

TRATAMIENTO DE DATOS PERSONALES OBTENIDOS MEDIANTE LA VIDEOVIGILANCIA EN EL CENTRO DE TRABAJO

AUTORA:

África MIR FERNÁNDEZ

DIRECTORA:

Prof^a. Dra. Esther MITJANS PERELLÓ

Trabajo Final de Grado 2013-14

Contenido

1	INTRODUCCIÓN:	4
2	LA VIDEO-VIGILANCIA Y LOS DERECHOS FUNDAMENTALES	7
2.1	EL DERECHO A LA INTIMIDAD.....	7
2.2	EL DERECHO A LA IMAGEN.....	8
2.3	EL DERECHO A LA PROTECCIÓN DE DATOS.....	9
3	LA VIDEO-VIGILANCIA	9
3.1	FUENTE DE CUESTIONES PROCESALES.....	9
3.2	CONCEPTO Y CLASES DE VIDEO-VIGILANCIA:.....	11
3.2.1	<i>La video-vigilancia por razones de seguridad</i>	11
3.2.2	<i>La video-vigilancia como mecanismo de control y vigilancia del empresario:</i>	12
4	LOS PRINCIPIOS DE JURISPRUDENCIA SOCIAL Y CONSTITUCIONAL	14
4.1	LA INICIAL DOCTRINA JUDICIAL PERMISIVA DE LA VIDEO-VIGILANCIA EMPRESARIAL:.....	14
4.2	INTERPRETACIÓN CORRECTORA EFECTUADA POR EL TRIBUNAL CONSTITUCIONAL:.....	16
5	JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL (TC) EN SU SENTENCIA STC 98/2000, 10 ABRIL:	16
5.1	EXPOSICIÓN DE LOS HECHOS.....	16
6	JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL (TC) EN SU SENTENCIA STC 186/2000, 10 JULIO	18
6.1	STC 186/2000.....	18
6.2	DETERMINACIÓN Y COMPROBACIÓN DEL TRIBUNAL CONSTITUCIONAL.....	19
6.2.1	<i>Juicio de idoneidad o adecuación</i>	19
6.2.2	<i>El Juicio de necesidad</i>	20
6.2.3	<i>Juicio de proporcionalidad en sentido estricto</i>	20
7	JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL (TC) EN SU SENTENCIA STC 29/2013, 11 FEBRERO	22
7.1	EXPOSICIÓN DE LOS HECHOS.....	22
7.2	DESCRIPCIÓN DE LOS HECHOS EN LA PROPIA SENTENCIA.....	22
7.3	RAZONAMIENTO DEL TRIBUNAL CONSTITUCIONAL:.....	24
8	LA ORIENTACIÓN INTERNACIONAL TENDENTE A SITUAR LOS LÍMITES DE LA VIDEO-VIGILANCIA EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS:	27
8.1	LA OIT: REPERTORIO DE RECOMENDACIONES PRÁCTICAS DE LA OIT DE OCTUBRE DE 1996, PROTECCIÓN DE LOS DATOS PERSONALES DE LOS TRABAJADORES:.....	27
8.2	GRUPO EUROPEO DE COMISARIOS SOBRE PROTECCIÓN DE DATOS PERSONALES (GTA):..	29
9	NORMATIVA LOPD Y LAS INSTRUCCIONES:	31
9.1	INSTRUCCIÓN 1/2006, DE 8 DE NOVIEMBRE, DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.31	
9.1.1	<i>Modelo de cartel identificativo</i>	34
9.2	INSTRUCCIÓN 1/2007, DE 16 DE MAYO, DE LA AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID: SISTEMAS DE CÁMARAS O VIDEOCÁMARAS EN EL ÁMBITO DE LOS ÓRGANOS Y ADMINISTRACIONES PÚBLICAS DE LA COMUNIDAD DE MADRID:.....	34
9.2.1	<i>La guía de video-vigilancia y la Instrucción 1/2007 de la APDCM en relación a la video-vigilancia empresarial</i>	35

9.3	INSTRUCCIÓN 1/2009, 10 DE FEBRERO, SOBRE EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL MEDIANTE CÁMARAS CON FINES DE VIDEO-VIGILANCIA:	37
9.3.1	<i>Ámbito de aplicación.</i>	38
9.3.2	<i>Aclaración de la Instrucción 1/2009 de la APDCAT versus Instrucción 1/2006 de la AEPD.</i> 38	
9.3.3	<i>Memoria de la Instrucción 1/2009.</i>	39
9.3.4	<i>Modelo de cartel identificativo.</i>	40
10	EL PODER DE ORGANIZACIÓN EMPRESARIAL Y LOS DERECHOS FUNDAMENTALES DEL TRABAJADOR:.....	41
10.1	EL PRINCIPIO DE PROPORCIONALIDAD	41
10.2	¿QUÉ OCURRE CUANDO UN EMPLEADOR INSTALA UN SISTEMA AUDIOVIDEOVISUAL DE CONTROL SIN CUMPLIR LOS REQUISITOS EXIGIDOS?	42
11	LA IMAGEN Y SONIDO COMO DATO PERSONAL Y LA VIDEO-VIGILANCIA:	43
11.1	FUNCIONES	44
11.2	OBJETO.....	44
11.3	CONTENIDO.....	45
12	CONCLUSIONES:	46
13	BIBLIOGRAFIA	47
ANEXO I	48
ANEXO II	49
ANEXO III	50

1 INTRODUCCIÓN:

Mi estudio queda sujeto al análisis de los diferentes temas vinculados a la utilización de la captación y grabación de la imagen y sonido mediante sistemas tecnológicos de video-cámaras en el ámbito laboral. Esta propuesta de estudio la escogí por mi interés en lo que implica la práctica de esta actividad desplegada por las empresas en el ámbito laboral. Y por otro lado, por ser un tema de vital importancia y actualidad.

Con este estudio, he querido centrar la metodología de trabajo en un análisis coherente y coordinado, es decir, desde una perspectiva Jurídico-laboral. De forma que he tenido que consultar fuentes de información que tenía a mi alcance, bien en soporte papel o bien en soporte digital.

Desarrollo el estudio con una parte teórica e introductoria sobre la video-vigilancia en el ámbito laboral y los derechos fundamentales que puedan quedar afectados por esta práctica empresarial. Y a medida que avanzo en el trabajo, me voy centrando en los principios de la jurisprudencia social y constitucional, la normativa nacional e internacional, justificando, en ocasiones, a la parte empleadora, y en otras, a la parte trabajadora. Para ello, es de vital importancia conocer el contexto en el cuál, se produce tal control empresarial.

Con mi trabajo he pretendido alcanzar los siguientes objetivos:

- Conocer de cerca, con qué fines, se lleva a cabo la utilización en los procesos de trabajo la aplicación de las nuevas tecnologías de la información y de la comunicación, en la facultad de control, ejercida por el empresario. En la medida en que la utilización de los medios tradicionales de supervisión se han quedado obsoletos.
- Cómo se cuestionan las nuevas formas de vigilancia por sus repercusiones en los derechos fundamentales a la intimidad, la propia imagen y protección de datos .
- Las consecuencias jurídicas, sustantivas y procesales, de la medida empresarial.
- A través del debate doctrinal, he querido comprobar los elementos que permiten alcanzar un punto de equilibrio entre el necesario respeto a los derechos fundamentales en el trabajo y las exigencias que se derivan del uso y el control de las nuevas tecnologías en la empresa.

Efectivamente, la recogida y/o el tratamiento de imágenes con fines de vigilancia es una praxis muy frecuente en nuestra sociedad. Es decir, en la actualidad abundan cámaras por doquier: ya sea en el lugar de trabajo, en los medios de transporte, en las grandes superficies, en los lugares de ocio, en los comercios de nuestro barrio, etc. La video-vigilancia generalmente tiene como finalidad salvaguardar la seguridad de los bienes y las personas o se utiliza en entornos empresariales con la finalidad de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Ambas finalidades constituyen bienes valiosos dignos de protección jurídica, pero sometidos al cumplimiento de ciertas condiciones. La utilización de medios tecnológicos para la vigilancia incide de forma negativa sobre los derechos de las personas lo que obliga a fijar garantías.

