JOSÉ LUIS GOÑI SEIN
Catedrático de Derecho del Trabajo y de la Seguridad Social
Universidad Pública de Navarra

LA VIDEOVIGILANCIA EMPRESARIAL Y LA PROTECCIÓN DE DATOS PERSONALES

THOMSON
CIVITAS

Primera edición, 2007

Editorial Aranzadi, SA
Camino de Galar, 15
31190 Cizur Menor (Navarra)
ISBN: 978-84-470-2701-9
Depósito Legal: NA 418/2007
Fotocomposición: Editorial Aranzadi, SA
Impresión: Rodona Industria Gráfica, SL
Polígono Agustinos, Calle A, Nave D-11
31013 - Pamplona

CAPÍTULO II

EL CONTROL EMPRESARIAL POR MEDIO DE CÁMARAS DE VÍDEO Y LA PROTECCIÓN DE DATOS

CAPÍTULO II

EL CONTROL EMPRESARIAL POR MEDIO DE CÁMARAS DE VÍDEO Y LA PROTECCIÓN DE DATOS

1. Claves jurídicas aplicables a la videovigilancia en el lugar de trabajo: el derecho a la autodeterminación informativa

La doctrina constitucional, que acabamos de referir, se caracteriza por observar el problema de la admisibilidad de los medios audiovisuales de control en los lugares de trabajo, desde un único aspecto configurativo del derecho subjetivo de la protección de la intimidad. La cuestión es analizada básicamente desde la perspectiva del derecho de intimidad negativa o excluyente, aunque se defina con cierta «holgura», alcanzando, tanto a la intimidad *strictu sensu,* que garantiza *«un ámbito propio y reservado frente a la acción y conocimiento de los demás»* (STC 231/1988, entre otras), como a la vida privada, que ofrece una mayor latitud.

Así, en el juicio de legitimidad de la instalación y empleo del sistema de vigilancia audiovisual lo que se valora es simplemente si se producen intromisiones ilegítimas en la intimidad de los trabajadores en los centros de trabajo, en ese espacio más o menos reducido pero irreductible de libertad y de vida privada en la relación de trabajo, que padece con la simple instalación de videocámaras por cuanto el trabajador se va a sentir constreñido de realizar cualquier acto o comentario ante el convencimiento de que van a ser escuchados y grabados por la empresa. Y, en consecuencia, los principios que se han sentado al respecto se limitan a reconocer al trabajador un cierto ámbito libre de intromisiones frente a las modalidades de control del empresario.

Pero, la intimidad, aun nutriéndose fundamentalmente en su aspecto externo de facultades de exclusión, comprende también una dimensión positiva, que también ha sido destacada por el Tribunal Constitucional. Es el derecho al control activo de las informaciones que afectan a la persona

y a no ser instrumentalizado a través del conocimiento adquirido de aspectos de su personalidad. El avance tecnológico y el desarrollo de los sistemas de comunicación han llevado al Tribunal Constitucional a incluir dentro de la estructura de este derecho no sólo el poder de resguardar un ámbito reservado frente al conocimiento no consentido de los demás, sino la protección de un interés que se conecta con el libre desarrollo de la personalidad, y que comporta un ámbito de poder que alcanza entre otros aspectos el de disposición de sus propios datos personales.

Esta dimensión positiva del derecho a la intimidad ha sido reconocida, entre otras, en la STC 119/2001, que considera que, para garantizar la efectividad del derecho *«se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada»*. La sentencia mantiene que la delimitación del derecho a la intimidad debe hacerse en función del libre desarrollo de la personalidad. Es decir, que la libertad vendría a delimitar su ámbito de actuación[1].

Este derecho mantiene una zona de intersección con otro instituto de garantía de los derechos fundamentales, previsto en el art. 18.4 CE, *«que es, además, en sí mismo, un derecho fundamental, el derecho a la libertad frente las potenciales agresiones a la dignidad y a la libertad de la persona provenientes del uso ilegítimo del tratamiento automatizado de datos»*, y que se ha dado en llamar la *«libertad informática»*. Es un derecho fundamental que garantiza a la persona un poder de control y de disposición sobre sus datos personales, que supone el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos (STC 290/2000)[2].

---

[1] Cfr. X. ARZOZ SANTISTEBAN: «Videovigilancia y derechos fundamentales: análisis de la constitucionalidad de la Ley Orgánica 4/1997», *Revista Española de Derecho Constitucional*, nº 64, 2002, pág. 142.

[2] Se ha dicho del derecho a la intimidad que es un derecho que «incluye el derecho a la autodeterminación informativa, que supone controlar las informaciones que afectan a la persona y a evitar un uso ilegítimo del tratamiento mecanizado de los que se almacenan en el ordenador y al acceso, la rectificación y la cancelación de las mismas y de protección frente a potenciales agresiones a la esfera privada de la persona derivadas del uso ilegítimo de la informática» (M. RODRÍGUEZ-PIÑERO Y BRAVO FERRER: «Intimidad del trabajador y contrato de trabajo», *Relaciones laborales*, nº 8 abril, 2004, pág. 1). Esta asimilación resulta excesiva y

La apreciación de la licitud de las medidas de control audiovisual en el lugar de trabajo no debería producirse únicamente en relación con la dimensión negativa (el *ius excludendi*) del derecho a la intimidad del trabajador, porque ello nos lleva a considerar únicamente una serie de elementos o manifestaciones de la intimidad del trabajador, y el derecho a la intimidad tiene hoy –como se acaba de señalar– una sustantividad específica que va más allá de la determinación espacial del derecho a la intimidad.

La instalación de los medios de videovigilancia afecta a ese otro poder de control y disposición de datos personales intrínseco al derecho a la intimidad, dado que los dispositivos permiten no sólo la captación sino la grabación de imágenes y sonidos, todo lo cual es susceptible de ser conservado, analizado y utilizado para diversos fines[3]. Hasta ahora se ha aceptado acríticamente la adopción de aquellos mecanismos de control en el ámbito laboral, sin tener en cuenta los principios fundamentales de protección de datos, hasta el punto de que no existe conciencia de que el control a través de sistemas audiovisuales implica también tratamiento de datos personales.

---

conlleva criterios poco diferenciadores. Hay una necesidad de reconsiderar la admisión en la intimidad de la libertad informática. No resulta exacto afirmar que dentro del derecho a la intimidad se encuentre el derecho de todo individuo a la protección de datos que le conciernen, o que éste sea una manifestación concreta del derecho a la intimidad. Una cosa es que ambos derechos participen de contenidos o rasgos comunes, en la medida en que estén implicados aspectos íntimos de la persona o que, a través de un análisis o tratamiento de informaciones que han perdido la condición de íntimos o secretos, se pueda acceder a la vida íntima, y otra cosa distinta es que la tutela informática se configure como una parte del derecho a la intimidad. Puede haber una zona de concurrencia derivado del interés común en mantener preservado y oculto una parte de la personalidad de la persona, pero lo protegido por el derecho a la autodeterminación informativa es más que la intimidad de la persona; es el derecho a disponer de todas las informaciones atinentes a su persona. Lo protegido no es sólo el espacio resguardado de la curiosidad ajena sino el derecho en general de la personalidad, la identidad, el patrimonio moral de la persona, mediante la posibilidad de ejercer un control sobre todo ello. En este derecho quedan cubiertos aspectos o manifestaciones que no cabría calificar de íntimos o privados. El Tribunal Constitucional, aun asumiendo que los dos derecho se concatenan, no deja de reconocer –como hemos visto en la STC 290/2000– que este último «constituye en sí mismo un derecho o libertad fundamental».

[3] Vid. L. A. FERNÁNDEZ VILLAZÓN: *Las facultades empresariales de control...*, op. cit., pág. 83.

La conformidad constitucional de la instalación se examina sólo en lo que conlleva de investigación en la zona nuclear de la personalidad y de perturbación psicológica en los trabajadores objeto de observación, relegando a un segundo plano, cuando no, obviando, el juicio de procedencia en relación con la posibilidad, condiciones y alcance del tratamiento de los datos en forma de imagen y sonido en el contexto laboral. Se omite, así, algo tan obvio como es la necesidad de un juicio previo sobre la legitimidad del interés empresarial, de tal manera que muchos dispositivos de control audiovisual se adoptan unilateralmente, bajo cualquier interés empresarial, presumiendo la legitimidad de la finalidad. Como ha destacado MARTÍNEZ FONS[4], el juicio de procedencia del control se traslada al momento de aplicación de los dispositivos de control, presumiendo incontestables las facultades empresariales de adopción de instrumentos de control hasta el instante de su efectiva aplicación.

Tampoco está previsto procedimiento alguno, en el que haya de garantizarse la transparencia y proporcionalidad. Tan sólo una consulta previa a los representantes legales [art. 64.1.4.d) ET], requisito procedimental que ha quedado desprovisto de toda virtualidad, al negar el TC en la STC 186/2000 dimensión constitucional. Las medidas se adoptan, pues, sin estar sujeto el empresario a un régimen de autorización previa, en el que pueda ejercerse un control de legitimidad e introducir restricciones y condiciones de uso necesarias.

Por otra parte, tampoco se tiene en cuenta el control *a posteriori* sobre el contenido de lo filmado, su conservación, y tratamiento, o la identificación de los responsables, ni se plantea la protección especial en lo que respecta al acceso de esas imágenes, o la posibilidad de que los trabajadores puedan ejercer su derecho de acceso y cancelación de las grabaciones que no son pertinentes o resultan excesivas con relación al fin para el que se recabaron.

Con todas esta limitaciones, el juicio de legitimidad de los sistemas de control audiovisual, basado únicamente en la dimensión de exclusión del derecho a la intimidad, resulta claramente insuficiente, por cuanto no atiende a todos los riesgos que supone la implantación de tales sistemas

---

[4] Ibídem, pág. 256.

de control, y quedan extramuros de la evaluación otros derechos de la persona como los que derivan de la normativa de protección de datos.

La orientación renovada del derecho a la intimidad y la reafirmación de un derecho autónomo a «controlar el flujo de informaciones relativas a la propia persona, sean éstas o no parte del ámbito íntimo en sentido estricto»[5], que se conecta a la garantía reconocida en el art. 18.4 CE, apunta rotundamente a favor de la unificación de todos los riesgos que derivan de la instalación de dichos dispositivos audiovisuales, así como de todos los derechos que entran en juego, por lo que la ponderación de intereses en tal caso debería hacerse no sólo desde la vertiente negativa del derecho, sino tomando en consideración también esa otra vertiente positiva del derecho a la intimidad, consistente en el poder de control y de autodeterminación informativa sobre datos personales, que otorga al trabajador el derecho a saber si se están grabando su imagen y conversaciones, a qué uso se están sometiendo, y el derecho a oponerse, en su caso, a esa posesión y uso.

2. La orientación internacional tendente a situar los límites de la videovigilancia en el ámbito de la protección de datos

La delimitación jurídica del espacio legítimo del poder de control audiovisual debería realizarse en el marco de la normativa de tratamiento de datos personales, toda vez que es, además, la perspectiva desde la que se viene observando y analizando actualmente la utilización de las técnicas de videovigilancia empresarial en distintas instancias internacionales, tanto supracomunitarias, como comunitarias.

A. Repertorio de Recomendaciones Prácticas de la OIT de octubre de 1996, sobre protección de los datos personales de los trabajadores[6]

Un enfoque del problema de la videovigilancia en la clave que venimos apuntando lo impulsó ya hace algún tiempo, la Organización Interna-

---

[5] R. Tascón López: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*, Madrid, Thomson-Civitas, APDCM, 2005, pág. 32.

