembre de 2001 (relativa a las técnicas biométricas y de reconocimiento fisonómico aplicadas por los bancos) y de 29 de noviembre de 2000 (el llamado «decálogo de la vigilancia por videocámara»). Decreto presidencial nº 250, de 22 de junio de 1999

[7] Véanse los informes anuales de la Comisión nacional francesa de informática y libertades (CNIL).

	(por el que se regula el acceso de vehículos a los centros urbanos y a las zonas de acceso restringido). Decreto nº 433, de 14 de noviembre de 1992, y Ley nº 4/1993 (relativa a museos, bibliotecas públicas y archivos). Decreto legislativo nº 45, de 4 de febrero de 2000 (barcos de pasajeros en rutas nacionales). Sección 4 de la Ley nº 300, de 20 de mayo de 1970 (el llamado «Estatuto de los trabajadores»).
Luxemburgo	Artículos 10 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.
Países Bajos	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. En 2004 se publicará una actualización de las directrices elaboradas en 1997. En 2003 se realizó una investigación sobre vigilancia por videocámara en todos los municipios. Desde el 1 de enero de 2004 está vigente una modificación del Código Penal en virtud de la cual se amplia el alcance del delito de grabar imágenes de lugares abiertos al público sin informar a los afectados. El gobierno propone que se modifique la Ley de administración municipal al objeto de atribuir competencias explícitas a los ayuntamientos y alcaldes para utilizar sistemas de vigilancia por videocámara en lugares públicos con fines públicos en determinadas condiciones (como la obligación de evaluar periódicamente la eficacia de la vigilancia por videocámara).
Portugal	Decreto ley nº 231/98, de 22 de julio de 1998 (relativo a la actividad privada en materia de seguridad y a los sistemas de autoprotección). Ley nº 38/98, de 4 de agosto de 1998 (relativa a las medidas que deberán adoptarse en caso de violencia relacionada con acontecimientos deportivos). Decreto ley nº 263/01, de 28 de septiembre de 2001 (relativo a las zonas de baile). Decreto ley nº 94/2002, de 12 de abril de 2002 (acontecimientos deportivos).
España	Ley Orgánica nº 4/1997 (por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos).

	Real Decreto nº 596/1999, por el que se aplica la Ley Orgánica nº 4/1997.
Suecia[8]	La vigilancia por videocámara se regula de manera específica en la Ley 1998/150 sobre vigilancia general por videocámara y la Ley 1995/1506 sobre vigilancia secreta por videocámara (en indagaciones criminales). Normalmente, la vigilancia general por videocámara requiere autorización de la junta administrativa municipal. Sin embargo, dicha autorización no es necesaria cuando se trata de vigilancia de oficinas de correos, sucursales de banco o tiendas, por ejemplo. La vigilancia secreta por videocámara debe contar con la autorización de un tribunal. El Ministro de Justicia puede apelar las decisiones de la junta administrativa municipal. La grabación de imágenes utilizando técnica digital se considera una forma de tratamiento de datos personales y entra en el marco de la supervisión por parte de la autoridad encargada de la inspección de datos, en la medida en que no está regulada de manera específica en la Ley sobre vigilancia general por videocámara. Un comité de investigación acaba de publicar un informe relativo a la vigilancia por videocámara (SOU 2002:110).
Reino Unido	Código profesional 2000 sobre circuitos cerrados de televisión (Delegado de Información). Actualmente en revisión.

También se han adoptado instrumentos reguladores importantes en Islandia (sección 4 de la Ley nº 77/2000), Noruega (título VII de la Ley nº 31, de 14 de abril de 2000), Suiza (recomendación del Delegado federal) y Hungría (recomendación de la autoridad de protección de datos, de 20 de diciembre de 2000).

[8] En Suecia la vigilancia general por videocámara requiere, en principio, la autorización de la junta administrativa municipal, pero están previstas varias excepciones, cuando se trata, por ejemplo, de vigilancia de oficinas de correos, sucursales de banco o tiendas. La vigilancia secreta por videocámara debe contar con la autorización de un tribunal. En virtud de la Ley relativa a la vigilancia general por videocámara, las decisiones de la junta administrativa municipal pueden ser objeto de recurso, interpuesto por el Ministerio de Justicia, por razones de seguridad pública. De conformidad con la ley sueca de protección de datos, la grabación de imágenes utilizando cámaras digitales se considera tratamiento de datos personales, por lo que forma parte del ámbito de supervisión de la autoridad competente para la protección de datos. La utilización de la vigilancia por videocámara para la prevención de delitos está actualmente siendo objeto de examen por un comité de investigación. Esté comité realizará una apreciación de la Ley sobre vigilancia general por videocámara, para determinar si es necesario introducir enmiendas. Comprobará igualmente el ámbito de aplicación de la Ley de protección de datos por lo que respecta a la vigilancia por videocámara y considerará la posibilidad de que sean necesarias leyes específicas en materia de tratamiento de datos personales en el contexto de la vigilancia por videocámara.