En particular, la video-vigilancia permite captar, y en su caso grabar, información de la persona en forma de imágenes. *"Cuando su uso afecta a personas identificadas o identificables esta información constituye un dato de carácter personal a efectos de la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre de protección de los datos de carácter personal (LOPD)".*

La aplicación de la Ley Orgánica a estos sistemas plantea cierto grado de dificultad en todos los ámbitos. Por una parte, el responsable debe ser capaz de identificar si el uso que hace de las videocámaras se encuentra sujeto a la Ley. Resulta complejo informar al titular de los datos y hacerlo con criterios fáciles de entender e identificar y homogéneos.

Sin embargo, a diferencia de la video-vigilancia desarrollada por las Fuerzas y Cuerpos de Seguridad que cuenta con legislación específica que la regula, la única regulación existente en el ámbito privado, la Ley 23/1992 de 30 de julio, de Seguridad Privada, derogada por la nueva Ley 5/2014, 4 de abril, de Seguridad Privada¹, no contenía ni contiene indicaciones precisas en materia de protección de datos. Y es evidente, y así lo ha destacado el Tribunal Constitucional en distintas sentencias, que la video-vigilancia es un medio particularmente invasivo y por ello resulta necesaria tanto la concurrencia de condiciones que legitimen los tratamientos, como la definición de los principios y garantías que deben aplicarse.

Por todo ello, y con la finalidad de adecuar estos tratamientos a la ley Orgánica 15/1999 se dictó la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con

¹<http://www.boe.es/buscar/pdf/1992/BOE-A-1992-18489-consolidado.pdf>.
[Consulta: 26/05/ 2014]

finés de vigilancia a través de sistemas de cámaras o videocámaras, junto a la de otras agencias de Protección de datos, la de la Comunidad Autónoma de Madrid y la de la Comunidad Autónoma de Cataluña, las cuales dictaron su respectivas instrucciones.

Pero junto a la video-vigilancia, vinculada a la seguridad o al control laboral, surgen nuevos usos y servicios basados en la captación y el tratamiento de imágenes registradas por videocámaras o webcams. Por eso, en los casos en los que estas imágenes pertenecen a personas identificadas o identificables resulta de aplicación la LOPD.

Es por ello, que nos planteamos si la cámara de vídeo en el lugar de trabajo no es más que una ampliación de la mirada del empresario y los micrófonos de la capacidad de audición de los servicios empresariales de vigilancia. En este supuesto, entre el control de antaño por parte del empleador y el nuevo control tecnológico, se daría un salto abismal, porque este nuevo control tecnológico se convertiría en un control permanente, por tanto sería un control con más intensidad.

2 La Video-vigilancia y los derechos fundamentales²

Partimos de un hipotético supuesto caso: un empresario despide a un trabajador justificándolo a efectos de: al incumplimiento de las obligaciones laborales por parte del asalariado. Por lo que se impugna el despido por el trabajador por la vía jurisdiccional, la prueba más importante del empresario en el proceso laboral es a través de una filmación obtenida mediante una cámara de video-vigilancia. Tal situación suscita previamente dos cuestiones: una en el orden sustantivo y otra en el orden procesal:

- En el orden sustantivo nos preguntamos, ¿Puede el empresario vigilar al trabajador mediante una videocámara? .
- En el orden procesal nos preguntamos, ¿Puede el empresario utilizar esas grabaciones como prueba en el posterior procesal laboral?. El tema no resulta insignificante.

En el sustantivo, el trabajador puede ver afectados derechos fundamentales por la utilización de la video-vigilancia. Estos Derechos fundamentales son recogidos en nuestra Norma Suprema: La Constitución Española: la dignidad de la persona (art.10.1), la libertad ideológica (art.16), Derecho a la intimidad personal o a su propia imagen (art.18.1) y la protección frente al tratamiento de datos de carácter personal (art.18.4).

Por lo tanto, el contenido asignable a los derechos fundamentales que pueden verse especialmente afectados por la toma video-gráfica en el lugar de trabajo son concretamente:

- **El derecho a la intimidad (art.18.1 CE)**
- **El derecho a la imagen (art.18.1 CE)**
- **El derecho a la Protección de datos (art.18.4 CE)**

2.1 El derecho a la intimidad

El derecho a la intimidad (art.18.1CE) que implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, *"según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana"*. Se

² ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726.Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch,Valencia,2010, pág. 46-47

garantiza, por tanto, *"el secreto sobre la propia esfera de la vida personal, prohibiendo a los terceros, particulares o poderes públicos, decidir sobre los contornos de la vida privada"* (por todas, SSTC 83/2002, de 22 de abril, y 70/2009, de 23 de marzo).

Igualmente y en relación al mismo derecho a la intimidad del trabajador reconocido por el Art.18.1 ET que garantiza su inviolabilidad, se admite una excepción a esta inviolabilidad y es la establecida en el Art.18 ET³.

2.2 El derecho a la imagen

El derecho a la imagen (art.18.1CE) constituye el poder de determinar la información referida a rasgos físicos personales que pueden ser objeto de conocimiento o difusión por parte de terceros. *"Este bien jurídico se salvaguarda reconociendo a la persona la facultad de evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de toda persona"*, en cuanto instrumento básico de identificación y proyección exterior, factor imprescindible para su propio reconocimiento como sujeto individual (por todas, SSTC 83/2002, de 22 de abril y 7/2007, de 16 de abril).⁴

Por tanto, la suscripción del contrato del trabajo no comporta para el asalariado la pérdida de los derechos que le corresponden en cuanto a ciudadano (STC 88/1985, de 19 de julio, STC 6/1995, de 10 de enero y STC 106/1996, de 12 junio). Hoy en día, no se puede negar que el trabajador pone a disposición del empleador únicamente su fuerza de trabajo y Nunca su persona.

Aunque, es indiscutible que la video-vigilancia, por la intensidad en que se produce, acaba afectando a derechos fundamentales del trabajador, especialmente (al derecho a la intimidad y a la imagen del trabajador).

No olvidemos que la propia Constitución Española es garantista del "Derecho al honor, a la intimidad personal y familiar y a la propia imagen" (art.18.1). Pues bien en relación a este derecho fundamental , la Ley Orgánica 1/1982, 5 de mayo, de protección Civil del Derecho al Honor, a la intimidad Personal y familiar y a la propia imagen, considerará intromisión ilegítimas en el ámbito de protección delimitado por

³ Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores:Art.18: *"Sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible"*.

⁴ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726.Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch,Valencia,2010, pág.34-35.

los artículos (7.1 , 7.2 y 7.5)⁵. Sin embargo la mencionada Ley Orgánica 1/1982 contempla y reconoce unas excepciones en las que no consideraría intromisiones ilegítimas (Art.8.1 y Art.8.2)⁶.

2.3 El derecho a la Protección de datos

El derecho a la Protección de Datos (art.18.4 CE), *"reconoce al ciudadano, la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos"*⁷.

3 La Video-vigilancia

3.1 fuente de cuestiones procesales.⁸

Aunque, en su art.90 de la LRJS, el legislador reconoce a las partes la posibilidad de aportar cuantos medios de prueba se encuentren regulados en la ley, lo que es una remisión a la LEC, concretamente a su art.299.1, que ordena los medios de prueba que puedan utilizarse en juicio.

⁵<http://www.boe.es/buscar/pdf/1982/BOE-A-1982-11196-consolidado.pdf>. [consulta: 24/03/2014].

La Ley Orgánica 1/1982, 5 de mayo, de protección Civil del Derecho al Honor, a la intimidad Personal y familiar y a la propia imagen: Art.7.1: *"El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas"*; Art.7.2: *"La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o producción"*; Art.7.5: *"La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo casos previstos en el Art.8.2."*

⁶ La Ley Orgánica 1/1982, 5 de mayo, de protección Civil del Derecho al Honor, a la intimidad Personal y familiar y a la propia imagen: Art.8.1: *"No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante"*; Art.8.2.a): *"El derecho a la propia imagen no impedirá: Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público"*.