[6] Oficina Internacional del Trabajo: *Protección de los datos personales de los trabajadores*, Ginebra, Oficina Internacional del Trabajo, 1997.

cional de los Trabajadores en el Repertorio de Recomendaciones Prácticas, adoptado en octubre de 1996 en Ginebra, en cumplimiento de una decisión tomada por el Consejo de Administración de la OIT en su 264ª reunión.

A diferencia de otros instrumentos de la OIT (convenios, recomendaciones), el Repertorio no comporta obligación alguna, y tiene por objeto suministrar orientaciones para la protección de datos personales de los trabajadores, bien para elaborar leyes, reglamentaciones, o bien para una regulación convencional o para adoptar medidas prácticas.

Dicho Repertorio contiene una serie de principios generales sobre protección de datos personales de los trabajadores, y disposiciones específicas respecto del acopio, conservación, almacenamiento, uso y comunicación de tales datos, inspirados en principios contemplados en instrumentos internacionales de protección de datos, como las líneas directrices de la OCDE, y el Convenio nº 108/1981 del Consejo de Europa.

Los referidos principios se aplican a la vigilancia empresarial, que *«engloba, sin limitarse a ella, la utilización de dispositivos como computadoras, cámaras de fotografía, cine y vídeo, aparatos de grabación sonora, teléfonos u otro material de comunicación, diferentes métodos de identificación y de localización y cualesquiera otros sistemas de vigilancia»* (3.3), en la medida en que implica tratamiento de datos personales del trabajador. Procede indicar que el Repertorio define el término *«tratamiento»* de forma amplia, abarcando *«el acopio, la conservación, la combinación, la comunicación o cualquier otra forma de utilización de datos personales»* (3.1).

Respecto del acopio de datos personales del trabajador, el Repertorio aboga, aparte de por la necesidad de demostrar la idoneidad de los datos personales que se acopian, por un principio de transparencia máxima, de forma tal que los trabajadores sepan la finalidad para la cual se someten a tratamiento los datos. Así se establece que *«cuando los trabajadores sean objeto de medidas de vigilancia, éstos deberían ser informados de antemano de las razones que las motivan, de las horas en que se aplican, de los métodos y técnicas utilizados y de los datos que serán acopiados»* (6.14).

El Repertorio obliga, además, a los empresarios a tener en cuenta las consecuencias que puede tener la vigilancia respecto de la vida privada y a dar preferencia a los medios que tengan los menores efectos en ese plano, al indicar que *«el empleador deberá reducir al mínimo su injerencia en la vida privada de aquéllos»* (6.14).

En cuanto a la vigilancia permanente o secreta, el Repertorio adopta un enfoque decididamente restrictivo, toda vez que *«se ha probado que una vigilancia permanente es causa de una ansiedad constante, que a su vez puede originar enfermedades físicas o perturbaciones psicológicas»* (Comentario del Repertorio de Recomendaciones Prácticas). Considera, así, que la vigilancia permanente *«se debe limitar a los casos en donde la vigilancia es necesaria para hacer frente a problemas específicos relacionados con la salud y la seguridad o la protección de los bienes»* (Comentario al punto 6.14.3).

Con idéntico carácter restrictivo, se indica que la vigilancia secreta sólo es aceptable en la medida en que está prevista por ciertas disposiciones de la legislación nacional o cuando existan sospechas suficientes de actividad delictiva u otras infracciones graves. No obstante, puntualiza esta excepción, destacando que *«no basta con sospechar tales actividades o infracciones»*, *sino que el empresario «está autorizado al uso de la vigilancia secreta únicamente cuando existan sospechas razonablemente justificadas»* (Comentario al punto 6.14.2).

Al tratar de los fines específicos del acopio, se apuesta por evitar un uso plurifuncional de los datos recabados. El Repertorio enuncia el principio, subrayado en todas las normas nacionales e internacionales en materia de protección de datos, según el cual *«los datos personales deberían utilizarse únicamente con el fin para el cual hayan sido acopiados»* (5.2) y somete toda nueva forma de utilización de los datos a dos condiciones: por un lado, que la nueva forma de utilización sea compatible con la finalidad inicial; y por otro, que el empleador adopte las medidas necesarias para evitar que la información quede tergiversada por haber cambiado el contexto (5.3).

Pero hay un caso en que prohíbe todo cambio de finalidad: es la utilización de las medidas adoptadas con miras a garantizar el funcionamiento seguro y adecuado de los centros informáticos y de los sistemas automati-

zados, para vigilar y juzgar el comportamiento y el rendimiento de los trabajadores (5.4). El Repertorio rechaza que se pueda ejercer un control permanente del trabajador por medio de medidas de seguridad; no obstante, entiende que no estaría sometido a esta restricción el descubrimiento accidental de infracciones no relacionadas con el objetivo de las medidas.

Una parte importante del Repertorio se dedica a prescribir los derechos individuales de los trabajadores sobre la protección de datos, que aparecen recogidos en la mayoría de las leyes sobre protección de datos. Se proclama, así y entre otros, el derecho de los trabajadores a tener acceso a todos sus datos personales independientemente de que sean objeto de un tratamiento automático o de que se conserven en un expediente manual o en cualquier otro fichero que comprenda datos personales suyos (11.2); el derecho a designar un representante de los trabajadores o de un compañero de su elección, que les ayude a ejercer el derecho de consulta (11.5); y el derecho de exigir la rectificación o la supresión de datos inexactos o incompletos, así como los sometidos a una forma de tratamiento que vulnere lo estipulado en el Repertorio.

Por último, el Repertorio reconoce un papel importante a los derechos colectivos en la protección de los trabajadores contra los riesgos provenientes del tratamiento de sus datos personales, al disponer, por un lado, que todas las negociaciones colectivas que tengan consecuencias para el tratamiento de datos personales de los trabajadores deberían regirse por los principios de protección de datos (12.1) y, por otro, que se debe informar y consultar a los representantes de los trabajadores en lo referente a la introducción o modificación de sistemas automatizados para el tratamiento de datos personales de los trabajadores, antes de la introducción de cualquier forma de vigilancia electrónica del comportamiento de los trabajadores en el lugar de trabajo [12.2.a) y b)].

B. Grupo Europeo de Comisarios sobre protección de datos personales (GTA)

Dentro de la Unión Europea, el Grupo de Trabajo sobre Protección de datos (GTA), instituido al amparo del artículo 29 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al trata-

miento de datos personales[7], ha encuadrado también en el ámbito del derecho a la autodeterminación informativa o del moderno derecho a la privacidad, la utilización de los dispositivos de vigilancia electrónica y el control que el empresario puede ejercer a través de los mismos.

El GTA 29 es un grupo consultivo compuesto por representantes de las autoridades de protección de datos de los Estados miembros, que actúa de forma independiente. Es, por tanto, un órgano de la Comunidad, que se ocupa, entre otras cosas, de examinar cualquier cuestión relativa a la aplicación de las medidas nacionales adoptadas en el marco de la Directiva sobre protección de datos, con el fin de contribuir a la aplicación uniforme de las mismas.

En su Dictamen nº 8/2001, *sobre tratamiento de datos personales en el contexto laboral*, sólo incidentalmente se ocupa del tema, pero asume ya claramente esta perspectiva, al afirmar que *«el tratamiento de datos en forma de imagen y sonido en el contexto laboral pertenece también al ámbito de la legislación relativa a la protección de datos y la videovigilancia de los trabajadores está cubierta por las disposiciones de la Directiva y las disposiciones nacionales de aplicación»*[8].

Posteriormente, el Grupo ha vuelto a ahondar más específicamente sobre el tema, en su Dictamen 4/2004, relativo al *Tratamiento de Datos Personales por medio de Videovigilancia*[9], adoptado el 11 de febrero de 2004, confirmando que el derecho a la autodeterminación informativa proporciona base y protección a los límites contractuales del poder de control empresarial, para impedir formas de control directo de la actividad laboral, o injustificadas o desproporcionadas.

El Grupo analiza el problema de la videovigilancia, desde un punto de vista general, esto es, se refiere a la videovigilancia destinada al control a distancia de acontecimientos, situaciones y sucesos de las personas en las más variadas situaciones. No obstante, tiene en cuenta, también, la dimensión laboral y se ocupa de examinar esas mismas actividades realizadas

---

[7] DO L 281 de 23 de noviembre de 1995.

[8] Adoptado el 13 de septiembre de 2001. El texto del documento se halla disponible en:
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.

[9] Disponible en: www.europa.eu.int/comm/privacy.

en el ámbito del empleo, poniendo de relieve en un apartado final, algunos principios específicos.

El Dictamen recuerda, en sus primeras páginas, que la propia Directiva 95/46/CE hace hincapié de manera expresa en que los principios de protección de la misma son aplicables a cualquier información (incluso la que esté constituida por imagen y sonido) relativa a una persona identificada o identificable. De modo particular, destaca que *«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»*.

El Documento se encarga, también, de señalar las áreas a las que la Directiva no se aplica, en todo o en parte. En concreto, identifica tres, de las cuales únicamente interesa destacar aquí –por su posible relación con el asunto que nos ocupa– la relativa a las operaciones de tratamiento de datos realizadas con fines de seguridad pública, defensa, seguridad del Estado, y para el ejercicio de las actividades del Estado en ámbitos del Derecho penal[10]. A este respecto, el Grupo destaca que 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). Precisa, además, que *«deberá especificarse siempre claramente quién es el responsable del tratamiento, a fin de que los interesados puedan ejercer sus derechos»*, lo que tiene que ver con el hecho de que cada vez es más frecuente que la vigilancia por videocámara la realicen conjuntamente la policía o entidades privadas (bancos, asociaciones privadas, empresas, etc.), lo que con-

[10] Las otras dos se refieren a: 1) Las operaciones de tratamiento realizadas por una persona física en el marco de una actividad meramente personal o familiar; 2) Las que se realicen con fines exclusivamente periodísticos o de expresión artística o literaria.

lleva un riesgo de confusión en cuanto al papel y la responsabilidad individuales.

La aplicabilidad de la Directiva se extiende tanto al tratamiento automatizado de datos personales de imágenes y sonidos captados mediante circuito cerrado de televisión y otros sistemas de vigilancia por videocámara, como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

En cuanto a las imágenes y sonidos susceptibles de ser considerados como «datos personales», el GTA menciona:

a) las imágenes que se utilizan en el marco de un sistema de circuito cerrado aunque no estén asociadas a datos personales del interesado

b) las que no se refieren a personas cuyos rostros hayan sido filmados, si contienen 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 imágenes 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) y las herramientas de comunicación utilizadas (por ejemplo, la conexión con un centro o el envío de imágenes a terminales remotos).

El Dictamen somete a los principios de la Directiva cualquier forma de vigilancia por videocámara que permita identificar a las personas y cita, a título de ejemplo, el caso de equipos colocados a la entrada o en el interior de un banco, cuando dichos equipos permiten identificar a los clientes.

Por lo que respecta a los principios de protección de la Directiva aplicables a la captación de imágenes o sonido por medio de circuitos cerrados u otros sistemas de videovigilancia, el Dictamen fija una serie de obligaciones o precauciones que deben tenerse en cuenta por el responsable de la instalación.

Sintéticamente enunciados, los principios que deben garantizarse en cualquier ámbito son los siguientes:

A) Principio de legalidad del tratamiento, lo que implica que debe verificarse si la vigilancia cumple las disposiciones generales y específicas. Particular énfasis pone el GTA en que *«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)»*.