5. ÁREAS EN LAS QUE LA DIRECTIVA 95/46/CE NO ES APLICABLE EN TODO O EN PARTE

La Directiva no es aplicable al tratamiento de datos constituidos por imagen y sonido cuando éstos se utilizan con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado en ámbitos del Derecho penal, así como para el ejercicio de otras actividades que no están comprendidas en el ámbito de aplicación del Derecho comunitario[9]. No obstante, al incorporar la Directiva 95/46/CE en la normativa nacional, muchos Estados miembros cubrieron estos ámbitos de manera general, aunque estipularon excepciones específicas.

A) En cualquier caso, en algunos países, las operaciones de tratamiento realizadas con los fines mencionados anteriormente también están sujetas a garantías, en cumplimiento del Convenio nº 108/1981 y de las recomendaciones pertinentes del Consejo de Europa, así como de determinadas disposiciones nacionales (véase el apartado 2 del artículo 3 y el considerando 16 de la Directiva 95/46/CE). A la luz de estas características peculiares y de la existencia de disposiciones específicas también relacionadas con las actividades de investigación llevadas a cabo por autoridades policiales y judiciales, así como con fines de seguridad del Estado[10] (que pueden incluir vigilancia por videocámara «oculta», es decir, realizada sin informar sobre el lugar), esta categoría de operaciones de tratamiento no se abordará de manera detallada en el presente documento.

No obstante, al Grupo le gustaría destacar que, al igual que algunas otras operaciones de tratamiento de datos personales que tampoco están comprendidas en el ámbito de aplicación de la Directiva, la vigilancia por videocámara realizada por motivos de necesidad real de seguridad pública o para la detección, prevención y control de delitos deberá cumplir los requisitos establecidos en el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales y, en ambos casos, estar cubierta por disposiciones específicas conocidas por el público, estar relacionada con la prevención de riesgos *concretos* y delitos *específicos* y ser proporcional a éstos (por ejemplo, en locales expuestos a tales riesgos o en relación con acontecimientos públicos los cuales es razonablemente posible que den lugar a tales delitos[11]). Deberán tenerse en cuenta los efectos que producen los sistemas de vigilancia por videocámara (por ejemplo, el hecho de que las actividades ilegales puedan trasladarse a otras áreas o sectores) y deberá especificarse siempre claramente quién es el responsable del tratamiento, a fin de que los interesados puedan ejercer sus derechos.

Éste último requisito también tiene que ver con el hecho de que cada vez es más frecuente que la vigilancia por videocámara la realicen conjuntamente

---

9 Véase el considerando 16.

10 Cabe hacer referencia aquí a los principios establecidos por el Tribunal Europeo de Derechos Humanos en el asunto Rotaru contra Rumania, examinado el 4 de mayo de 2000. Véase más arriba.

11 Por ejemplo, una circular emitida en Francia el 22 de octubre de 1996 relativa a los lugares aislados y las tiendas que cierran tarde por la noche.

la policía y otras autoridades públicas (por ejemplo, autoridades locales) o entidades privadas (bancos, asociaciones deportivas, empresas de transporte, etc.), lo que conlleva un riesgo de confusión en cuanto al papel y la responsabilidad individuales en relación con las tareas que se van a realizar[12].

B) En segundo lugar, la Directiva no es aplicable a las operaciones de tratamiento realizadas por una persona física en el marco de una actividad meramente personal o familiar (véase el apartado 2 del artículo 3 y el considerando 12).

Si bien este supuesto puede ser pertinente cuando, por ejemplo, la vigilancia por videocámara la realiza una persona para controlar a distancia lo que ocurre dentro de su propia casa (por ejemplo, para evitar robos o en relación con la gestión de la llamada «e-family»), no ocurre lo mismo cuando el equipo de vigilancia por videocámara se ha instalado en el exterior de la casa o en las proximidades de un local privado, con vistas a proteger la propiedad o a garantizar la seguridad.

En este caso puede ser, en primer lugar, que el sistema no lo hayan puesto en marcha propietarios individuales para vigilar las puertas que dan acceso a su propiedad, sino más bien varios propietarios, con arreglo a un acuerdo, o un consorcio o comunidad de vecinos, con el objeto de controlar varias entradas y áreas de un bloque, lo que hace que la Directiva sea aplicable a las actividades pertinentes.

Siempre que el sistema se utilice en beneficio de un hogar individual y con el objeto de controlar una única puerta, un único descansillo, aparcamiento, etc., el hecho de que la Directiva no sea aplicable debido a su utilización exclusivamente personal, así como a la indisponibilidad de los datos para terceras partes, no exime al responsable del tratamiento de respetar los derechos e intereses legítimos de sus vecinos y demás personas de paso. En los Estados miembros de la UE, en realidad, estos derechos e intereses están protegidos, independientemente de los principios de la protección de datos, por las disposiciones generales (código civil) que protegen los derechos, la imagen, la vida familiar y el ámbito privado de las personas (pensemos, por ejemplo, en el ángulo visual de una cámara instalada en el exterior de un apartamento, lo que permite grabar, sistemáticamente, a los clientes de una clínica o un bufete de abogados situados en el mismo piso y, de este modo, inmiscuirse de manera ilegal en el secreto profesional).