⁷ <http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/index-ides-idphp.php> [10/03/2014]

⁸ ETXEBERRIA GURIDI ,José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726.Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch, Valencia, 2010, pág. 65-69.

Pues bien, en el precepto mencionado (art.90 LRJS) nos indica concretamente: "*un medio de prueba para acreditar los hechos controvertidos o necesitados de prueba, incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos (...)*", estableciendo en el mismo precepto para su aceptación un requisito: "*que no se hayan obtenido, directamente o indirectamente, mediante procedimientos que supongan la violación de los derechos procesales o libertades públicas*".

Por tanto, encontramos en la Ley Laboral la posibilidad de emplear la video-vigilancia como medios probatorios en el proceso laboral, aunque eso sí, cumpliendo con el requisito ya mencionado.

En todo caso, la decisión del juez de aceptar o no la práctica de la prueba es fundamental en el proceso, puesto que es contenido esencial en el derecho a la tutela judicial efectiva, reconocido en el art.24 CE "*a utilizar los medios de prueba pertinentes para su defensa*", y además, porque se podría dejar al solicitante en situación de indefensión.

En cualquier caso, el conflicto de intereses entre el empleador y el empleado es inevitable cuando el primero opta por hacer uso de mecanismos de video-vigilancia en el centro de trabajo, dado que la video-vigilancia afecta a los derechos fundamentales del trabajador (intimidad, imagen y protección de datos). Por ello, ante tales situaciones y en aplicación al principio configurado por el propio TC "*Principio de Proporcionalidad*", el eje para decidir los casos concretos. Serán los jueces los que en los supuestos concretos apliquen el mencionado principio.

En todo caso, el Juez dará por buena la utilización de la video-vigilancia como prueba, si cumple además con los requisitos del juicio de idoneidad, necesidad y proporcionalidad en sentido estricto, remarcando que se aceptará la instalación de la videocámara si fuera la única manera de probar una irregularidad. Si es así, si cumple todos los requisitos mencionados, entonces el Juez considerará lícita la prueba y la aceptará. En caso contrario, si se produjera un "*choque de trenes*" entre derechos fundamentales del trabajador y la facultad de dirección y control del empresario que se vea afectado el Principio de Proporcionalidad, con una infracción grave de los derechos fundamentales del asalariado, no lo aceptará. Considerando la prueba ilícita, y por tanto, aportación inexistente e ineficaz. Resumiendo, si la fuente de prueba no ha afectado de manera evidente el principio de proporcionalidad, derechos fundamentales, se admitirá el medio de prueba, en caso contrario, no será admisible ante el Juez.

3.2 Concepto y clases de video-vigilancia⁹:

Entendemos como video-vigilancia la actividad de vigilancia y protección de las personas y bienes ejercida a través de un sistema de seguridad electrónico que combina la captación y grabación de imágenes y/o sonidos como medio preventivo contra robo o intrusión, cuyas señales son tratadas por una Central de Alarmas de una empresa de seguridad privada y que está sujeta de generar una intervención policial. Dicha definición está conceptualizada dentro del ámbito de la seguridad privada. Pero aplicando el concepto al ámbito laboral, nos encontramos ante un mecanismo de control y vigilancia basado en un sistema de captación de imágenes y/o grabación de sonidos utilizados por el empleador en el lugar de trabajo.

Ahora bien, en las diferentes clases de video-vigilancia, es importante que nos centremos entre la 1) utilizada por un empresario en su centro de trabajo a través de empresas de seguridad privada, de aquella 2) utilizada por las Fuerzas y Cuerpo de Seguridad en lugares públicos¹⁰:

3.2.1 La video-vigilancia por razones de seguridad

La video-vigilancia realizada a través de empresas de seguridad privada en el ámbito laboral ofrecen servicios de vigilancia y seguridad de personas y bienes, que tienen la consideración de actividades complementarias y subordinadas a la seguridad pública (art.1 Ley 23/1992). La Ley 23/1992¹¹ faculta a estas empresas de seguridad privada especialmente para instalar y mantener aparatos, dispositivos y sistemas de seguridad (art.5.1.e)) y el Reglamento de seguridad privada (Real Decreto 2363/1994, de 9 de diciembre. art.39) reconoce el ejercicio exclusivo para la instalación y mantenimiento de sistemas de seguridad electrónica contra robo o intrusión y contra incendios a las empresas de seguridad privada que estén previamente autorizadas mediante su

⁹ ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726.Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch,Valencia,2010, pág. 46-47.

¹⁰ 2) La video-vigilancia utilizada por las Fuerzas y Cuerpos de Seguridad en lugares públicos se regula mediante la Ley Orgánica 4/1997, de 4 de agosto, desarrollada y ejecutada mediante el Real decreto 596/1999, de 16 de abril. Por lo que, la instalación y uso de videocámaras o de cualquier otro medio análogo de captación, tratamiento y reproducción de imágenes por las Fuerzas y Cuerpos de Seguridad del Estado está sujeta a un régimen de autorización previa por órganos con participación judicial. Aplicándose el principio de proporcionalidad, y ello conlleva doble vertiente que es de idoneidad e intervención mínima, que exige la consideración entre la finalidad pretendida y la posible afectación de los derechos fundamentales de los individuos.

¹¹ <http://www.boe.es/buscar/pdf/1992/BOE-A-1992-18489-consolidado.pdf>. [Consulta: 26/05/ 2014].

inscripción en un Registro que se llevará en el Ministerio de interior.

El procedimiento de estas empresas de seguridad privada en el ámbito de los lugares de trabajo la Ley 23/1992 (art.3) establece un límite sustancial:

No pueden intervenir en la celebración de reuniones y manifestaciones, ni el desarrollo de conflictos políticos o laborales, ni ejercer ningún tipo de control sobre opiniones políticas, sindicales o religiosas, quedándoles terminantemente prohibido la creación o mantenimiento de bancos con esta finalidad. Y se les veta la comunicación a terceros de cualquier información obtenida en el ejercicio de sus funciones. Cabe destacar que la actuación de dichas empresas en relación a la utilización de video-vigilancia está sometido al régimen jurídico establecido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (LOPD). Corresponde a la Agencia de Protección de Datos las funciones de control y vigilancia de la actividad de las empresas de seguridad privada respecto a los datos personales.

3.2.2 La video-vigilancia como mecanismo de control y vigilancia del empresario:¹²

Si nos situamos dentro del contexto de la Libertad de empresa (art.38 CE), el contrato laboral, y la relación jurídico-laboral, permite al empleador, en el ejercicio de su función de control y dirección de la actividad laboral, adoptar medidas que estime más oportunas de vigilancia y control para poder comprobar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Así lo reconoce, hace ya mucho tiempo el art.20.3 ET, estableciendo como único límite a la adopción y aplicación de las medidas que el empresario pueda adoptar en el ejercicio de su actividad de vigilancia y control, la consideración adecuada a la dignidad humana del trabajador y, de igual forma, a la capacidad real de los trabajadores con algún grado de discapacidad. En la misma línea, el propio ET en su (art.4.2.e)): reconoce al trabajador, en relación de trabajo, el derecho "al respeto de su intimidad y a la consideración debida a su dignidad".

Pero sin cuestionar la facultad del empresario de dirigir y controlar, hecho "necesario para la buena marcha de la organización productiva" (STC 98/2000, de 10 de abril y STC 186/2000, de 10 de julio). Cabe decir que nada tiene que ver la situación actual con la que se vivía antes en relación al control visual humano que ejercía el empleador pues hoy en día, la video-vigilancia permite al empresario un pleno y excelente control

¹² ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726.Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch,Valencia,2010, pág. 49-50.

no sólo de su patrimonio, sino también de la actividad laboral de sus trabajadores, con el fin de asegurar la buena marcha de la organización productiva. Consiguiendo así, una total fiscalización de la actividad del trabajador, de forma que conoce su actuación de manera continuada, con la finalidad de detectar actitudes fraudulentas o desleales. Pero no hay que descuidar que dicha fiscalización puntual de un determinado trabajador o grupo de trabajadores debe ser una medida excepcional que deberá justificarse y acompañarse de toda una serie de garantías.