B) Especificidad, especificación y legalidad de los fines. Que determina que los fines deben ser claros e inequívocos con el objetivo de ofrecer un criterio preciso a la hora de evaluar la compatibilidad de los fines e impedir que las imágenes captadas puedan ser utilizadas con otros fines.

C) Legitimidad del tratamiento. Supone que, al margen de los casos en que debe cumplirse por obligación legal (por ej. bancos o casinos) o resulte necesario para proteger intereses vitales (v. gr. control en unidades de reanimación), concurra una misión de interés público, lo que requiere un análisis minucioso del ámbito de las misiones, los poderes y los intereses legítimos del responsable del tratamiento, evitándose totalmente la superficialidad y la extensión infundada de dichos intereses legítimos.

D) Proporcionalidad del recurso a la videovigilancia, que comporta que este sistema sólo podrá ser utilizado, cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no requieran captación de imágenes (por ej. la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, etc.) claramente insuficientes o inaplicables en relación con los fines legítimos mencionados anteriormente. El Grupo considera que, 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 periféri-

cas o cerca de las paradas de autobús, no ocurre lo mismo cuando se trata de un sistema destinado a identificar a ciudadanos responsables de infracciones de menor importancia, como, por ejemplo, detectar a personas responsables de robos ocasionales en piscinas cubiertas. A juicio del Grupo, la proporcionalidad debe evaluarse con criterios más estrictos cuando se trata de lugares cerrados al público.

E) Proporcionalidad en la realización de las actividades de videovigilancia, que implica evaluación minuciosa de la proporcionalidad de las medidas relativas al tratamiento de datos y que obliga a tener en cuenta una serie de circunstancias como el ángulo visual con arreglo a los fines perseguidos, el tipo de equipo utilizado para filmar, la localización de las cámaras, utilización del plano fijo o móvil, posibilidad de aumentar las imágenes o realizar primeros planos durante la grabación o después, la congelación de imágenes, conexión con un centro para evitar señales de alarma sonoras o visuales. Asimismo, se considera necesario valorar si es necesario retener las imágenes y el plazo. La posición del Grupo es que, 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.

F) Información a los interesados: Implica suministro de información adecuada a los interesados, quienes deberán estar al corriente de que la vigilancia por videocámara está en marcha, y deberán ser informados sobre los lugares que se encuentran bajo control, aunque no es necesario especificar la ubicación precisa del equipo. La información deberá colocarse a una distancia razonable de los lugares controlados y estar a la vista; podrá suministrarse de manera resumida e incluir símbolos que ya hayan resultado útiles en relación con la vigilancia por videocámara. En todos los casos, deberá especificarse cuáles son los fines de la vigilancia por videocámara y quién es el responsable del tratamiento.

Para garantizar la seguridad y el adecuado uso de los sistema de videovigilancia, el Grupo juzga necesario adoptar una serie de medidas de organización. Tales medidas comprenden la restricción del acceso a las imáge-

nes; esto es, que sólo un número limitado de personas físicas esté autorizado a visualizar o acceder a las imágenes grabadas, cuando existan, y exclusivamente para los fines perseguidos por la vigilancia por videocámara o con vistas al mantenimiento del equipo. A este respecto, cuando la videovigilancia está destinada únicamente para prevenir, detectar y controlar infracciones, se propone como solución la utilización de dos claves de acceso (una de las cuales estaría en posesión del responsable del tratamiento y la otra de la policía), a fin de garantizar que las imágenes sólo las vea la policía y no personal sin autorización. Aparte se reconoce como imprescindible la adopción de medidas de seguridad, para evitar entre otras eventualidades, la difusión de información, así como el preservar la calidad de las imágenes grabadas, cuando existan, y la adecuada formación de los operadores implicados en las actividades de videovigilancia.

La usual brevedad del período de retención de los datos personales recogidos (imágenes y sonidos) hace que la posibilidad de aplicación de los derechos de las personas recogidos en la Directiva 95/46, se torne un poco limitada. No obstante, el Documento afirma la vigencia de estos derechos, haciendo especial hincapié en el derecho de oposición al tratamiento de datos que le conciernan por razones legítimas de su situación particular.

Por último, el Grupo analiza, en el referido Documento, el caso específico de la videovigilancia en el ámbito del empleo, y el principio de que parte es que los sistemas de videovigilancia destinados directamente a controlar, a partir de un local remoto, la calidad y cantidad de actividad de trabajo, al implicar tratamiento de datos, por regla general no deben ser permitidos. No obstante, admite que puedan ser utilizados con las debidas salvaguardas, cuando se trata de cumplir con los requisitos de seguridad del producto o de los ocupados, aunque ello implique indirectamente una vigilancia a distancia, indicando que deben ser de aplicación en todos estos casos los principios antes expuestos y cualesquiera otros derechos establecidos por la normativa nacional o los acuerdos colectivos.

La videovigilancia no debe alcanzar, según el Grupo, instalaciones reservadas al uso privado de los empleados o las no destinadas al cumplimiento de las tareas relacionadas con el empleo (como servicios, duchas, vestuarios o zonas de descanso).

Asimismo, considera que las imágenes recogidas exclusivamente para la salvaguarda de la propiedad y/o detección, prevención o control de infracciones graves no deben ser utilizadas para culpar a los trabajadores de pequeñas infracciones disciplinarias.

Insiste, también, en que debe facilitarse información a los trabajadores, incluyendo la identidad del responsable del tratamiento, la finalidad de la vigilancia, así como otras informaciones necesarias para garantizar el tratamiento justo en lo que respecta al interesado, por ejemplo en qué casos las grabaciones van a se examinadas por la dirección de la empresa, el período de grabación y cuándo ésta se revelará a las autoridades judiciales.

3. La escasa penetración de esta orientación en el ordenamiento jurídico español

La aplicación de los principios de la protección de datos a la cuestión que nos ocupa, aunque es en sí mismo congruente con el planteamiento constitucional y encuentra base en instrumentos jurídicos internacionales relevantes en materia de protección de datos, no termina de encontrar en el ordenamiento jurídico interno una adecuada plasmación normativa. Dadas las dificultades que se suscitan para coordinar el uso de los sistemas de grabación de imágenes, y el derecho a la autodeterminación informativa, el legislador de momento sólo ha preferido optar por unas vagas remisiones, antes bien que por una regulación específica.

A. El art. 2.3.e) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Procede destacar, en primer lugar, la normativa base en materia de protección de datos que está constituida en nuestro país, por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal (LOPD), que contiene regulaciones generales y también algunas previsiones específicas, sobre problemas concretos.

Respecto del tema que nos ocupa, el tratamiento es mínimo, por no decir inexistente. No se contempla de forma expresa la sujeción de la videovigilancia a los principios de protección de la misma, pero tampoco

se excluye. La Ley admite, al menos, que las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad sean susceptibles de tratamiento de datos personales. Si bien no lo regula y se remite, en su artículo 2.3.e), a la legislación específica sobre la materia, que no es otra que la ya comentada Ley Orgánica 4/1997 de videovigilancia. Pero ello al margen, sobre el tratamiento equivalente que puedan realizar otros sujetos particulares, guarda absoluto silencio.

Lo cual no es óbice para afirmar la aplicación de la normativa de protección de datos a la videovigilancia, pues es evidente que las imágenes y sonidos tomados por cualquier cámara pueden constituir datos de carácter personal susceptibles de tratamiento en el sentido del artículo 2.1 de la LO 15/1999. Como ha quedado señalado anteriormente, la posibilidad de tratamiento de los datos relativos a las personas físicas constituidas por sonidos e imagen es destacada en los considerandos de la Directiva 95/46/CE, que está en el origen de esta Ley Orgánica. En concreto, en el Considerando 14, se afirma textualmente que «*(...) habida cuenta de la importancia que en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos*».

B. El art 2.2 de la Ley Orgánica 4/1997, de 4 de agosto, reguladora de la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos

Otro texto legal apropiado para regular el tratamiento automatizado de las imágenes procedentes de la videovigilancia es la Ley Orgánica 4/1997, reguladora de la utilización de las videocámaras por las Fuerzas y Cuerpos de seguridad. Pero tampoco esta Ley Orgánica 4/1997, pese a ser algo más precisa que la anterior, llega a colmar las necesidades de regulación existentes en esta materia. En su artículo 2.2, se limita a disponer que «*sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*».

Aquí también se ha recurrido a esta vía indirecta del reenvío normativo, más bien que al directo que trataría de definir *«la posibilidad, condiciones y alcance de un tratamiento automatizado de las imágenes y sonidos o sobre la posibilidad de una organización automatizada de las grabaciones»*[11], lo cual supone una renuncia tácita a ahondar en la aplicabilidad de la normativa de protección datos a las imágenes grabadas mediante sistemas de videovigilancia, puesto que la LO 15/1999, como se ha observado antes, tampoco entra en tales refinamientos.

Cabe decir, no obstante, que la disposición de la LO 4/1997 es mucho más precisa porque da por válidas las disposiciones de protección de datos en materia de videovigilancia. De alguna manera supone el reconocimiento de que la captación y grabación de imágenes están sujetos a la normativa de protección da datos[12]. Falta por proveer a la adecuada instrumentación técnica para delimitar qué ámbito de protección de la autodeterminación informativa se aplica a la videovigilancia y en concreto a la practicada dentro de la empresa.

4. Posición mantenida por la Agencia Española de Protección de Datos

Ante el juego de remisiones cruzadas diseñado por el legislador y el vacío normativo existente, especial relevancia adquiere la Agencia de Protección de Datos, que asume un papel interpretativo de la LOPD en su función de garante del cumplimiento de la normativa de protección de datos. Hay distintas decisiones adoptadas sobre la materia, desde un informe hasta una instrucción pasando por varias resoluciones sancionadoras, y en todas ellas se trasluce respecto de la videovigilancia una clara

---

[11] X. ARZOZ SANTISTEBAN: «Videovigilancia y derechos fundamentales: Análisis de la Constitución...», op. cit., pág. 151.

[12] Tesis compartida, entre otros, por: J. L. REQUERO IBÁÑEZ: «Aspectos administrativos de la videovigilancia», *Revista Vasca de Derecho Procesal y Arbitrajes*, nº 1, 1997, pág. 28; R. MARTÍNEZ MARTÍNEZ: *Tecnologías de la información, policía y Constitución*, Valencia, 2001, págs. 338 y ss. No obstante, la cuestión no es del todo pacífica porque algún autor opina lo contrario. Así X. ARZOZ SANTISTEBAN («Videovigilancia y derechos fundamentales: Análisis de la Constitución...», op. cit., pág. 152), quien afirma que «esta disposición no puede considerarse como una habilitación para el tratamiento automatizado de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las FCS».

aceptación de la posibilidad de tratamiento automatizado de las imágenes tomadas mediante cámaras de vídeo.

A. Informe Jurídico sobre «Videovigilancia en el lugar de trabajo»

Por lo pronto, debe destacarse el Informe Jurídico sobre «Videovigilancia en el lugar de trabajo»[13], emitido en 2001 por la Agencia Española de Protección de Datos, a propósito de una pregunta formulada con relación a *«si resulta conforme a lo establecido en la LOPD la instalación de cámaras para el control de la actividad de los trabajadores de la entidad consultante»*. La Agencia, con buen criterio, antes de dar contestación a la pregunta, aborda la problemática que nos ocupa aquí y ahora; esto es, la de si las imágenes y sonidos obtenidos por tales sistemas de registro se encuentran sometidos a lo dispuesto en la LO 15/1999, de protección de datos personales.