Deberá prestarse especial atención a la orientación del equipo de vídeo, a la obligación de enviar avisos e información y al borrado oportuno de las

[12] Un ejemplo significativo de este riesgo lo constituyen las actividades que llevan a cabo varios municipios de Italia a fin de controlar, mediante vigilancia por videocámara, zonas públicas frecuentadas por la noche por prostitutas. En el pasado, algunos municipios reclamaron su competencia en la prevención de este fenómeno (lo cual es discutible), mientras que otros únicamente emitieron mandatos en los que se prohibía a los clientes de las prostitutas aparcar o conducir sus vehículos en esas zonas y se les amenazaba con enviar una fotografía a sus hogares si no obedecían. La autoridad competente italiana ha adoptado una decisión a fin de aclarar cuáles son las medidas adecuadas para la acusación de violación de las disposiciones pertinentes.

imágenes (en el plazo de unas horas) si no se ha producido allanamiento de morada ni otros delitos.

C) Por último, en el artículo 9 de la Directiva se estipula que los Estados miembros establecerán exenciones y excepciones respecto de algunas de las disposiciones cuando el tratamiento se realice con fines exclusivamente periodísticos o de expresión artística o literaria, en particular en el sector audiovisual (véase el considerando 17). Sólo se establecerán excepciones en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión[13]. En este sentido, se prestará especial atención a la hora de instalar cámaras *web* o cámaras virtuales, a fin de evitar defectos y carencias en la protección de las personas físicas en el marco de la vigilancia por videocámara con fines que resulte que consisten en actividades publicitarias o de promoción turística[14].

6. VIGILANCIA POR VIDEOCÁMARA Y TRATAMIENTO DE DATOS PERSONALES

A la luz de las diversas situaciones mencionadas, el Grupo considera 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 fichero.

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 (PIN) captados durante la vigilancia de cajeros automáticos;

c) independientemente del método utilizado para el tratamiento (por ejemplo, sistemas de vídeo 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 límite de velocidad y no tiene nada que ver

---

13 Véase la Recomendación 1/97 del Grupo sobre la Ley de protección de datos y los medios.

14 Una cámara *web* instalada subrepticiamente cerca de las escaleras que conducen a la salida de una estación de metro de Milán mostraban directamente en la red imágenes de las partes íntimas de mujeres que pasaban por ahí, con fines aparentemente relacionados con actividades periodísticas. El hecho de que las personas implicadas no pudieran ser identificadas evitó que la autoridad nacional de protección de datos tomara medidas en el asunto.

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 provechosa 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 tráfico en las autopistas.

7. OBLIGACIONES Y PRECAUCIONES ADECUADAS RELATIVAS AL RESPONSABLE DEL TRATAMIENTO DE DATOS

A) Legalidad del tratamiento

Habida cuenta de que el tratamiento deberá ser lícito (véase la letra a) del artículo 6 de la Directiva), el responsable del tratamiento verificará previamente si la vigilancia cumple las disposiciones generales y específicas del sector (como leyes, reglamentos o códigos de conducta con pertinencia legal). Dichas disposiciones también han podido establecerse por motivos de seguridad pública o por motivos diferentes a los relativos a la protección de datos personales (por ejemplo, la necesidad de obtener autorizaciones *ad hoc* por parte de organismos administrativos específicos y de cumplir sus instrucciones).

Se tomarán todas las medidas adecuadas para garantizar que la vigilancia por videocámara cumple los principios de la protección de datos, y se evitarán las referencias inadecuadas a la intimidad[15].

En este sentido, también se tendrán en cuenta las buenas prácticas que figuren en las recomendaciones elaboradas por autoridades de control o en otros instrumentos de autorregulación.

[15] Recientemente, un banco y una comisaría local fueron incapaces de satisfacer la solicitud de un cliente, que pedía que, de las imágenes grabadas por una cámara que también filmaba un cajero automático, se extrajeran las correspondientes a un ladrón que, tras robar la tarjeta de crédito del cliente, la había utilizado para sacar dinero ilegalmente en dicho cajero (por motivos supuestamente relacionados con la «intimidad»).

Conviene, también, verificar las demás disposiciones nacionales (incluidos los principios constitucionales y los códigos civiles y penales), en particular las que se refieren al «derecho a la imagen»[16] o a la protección del domicilio propio; deberá tenerse en cuenta la jurisprudencia pertinente, en la que es posible que se establezca que algunos lugares fuera del hogar (como habitaciones de hotel, oficinas, aseos, cabinas telefónicas interiores, etc.) se considerarán lugares privados.

Cuando el equipo haya sido instalado por entidades privadas o por organismos públicos, en particular por autoridades locales, supuestamente por motivos de seguridad o para detectar, prevenir y controlar delitos, se prestará especial atención, a la hora de determinar dichos motivos o informar sobre ellos, a las tareas que debe realizar el responsable del tratamiento con arreglo a la normativa (teniendo en cuenta que, según la normativa, determinadas funciones públicas sólo pueden ser ejercidas por organismos no administrativos específicos, en concreto, por la autoridad competente).