Pero al tiempo que se permite al empresario la adopción de medidas que estime más oportunas de vigilancia y control para comprobar el cumplimiento por el trabajador de sus obligaciones y deberes laborales aunque con las limitaciones recogidas en nuestro ordenamiento jurídico " al respeto de su intimidad y a la consideración debida a su dignidad del trabajador y la capacidad real de los trabajadores disminuidos". Por otro lado, el propio Estatuto de los Trabajadores (ET) establece un requisito al respecto en su artículo (64.4 d)): El comité de empresa debe emitir un informe previo. Este derecho aplicable de igual modo, a los delegados sindicales en aplicación del art.10.3 de la Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical, exige que la empresa que quiera instalar videocámaras informe a los representantes de los trabajadores cómo se va a realizar el control, las pautas que se van a seguir en la instalación de la videovigilancia, sus objetivos, si se van a grabar o no las imágenes (el hecho de no grabarlas lo único que implicaría es visualizar las imágenes en tiempo real sin quedar registradas en ningún fichero), sobre el acceso a las mismas, su conservación y cancelación,...entendiéndose que dicha información facilitada por el empresario a los trabajadores se rige bajo las exigencias de buena fe que marca la relación laboral.

4 Los principios de jurisprudencia social y constitucional.

4.1 La inicial Doctrina Judicial Permisiva de la Video-vigilancia empresarial:

Como consecuencia de un proceso de simplificación del contenido del derecho que afecta al trabajador, se ha llegado a excluir del ámbito protegido del derecho a la dignidad e intimidad del trabajador las relaciones profesionales o la actividad laboral, de manera que se ha permitido cualquier dispositivo de control de la actividad laboral del trabajador.

De manera que los Tribunales, durante mucho tiempo, han admitido y sin muchas contemplaciones la cuestión de los empleadores donde sin lugar a dudas podían utilizar mecanismos que permitieran la captación de imágenes para comprobar el cumplimiento por el empleado de sus obligaciones y deberes laborales, asentando su admisión discrecional que el centro de trabajo es un lugar público en el que el derecho a la intimidad no se ve afectada.

La consideración del respeto a la dignidad humana del trabajador como límite impuesto a la utilización de mecanismos de vigilancia y control empresarial en el propio art.20.3 ET apenas durante este tiempo tuvo modulación alguna hacia la mirada fiscalizadora del empresario. Tan sólo se tenía en cuenta en los espacios reservados al uso privativo de los trabajadores, como los servicios higiénicos, vestuarios, zonas de descanso, con ello se asentaba una caracterización espacial de la intimidad. Y por consiguiente, la protección de la intimidad del trabajador se delimitaba, al ámbito espacial, que cada empleador mantenía reservado para sus empleados, y no en función de la inviolabilidad de la persona que puede afirmarse en cualquier lugar.

Tal permisividad, en un principio ha permitido propiciar la inicial Jurisprudencia del Tribunal Constitucional, declarando en su STC 142/1993 que la intimidad: *"no comprende en principio los hechos referidos a las relaciones sociales y profesionales que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada"*.

De manera que esta posición relativa a esta cuestión¹³ se ha ido observando en la mayoría de las sentencias que hasta mediados del año 2000 se fueron dictando:

- En la STSJ de Cataluña de 25 de abril de 1994¹⁴, se acepta con total naturalidad, la instalación en un hotel, para fines de control de la actividad laboral, de un circuito cerrado de televisión, con cámaras de filmación y grabación de sonido, ubicadas a modo de luces empotradas, y con un radio de acción que abarca el mostrador de recepción, su caja, el departamento de reservas, la entrada de servicio, el restaurante, la barra del bar, el vestuario, el parking y el office de la cocina, apuntando que la medida no vulnera el derecho a la intimidad porque de *"entenderlo así, supondría extender la protección de tales derechos a instalaciones que suponen la práctica totalidad de espacios públicos del hotel en el que éste presta sus servicios a los clientes, y en consecuencia donde los trabajadores desarrollan su actividad"*.
- En la STSJ de Cataluña de 28 de 1 marzo de 1995¹⁵, siguiendo la misma línea que la sentencia anterior. En la valoración del Tribunal, obvia también, el ámbito configurador del derecho a la intimidad y, por tanto, considera lícita la instalación en un centro de trabajo dotado de un sistema de imagen de circuito cerrado consistente en una cámara de vídeo, situada en la nave central del centro de trabajo, conectada a una pantalla, desde la que se hacía el seguimiento de los trabajadores, basándose en el art. 20.3 ET¹⁶ permite al empresario utilizar los medios que estime necesarios para efectuar el control y vigilancia por los trabajadores de sus obligaciones y derechos laborales, que entre tales medios, nada impide que pueda utilizarse un sistema visual electrónico, a través de cámaras captadora de imagen siempre que se guarde la consideración debida a la dignidad humana del empleado, y que según sentencia, no se estimó vulnerada, puesto que el uso del dispositivo de video-vigilancia no constaba como probado que se había extralimitado fuera del ámbito estrictamente laboral, que era su finalidad. Y por considerar, que el lugar donde se

¹³SÁNCHEZ-RODAS NAVARRO, Cristina, Videocámaras y poder de vigilancia, Aranzadi Social, num.5, Tomo IX, 1999, pág.1127. *"Quiere con ello decirse que intramuros de la empresa y en horario laboral apenas existe espacio de intimidad que salvaguardar por cuanto que en tales circunstancias la obligación del trabajador es cumplir con su prestación laboral..."*

¹⁴GOÑI SEIN, José Luis, "La Video-vigilancia empresarial y la Protección de datos Personales", Thomson-Aranzadi, Pamplona, 2007.pág. 28-29.

¹⁵SSTSJ de Cataluña de 1 de marzo de 1995 (AS1995/1086).

¹⁶ Artículo 20.3 ET: *"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso"*.

lleva a cabo el trabajo, no es coincidente con el ámbito de la vida íntima de las personas, sino que cobra una dimensión pública.

4.2 Interpretación Correctora efectuada por el Tribunal Constitucional:

La consolidada doctrina judicial sobre la permisividad de los mecanismos audiovisuales en los puestos de trabajo para el control de la actividad de los trabajadores, ha quedado, sin embargo, desautorizada por el propio Tribunal Constitucional en las SSTC 98/2000 y 186/2000. Dichas sentencias, serán objeto de análisis y estudio en las siguientes páginas. Sentencias del Constitucional que marcarán un punto de inflexión importante en lo que se refiere, a la consideración de la intimidad en el lugar de trabajo, como respecto de los límites a la posible utilización de los sistemas de video-vigilancia en el ámbito laboral.

5 Jurisprudencia del Tribunal Constitucional (TC) en su sentencia STC 98/2000, 10 abril:

5.1 Exposición de los hechos

- 1. La STC 98/2000** censura la decisión de la empresa Casino de La Toja de instalar micrófonos en las zonas de caja y de ruleta francesa que permitían grabar las conversaciones en esas zonas con el objetivo de reforzar la seguridad del casino y poder resolver mejor las eventuales reclamaciones de los clientes.
- 2.** Este sistema permite registrar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial y por tanto innecesarios desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir cohibidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa. Se trata, en suma, de una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE, *"pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores del casino mantengan entre sí o con los clientes"* (FJ 9).
- 3.** En base a todo lo anterior, las limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial

merecedor de tutela y protección, es decir, que si existen otras medidas de satisfacer dicho interés empresarial menos agresivas y lesivas del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y lesivas. En definitiva, se trata, de aplicar el principio de proporcionalidad.