El principio de fondo es que, según el parecer de la Agencia, las imágenes y sonidos tomados en el lugar de trabajo *«podrán ser considerados datos de carácter personal en caso de que los mismos permitan la identificación de las personas que aparecen en dicha imágenes, no encontrándose amparadas en la Ley Orgánica en caso contrario»*.

Esto es de fundamental relieve porque supone aceptar con carácter general la extensibilidad de la tutela, que la Ley Orgánica de Protección de Datos asegura a las personas físicas identificadas o identificables, a la videovigilancia; o sea a las imágenes y sonidos que se pueden captar de las personas mediante videocámaras.

Descendiendo, luego, al examen de la concreta cuestión planteada; a saber, si la instalación de videocámaras en el lugar de trabajo está sujeta a la LOPD, la Agencia observa que, si se toman imágenes del lugar de trabajo, la identificación es posible, pues *«siempre aparecerían en las mismas los trabajadores de la empresa en su lugar de actividad (lo que les hace perfectamente identificables)»*. Aparte si hay registro de imágenes, la posibilidad de tratamiento de imágenes es mayor porque *«siempre cabría tal identificación derivada de la mera constancia de las cintas grabadas,*

[13] Disponible en: https://www.agpd.es/index.php?idSeccion = 237.

toda vez que el trabajador se encontraría en su lugar de actividad, siendo perfectamente posible encontrar las imágenes del mismo con el simple conocimiento de su horario».

Por todo lo cual considera que la grabación en vídeo de imágenes de los trabajadores en estas condiciones queda sometido a la LOPD.

B. Resoluciones de la Agencia Española de Protección de Datos dictadas en materia de videovigilancia

Paralelamente a esta orientación general, la Agencia Española de Protección de Datos ha dictado varias Resoluciones en materia sancionadora donde también se ha decantado inequívocamente en favor de la aplicación de la LOPD a la instalación de cámaras de vídeo con carácter general, así como a la adopción para el control de la actividad de los trabajadores, dejando, sin embargo, en la penumbra el alcance de esa aplicación, al reenviarlo al criterio constitucional de la proporcionalidad.

Trataré de ofrecer, en primer lugar, una visión panorámica de las resoluciones relativas a la instalación de sistemas de captación de imágenes para el mantenimiento de la seguridad en zonas públicas o cuyo campo de visión abarca parte de la vía pública y, posteriormente, de las que se refieren a los sistemas utilizados en el ámbito de la empresa, bien con fines de seguridad o bien para el control de la actividad laboral.

a) Sobre instalación de cámaras de vídeo en lugares públicos

Cabe citar, en primer lugar, el caso de un establecimiento público, «Cafetería Restaurante TM», también conocido como «TOP MODELS», dedicado a prestar servicios de bar-restaurante y alquiler de habitaciones por horas, que contaba con dos cámaras de seguridad instaladas en su fachada exterior, junto a la puerta principal de entrada, ocultas tras unos focos de iluminación y orientadas hacia la vía pública; y otras varias instaladas en su interior como medida de seguridad para evitar incidentes y vigilar el posible consumo ilícito de drogas. En la Resolución sancionadora dictada, se afirma que las imágenes de vídeo son datos de carácter personal conforme al art. 3 c) LOPD, ya que reflejan la identidad de las personas al captar a una persona física identificada o identificable, ya sean éstos terceros o empleados de la empresa, por lo que tales imágenes

constituyen, en sí mismas consideradas, un tratamiento de datos en los términos de la LOPD. No obstante, la Agencia de Protección de Datos, tras comprobar que habían sido retiradas las cámaras después del informe realizado por la Policía local, y que el establecimiento había cesado en su actividad como consecuencia de la paralización y clausura de la actividad decretado por el Ayuntamiento por carecer de licencia de instalación, apertura y funcionamiento de restaurante, decide no sancionar y proceder al archivo[14].

Consta, también, otro caso de un particular, que, debido a los actos vandálicos que se venían produciendo en el vehículo de su propiedad, instala dos videocámaras fijas en el frontis de su casa, orientadas hacia la vía pública. Ello genera en los vecinos un malestar y preocupación porque se sienten vigilados y presentan varias denuncias ante la Policía local, que son trasladadas, a través de la Delegación de Gobierno en Canarias, a la Agencia de Protección de Datos. En la inspección realizada por la Agencia se comprueba que no hay ningún cartel o indicación de la presencia de las videocámaras situadas en el exterior del edificio y que las imágenes captadas son almacenadas en soporte magnético (cintas en formato VHS) que permiten el almacenamiento de ocho horas de grabación, sobre las que se pueden realizar búsquedas de forma secuencial, disponiéndose de un total de seis cintas, que permiten la grabación por un período de tres días. La Agencia da por supuesto, también en este caso, la aplicación de la LOPD a los hechos expuestos, porque considera que la captación y grabación de las imágenes con fines de vigilancia y control constituye tratamiento de datos, y sanciona al particular a dos multas de 601,01 euros cada una por incurrir en sendos motivos de infracción: una por la recogida de imágenes sin proporcionar a quienes pudieran aparecer en ellas la información que exige el art. 5 LOPD y, otra por la ausencia del consentimiento inequívoco del afectado (art. 6.1 LOPD)[15].

Relacionado también con la protección de vehículos de motor, se registra otro caso que enfrenta al propietario de un coche con otro afectado por

---

[14] Resolución de Archivo de Actuaciones de 28 de febrero de 2006; Exp. Nº E/00528/2004.

[15] Resolución R/00806/2005, de 13 de diciembre de 2005. Proc. Nº PS/00098/2005.

la instalación de cámara de vídeo. El imputado instaló una cámara encima del marco de la puerta de acceso a una plaza de garaje de su propiedad para captar imágenes que eran incorporados a un aparato grabador-reproductor de vídeo en formato VHS. Ni la Comunidad de propietarios de la finca donde se encontraba instalada la cámara ni el presidente de dicha finca habían autorizado la instalación. No obstante, el propietario pudo aportar un escrito con 10 firmas de un total de 16 propietarios en el que manifestaban su consentimiento para la instalación de una cámara de videovigilancia en la plaza de garaje de su propiedad. En las imágenes grabadas se podía observar que la cámara de vídeo capturaba imágenes de la plaza propiedad del denunciante, de la contigua y de la bajada de vehículos que se encuentra situada detrás. Parte de las grabaciones fueron utilizadas para interponer por el denunciado una demanda contra el denunciante, ya que, supuestamente, aparece vomitando y orinando en el coche del denunciado. La Agencia tramita el expediente sancionador sobre la base de entender, como en los casos anteriores, que la captación y grabación de imágenes con fines de vigilancia y control se encuentra plenamente sometida a lo dispuesto en la LOPD. Y tras imputar al denunciado infracción del art. 6 LOPD por falta de consentimiento del afectado y del art. 26.1 LOPD por falta de notificación e inscripción registral del fichero, le sanciona con dos multas de 601 euros cada una[16].

En el ámbito de la Comunidad de Propietarios, se conoce algún otro caso de instalación de videocámaras en que la Agencia ha procedido a aplicar la LOPD, admitiendo su plena vigencia. Es el del «Centro Comercial Nilo» que tenía instaladas catorce cámaras de videovigilancia, de las cuales dos se hallaban en la fachada principal del inmueble de la Comunidad y otra en el callejón de uso público colindante al inmueble, cuyos campos de visión enfocaban a los transeúntes que circulaban por la vía pública, así como otras dos cámaras en el interior de la cafetería del inmueble. Las imágenes captadas eran almacenadas en soporte magnético (cintas formato VHS y disco duro extraíble) que permite el almacenamiento de 36 horas de grabación. En el menú de búsqueda de grabaciones se podían realizar búsquedas utilizando como criterio la fecha y hora de

[16] Resolución R/00294/2006, de 23 de mayo de 2006, Proc. Nº PS/00248/2005.

la grabación. En las zonas captadas se encontraban carteles avisando de la presencia de las mismas, a excepción de aquellas que se correspondían con la vía pública. El monitor que recogía las imágenes captadas, se encontraba colocado de forma visible en la recepción de los apartamentos. La Agencia sanciona a la entidad por idénticos motivos que en el caso anterior, aunque con imposición de multa en cuantía superior por la infracción del art. 6.1 LOPD (6.000 euros)[17].

b) Sobre la instalación de cámaras de vídeo en el ámbito empresarial

Podemos destacar, en primer lugar, la Resolución relativa a la instalación en un Museo de la Comunidad Valenciana por una empresa de seguridad de un sistema de grabación de imágenes de circuito cerrado en el cuarto de control con motivo de una incidencia producida en dicho lugar, consistente en falsa alarma de incendio que fue desatendida y que provocó una inundación del centro de control por espuma anti-incendios. La cámara de grabación se instaló para supervisión de la medidas de seguridad y para la supervisión de las labores desempeñadas por los trabajadores, quienes fueron informados verbalmente de que se pretendía la supervisión de los sistemas de seguridad, pero no de que tales imágenes pudieran utilizarse para la supervisión y control de su trabajo. La empresa de seguridad disponía de 10 cintas. Cada día utilizaba una de las cintas, y al cabo de cinco o seis días, dichas cintas grabadas las recogía el supervisor de zona que las llevaba a la delegación, en donde el supervisor, si había ocurrido algún incidente en el Museo las visionaba, y si no había sucedido incidente alguno las volvía a llevar al Museo para su reutilización. Las cintas grabadas fueron aportadas como prueba en varios procesos judiciales tramitados con motivo de las demandas por despido presentadas por los trabajadores contra la empresa de seguridad.

La parte imputada negaba que le fuera de aplicación la LOPD, al considerar que no se trata de datos personales, pues únicamente se tomaron imágenes de la persona que en muchos casos es grabada de espaldas, la cinta sólo grababa el lugar de trabajo y no se habían creado ficheros con

[17] Resolución R/00035/2006, de 8 de febrero de 2006, Proc. Nº PS/00100/2005.

datos personales. Sin embargo, la Agencia rechaza tales manifestaciones, una vez comprobado que las cintas grabadas habían sido utilizadas por la empresa de seguridad para adoptar la medida de despido disciplinario contra los vigilantes del Museo. A la Agencia no le queda duda alguna de que las imágenes contienen información concerniente a personas físicas identificables o determinables por ser claramente identificables y, además, de que se ha constituido un fichero con las cintas de grabación, toda vez que éstas se conservaban una vez utilizadas durante cinco o seis días y puesto que con el conocimiento del horario del trabajador era posible la localización del mismo.

Partiendo, pues, de la aplicabilidad de la LOPD, lo único que reprocha la Agencia a la empresa de seguridad es el no haber suministrado a los vigilantes, previamente a la captación de sus datos personales, la información a que se refiere el art. 5.1 LOPD, por cuanto no se informó a los interesados de modo expreso, preciso e inequívoco de los extremos que cita; razón por la cual considera que ha incurrido en una infracción leve y le impone una multa de 601,1 euros.

No obstante, la Agencia acepta la legitimidad de la instalación del sistema de seguridad para el control y verificación del cumplimiento del trabajador de sus obligaciones laborales, invocando la doctrina sentada por el Tribunal Constitucional en la STC 186/2000, de 10 de julio, que cita la parte imputada. La Agencia no encuentra en ello infracción alguna porque considera que el artículo 20.3 del Estatuto de los Trabajadores *«habilita al empresario para tratar los datos de sus trabajadores sin su consentimiento, siempre que la medida adoptada no supere el juicio de proporcionalidad a que hace referencia el Tribunal Constitucional». Según la Agencia, este Tribunal «ha considerado que la medida adoptada por la empresa en un caso similar al aquí enjuiciado sí supera el juicio de proporcionalidad, por lo que ha de entenderse que la actuación del empresario en este caso se encuentra amparada legalmente en el Estatuto de los Trabajadores»*[18].