Esta cuestión se ha planteado de manera específica con respecto a unas cuantas autoridades locales que no tienen competencia directa en los asuntos del orden público y la seguridad pública, y que, no obstante, realizan actividades auxiliares destinadas a la vigilancia. De la misma forma, la vigilancia, para cuya justificación se suele aducir su utilización en el control de la delincuencia, en realidad tiene como objetivo aportar pruebas en caso de que se cometan delitos.

B) Especificidad, especificación y legalidad de los fines

El responsable del tratamiento se asegurará de que los fines sean claros e inequívocos, también con el objeto de ofrecer un criterio preciso a la hora de evaluar la compatibilidad de los fines perseguidos por el tratamiento (véase la letra b) del artículo 6 de la Directiva).

Esta claridad también es necesaria con vistas a enumerar los fines, tanto en la información que se facilitará a los interesados como en la notificación pertinente, así como en lo relativo al control previo que posiblemente se lleve a cabo en relación con el tratamiento, de conformidad con el artículo 20 de la Directiva.

Quedará claramente excluido que las imágenes captadas puedan ser utilizadas con otros fines, en concreto en lo que se refiere a las posibilidades técnicas de reproducción (por ejemplo, prohibiendo expresamente su copia).

Se hará referencia a los fines pertinentes en un documento en el que también se resumirán otras características importantes de la política de privacidad (respecto a cuestiones tan importantes como el momento en que se borran las imágenes, las posibles peticiones de acceso por parte de los interesados y la consulta lícita de los datos).

C) Principios relativos a la legitimación del tratamiento de datos

[16] En Francia y en Bélgica, este derecho requiere «consentimiento previo».

El responsable del tratamiento verificará que la vigilancia por videocámara no sólo cumple las disposiciones específicas a las que se hace referencia en el apartado A), sino también, como mínimo, uno de los principios relativos a la legitimación del tratamiento de datos que figuran en el artículo 7 de la Directiva (con relación específica a la protección de datos personales).

Aparte de los casos, menos frecuentes, en los que debe cumplirse una obligación legal (se ha hecho referencia a las actividades en un casino) o en los que el tratamiento es necesario para proteger intereses vitales (por ejemplo, para el control a distancia de pacientes en unidades de reanimación), a menudo es necesario que el responsable del tratamiento cumpla una misión de interés público o inherente al ejercicio del poder público, posiblemente a través del cumplimiento de normativa específica (por ejemplo, para detectar delitos de tráfico o comportamientos violentos en medios de transporte públicos en zonas de alta criminalidad), con arreglo a la letra e) del artículo 7 de la Directiva; por otra parte, el responsable del tratamiento puede perseguir un interés legítimo sobre el que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado (véase la letra f) del artículo 7).

En ambos casos y, en particular, en éste último, la naturaleza sensible de las operaciones de tratamiento requiere un análisis minucioso del ámbito de las misiones, los poderes y los intereses legítimos relativos al responsable del tratamiento. A la hora de realizar dichos análisis, deberán evitarse totalmente la superficialidad y la extensión sin fundamento del ámbito de dichas misiones y poderes.

En lo que se refiere, en concreto, al equilibrio entre los diferentes intereses, deberá prestarse especial atención (escuchando previamente a las partes interesadas) a la posibilidad de que un interés que merezca protección pueda entrar en conflicto con la instalación del sistema o con determinados acuerdos de retención de datos u otras operaciones de tratamiento[17].

Por último, en lo relativo a la obtención del consentimiento del interesado, éste último deberá ser inequívoco y estar basado en información clara. El consentimiento se otorgará por separado y estará específicamente vinculado a las actividades de vigilancia relativas a un lugar en el que se desarrolle la vida privada de una persona[18].

La legalidad del tratamiento se evaluará teniendo en cuenta las disposiciones de la Directiva por las que se establecen garantías específicas en cuanto al tratamiento de datos relativos a infracciones (véase el apartado 5 del artículo 8 de la Directiva)[19].

---

17 En la letra b de la sección 6 de la nueva Ley federal alemana de protección de datos, que entró en vigor el 23 de mayo de 2001, la observación de zonas abiertas al público mediante dispositivos ópticos y electrónicos está permitida si, entre otras cosas, no hay motivos para pensar que prevalecen intereses del titular de los datos que deben ser protegidos.

18 Se prestará especial atención a la posibilidad real de manifestar un consentimiento válido en el sentido contemplado en la letra h) del artículo 2 de la Directiva 95/46/CE («toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan») en caso de instalación de vigilancia por videocámara en una copropiedad (comunidad de vecinos, etc.).

19 Cabe hacer referencia aquí al artículo 8 de la Ley portuguesa nº 67/98 en lo relativo a los datos concernientes a personas sospechosas de haber participado en actividades ilegales o criminales.