4. Por tanto, la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación, teniendo en cuenta de que la empresa ya disponía de otros sistemas de seguridad que es el sistema de audición que pretende implantar.
5. No existe normativa específica que regule la instalación y utilización de estos mecanismos de control y vigilancia basados en sistemas de captación de imágenes o grabación de sonidos dentro de los centros de trabajo, por lo que serán los órganos jurisdiccionales (y, en último caso, el TC) los encargados de ponderar, en caso de conflicto, en qué circunstancias puede considerarse legítimo su uso por parte del empresario, para ejercer el poder de dirección que le reconoce el art.20 LET, atendiendo siempre al respeto de los derechos fundamentales del trabajador, y muy especialmente al derecho a la intimidad personal que protege el art.18.1 CE, teniendo siempre presente el principio de proporcionalidad.
6. En definitiva, a juicio del Tribunal Constitucional *“la implantación del sistema de audición y grabación no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial, pues la finalidad que se persigue (dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes del casino)”*. Dado que la implantación de este sistema, como ya se ha dicho en líneas anteriores, permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde una perspectiva de control del cumplimiento laboral.

6 Jurisprudencia del Tribunal Constitucional (TC) en su sentencia STC 186/2000, 10 julio.

6.1 STC 186/2000

La **STC 186/2000** enjuicia por su parte el caso de una empresa que, ante la sospecha de la existencia de irregularidades en su economato motivadas por la existencia de un llamativo descuadre contable, decidió instalar un circuito cerrado de televisión para controlar la actividad laboral de tres de sus cajeros. Las cintas de vídeo grabadas revelaron que uno de ellos realizó de forma continuada maniobras en el cobro de artículos a los clientes del economato, detrayendo diferentes cantidades de la caja. Por este motivo fue expedientado y despedido de la empresa. Tras agotar sin éxito la vía judicial laboral, el trabajador acudió en vía de amparo ante el Tribunal Constitucional para denunciar que ese tipo de control laboral vulneró su derecho a la intimidad personal y a la propia imagen (art. 18.1 CE), y que la instalación de esa medida de control laboral no fue comunicada al Comité de empresa, según exige el Estatuto de los Trabajadores.

En esta ocasión el Tribunal Constitucional denegó el amparo solicitado afirmando que *“la intimidad del recurrente no resulta agredida por el mero hecho de filmar cómo desempeñaba las tareas encomendadas en su puesto de trabajo, pues esa medida no resulta arbitraria ni caprichosa, ni se pretendía con la misma divulgar su conducta, sino que se trataba de obtener un conocimiento de cuál era su comportamiento laboral, pretensión justificada por la circunstancia de haberse detectado irregularidades en la actuación profesional del trabajador, constitutivas de transgresión a la buena fe contractual. Se trataba, en suma, de verificar las fundadas sospechas de la empresa sobre la irregular conducta del trabajador, sospechas que efectivamente resultaron corroboradas por las grabaciones video-gráficas, y de tener una prueba fehaciente de la comisión de tales hechos, para el caso de que el trabajador impugnase, como así lo hizo, la sanción de despido disciplinario que la empresa le impuso por tales hechos”* (FJ 7). Para añadir que *“el hecho de que la instalación del circuito cerrado de televisión no fuera previamente puesta en conocimiento del Comité de empresa y de los trabajadores afectados [...] carece de trascendencia desde la perspectiva constitucional, pues [constituye], una cuestión de mera legalidad ordinaria”*.

6.2 Determinación y comprobación del Tribunal Constitucional

En la **STC 186/2000**, el **Tribunal Constitucional** determina que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario comprobar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (**juicio de idoneidad**), si además es necesaria,

en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (**juicio de necesidad**), y, finalmente si es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (**juicio de proporcionalidad en sentido estricto**). De todo ello deben ser informados previamente los representantes de los trabajadores.

Conforme a la doctrina del Tribunal Constitucional, el **principio de Proporcionalidad** requiere el cumplimiento de estos tres requisitos:

- **Juicio de idoneidad o adecuación**
- **El Juicio de necesidad**
- **Juicio de proporcionalidad en sentido estricto**

6.2.1 Juicio de idoneidad o adecuación

El juicio de idoneidad o adecuación: La medida de utilización de video-vigilancia elegida por el empleador deberá ser adecuada para conseguir el objetivo o el fin perseguido. El TC, entiende que se da por cumplido este requisito cuando, existan razonables sospechas de la actuación por parte del trabajador de graves irregularidades en su puesto de trabajo, donde el empresario opta por instalar un circuito cerrado de televisión enfocando directamente al trabajador en su puesto de trabajo. Pues bien, el TC consideró en su STC 186/2000, que la medida adoptada por el empresario resultó idónea para poder comprobar *"si el empleado cometía efectivamente las irregularidades sospechadas por el empleador y en tal caso poder adoptar las medidas disciplinarias correspondientes"*.

A todo ello, hay que añadir que el único objetivo de la instalación de dicha video-vigilancia debe ser con la finalidad de la existencia de comprobar razonables

sospechas y nunca ser una intromisión en la intimidad de los trabajadores¹⁷.

6.2.2 El Juicio de necesidad

El Juicio de necesidad: La medida de utilización de video-vigilancia en el centro de trabajo debe resultar necesaria, es decir, que no exista otra medida más moderada con los derechos fundamentales del trabajador para obtener el mismo objetivo con la misma eficacia. Por ello, decimos que esta medida de video-vigilancia debe ser como *ultima ratio*. El TC, al respecto, mantiene en su STC 186/2000, 10 de julio, que existiendo razonables sospechas de la actuación del asalariado de graves irregularidades en su puesto de trabajo, pues la grabación sirve de prueba procesal de los hechos.

6.2.3 Juicio de proporcionalidad en sentido estricto

El Juicio de proporcionalidad en sentido estricto: la medida de utilización de video-vigilancia debe ser ponderada o equilibrada. Es decir, deberá derivarse de la misma más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto¹⁸. En este sentido, el TC exige que la grabación se limite a zonas comunes y a una duración temporal limitada. Respecto a las zonas comunes, el juicio de proporcionalidad exige que el control por video-vigilancia se limite al ámbito físico imprescindible, sin que por ello, sea posible un control genérico de todo el espacio laboral. En la misma dirección, no se pueden controlar espacios especialmente íntimos o protegidos por el Derecho a la intimidad (duchas, baños, taquillas...).

Por tanto, en esta STC 186/2000, nuestro máximo intérprete de nuestra carta magna (TC) da por buena la instalación de un dispositivo de vigilancia por el empleador, basándose en las razonables sospechas donde la actuación del trabajador de graves irregularidades en su puesto de trabajo y que la opción de establecer por parte del empresario un circuito cerrado de televisión enfocando directamente al empleado en

¹⁷ http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf [Consulta: 20/03/2014].

El repertorio de recomendaciones de la OIT, Protección de los datos personales de los Trabajadores, OIT, Ginebra 1997: *"Los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información, no deberían servir para controlar el comportamiento de los trabajadores"*.

¹⁸ En relación de las STC 98/2000, de 10 de abril y STC 186/2000, 10 de julio: Anuario de facultade de Dereito da Universidade da Coruña, num.5/2001, dentro de este juicio de Proporcionalidad en sentido estricto diferencian el juicio de alteración y el juicio de justificación. Conforme al primero: El juicio de alteración: la medida del empresario de instalar un sistema de video-vigilancia no debe alterar el contenido esencial del derecho fundamental. Conforme al segundo: El juicio de justificación: La medida del empresario, además, de dar restricción del derecho fundamental en grado tolerable a la luz del fin perseguido.

su lugar de trabajo, se constata *"que la grabación de imágenes se limitó a una duración temporal limitada, suficiente como para poder comprobar que no se trataba de un hecho aislado o de un mal entendido, sino que la conducta ejercida por el empleado era una conducta ilícita y reiterada"*. En esta conclusión, queda reflejada la prohibición de la instalación de dispositivos de vigilancia de manera permanente en el centro de trabajo¹⁹. Por todo ello, en esta Sentencia, el Tribunal Constitucional negó el amparo al trabajador.

¹⁹http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf [Consulta:20/03/2014].

La OIT en su repertorio de recomendaciones prácticas, Protección de datos personales de los trabajadores, OIT, Ginebra, 1997,pp.21, tanjante mantiene 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. Por ello, defiende que se debe delimitar 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.