Un segundo caso en que se ha puesto a prueba la posibilidad de aplicación de la normativa de tratamiento de datos al control empresarial a través

[18] Resolución de 10 de diciembre de 2004, Proc. Nº/PS/00109/2004.

de cámaras de vídeo es el caso de la Gerencia Municipal de Urbanismo del Ayuntamiento de Málaga contra uno de los empleados de la misma. La Gerencia decide un buen día instalar en sus edificios varias cámaras de vídeo como recurso adicional a la seguridad, con el fin de controlar la seguridad y vigilar las dependencias de la mencionada Gerencia. También serán utilizadas para el control horario de los trabajadores. La grabación se realizaba en el disco duro del servidor de las cámaras. Las filmaciones eran conservadas durante quince días. No se llegó a informar de la existencia de las cámaras ni de las grabaciones que se realizaban. El denunciante se queja de que la única finalidad de la instalación del sistema de vídeo es el control de los trabajadores en lo referente a si realizan correctamente el preceptivo fichaje de control horario en un reloj, ya que por su ubicación se puede descartar la justificación por motivos de seguridad y autoprotección.

La Agencia se declara competente para conocer del asunto y siguiendo más o menos la línea de razonamiento de la Resolución anterior, declara a la Gerencia Municipal de Urbanismo del Ayuntamiento de Málaga responsable de una infracción del art. 5 de la LOPD por falta de información a los empleados y a los visitantes de la captación y grabación de sus imágenes. No obstante, se observan varios elementos de diferenciación con respecto a la resolución anterior: Uno, que, aun habiéndose admitido como en el caso anterior la existencia de un fichero estructurado de datos de carácter personal, ya que Gerencia cuenta con un dispositivo de cintas de grabación cuyos datos se conservaban durante quince días, no se considera que haya incurrido en infracción alguna respecto de este hecho. Dos, la distinta consecuencia aplicada respecto de la infracción del art. 5 LOPD, pues en este caso se deja sin sanción, requiriéndole simplemente para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del art. 5 LOPD, sin que concurra motivo alguno o se dé razón que justifique ese desigual trato. Tres, probablemente se trate de un error, pero, a propósito de la validez del sistema de vídeo como mecanismo de control del cumplimiento del horario de los trabajadores, en el fundamento jurídico 5 se afirma, no sin incurrir en cierta contradicción, que *«el Tribunal Constitucional ha considerado que la medida adoptada por la empresa en un caso similar al aquí enjuiciado no supera el juicio de proporcionalidad, por lo que ha de entenderse que la*

actuación del empresario en este caso se encuentra amparada legalmente en el Estatuto de los Trabajadores». Por el contrario, en el caso anterior se dice que *«sí supera el juicio de proporcionalidad»*[19].

La Agencia ha tenido ocasión de analizar al menos un tercer caso de videovigilancia en la empresa. No se ofrecen muchos detalles pero los suficientes para tomar conocimiento básico del asunto. Se trata de una denuncia, presentada por una trabajadora contra la entidad Agencia de Viajes NISAMAR, SL por instalación de videocámaras. La denunciante fue informada por escrito de la instalación de las videocámaras en las dependencias de la empresa, aunque se negó a firmar. La misma solicitó cancelación de las imágenes grabadas en las que apareciera. La entidad denunciada dispone de carteles informativos, advirtiendo de la existencia de las mismas. En el Registro General de Protección de Datos figuran inscritos a nombre de NISAMAR, los ficheros «Empleados» y «Vídeo».

En este caso la Agencia, que analiza la cuestión desde la perspectiva de la protección de datos, no encuentra infracción alguna de la LOPD. Considera que la entidad informó a los empleados y a los clientes de la instalación de las videocámaras con anterioridad a la puesta en funcionamiento de las mismas, de la finalidad de las grabaciones que se preveía realizar y del resto de las condiciones que se recogen en el artículo 5 de la LOPD. Por lo que acuerda el archivo de las actuaciones[20].

c) *Conclusiones y valoración de estas primeras Resoluciones de la Agencia*

Las Resoluciones expuestas contienen argumentaciones y pronunciamientos de la Agencia Nacional de Protección de Datos que excluyen cualquier duda sobre la aplicación de los principios de protección de datos a la instalación y uso de equipos de vídeo para la vigilancia o el control de las personas y, muy significativamente, al ámbito laboral. La Agencia se reclama competente para conocer de la legalidad de cualquier sistema de grabación de imagen cuando aporte información sobre una persona y

---

[19] Resolución R/00451/2005, de 20 de julio de 2005, Proc. Nº AAPP/00029/2004.

[20] Resolución de archivo de actuaciones de 8 de febrero de 2006 Exp. Nº E/00404/2005.

la hagan identificable, independientemente del vacío legal existente sobre el carácter específico y sensible del tratamiento de datos constituidos por imagen y sonido.

Del examen sucinto que acaba de realizarse cabe deducir varias conclusiones de carácter general: a saber: Primera, las cámaras de vídeo, en la medida en que reproducen las imágenes relativas a personas físicas identificadas o identificables son datos personales y, por tanto, se encuentran plenamente sometidas a la normativa de protección de datos. Segunda, si las imágenes captadas por las videocámaras se encuentran almacenadas, por ejemplo, en soporte magnético (cintas formato VHS) o algo parecido permitiendo búsquedas y reproducción de imágenes, se considerará constituido un fichero. Tercera, en ese caso, dicho fichero deberá ser declarado en la Agencia de Protección de Datos. Cuarta, la captación y grabación de las imágenes con fines de vigilancia y control, señaladamente en vía pública, está sometido al consentimiento de los titulares, salvo que estuviera acogido a las disposiciones de la Ley Orgánica 4/1997 y se dispusiera de habilitación legal. Quinta, no basta con informar a la policía de la instalación de un sistema de videovigilancia.

En el ámbito laboral, las Resoluciones son igual de contundentes en cuanto a la exigencia de los requisitos señalados, pero no aventan, en verdad, el problema jurídico de fondo, esto es, si es posible utilizar las cámaras de vídeo para el control de la actividad laboral. Las Resoluciones son extraordinariamente simples; han hecho de la STC 186/2000 y del juicio de proporcionalidad que consagra, prácticamente su único argumento jurídico. Todo su razonamiento consiste en decir –como se ha expuesto– que el art. 20.3 ET habilita al empresario para tratar los datos de sus trabajadores sin su consentimiento, siempre que la medida adoptada no supere el juicio de proporcionalidad, afirmando a continuación que existe una identidad con el caso resuelto en la referida sentencia.

Sin embargo, la Agencia no debería limitarse sólo al juicio de proporcionalidad, juicio que, por otra parte, tampoco se realiza en ninguna de las tres Resoluciones, sino que dada la naturaleza sensible de las operaciones de tratamiento, debería valorar si la videovigilancia empresarial cumple los principios de la protección de datos. Se requiere, en concreto y muy señaladamente –de acuerdo con lo declarado por el GTA–, un análisis

minucioso del interés legítimo del empresario, evitando la superficialidad y la extensión sin fundamento de dichos intereses legítimos, así como de los fines, asegurándose de que son claros y específicos con el fin de tener un criterio preciso a la hora de evaluar su compatibilidad con los fines realmente ejercidos. Se hace ineludible, además, examinar si existe la necesaria proporcionalidad entre los datos y el fin perseguido, verificando el empleo de sistemas idóneos con respecto a dicho fin y si se ha minimizado por parte del responsable del tratamiento, teniendo en cuenta que las imágenes y sonidos han de ser adecuados, pertinentes y no excesivos.

La Agencia, por otra parte, no hace bien detrayendo de la STC 186/2000 una asimilación al caso resuelto en la misma. No está tan claro que en los casos analizados por la Agencia se dé una necesidad tan justificada como la que pudo haber en el asunto resuelto por la STC 186/2000. Habría que valorar si la incidencia detectada en los sistemas de seguridad (la desatención de una falsa alarma de incendio por los vigilantes de seguridad del Museo) o el simple interés en comprobar si los trabajadores realizan correctamente el preceptivo fichaje de control horario en un reloj, supuestos enjuiciados por la Agencia, tienen el mismo grado de relevancia que las sospechas de graves irregularidades (sustracciones y descuadres contables) detectadas en el caso de los empleados de caja de un economato, donde el TC consideró justificada la medida de videovigilancia adoptada.

Parece que esta sentencia del TC le ha sumido a la Agencia en una cierta inhibición. Le ha hecho creer que el juicio de proporcionalidad desplaza cualquier otra consideración de la normativa de protección de datos en lo tocante a la vigilancia por videocámara en el contexto laboral, amén de inducirle a pensar que por regla general la videovigilancia para el control directo del trabajador puede no estar prohibido.

Sin embargo, no es el criterio mantenido por el GTA, que –como ya se ha visto anteriormente– no descarta la aplicación de los principios generales de protección de datos y que, además, expresamente excluye la videovigilancia para el control directo de los trabajadores, al declarar que «por regla general no deberá estar permitido».

C. Instrucción 1/2006, de 8 de noviembre, sobre tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras

El proceso de reafirmación, por parte de la Agencia, de la aplicación de los principios de protección de datos al tratamiento de las imágenes y sonidos se ha visto culminado con la reciente publicación de la Instrucción 1/2006 de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (BOE de 12 de diciembre de 2006).

La instrucción parte de la noción de que las *«imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999 y el artículo 1.4 del Real Decreto 1322/1994 de 20 de junio, que considera como dato personal la información gráfica o fotográfica»*, y pretende que en toda instalación de videocámaras con fines de vigilancia se respeten los principios de protección de datos y, muy señaladamente, el principio de proporcionalidad, incorporado por el Tribunal Constitucional a propósito de la videovigilancia en el lugar de trabajo.

El Texto no es aplicable a los datos personales grabados para uso o finalidad doméstica y al tratamiento de imágenes cuando éstas se utilizan para el ejercicio de sus funciones por parte de las Fuerzas y Cuerpos de Seguridad. Por tanto, las operaciones de vigilancia por videocámara realizadas por el empresario, al no estar comprendidas en las referidas excepciones, están sujetas a las garantías de protección establecidas.

En su articulado, se pone especial énfasis en la aplicación de determinados requisitos exigidos por la legislación vigente, en especial, el relativo al consentimiento para el tratamiento y comunicación de los datos (arts. 6 y 11 LOPD), bien que pueda no ser exigible en el contexto de las relaciones laborales al operar la excepción prevista en el art. 6.2 LOP, y se regula el contenido del deber de información previsto en el art. 5 de la LOPD, así como el ejercicio de los derechos de las personas afectadas.

También se establecen algunas precisiones sobre la cancelación de datos y la notificación de la creación de ficheros a la Agencia, para su inscripción en el Registro General de la misma. Y se concede un plazo de tres meses a los responsables de ficheros de videovigilancia ya inscritos

para que adapten sus distintivos informativos a las nuevas exigencias de la Instrucción, en concreto, para que incluyan una referencia a la Ley Orgánica 15/1999, a la finalidad para la que se tratan los datos y al responsable ante quien pueden ejercitarse los derechos.