Podrán tomarse medidas y disposiciones adicionales como resultado de la evaluación preliminar del tratamiento con arreglo al mecanismo de control previo, cuando la vigilancia por videocámara implique riesgos específicos para los derechos y libertades de los interesados (véase el artículo 20 de la Directiva 95/46/CE).

Cuando las operaciones de tratamiento mediante vigilancia por videocámara las llevan a cabo organismos públicos, deberán basarse siempre en disposiciones legales específicas.

D) Proporcionalidad del recurso a la vigilancia por videocámara

El principio según el cual los datos deberán ser adecuados y proporcionales al fin perseguido significa, en primer lugar, que el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir:

con fines que realmente justifiquen el recurso a tales sistemas.

Dicho principio de proporcionalidad supone que se pueden utilizar estos sistemas cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no requieran captación de imágenes (por ejemplo, la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, sistemas mejores y más potentes de alumbrado nocturno en las calles, etc.) resulten claramente insuficientes o inaplicables en relación con los fines legítimos mencionados anteriormente.

El mismo principio también es aplicable a la selección de la tecnología adecuada, los criterios de utilización del equipo en concreto y la especificación de disposiciones para el tratamiento de datos en relación también con las normas de acceso y el período de retención.

Deberá evitarse, por ejemplo, que un organismo administrativo pueda instalar equipos de vigilancia por videocámara en relación con infracciones de menor importancia (por ejemplo, para reforzar la prohibición de fumar en los colegios y otros lugares públicos o la prohibición de tirar colillas y papeles al suelo en los lugares públicos).

Dicho de otro modo, es necesario aplicar, caso por caso, el *principio de idoneidad* con respecto a los fines perseguidos, lo que implica una especie de *obligación de minimización de los datos* por parte del responsable del tratamiento.

Si bien un sistema proporcionado de vigilancia por videocámara y alerta puede considerarse lícito cuando se producen varios episodios de violencia en una zona próxima a un estadio o se cometen agresiones repetidas a bordo de autobuses en zonas periféricas o cerca de las paradas de autobús, no ocurre lo mismo cuando se trata de un sistema destinado a evitar que se insulte a los conductores de autobús o que se ensucien los vehículos (tal y como le ha sido descrito a una autoridad de protección de datos), a identificar a ciudadanos responsables de infracciones de menor importancia, como dejar las bolsas de basura fuera del cubo o en zonas en

las que está prohibido tirar basura, o a detectar a personas responsables de robos ocasionales en piscinas cubiertas.

La proporcionalidad deberá evaluarse basándose en criterios más estrictos en lo que se refiere a lugares cerrados al público.

El intercambio de información y experiencias entre las autoridades competentes de los diferentes Estados miembros puede ser útil en este sentido[20].

Las consideraciones anteriores se refieren, en concreto, al uso cada vez más frecuente de vigilancia por videocámara con fines de autodefensa y protección de la propiedad (sobre todo, cerca de edificios públicos y oficinas, incluidas las áreas circundantes). Para este tipo de utilización se requiere la evaluación, desde un punto de vista más general, de los efectos indirectos derivados del recurso masivo a la vigilancia por videocámara (es decir, si la instalación de varios dispositivos es realmente un factor disuasorio o si los infractores o vándalos pueden, simplemente, desplazarse a otras zonas y actividades).

E) Proporcionalidad en la realización de actividades de vigilancia por videocámara

El principio según el cual los datos deben ser adecuados, pertinentes y no excesivos implica la evaluación minuciosa de la *proporcionalidad de las medidas* relativas al tratamiento de datos, una vez que la legalidad del mismo haya quedado validada.

Las *medidas para la grabación* se establecerán teniendo en cuenta, en primer lugar, los siguientes aspectos:

a) El ángulo visual con arreglo a los fines perseguidos[21] (por ejemplo, si la vigilancia se realiza en un lugar público, el ángulo deberá establecerse de manera que no permita visualizar detalles o rasgos físicos que resulten irrelevantes para los fines perseguidos, o zonas situadas en el interior de lugares privados cercanos, en particular, si se utiliza el zoom).

b) El tipo de equipo que se utilizará para filmar, es decir, fijo o móvil.

c) Medidas reales de instalación, es decir, situación de las cámaras, utilización de plano fijo o cámaras móviles, etc.

---

20 Esto permitiría, además, armonizar mejor los enfoques reguladores y las decisiones administrativas, que, en algunos casos, no se han puesto de acuerdo (como ha ocurrido, por ejemplo, con las salas de bingo).

21 Se pueden encontrar ejemplos de precauciones específicas que deben tomarse en relación con el ángulo visual en dos disposiciones de la autoridad italiana de protección de datos. Un organismo de asistencia sanitaria tenía previsto crear un sistema que permitiese que los familiares de pacientes en coma, en cuarentena o con enfermedades graves, tratados en unidades de cuidados intensivos, pudieran observarlos continuamente desde la distancia, por lo que se comunicó a dicho organismo que debería tomar las medidas necesarias para evitar la visualización simultánea de otros pacientes. En otro caso, la autoridad señaló a los órganos administrativos de la policía que un sistema para la detección del exceso de velocidad sólo podía filmar las matrículas pertinentes y no el interior de los vehículos.

d) Posibilidad de aumentar las imágenes o realizar primeros planos, durante la grabación o después, es decir, una vez que se han almacenado las imágenes, y posibilidad de desenfocar o borrar imágenes individuales.

e) Congelación de imágenes.

f) Conexión con un «centro» para enviar señales de alarma sonoras o visuales.

g) Medidas que se toman como resultado de la vigilancia por videocámara, es decir, cierre de entradas, convocatoria del personal de vigilancia, etc.