7 Jurisprudencia del Tribunal Constitucional (TC) en su sentencia STC 29/2013, 11 febrero

7.1 Exposición de los hechos

La reciente **STC 29/2013**, de 11 de febrero (recurso de amparo núm. 10522-2009), declara una doctrina que sujeta el ejercicio de las facultades del empresario al cumplimiento del deber de información previa a los trabajadores acerca del contenido y objetivo específicos de la correspondiente medida de vigilancia y control. Un Recurso de amparo al TC que gira en torno al uso de una instalación de video-vigilancia dedicada al control de accesos a edificios de una universidad para justificar el incumplimiento reiterado de una determinada persona de su jornada laboral.

El recurso lo interpuso el Sr. Fraile, un trabajador de la Universidad de Sevilla, que había sido sancionado con la suspensión temporal de empleo y sueldo por incumplir injustificada y reiteradamente su jornada laboral. En prueba de la infracción corregida, la Universidad, que desde hacía tiempo sospechaba que el Sr. Fraile no cumplía con su horario laboral, se decidió hacer uso de las grabaciones de las cámaras de video-vigilancia que tenía instaladas en los accesos al recinto universitario para controlar el acceso a sus campus y centros. Dos de esas cámaras apuntaban al acceso directo del despacho del Sr. Fraile.

7.2 Descripción de los hechos en la propia sentencia.

"El recurrente en amparo presta sus servicios desde octubre de 1989 en la Universidad de Sevilla, con la categoría profesional del director de servicio habilitado, desarrollando sus funciones como subdirector de la unidad técnica de orientación e inserción profesional. Ante la sospecha de irregularidades en el cumplimiento de su jornada laboral, el director de recursos humanos decidió que el jefe de la unidad de seguridad articulase los medios precisos para determinar las horas de entrada y salida del demandante de su puesto de trabajo durante los meses de enero y febrero de 2006 para lo que debía valerse, si fuera necesario, de la información de las cámaras de video instaladas en los accesos a las dependencias. En consecuencia, en marzo de 2006, se acordó la incoación de un expediente disciplinario. Por resolución rectoral de 31 de mayo de 2006 se le impusieron tres sanciones de suspensión de empleo y sueldo de tres meses cada una, por la comisión de tres faltas muy graves, pudiendo ser por: faltas reiteradas e injustificadas de puntualidad en la

*entrada al trabajo durante diez o más días en un mes, cometidas los meses de enero y febrero de 2006 [Art.54.2 a) de LET y apartado 1.C.8 del anexo III del convenio colectivo aplicable]; transgresión de la buena fe contractual y abuso de confianza, consistente en hacer constar en las hojas de control de asistencia una hora de entrada al trabajo que no se corresponde con la real [art.54.2 d) LET y apartado 1.C 4 del anexo III del convenio colectivo]; y faltas de asistencia injustificadas al trabajo durante más de tres días en un mes, cometidas los días 16,17,20,21 y 22 de febrero de 2006 [art.54.2 a) **LET y apartado 1.C 7 del anexo III del convenio colectivo**]*".

En consecuencia, la Universidad de Sevilla, debida a la existencia de serios indicios de que el sujeto en cuestión, incurría de forma reiterada al incumplimiento de la jornada laboral, decide para comprobar tales irregularidades y sin información previa al trabajador, utilizar una instalación de video-vigilancia instalada en el campus con otra finalidad (control de acceso de las personas de la comunidad universitaria y del personal de empresas externas a sus campus y centro), aprovechando que dos de las cámaras que componen la instalación controlan los dos únicos accesos a las dependencias donde presta servicios el trabajador, según se refleja en la Sentencia del Tribunal Constitucional.

De forma, que el control realizado por parte de la Universidad de Sevilla, a través de las imágenes grabadas por esas cámaras, la Universidad pudo verificar que mientras que en las hojas de control de asistencia de su unidad administrativa, correspondientes a los meses de enero y febrero de 2006, el citado trabajador firmó cada día como momento de entrada las 8:00 horas y, de salida, las 15:00 horas. Las imágenes grabadas por las cámaras demostraban, sin embargo, que durante esos días, en más de dos docenas de veces, el Sr. Fraile entró a trabajar con un retraso de entre treinta minutos y varias horas.

El Trabajador impugnó dichas sanciones ante los Juzgados de lo Social. En particular razonó que la utilización de las imágenes grabadas para fines de control laboral no había sido autorizada de modo expreso por la AEPD ni comunicada formalmente tampoco a los trabajadores de la Universidad, que en consecuencia desconocían simplemente esa posibilidad. Tanto el Juzgado de lo Social, en primera instancia, como la Sala de lo Social del Tribunal Superior de Justicia de Andalucía, después y por dos veces, rechazaron la pretensión del recurrente y afirmaron, en su lugar, la plena legitimidad de la prueba video-gráfica utilizada por la Universidad, dichas

resoluciones irán en la línea que el propio TC a través de sentencias como la 186/2000, donde se permitía **excepcionalmente un control oculto**..

Con estos antecedentes el asunto termina finalmente en el Tribunal Constitucional. En su demanda de amparo el Sr. Fraile insistió en que la utilización no consentida ni previamente conocida de las imágenes grabadas por las cámaras de seguridad del recinto universitario para controlar su actividad laboral vulneró **su derecho a la protección de datos de carácter personal (art. 18.4 CE)**, según ha sido **interpretado entre otras**, pero de modo principal, por **la STC 292/2000, de 30 de noviembre**.

La cuestión debatida, en el caso que nos ocupa, no está en la instalación oculta (supuesto excepcional) que ataca al derecho fundamental a la intimidad reflejado en art.18.1 CE, y por el que el TC, ya se ha pronunciado en varias ocasiones argumentando que no se vulnera dicho derecho siempre y cuando no se supere el juicio de proporcionalidad. Sino que en este caso, el derecho afectado es el derecho a la protección de datos de carácter personal del 18.4 de la constitución y, más concretamente, en la ausencia de la información que debe ofrecerse al afectado sobre los tratamientos de datos que se pretende efectuar. La Universidad no informó al trabajador de que iba a utilizar las imágenes de las cámaras para un fin distinto al que justificó su instalación, esa falta de información afecta a una de las garantías nucleares del derecho fundamental y, por lo tanto, el uso dado por la Universidad a esas imágenes es contrario a derecho. En mi opinión, en aquellas sentencias en las que el TC se ha pronunciado a favor del las instalaciones ocultas, recordar STC 186/2000, pues se habrían dictado en contrario en otro sentido, es decir, a favor de los recurrentes si hubiesen invocado en su recurso el art.18.4 CE pero como así no se hizo entonces, el Tribunal, se limitó a valorarlo des del punto de vista únicamente del derecho a la intimidad (art.18.1 CE), dando razón a la empresa.

7.3 Razonamiento del Tribunal Constitucional:

Es evidente que nos encontramos dentro del núcleo esencial del derecho fundamental del art. 18.4. CE, puesto que la Video-vigilancia, ofrece múltiples medios de tratamiento de datos. Sistemas que se amplían y perfeccionan a un ritmo vertiginoso y que se añaden a otros más conocidos (circuitos cerrados de televisión, grabación por dispositivos webcam, digitalización de imágenes o, en particular, instalación de cámaras, incluidas aquellas que se instalan en el lugar de trabajo).

Para el examen del acto empresarial controvertido desde la perspectiva del derecho a

la información del afectado, resulta importante mencionar la STC 292/2000, de 30 de noviembre, del Pleno de este Tribunal. Pues es en esta resolución del TC donde encontramos la solución para el presente recurso y no en otros precedentes de este mismo Tribunal, como son las SSTC 98/2000, de 10 de abril; y 186/2000, de 10 de julio.

Nos recuerda el (FFJJ 4) de la SSTC 292/2000, en efecto, que *" el constituyente quiso garantizar mediante el actual art.18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el FFJJ 5 que: la peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental, tan afín como es el de la intimidad, radica, pues, en su distinta función. En su FFJJ 6, insiste subrayando que: la función del derecho fundamental a la intimidad art.18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de la intromisión de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho afectado....Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que poseen por terceros, quiénes los poseen, y con qué fin"*.

Aunque, es verdad que esa exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles y legalmente previstas, pero no debe olvidarse que la Constitución ha querido que la ley, y sólo la ley, pueda fijar los límites a un derecho fundamental exigiendo además que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido (SSTC57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero, FJ 2 y en relación con el derecho a la protección de datos personales, STC 292/2000, FFJJ 11 y 16).