En términos generales, se puede decir que la aclaración normativa a la que subviene la Instrucción es congruente con el planteamiento de la Directiva 95/46/CE y del referido Real Decreto 1322/1994, que –como luego se pondrá de manifiesto– habían afirmado la aplicabilidad de la normativa de protección de datos a la vigilancia por videocámara. Cuestión distinta es la mayor o menor fidelidad que la referida Instrucción pueda guardar con respecto a las normas y criterios de la jurisprudencia constitucional que intenta adecuar, y cuyo espíritu debe prevalecer siempre. No se quiere poner en entredicho la necesaria y eficaz labor de precisión llevada a cabo por la Agencia. Pero sí observar alguna duda sobre el obligado respeto a las normas que planea respecto de ciertos aspectos; como por ejemplo, la determinación del plazo de cancelación de las imágeners grabadas, donde, tal vez, se ha podido innovar la norma, o con relación a la respuesta que debe dar el responsable del tratamiento a la solicitud de derecho de acceso del afectado donde quizás no se explicitan todas las posibilidades permitidas por la norma reglamentaria, con lo que tampoco está en línea directa de transposición; aspectos que se abordarán más adelante.

5. Alguna decisión judicial: Sentencia de la Audiencia Nacional (Sala de lo Contencioso-Administrativo) de 24 de enero de 2003

En el ámbito judicial, se encuentra alguna decisión, que ha fijado una doctrina que pudiera considerarse como general sobre la aplicabilidad de la normativa de protección de datos a la utilización de sistemas de grabación de imágenes en el contexto laboral.

Es la sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, de 24 de enero de 2003[21], que se enfrenta a un supuesto de instalación en la redacción del diario Marca de una cámara, denominada

[21] Nº de recurso: 400/2001.

webcam, que recoge una imagen cada quince segundos de los empleados y la deposita en el servidor de internet ubicado en la empresa, de forma que cada nueva imagen borra la anterior. La transmisión de las imágenes a través de internet mediante sucesión de fotos fijas se produce durante las 24 horas del día todos los días de la semana y su única finalidad es reflejar el movimiento y la actividad de la redacción. A dichas fotografías que reproducen la imagen de los trabajadores se podía acceder desde la página **www.marca.es/webcam/.**

El referido pronunciamiento examina si tal captación y reproducción de imágenes constituye vulneración de la normativa de protección de datos, según lo declarado por la Agencia de Protección de Datos que impuso a la empresa editora (Recoletos Compañía Editorial, SA) una multa de 1.000.000 de pesetas por considerar tales hechos constitutivos de una infracción grave. La Audiencia Nacional admite la existencia de tratamiento de datos y confirma la Resolución dictada por la Agencia, desestimando los recursos planteados por la empresa.

La Sala parte de que, dentro de la definición amplia de «datos de carácter personal» contenida por el art. 3 a) LOPD, deben incluirse los datos consistentes en imágenes. Y sentado esto considera que el tratamiento de datos ha existido, pues el hecho de que las imágenes cambien cada quince segundos y no queden guardadas en archivo alguno no excluye la existencia de tratamiento de datos, y porque, además, las imágenes captadas por la cámara situada en la redacción del diario Marca ofrecen imágenes en las que se podía identificar a las personas que allí aparecen, así como por haber sido difundidas sin el consentimiento de los afectados. El Tribunal excluye la existencia de un consentimiento tácito, pues que *«los trabajadores hayan soportado la captación de imágenes con una cámara situada en la redacción o hayan permanecido inactivos ante esta iniciativa de la empresa no permite afirmar que estén conformes con ella ni que hayan dado su consentimiento cuando ni siquiera consta que hubiesen sido previamente informados sobre las características y el alcance del tratamiento de datos que iba a realizarse».*

En suma, la Audiencia Nacional viene aquí a reafirmar la aplicación de la normativa de protección de datos a la videovigilancia en el lugar de trabajo, y ello con independencia de que la LOPD, que es un texto incom-

pleto, sólo marginalmente haya tenido como propósito incorporar el tratamiento de las imágenes y sonidos grabados a la regulación de la Ley.

6. La consideración de la imagen y sonido del trabajador como datos de carácter personal: requisitos

Amén de lo hasta aquí expuesto, es incuestionable que el concepto de dato personal cubre, desde el punto de vista de su contenido, la imagen y el sonido de las personas. La LOPD no lo contempla expresamente, pero es evidente que en la definición dada de «datos de carácter personal» como *«cualquier información concerniente a personas físicas identificadas o identificables»* [art. 3.a) LO 19/1999], están englobados estos aspectos. Es difícil imaginar algo más personal e identificador que la propia imagen física o las características de la voz[22].

De todas formas, y por si esta definición no fuera del todo suficiente, el artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, que, aunque dictado en desarrollo de la ya derogada LORTAD (LO 5/1992), continúa en vigor por virtud de la disposición transitoria tercera de la LOPD, se encarga de disipar cualquier duda al considerar dato de carácter personal a *«toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable»*.

Interesa destacar que el régimen de protección de datos establecido por la LOPD, alcanza a datos de carácter personal constituidos, bien conjunta o bien separadamente, por las imágenes y los sonidos. Esto quiere decir que no es preciso que concurran los dos aspectos de imagen y sonido[23]; basta la mera grabación de imágenes, aunque no conlleve la de sonido, para que pueda considerarse igualmente un tratamiento sometido a la Ley.

---

[22] E. ACED FÉLEZ: «La protección de datos personales y la videovigilancia», www: datos personales.org, *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 5, noviembre 2003.

[23] J. HERNÁNDEZ MARTÍNEZ: «Videovigilancia y protección de datos», disponible en *http://www.tuguialegal.com/articulo38.htm*.

Pero lo que está incluido en el ámbito de aplicación de la LOPD no es cualquier imagen o sonido de personas. A los efectos de esta Ley, sólo tendrá carácter de dato personal aquella imagen o sonido que se refiera a alguien que esté identificado o sea identificable. No hay dato personal si la imagen que se obtenga no es posible vincularla a alguna persona. En consecuencia, la Ley no es de aplicación a los datos constituidos por imagen y sonido que carezcan del carácter identificable de las persona; esto es, a los llamados datos despersonalizados o «datos disociados», donde la imagen no puede asociarse a una persona determinada o determinable.

Ahora bien, para que exista dato de carácter personal *«no es imprescindible* –como ha señalado la Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1) en su sentencia de 8 de marzo de 2002[24]–, *una plena coincidencia entre el dato y una persona concreta, sino que es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados, tal y como se desprende del (...) artículo 3 de la Ley, en sus apartados a) y f) y también del Considerando 26 de la Directiva 95/46/CE que expresamente señala que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona».*

Por su parte el GTA, en su Dictamen 4/2004, ha precisado que los datos constituidos por imagen y sonido son personales aunque no estén asociados a los datos personales del interesado, incluso si no se refieren a personas cuyos rostros hayan sido filmados, añadiendo que 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.

De lo anterior resulta que si los equipos instalados implican captación de imágenes de personas físicas identificables o determinables, en cuanto pueden ser claramente identificadas e individualizadas tanto por el responsable como por otras personas, la normativa de protección de datos es plenamente aplicable.

---

[24] JUR 2002, 143289, Ponente Dª Nieves Buisán García.

Así lo viene entendiendo, como se ha tenido ocasión de comprobar, la Agencia de Protección de Datos, tanto cuando se trata de equipos colocados en lugares públicos o en lugares privados pero que permiten la vigilancia en vía pública (por ejemplo, las cámaras de seguridad instaladas en el exterior de los edificios particulares para vigilar los accesos), como cuando se refiere en particular a las cámaras instaladas en los centros de trabajo.

En este último supuesto, dejando al margen la más que dudosa tesis de que el art. 20. 3 ET habilita al empresario para la instalación de cámaras en el centro de trabajo, con fines de control de la actividad laboral, como parece deducirse de las Resoluciones dictadas por la Agencia, lo cierto es que la Agencia no duda en aplicar la normativa de protección de datos, sus principios y algunas de sus exigencias básicas (señaladamente, información al afectado), cuando las cámaras captan las imágenes de los empleados de las empresas, siempre que su identificabilidad sea posible.

Valga, como ejemplo, el supuesto, antes comentado, del Museo en el que se instala una cámara de grabación para la supervisión de los sistemas de seguridad y armas y también para el control de la actividad laboral de los vigilantes de seguridad. Ante la manifestación realizada por la empresa imputada de que no se trata de datos personales, ya que únicamente se toman imágenes de la persona que en muchos casos es grabada de espaldas, la Agencia considera que los mismos han de reputarse como auténticos datos de carácter personal al resultar fácilmente identificables los trabajadores a quienes se refieren las imágenes, máxime cuando las imágenes captadas fueron utilizadas como prueba para imponer sanciones disciplinarias a los trabajadores[25].

7. El tratamiento de datos constituidos por las imágenes del trabajador

Para que las imágenes de un trabajador captadas por un sistema de grabación entren dentro del ámbito de aplicación de la normativa de protección de datos es preciso que concurra otro requisito adicional, cual es que exista una actuación que constituya un «tratamiento de datos». La Directiva 95/46/CE en su art. 3 prevé que las *«disposiciones de la presente*

[25] Resolución de 10 de diciembre de 2004, Proc. Nº PS/00109/2004.

Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero». Por su parte, el artículo 2.1 de la LOPD establece que *«La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento...».* De todo ello resulta, como principio, que la Ley sólo se aplicará al tratamiento de los datos personales. Así, si no hay una actuación que suponga tratamiento de datos, las disposiciones de la Ley no serán de aplicación.

El concepto de tratamiento de datos queda precisado en el art. 3, c) de la Ley Orgánica 15/1999, que lo relaciona con aquellas *«operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».*

La Ley no limita la consideración de tratamiento sólo al caso en que dicho tratamiento sea automatizado, lo que en el caso de la videovigilancia simple sin conservación de imágenes limitaría su campo de aplicación, aunque cada vez se tiende más a utilizar soluciones de videovigilanicia sobre IP centralizadas con sistemas de grabación digital conectados en red, que ofrecen múltiples ventajas y aplicaciones, como la facilidad de integración de otros sistemas de control, el tratamiento avanzado de imágenes, etc. Sus previsiones incluyen también el tratamiento manual o no informatizado, que es de momento el sistema más utilizado en el ámbito de la empresa.

De acuerdo con ello, ha de entenderse que cuando la obtención de imágenes se realiza mediante sistemas de grabación digital, bajo el control de un ordenador, se está ante un tratamiento automatizadó, siendo éste un caso de tratamiento totalmente automatizado en el sentido del art. 3 de la Directiva. Dentro del mismo, la doctrina considera incluido el supuesto en concreto de la utilización de técnicas biométricas, consistentes en reconocimientos de rostros para su cotejo o comparación con otros rostros previamente almacenados en una base de datos[26].

---

[26] J. HERNÁNDEZ MARTÍNEZ: «Videovigilancia y protección de datos», disponible en http://www.tuguialegal.com/articulo38.htm.

El asunto problemático se halla en el caso de las cámaras de circuito cerrado de televisión (CCTV). Se ha planteado la cuestión de si es necesario que los datos de carácter personal constituidos por imágenes o sonidos estén almacenadas o registrados en fichero. En la doctrina científica diversos autores afirman dicha necesidad.

En esta línea se sitúa, por ejemplo, ARZOZ, quien se ha mostrado contrario a la aplicación de la legislación de protección de datos a la simple videovigilancia por considerar que una grabación de imágenes y sonidos, una cinta de vídeo, no representa o no contiene tratamiento de datos, ya que lo decisivo, según el art. 3 de la LOPD, es que las imágenes o voces grabadas estén organizadas de forma que puedan ser buscadas a partir de los datos personales de las personas[27].