En segundo lugar, deberá tenerse en cuenta la *decisión que se va a tomar en cuanto a la retención de las imágenes y el plazo* (éste último deberá ser bastante breve y estar en consonancia con las características específicas de cada caso).

Si bien en algunos casos un sistema que sólo permita la visualización de imágenes en circuito cerrado, sin necesidad de grabar, puede ser suficiente (por ejemplo, en el caso de las cajas de un supermercado), en otros (por ejemplo, para proteger lugares privados), puede que esté justificado grabar imágenes durante unas cuantas horas y borrarlas automáticamente, sin exceder nunca el final del día o, como mucho, el final de la semana. Obviamente, esta regla tiene excepciones, como cuando se emite una señal de alarma o se realiza una petición que merece especial atención; en esos casos, hay motivos suficientes para esperar, durante un período breve, una posible decisión por parte de las autoridades policiales o judiciales.

Por poner otro ejemplo, un sistema cuyo objetivo es detectar el acceso no autorizado de vehículos a centros urbanos y zonas de tráfico restringido, sólo deberá grabar imágenes en caso de que se cometa una infracción.

La cuestión de la proporcionalidad también deberá tenerse en cuenta debidamente siempre que se considere que son necesarios períodos de retención más breves, que no deberán superar una semana[22] (por ejemplo, imágenes de vigilancia por videocámara que puedan utilizarse para identificar a las personas que frecuentan un banco antes de que se cometa un robo).

En tercer lugar, deberá prestarse atención a los *casos en los que se facilita la identificación de una persona* mediante la asociación de imágenes del rostro de dicha persona con otra información relativa a conductas o actividades reproducidas (por ejemplo, en caso de asociación de imágenes y actividades realizadas por los clientes de un banco en un momento fácilmente identificable).

En este sentido, deberá tenerse en cuenta la clara diferencia que existe entre la retención temporal de imágenes de vigilancia por videocámara captadas con un equipo situado a la entrada de un banco y la creación de bancos de datos que incluyan fotos y huellas dactilares facilitadas por los clientes del banco con su consentimiento, lo que supone una intrusión en mayor medida.

[22] Las autoridades de protección de datos danesa y sueca se manifestaron a favor de que las grabaciones de imágenes sólo pudieran almacenarse durante un breve período que no excediera los treinta días.

Por último, deberá prestarse atención a las decisiones que se tomen con respecto tanto a la *posible comunicación de los datos a terceras partes* (lo que, en principio, no deberá implicar a entidades que no estén relacionadas con las actividades de vigilancia por videocámara) como a su *posible revelación, total o parcial, en el extranjero o, incluso, en la red* (también a la luz de las disposiciones relativas a la protección adecuada; véase el artículo 25 y siguientes de la Directiva).

Obviamente, el requisito según el cual las imágenes deberán ser pertinentes y no excesivas, también se refiere a la combinación de información procedente de diferentes responsables del tratamiento de sistemas de vigilancia por videocámara.

Las garantías mencionadas más arriba pretenden implantar, también de manera operacional, el principio al que se hace referencia en la normativa nacional de varios países: *el principio de moderación en el uso de datos personales* (cuyo objetivo consiste en evitar o reducir al mínimo posible el tratamiento de datos personales).

Este principio debería aplicarse en todos los sectores, teniendo en cuenta, también, el hecho de que muchos objetivos pueden alcanzarse realmente sin recurrir a datos personales, o utilizando datos realmente anónimos, a pesar de que, inicialmente, pueda parecer necesario utilizar información personal.

Las consideraciones anteriores también son aplicables cuando se da la necesidad justificada de racionalizar los recursos comerciales[23] o de mejorar los servicios prestados a los usuarios[24].

F) Información a los interesados

La idoneidad y la naturaleza abierta de la utilización del equipo de vigilancia por videocámara implican el suministro de información adecuada a los interesados, con arreglo a los artículos 10 y 11 de la Directiva.

Los interesados serán informados con arreglo a los artículos 10 y 11 de la Directiva. Deberán estar al corriente de que la vigilancia por videocámara está en marcha, incluso cuando ésta esté relacionada con acontecimientos públicos y espectáculos o con actividades de publicidad (cámaras *web*); deberán ser informados de manera detallada sobre los lugares que se encuentran bajo control.

No es necesario especificar la ubicación precisa del equipo de vigilancia; sin embargo, deberá quedar bien claro el contexto de la vigilancia.

---

23 Podría ser el caso, por ejemplo, para calcular la cantidad de cajas que deben mantenerse abiertas simultáneamente en un supermercado, en función del número de clientes que entren, o para trazar itinerarios de compra optimizados para los clientes de un supermercado.