En aplicación a esa doctrina Constitucional, se concluye que no hay una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales y que tampoco podría situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. Esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su

núcleo esencial.

Por ello, al igual que el interés público en sancionar infracciones administrativas resulta insuficiente para que la Administración pueda sustraer al interesado información relativa al fichero y sus datos, según refleja el art. 5.1 y 2 LOPD (STC 292/2000, de 30 de noviembre, FJ 18), tampoco el interés privado del empresario podrá justificar que el tratamiento de datos sea empleado en contra del trabajador sin una información previa sobre el control laboral puesto en práctica. Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts.6.2 LOPD y 20 LET), o que pueda ser proporcionado al fin perseguido, en el caso de que se trate. Es decir, el control empresarial por esa vía, aunque podrá producirse, el empleador deberá asegurar también la debida información previa.

Pues ahora bien, en el caso enjuiciado de la Universidad de Sevilla, las cámaras de video-vigilancia instaladas en el recinto universitario , zonas de paso público y no dentro del lugar de trabajo, donde reprodujeron la imagen del recurrente y permitieron el control de su jornada de trabajo; captaron, por tanto, su imagen que constituye un dato de carácter personal, y se emplearon para el seguimiento del cumplimiento de su contrato. De los hechos probados se deriva que la persona jurídica titular del establecimiento donde se encuentran instaladas las video-cámaras es la Universidad de Sevilla y que ella fue quien utilizó al fin descrito las grabaciones, siendo la responsable del tratamiento de los datos sin haber informado al trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen.

Además, el hecho de que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección Datos no es proporcional ni contrarresta la vulneración producida del derecho a la protección de datos de carácter personal. Pues era necesaria, además de *"la información previa y expresa, precisa, clara e inequívoca"* a los trabajadores de la finalidad del control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas , durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimiento del contrato del trabajo.

Finalmente, las sanciones impuestas con base en esa única prueba, generador de la vulneración del art.18.4 CE, se declararon nulas. Y es que privada a la persona de su facultad de disposición y control sobre sus datos personales, afecta por ello, su derecho fundamental a la protección de datos.

8 La orientación internacional tendente a situar los límites de la video-vigilancia 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. Además, de la perspectiva desde la que se viene apuntando y analizando actualmente la utilización de las técnicas de video-vigilancia empresarial en distintas instancias internacionales, tanto supranacionales, como comunitarias.

8.1 La OIT: Repertorio de Recomendaciones Prácticas de la OIT de octubre de 1996, Protección de los datos personales de los trabajadores:

El enfoque del problema sobre la video-vigilancia en la medida que se viene apuntando lo impulsó ya hace algún tiempo, la propia Organización Internacional de los Trabajadores en el Repertorio de Recomendaciones Prácticas adoptado en octubre de 1996, concretamente en la ciudad de Ginebra.

Este **repertorio de recomendaciones practicas**²⁰ fue adoptado por una Reunión de expertos sobre la protección de la vida privada de los trabajadores de la OIT. La reunión se efectuó en Ginebra, del 1 al 7 de octubre de 1996, en cumplimiento de una decisión tomada por el Consejo de Administración de la OIT en su 264ª reunión (noviembre de 1995). En la reunión participaron veinticuatro expertos, de los cuales ocho fueron designados por consulta previa con los gobiernos, ocho por consulta previa con el Grupo de los Empleadores y ocho por consulta previa con el Grupo de los Trabajadores del Consejo de Administración.

La finalidad del repertorio de recomendaciones practicas es suministrar orientaciones para la protección de datos personales de los trabajadores. A diferencia de otros instrumentos de la OIT, como los convenios, que son tratados internacionales de carácter obligatorio, o las recomendaciones, que no tienen carácter obligatorio pero comportan ciertas obligaciones en cuanto a los procedimientos, los repertorios de recomendaciones practicas son de una gran flexibilidad ya que no contienen ninguna disposición obligatoria. En cambio, presentan las bases para que los empleadores y los trabajadores puedan determinar reglas en función de sus expectativas y de sus necesidades. Dicho de otra forma, este Repertorio contiene una serie de principios generales sobre protección de datos personales de los

²⁰ http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf [Consulta: 20/03/2014].
OFICINA INTERNACIONAL DEL TRABAJO: Publicación: Repertorio de recomendaciones prácticas: Protección de los datos personales de los trabajadores, OIT, Ginebra 1997.

trabajadores, y disposiciones específicas respecto del acopio, conservación, almacenamiento, uso y comunicación de tales datos, inspirados en principios contemplados en instrumentos de carácter internacional de protección de datos, como las líneas directrices de la OCDE²¹ y el Convenio nº 108/1981 del Consejo de Europa.

En consideración con la OIT²²:

Los mencionados principios se aplican a la vigilancia empresarial, que a efectos del presente repertorio de recomendaciones prácticas, dice lo siguiente: *"la palabra <<vigilancia>>, 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".*(Comentario al punto 3.3).

Respecto al concepto de tratamiento de datos personales del trabajador. Cabe mencionar, que el Repertorio define éste término <<Tratamiento>> de forma amplia, *"el acopio, la conservación, la combinación, la comunicación o cualquier otra forma de utilización de datos personales".* (Comentario al punto 3.2).

Y en relación con el <<Acopio>> de datos personales del trabajador, el Repertorio defiende, un principio de transparencia máxima, de manera que los trabajadores sepan la finalidad para la cual se someten a tratamientos de datos. Así se establece que *"Cuando los trabajadores sean objeto de medidas de vigilancia, estos 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".*(comentario al punto 6.14).

Además, en el mismo punto anterior, el Repertorio obliga 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 sentido, al decir que *"el empleador deberá reducir al mínimo su injerencia en la vida privada de aquéllos".* (Comentario al punto 6.14).

²¹ **OCDE:** La Organización para la Cooperación y el Desarrollo Económicos, es una organización de cooperación internacional, compuesta por 34 estados, cuyo objetivo es coordinar sus políticas económicas y sociales. En la OCDE, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y colaborar a su desarrollo y al de los países no miembros.

²² http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf [Consulta:20/03/ 2014].

Publicación: Repertorio de recomendaciones prácticas: Protección de los datos personales de los trabajadores, OIT, Ginebra 1997.

En cuanto a la <<vigilancia secreta>>, en su Repertorio, contiene un carácter más restrictivo, donde la vigilancia secreta sólo es aceptable en la medida en que se *"realice de conformidad con la legislación nacional o en el caso en el que existan sospechas suficientes de actividad delictiva u otras infracciones graves"*. Aunque, hay que destacar que *"no basta con la existencia de la <<sospecha suficiente>> de tales actividades o infracción por parte del empleado"*, sino que el empresario *"está autorizado al uso de la vigilancia secreta únicamente cuando existan sospechas razonables justificadas"*. (Comentario al punto 6.14.2).

Con el mismo carácter restrictivo, se pronuncia sobre la vigilancia permanente, donde el Repertorio adopta un punto más taxativo, de manera que *"Se ha constatado que una vigilancia continuada es causa de una ansiedad constante, que a sus vez puede originar enfermedades físicas o perturbaciones psicológicas"*. Por ello, 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).

Por otro lado, los representantes de los trabajadores, cuando los haya, y de conformidad con la legislación y la practica nacionales, deberían ser informados y consultados : *"acerca de la instalación o modificación de sistemas automatizados de tratamiento de los datos personales de los trabajadores; y antes, de la instalación de cualquier sistema de vigilancia electrónica del comportamiento de los trabajadores en el lugar de trabajo"*. (Comentario al punto 12.2).

8.2 Grupo Europeo de Comisarios sobre Protección de Datos Personales (GTA)²³:

Dentro de la Unión Europea, el Grupo de Trabajo sobre Protección de datos (**GTA**), instituido **al amparo del Art.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 tratamiento de datos personales, 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.

²³ GOÑI SEIN, José Luis, "La Video-vigilancia empresarial y la Protección de datos Personales", Thomson-Aranzadi, Pamplona, 2007.pág.66-67.