En parecido sentido se ha pronunciado también ACED FERNÁNDEZ, al indicar que *«no basta con que exista una captación de datos personales mediante las cámaras de vigilancia, esta captación o el uso posterior de dichas imágenes debe constituir un tratamiento en el sentido de la Directiva, parcial o totalmente automatizado»*, añadiendo que en *«el caso de que el tratamiento sea manual, éste sólo estará sometido a las disposiciones de la Directiva cuando se produzca una estructuración de los datos personales incluyéndolos en un fichero manual»*.

Ciertamente, la Directiva es bastante explícita al respecto al afirmar en su considerando 15 que *«los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos se encuentren contenidos o se destinan a encontrarse en un archivo estructurado según los criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata»*.

De parecido tenor es, también, la LO 15/1999, pues habla de que la Ley *«será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptible de tratamiento...»* (art. 2.1).

Sin embargo, tanto la Agencia de Protección de Datos como la Audiencia Nacional parecen ignorar este requisito del almacenamiento o registro

---

[27] Así, X. ARZOZ SANTISTEBAN: «Videovigilancia y derechos fundamentales: Análisis de la Constitución...», op. cit., pág. 151.

de imágenes o sonidos, acogiéndose simplemente a la definición del art. 3. c) de la LOPD que no efectúa ningún tipo de precisión al respecto, y decantándose por la solución negativa.

En la Resolución de 28 de febrero de 2006 relativa a la instalación de videocámaras en las inmediaciones y dentro del establecimiento TOP MODELS que venía prestando servicios de bar-restaurante y alquiler de habitaciones por horas, la Agencia sostiene *que «De acuerdo con aquella definición de tratamiento de datos personales, la mera captación de imágenes de las personas que transitan una vía pública puede considerarse un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada»*. Idéntica aseveración se contiene también en la Resolución de 27 de febrero de 2006 en el caso de la COMUNIDAD DE PROPIETARIOS CENTRO INDUSTRIAL NILO, y ello sin atender a que el sistema instalado se completaba en este caso con un dispositivo de grabación de vídeo en formato VHS.

La Audiencia Nacional se ha pronunciado de forma directa sobre la cuestión, tras la impugnación de la Resolución dictada por la Agencia en el procedimiento sancionador incoado contra la empresa editora del diario Marca. En la sentencia ya comentada, de 24 de enero de 2003, se indica que *«no cabe excluir que haya existido (tratamiento de datos) por el hecho de que las imágenes cambiantes cada quince segundos no queden guardadas ni registradas en archivo alguno, pues según el precepto [art. 3.c) LOPD]... el tratamiento no exige la conservación de los datos, bastando con su recogida o grabación»*.

De manera que se puede decir que la restricción de la Directiva y de la LOPD aparece hoy desarmada ante el criterio adoptado por la propia Agencia y la Audiencia Nacional; de tal manera que la mera captación de imágenes, sea o no con fines de vigilancia y control de las personas y, en concreto, de los trabajadores, aunque no haya almacenamiento o conservación de imágenes, ni se cree un fichero o cualquier otro archivo (por ejemplo, cintas de vídeo), e independientemente de que los archivos estén organizados, constituye un supuesto específico de tratamiento de datos.

Y no parece desacertada tal decisión por cuanto la libertad y el derecho de autodeterminación informativa padecen ya con la simple toma de conocimiento intrusiva de la imagen de que puede ser objeto una persona, a

través de los sistemas de videovigilancia, que simplemente reproducen la imagen de las personas; aunque, claro está, mucho más, cuando se accede a los soportes destinados a la grabación de esas imágenes y sonidos para extraer datos concretos de las personas observadas y, en su caso, elaborar un perfil de las mismas. Entiendo que el hacer hincapié en el elemento del almacenamiento o conservación, o del «conjunto organizado de datos personales», a que alude el art. 3 de la LO 15/1999 para definir el concepto de archivo, lleva a una reducción injustificada del ámbito protegido por el art. 18.4 CE.

Esta posición concuerda, por otra parte, con las directrices establecidas sobre el tratamiento de datos personales en el contexto laboral por el GTA 29, que no ha efectuado reparo alguno a la hora de extender los principios de protección de datos de la Directiva 9546/CE a la videovigilancia en el lugar de trabajo aun sin registro, tal y como se ha observado anteriormente, y es, además, coincidente con la tendencia de otros ordenamientos con mayor experiencia que la nuestra en la regulación de la protección de datos de carácter personal, que aplican dicha normativa a las cámaras de vídeo, como es el caso de Suecia o Alemania.

8. El consentimiento del trabajador afectado

Un elemento central del derecho a la autodeterminación informativa y del régimen de protección de datos de carácter personal establecido por la LOPD lo constituye el consentimiento del afectado. Siendo el derecho fundamental a la protección de datos un poder de disposición y de control sobre los propios datos, el consentimiento se convierte en un «principio cardinal»[28], pues no hay otra posibilidad de ejercer esos poderes más que a través del consentimiento. *«Los poderes de control y de disposición se*

---

[28] R. TASCÓN LÓPEZ: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*, cit., pág 104. Sobre la importancia que representa el consentimiento puede verse, entre otros, a: M. A. DAVARA RODRÍGUEZ: «La sociedad de la información y el tratamiento de datos de carácter personal», en AA. VV. (DAVARA RODRÍGUEZ, M. A., Coord.), *Encuentros sobre Informática y Derecho*, Madrid, Aranzadi-Universidad Pontificia de Comillas, 1998, pág. 28; J. M. FERNÁNDEZ LÓPEZ: «El consentimiento del interesado para el tratamiento de sus datos personales», www: datos Datos personales.org. *Revista de la Agencia de protección de Datos de la Comunidad de Madrid*, nº 3, 2003.

concretan jurídicamente –como ha dicho el Tribunal Constitucional en la STC 292/2000– *en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular*». Todo gira, pues, alrededor del consentimiento del interesado. Por regla general, sin el consentimiento no cabe llevar a cabo lícitamente operaciones de tratamiento de datos personales[29].

El consentimiento como principio general se encuentra formalmente recogido en el artículo 6.1 de la LOPD, según el cual «*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa*». La literalidad del precepto parece darnos a entender, por un lado, ese carácter inexcusable del consentimiento que se deduce del propio contenido del derecho a la autodeterminación informativa, pero, por otro, la posibilidad de que pueda haber excepciones a esta regla general. De hecho son bastantes los supuestos en los que la propia Ley dispone otra cosa, por lo que este principio pierde de alguna manera ese pretendido carácter de generalidad y «*queda prácticamente relegado a la categoría de una mera condición de licitud, entre las muchas previstas por la norma, desvirtuando en buena media, la regla de orden en virtud de la cual y como punto de partida, el consentimiento parecía necesario*»[30].

Las excepciones al consentimiento se encuentran previstas en el apartado siguiente (art. 6.2 LOPD), siendo de especial relevancia a los efectos que aquí importa, el regulado en el inciso segundo del referido apartado, que establece que no será necesario el consentimiento «*cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento*».

Dejando al margen la compleja problemática que plantean estas exenciones[31], procede su análisis desde la perspectiva del acopio de datos a

---

[29] M. A. DAVARA RODRÍGUEZ: *Nueva guía práctica de protección de datos. Desde la óptica del titular del fichero*, ASNEF, Madrid, 2001, pág. 59.

[30] R. TASCÓN LOPEZ: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*, cit., pág. 107.

[31] Tratada con amplitud y rigor en el estudio realizado por Mª B. CARDONA HUBERT: *Informática y contrato de trabajo*, Tirant lo Blanch, Valencia 1999, págs.

través de los sistemas de videovigilancia, y, en particular, en el contexto laboral, porque plantea ciertas dudas la incidencia que el consentimiento del trabajador puede asumir en la concreta determinación por el empresario de un sistema de grabación.

Con carácter general, parece obvio que, siendo el consentimiento el requisito ineludible para el tratamiento de los datos de carácter personal, dicho requisito resulte exigible en los supuestos de captación de imágenes que constituyan en sí mismas un tratamiento de datos en los términos de la LOPD y no se refieran a partes que tienen entre sí una relación contractual alguna.

La Agencia Española de Protección de Datos viene aplicando con rigurosidad la necesidad de contar con el consentimiento del afectado, sancionando en los diversos supuestos de instalación de cámaras en que se captan imágenes de personas en la vía pública o de particulares a los que no se ha pedido autorización. Así lo ha hecho, por ejemplo, en el caso de la COMUNIDAD DE PROPIETARIOS CENTRO INDUSTRIAL NILO, que captó y almacenó en un dispositivo de grabación de vídeo en formato VHS, datos personales de los transeúntes en la vía pública[12], así como en el supuesto del propietario de un vehículo que graba las imágenes de los viandantes que se introducen en el área de visión de las dos cámaras, instaladas en el frontis de su casa para vigilar la seguridad de su vehículo[13].

---

117 y siguientes; así como, y entre otros, por R. TASCÓN LÓPEZ: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*, cit., págs. 107 y siguientes.

[12] Resolución R/00035/2006, de 8 de febrero de 2006, Proc. Nº PS/00100/2005.

[13] Resolución R/00806/2005, de 13 de diciembre de 2005, Proc. Nº PS/00098/2005: «En el presente expediente, cabe apreciar que la persona denunciada captó imágenes de la vía pública, de conformidad con lo anteriormente expuesto. Dichas imágenes, capturadas en un soporte magnético incorporarían datos personales de los viandantes que se introdujeran dentro de su campo de visión y, pese a que del visionado de las dos cintas aportadas no se ha podido constatar la existencia de los mismos, no cabe duda que, del uso dado a los dispositivos de captura de las imágenes, así como consecuencia de la finalidad perseguida, los datos de carácter personal de los transeúntes serían objeto de captación por dichas cámaras y, por tanto, los datos personales captados deberían estar sometidos al consentimiento de sus titulares, de conformidad con lo que determina la LOPD.

Dicho tratamiento, por tanto, ha de contar con el consentimiento del afectado, circunstancia que no se ha acreditado por lo que cabe estimar cometida la infracción por la que se ha instruido el presente procedimiento, y por tanto sancionable, de conformidad con lo que dispone el artículo 44.3.d) de dicha norma, que esta-

Respecto de la forma en que ha de prestarse el consentimiento para la validez de la declaración, la LOPD no parece requerir ningún requisito especial. Únicamente para los datos especialmente protegidos y en especial para los relativos a la ideología, afiliación sindical, religión y creencias, se exige que el consentimiento sea expreso y además otorgado por escrito[34], pero eso tiene escasa relevancia para lo que aquí se trata, pues, el empresario no puede recabar esos datos, mientras los datos no tengan un claro interés contractual, ni siquiera con consentimiento expreso y por escrito del trabajador[35], y es muy difícil imaginar algún supuesto en que pudiera venir justificada la instalación de un sistema de grabación basado en alguno de los referidos motivos. No constituye, por tanto, un requisito esencial del consentimiento el que se preste por escrito o con formalidades determinadas.

No obstante, el artículo 6 LOPD indica que el consentimiento del afectado debe ser inequívoco. La Ley no aclara el sentido del término «inequívoco» y constituye todo un dilema interpretar su significado. En la doctrina hay planteado un vivo debate acerca de si junto al consentimiento expreso, son admisibles otras formas de consentimiento, como el tácito, para el tratamiento de datos, sin que se haya alcanzado hasta el momento una solución muy fiable o segura. De todas formas este precepto no puede ser interpretado sin ponerlo en relación con el art. 5 LOPD, que reconoce el derecho a la información del afectado; un derecho que es la principal garantía del consentimiento, ya que *«sólo cuando se ha atendido debidamente este derecho, cuando se ha informado, cabe afirmar que el consentimiento es válido, o no está viciado de error»*[36].