24 Para facilitar el acceso a un lugar de trabajo o a un medio de transporte específico para los que sea necesario realizar controles de identidad, puede ser suficiente con utilizar tarjetas con fotografía, si es posible en medios informáticos, sin necesidad de implantar un sistema de reconocimiento fisonómico.

La información deberá colocarse a una distancia razonable de los lugares controlados (a diferencia de lo ocurrido en algunos casos, en los que la colocación de las placas informativas a quinientos metros de las zonas vigiladas se ha considerado aceptable), incluso a la luz de las medidas tomadas para la grabación.

La información deberá estar a la vista y podrá suministrarse de manera resumida, a condición de que sea eficaz; podrá incluir símbolos que ya hayan resultado útiles en relación con la vigilancia por videocámara, así como indicaciones de prohibido fumar (lo que diferirá en función de si se graban o no imágenes). En todos los casos, deberá especificarse cuáles son los fines de la vigilancia por videocámara y quién es el responsable del tratamiento. El formato de la información deberá adaptarse a cada situación[25].

Sólo se permitirán restricciones específicas y bien fundadas a los requisitos informativos en los casos a los que se refieren los artículos 10, 11 y 13 de la Directiva (por ejemplo, podrá aplicarse una restricción temporal a los datos recogidos en el transcurso de investigaciones realizadas, en el marco de la Ley, por el abogado defensor, o con vistas a ejercer el derecho a la defensa, siempre y cuando la aportación de información pueda poner en peligro el logro de los fines específicos perseguidos).

Por último, se prestará especial atención al modo adecuado de facilitar la información a las personas invidentes.

G) Requisitos adicionales

En relación con estos requisitos adicionales, precauciones y garantías (tal y como se mencionan en la normativa sobre protección de datos y se resumen más arriba, en el punto 3), así como con relación a la necesidad de que el tratamiento de datos personales sea notificado a una autoridad independiente y esté sujeto a la supervisión de la misma con arreglo a los artículos 18, 19 y 28 de la Directiva, al Grupo le gustaría destacar, en concreto, las cuestiones siguientes:

a) Un número limitado de personas físicas, que deberá especificarse, estará autorizado a visualizar o acceder a las imágenes grabadas, cuando existan, exclusivamente para los fines perseguidos por la vigilancia por videocámara o con vistas al mantenimiento del equipo en cuestión, a fin de verificar su funcionamiento; por otra parte, esto puede ocurrir en base a una petición de acceso del interesado o una orden emitida por una autoridad policial o judicial con fines de investigación criminal.

   Siempre que la vigilancia por videocámara esté destinada únicamente a prevenir, detectar y controlar infracciones, la solución consistente en utilizar dos claves de acceso (una de las cuales estaría en posesión del responsable del tratamiento y la otra de la policía) podrá resultar útil en muchos casos para garantizar que las imágenes sólo las verá la policía, y no personal sin autorización (sin perjuicio de que el interesado ejerza su derecho legítimo de acceso a través de una solicitud presentada durante el breve período de retención de las imágenes).

[25] Esto podría calificarse de enfoque «modulado».

b) Deberán aplicarse medidas de seguridad, a fin de evitar que se produzcan las eventualidades a las que se hace referencia en el artículo 17 de la Directiva, incluida la difusión de información que pudiera ser útil para proteger un derecho del interesado, a una tercera parte o al propio responsable del tratamiento (también con vistas a evitar la manipulación, la modificación o la destrucción de datos y otros elementos que puedan servir de prueba).

c) La calidad de las imágenes grabadas, cuando existan, también es fundamental (en concreto si se utilizan repetidamente los mismos medios de grabación, lo que implica el riesgo de no borrar completamente imágenes grabadas previamente).

d) Por último, es fundamental que los operadores implicados en las actividades de vigilancia por videocámara estén adecuadamente formados y al corriente de las medidas que deben tomar para cumplir plenamente los requisitos pertinentes. También se podrá considerar una medida útil la formación de los responsables del tratamiento y de los operadores en cuestiones relacionadas con los riesgos pertinentes y en los mecanismos para la correcta identificación de los sujetos que aparecen en la imagen.

H) Derechos del interesado

El carácter peculiar de los datos personales recogidos no impide que los interesados ejerzan los derechos a los que se hace referencia en los artículos 13 y 14 de la Directiva, prestando especial atención al derecho de oposición al tratamiento. De hecho, con arreglo a la Directiva 95/46, el interesado podrá oponerse, en cualquier momento, al tratamiento de datos que le conciernan[26] por razones legítimas propias de su situación particular.

El derecho del interesado al olvido y la usual brevedad del período de retención de las imágenes reducen el ámbito de aplicación del derecho del interesado a acceder a los datos personales que lo hacen identificable; no obstante, este derecho deberá protegerse especialmente en caso de que tenga lugar una petición detallada, como permitir la fácil recuperación de las imágenes pertinentes. Asimismo, deberá tenerse en cuenta la necesidad de proteger temporalmente los derechos de terceras partes.