En particular, respecto de la videovigilancia, lo que cabe decir es que la Agencia Española de Protección de Datos ha adoptado una postura, en

---

blece como tal: "Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción grave"».

[34] Artículo 7.2 LOPD.

[35] J. J. FERNÁNDEZ DOMÍNGUEZ y S. RODRÍGUEZ ESCANCIANO: *Utilización y control de datos laborales automatizados*, Agencia de Protección de Datos, Madrid, 1997, págs. 184 y siguientes.

[36] J. APARICIO SALOM: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, cit., pág. 67.

términos generales, bastante restrictiva, exigiendo la prueba del consentimiento de los afectados. Lo podemos ver en la Resolución, antes comentada, del propietario del vehículo que para proteger su vehículo instala cámaras de vídeo captando imágenes en vía pública[37] y, de una forma mucho más palmaria, en la de ese otro particular que instala en la plaza de garaje de su propiedad una cámara que extiende su campo de visión a otros coches distintos del suyo y a zonas comunes, donde la Agencia considera incumplido tal requisito a pesar de que el imputado había aportado un escrito con 10 firmas de un total de 16 vecinos del inmueble manifestando su consentimiento para la instalación de dicha cámara de vídeo[38]. Conforme se deduce de esas Resoluciones, para la licitud de la instalación de un sistema de grabación de imágenes de personas que supone tratamiento de datos, se requiere una forma de otorgamiento expreso del consentimiento de los afectados.

Para la Agencia, la única posibilidad de quedar eximido de esa aceptación es contando con una habilitación legal. Y esa habilitación, en un contexto abierto y público, no de relación privada, negocial o laboral, no es otra que la prevista en la Ley Orgánica 4/1997, de 4 de agosto, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

La consecuencia práctica de todo ello es que la posible instalación de cámaras que capten imágenes de la vía pública, dada la imposibilidad de obtener el consentimiento previo de los viandantes que se introduzcan en su ángulo de visión, queda, así, supeditada, con carácter general, a la obtención de una autorización previa conforme a la Ley 4/1997.

La postura de la Agencia, cuando se trata de instalación de sistemas de grabación en el ámbito de la empresa, resulta, sin embargo, mucho más matizada o flexible. En estos casos la Agencia admite que puede no ser necesario el consentimiento, teniendo en cuenta las excepciones previstas en el artículo 6 de la LOPD, párrafo 1° («salvo que la ley disponga lo contrario») y párrafo 2°, inciso segundo («o cuando en una relación laboral

---

[37] Resolución R/00806/2005, de 13 de diciembre de 2005, Proc. N° PS/00098/2005.

[38] Resolución R/00294/2006, de 23 de mayo de 2006, Proc. N° PS/00248/2005.

sean necesarios para su mantenimiento o cumplimiento»), y de conformidad con lo dispuesto en el art. 20.3 del Estatuto de los Trabajadores, que otorga al empresario la facultad de adoptar las medidas más oportunas de vigilancia y control del cumplimiento por el trabajador de sus obligaciones laborales.

La Agencia presume que la autorización legal al empresario para adoptar las medidas de control de sus trabajadores, así como el consentimiento prestado para la celebración del contrato de trabajo, llevan implícito el consentimiento de los trabajadores para la instalación de sistemas de videovigilancia de los trabajadores en el ámbito laboral. No obstante, matiza esta presunción generalizada de consentimiento, poniendo como condición para admitirla que la *«medida adoptada supere el juicio de proporcionalidad a que hace referencia el Tribunal Constitucional»*. Interpretando de esta manera el consentimiento, la Agencia ha encontrado legítimo, por ejemplo, el que la Gerencia Municipal de Urbanismo del Ayuntamiento de Málaga instalara cámaras de vídeo para poder verificar el cumplimiento del horario de los trabajadores[39], o que la empresa de seguridad de un Museo de Valencia instalara una cámara de vídeo para controlar a los empleados que vigilan las instalaciones[40].

A este respecto, ya se ha comentado que lo que hace la Agencia es partir de una presunción genérica de consentimiento, pues en ninguno de los referidos casos se lleva a cabo un juicio de proporcionalidad. Aún más, en algún otro caso incluso ni siquiera admite que la validez del sistema tenga que supeditarse al juicio de proporcionalidad, pues esa condición ni siquiera se recoge: tan sólo se analiza si hubo información a los empleados de la instalación de las videocámaras con anterioridad a la puesta en funcionamiento de las mismas[41], con lo que deja en el aire la inquietante

[39] Resolución R/00451/2005, de 20 de julio de 2005, Proc.- Nº AAPP/00029/2004.

[40] Resolución R/00681/12004, de 10 de diciembre de 2004, Proc. Nº PS/00109/2004.

[41] Así ocurre en la ya citada Resolución de Archivo de actuaciones de 8 de febrero de 2006, Expediente nº: E/00404/2005, relativo a una Agencia de viajes que instala en el interior de la entidad cámaras de vídeo que captan imágenes de sus empleados, y que, además, guarda las imágenes en sendos ficheros que llevan por nombre «Empleados» y «Vídeo». La Agencia estima que no hay infracción de la LOPD porque la «información suministrada por NISAMAR cumplía las exigencias contenidas en el artículo transcrito (art. 5), pues en el mismo se informaba de

cuestión de si basta la información previa a los trabajadores para entender lícito el tratamiento de datos personales constituidos por imágenes y sonidos.

Todo ello resulta muy discutible, porque aun cuando pueda presumirse el consentimiento de la habilitación legal, ello no prejuzga la legitimidad de cualquier sistema de grabación en la empresa; o dicho de otra manera, no cabe deducir de la habilitación legal y mucho menos de la simple información previa, una especie de patente de corso para adoptar discrecionalmente, cuando y como quiera el empresario, los mecanismos de videovigilancia en la empresa. Es preciso advertir que la Directiva 95/46/CE limita la legitimidad del tratamiento de datos personales, entre otros supuestos y destacando los que tienen relación con lo aquí analizado, sólo a los casos en que *«es necesario para la ejecución de un contrato en el que el interesado sea parte»* [art. 7.a)], o *«es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento (...), siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requiera protección con arreglo al apartado 1 del artículo 1 de la presente Directiva»* [art. 7.f)]. Por tanto, la Directiva está autorizando el consentimiento implícito, pero siempre que concurra una necesidad o un interés legítimo Y eso es lo primero y básico que la Agencia debe sopesar, incluso en el ámbito de la empresa, porque no es ningún territorio franco, donde no operen los derechos fundamentales. Debe entenderse, pues, que cuando el art. 6.1 LOPD excepciona el principio del consentimiento en los supuestos de autorización legal, sólo puede comprenderse dicha excepción mediante su relación con el interés legítimo, de modo que la captación de imágenes puede no ser válida si no concurre un interés legítimo importante, capaz de prevalecer sobre los derechos de los trabajadores.

Así las cosas, cabría preguntarse por el margen de operatividad del consentimiento de los trabajadores a la hora de determinar la instalación de un sistema de grabación de imágenes de los trabajadores. ¿Puede el empresario sortear todas esta limitaciones y recabar el consentimiento di-

---

forma expresa, precisa e inequívoca de la existencia de las referidas cámaras de vigilancia previamente a la grabación de imágenes, de la finalidad de las grabaciones que se preveía realizar y del resto de las condiciones que se recogen en el artículo 5 de la LOPD».

recto y expreso de los trabajadores, toda vez que el art. 6.1 LOPD permite el tratamiento de datos personales si el afectado presta su consentimiento?

Entiendo que, una vez constituida la relación laboral, el consentimiento del trabajador tiene escasa relevancia; sólo muy relativamente puede funcionar como una causa de legitimación de la adopción de los dispositivos de control audiovisual. Porque, cuando existe un interés justificativo para instalar los dispositivos de control audiovisual deviene irrelevante el consentimiento, pues se otorgue o no el consentimiento, el empresario siempre podrá ejercer ese control audiovisual. Concurriendo dicho interés legítimo, el empresario está simplemente obligado a informar de la existencia del tratamiento y demás circunstancias mencionadas en el artículo 5, 1 LOPD, «no a solicitar y obtener el consentimiento»[42].

Y si no hay un interés específico legítimo, el recurso al consentimiento individual y expreso del trabajador constituye sencillamente un abuso; el consentimiento que se preste no garantiza la legitimidad del tratamiento, pues supondrá una renuncia de derechos fundamentales en el trabajo prohibida en el ordenamiento laboral y, por tanto, sin eficacia alguna. El simple consentimiento no puede utilizarse, pues, como aval para legitimar la adopción de mecanismos de control audiovisual, ni para extender la posibilidad de tratamiento de datos a fines que no resultan legítimos.

Cuestión distinta es que el sometimiento a un sistema de grabación no responda a un requerimiento organizativo, ni a razones de estricta necesidad, sino que venga cualificado por un simple interés empresarial (v. gr. publicidad o promoción de un producto) no pactado. El Tribunal Constitucional ya ha tenido ocasión de señalar en la STC 99/1994, que, dada la posición prevalente que alcanzan los derechos fundamentales en nuestro ordenamiento jurídico, no basta la sola afirmación del interés empresarial para imponer semejante restricción de derecho fundamentales, si no viene impuesta por la naturaleza de las tareas expresamente contratadas. Esta importante declaración se realiza precisamente en un caso de negativa de un trabajador, deshuesador de jamones, a salir ante las cámaras de televisión en una muestra de un producto (jamón ibérico) para la presentación

---

[42] J. APARICIO SALOM: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, cit., pág. 65.

de la denominación de origen del jamón de bellota, fabricado por su empresa. De manera que, cuando la captación de imágenes del trabajador no estuviera prevista en el contrato, la empresa no puede imponer el sometimiento a dicho acto de tratamiento de datos personales, si el interesado no quiere; dicho de otra manera, el empleador está obligado a obtener directamente del trabajador afectado el consentimiento. En todos estos casos, es evidente la operatividad del consentimiento, hasta el punto de que constituye un requisito de licitud para la captación de imágenes del trabajador y, en consecuencia, del tratamiento de datos personales del trabajador.

De todas formas, hay que entender que para la legitimidad del tratamiento no sirve cualquier interés empresarial. El tratamiento de datos personales constituido por imágenes y sonidos sólo puede efectuarse si el interés perseguido por el empresario guarda conexión con la actividad laboral y el empleo del trabajador.

Tal es la conclusión alcanzada también en los documentos internacionales más relevantes en el ámbito de tratamiento de datos personales, como pueden ser la Recomendación nº 2 del Consejo de Europa de 18 de enero de 1989, sobre protección de datos personales utilizados por motivos laborales o el Repertorio de Recomendaciones prácticas de la OIT de 1996 sobre protección de datos del trabajador. En ambos se establece como *conditio sine qua non* para el tratamiento de datos personales, que exista una relación directa de cada dato personal con la específica relación de trabajo y se cumplan las disposiciones de la legislación nacional.

En suma, cabe señalar con BELLAVISTA que el consentimiento del trabajador no representa nunca el único (y por tanto suficiente) presupuesto de legitimidad del tratamiento de datos personales constituidos por imagen y sonido, sino que ha de ir acompañado de condiciones y procedimientos dirigidos a garantizar el estrecho anclaje entre las concretas tipologías de datos personales recogidos y la objetiva finalidad de gestión de la relación laboral[43].

---

[43] A. BELLAVISTA: «Poteri dell'imprenditore e privacy del lavoratore», cit., pág. 50.