Cualquier restricción basada en los esfuerzos necesarios para recuperar las imágenes, cuando dichos esfuerzos resulten claramente desproporcionados en materia de investigación, coste y recursos, a causa de la brevedad del período de retención de las imágenes, se establecerá únicamente a través del Derecho derivado (véase el primer apartado del artículo 13 de la Directiva) y se prestará la debida atención al derecho del interesado a la defensa con respecto a acontecimientos específicos que puedan haber ocurrido en el período considerado.

[26] Excepto en los casos en los que la legislación nacional disponga lo contrario.

I) Garantías adicionales relacionadas con operaciones de tratamiento específicas

Se prohibirá la vigilancia por videocámara realizada exclusivamente a causa del origen racial de las personas, sus ideas políticas o religiosas, su pertenencia a sindicatos o sus hábitos sexuales (véase el artículo 8 de la Directiva).

Sin pretender establecer una lista exhaustiva de las diversas aplicaciones de la vigilancia por videocámara, el Grupo desea hacer hincapié en la necesidad de prestar más atención (en principio, cuando resulte apropiado, en el marco del control previo de las operaciones de tratamiento al que hace referencia el artículo 20 de la Directiva) a unos cuantos contextos en los que se recogen imágenes relativas a personas identificadas o identificables, ya que dichos contextos deberán evaluarse caso por caso.

Se hace referencia, en concreto, a los siguientes supuestos como resultado de experiencias o pruebas que ya están en marcha:

a) Interconexión permanente de sistemas de vigilancia por videocámara gestionados por diferentes responsables del tratamiento.
b) Posible asociación de imágenes y datos biométricos como huellas dactilares (por ejemplo, a la entrada de bancos).
c) Utilización de sistemas de identificación vocal.
d) Introducción, con arreglo a principios de proporcionalidad y en base a disposiciones específicas, de sistemas de indexación relativos a imágenes grabadas o sistemas de recuperación simultánea automática, en particular a través de datos de identificación.
e) Utilización de sistemas de reconocimiento fisonómico que no se limiten a la identificación de camuflajes de personas de paso, como barbas y pelucas falsas, sino que se basen en la localización de presuntos delincuentes, es decir, en la capacidad del sistema para identificar automáticamente a determinados individuos, a partir de plantillas o retratos robot que resulten de determinados rasgos externos (como el color de la piel o los ojos, la prominencia de los pómulos, etc.) o con arreglo a comportamientos anormales predefinidos (movimientos repentinos, paso por el mismo lugar incluso a intervalos determinados, manera de aparcar un vehículo, etc.). En este sentido, la intervención humana también es adecuada a la luz de los posibles errores que ocurran en tales casos, como se menciona más abajo, en el punto f).
f) Posibilidad de localizar, automáticamente, itinerarios y pistas, o de reconstruir o prever el comportamiento de una persona.
g) Toma de decisiones automatizadas basadas en el perfil de una persona o en análisis inteligentes y sistemas de intervención que no estén relacionados con señales de alarma estándar (como el hecho de entrar en un lugar sin la identificación necesaria o una alarma de incendio).

8. VIGILANCIA POR VIDEOCÁMARA EN EL CONTEXTO LABORAL

Este Grupo, ya en su «Dictamen nº 8/2001 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[27], puso de relieve, de manera más general, unos cuantos 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)[28].

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 cuándo ésta se revelará a las autoridades judiciales. En el contexto laboral, la información facilitada en forma de símbolo, por ejemplo, no se considerará suficiente.

9. CONCLUSIÓN

El Grupo ha elaborado el presente documento de trabajo para contribuir a la aplicación uniforme de las medidas nacionales adoptadas en el marco de la Directiva 95/46/CE, en el ámbito de la vigilancia por videocámara.

*** * ***

27 Ambos documentos están disponibles en la siguiente dirección: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index/htm.

28 En estos casos, además de las consideraciones realizadas en el presente documento, deberá tenerse en cuenta también, de manera específica, la necesidad de respetar los derechos a los que se hace referencia en los acuerdos colectivos, que a veces se basan en la información colectiva de empleados o de sus sindicados correspondientes (es decir, aparte de la información que deberá facilitarse sobre la persona, de conformidad con las leyes de protección de datos); en otros casos, deberá firmarse un acuerdo previo con los representantes de los empleados o con los sindicatos en cuanto a la aplicación de medidas, también en lo que se refiere a la duración de la vigilancia y otras medidas relativas a la grabación. En algunos países, puede ser necesaria la intervención del Estado si las partes implicadas no se ponen de acuerdo.

En este contexto, también es fundamental que los Estados miembros aporten directrices relativas a la actividad de los productores, proveedores de servicios y distribuidores, e investigadores, con vistas al desarrollo de tecnologías, programas informáticos y dispositivos técnicos en consonancia con los principios a los que se hace referencia en el presente documento.

*** * ***

Hecho en Bruselas, el 11 de febrero de 2004
Por el Grupo
El Presidente
Stefano RODOTA