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 95/46/CE, sobre Protección de datos, con el fin de contribuir a la aplicación uniforme de las mismas.

En su **Dictamen nº8/2001**, sobre tratamiento de datos Personales en el ámbito laboral, asume ya claramente este punto, 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 video-vigilancia de los trabajadores está cubierta por las disposiciones de la Directiva y las disposiciones nacionales de aplicación"*²⁴.

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 la Video-vigilancia²⁵, adoptado el 11 de febrero de 2004, declarando y 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.

En consecuencia, se ha podido constatar que los textos internacionales no dejan lugar a dudas al respecto. Tanto el Repertorio de Recomendaciones Prácticas sobre la protección de datos personales de los trabajadores, de la OIT de 1996, como el Dictamen 4/2004 del GTA, excluyen por completo la posibilidad de adoptar sistemas de video-vigilancia destinados directamente a controlar la calidad y cantidad de trabajo.

El Tribunal Constitucional ha juzgado de modo igualmente restrictivo el recurso a tal sistema de video-vigilancia empresarial, excluyendo la posibilidad de ejercer a través de tal método un control continuado e indiscriminado del cumplimiento por los trabajadores de sus obligaciones laborales²⁶

²⁴. https://www.apda.ad/system/files/wp67_es.pdf. [Consulta: 14/04/ 2014].

²⁵. https://www.apda.ad/system/files/wp89_es.pdf. [Consulta: 14/04/ 2014].

²⁶ STC 98/2000, de 10 de abril.

9 Normativa LOPD y las instrucciones:²⁷

Es importante remarcar que la instalación de video-vigilancia en el centro de trabajo bajo la responsabilidad del empresario sin que por ello haya realizado contratación alguna con una empresa de seguridad privada, carecerá de marco jurídico determinado, quedando a disposición de la ponderación que realicen los jueces en el caso concreto del cual se trate, es decir, dependiendo de los intereses en juego (la facultad del empresario de dirección y control y los derechos fundamentales del trabajador). Pero los datos obtenidos mediante dispositivos de captación de imágenes y sonidos en el lugar de trabajo cuentan con un marco jurídico concreto.

9.1 Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos.

Además, de **la LOPD**, tenemos que tener en cuenta la **Instrucción 1/2006**, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia realizados a través de sistemas de cámaras o videocámaras.

Por lo tanto, la Agencia Española de Protección de Datos (LOPD), ha creado, en el ejercicio de la competencia que le atribuye el Art.37.1.c²⁸ LOPD: una Instrucción para adecuar los tratamientos de imágenes con un doble objetivo²⁹.

Esta Instrucción precisa en la instalación de las videocámaras el respeto al principio de proporcionalidad también en el tratamiento de imágenes, principio ya comentado en párrafos anteriores. Para ello se debe ponderar el objetivo a alcanzar y la intromisión en la intimidad de las personas que comporta la utilización de la videocámara como *última ratio*, en el caso que no sea posible emplear otros

²⁷ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726. Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch, Valencia, 2010, pág.62-63.

²⁸<https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf>. [Consulta 17/04/2014]. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: Art.37.1.c: "*Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las Instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley*".

²⁹ Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras: En ejercicio de la competencia que le atribuye el artículo 37.1.c) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Agencia Española de Protección de Datos dicte una Instrucción con un **doble objetivo: 1º)** la adecuación de los tratamientos de imágenes con fines de vigilancia a los principios de la citada LOPD y **2º)** garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos. Es decir, se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona.

mecanismos menos invasivos con respecto a los derechos fundamentales de las personas para obtener un fin legítimo.

La instrucción 1/2006, se aplica al tratamiento³⁰ de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras o videocámaras. Y deja fuera de su ámbito objetivo: los datos personales de aquellas imágenes que se hayan obtenido mediante la utilización de cámaras y videocámaras por las Fuerzas y cuerpos de Seguridad³¹ y el tratamiento de imágenes que se hayan realizado en el ámbito personal y doméstico, es decir, el realizado por una persona física en un marco exclusivamente privado o familiar.

La Instrucción pretende adecuar los tratamientos a los criterios marcados por la jurisprudencia del Tribunal Constitucional al considerar que el tratamiento de datos personales no exige la conservación de los mismos, sino que basta su recogida o grabación. En el mismo sentido se han pronunciado las legislaciones que sobre esta han adoptado los distintos Estados miembros de la Unión Europea, cumpliendo así el mandato contenido en la Directiva 95/46/CE. Además, la Instrucción exige el consentimiento del afectado para el tratamiento de las imágenes e impone el deber de información para los responsables de la videovigilancia, ambos en los términos de la LOPD (arts.5, 6 y 11, respectivamente)³².

Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el art.3 de la ley Orgánica 15/1999 y el art.1.4 del Real Decreto 1322/1994 de 20 de junio, que considera como dato personal la información gráfica o fotográfica" y

³⁰ http://www.agpd.es/porta/webAGPD/canal/documentacion/legislacion/estatal/common/pdfs/Instruccion_1_2006_videovigilancia.pdf. [Consulta: 17/03/ 2014].

La instrucción 1/2006 entiende por tratamiento: *"grabación, captación, transmisión, conservación y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas"*. Además, la instrucción considera identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la instrucción.

³¹ Se regirán por su normativa específica, especialmente la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

³² Se debe puntualizar que el empresario debe adoptar las medidas precisas para garantizar que los trabajadores conozcan de la instalación de videocámaras, solicitando a sus empleados la firma de un documento que acredite tener conocimiento de la existencia del sistema de videovigilancia. El propio autor matiza que cumplido con el deber de información a sus empleados, el empresario no requiere su consentimiento expreso por lo que *" en caso de concurrir una negativa a firmar por parte del empleado afectado por dicha captación dicho documento, el empresario quedará igualmente habilitado para seguir captando y grabando dichas imágenes"*. Y en caso de falta de información, la Agencia Española de Protección de Datos impondrá una sanción al empresario.

además, en el tratamiento de las imágenes, requieren también el Principio de Proporcionalidad³³.

Por todo ello, la Instrucción, reconoce a los ciudadanos el derecho de acceso, rectificación y cancelación conforme a la normativa de la LOPD³⁴.

Recoge expresamente la instrucción que los datos se deben cancelar en el plazo máximo de un mes (art.6) y que el responsable de los ficheros de video-vigilancia, antes de crearlos, debe notificar tal acción a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma (art.7)³⁵. En la misma línea, se impone al responsable de los ficheros dos obligaciones más: deben adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado y debe informar a las personas con acceso a los datos del deber de secreto respecto a los mismos. Y no se ha de olvidar, que el tratamiento de los datos obtenidos mediante la video-vigilancia en el centro de trabajo, en relación a la responsabilidad administrativa: Si el empresario opta por un sistema de video-vigilancia con circuito cerrado, será el responsable único, ante la Agencia Española de Protección de Datos, pues es quién posee la condición de responsable único; mientras que si se utiliza un sistema de video-vigilancia con circuito abierto, es decir, con contratación de una empresa de seguridad privada, ésta pues será la que deberá responder ante la Agencia ya mencionada.

³³ Las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras. Por lo tanto, las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos a no ser que resulte imprescindible para la finalidad de vigilancia que se pretende, o sea imposible evitarlo por razón de la ubicación de aquéllas. Pero en todo caso, debe evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida. También hay que remarcar que de acuerdo con este Principio de Proporcionalidad, el fin de la video-vigilancia debe ser lícito, es decir, el proteger intereses vitales, como la salud y la seguridad de los bienes y personas presentes en el centro de trabajo.

³⁴ En la Instrucción 1/2006, concretamente, en su art.5: Derechos de las personas: *"dispone que para el ejercicio de estos derechos la persona afectada deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. Añade que el responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento. Por último, prescribe que la persona interesada al que se deniegue total o parcialmente el ejercicio de los derechos nombrados, podrá reclamar su tutela ante el Director de la Agencia Española de Protección de Datos"*.

³⁵ Hay que puntualizar: Se podrán conservar estas imágenes por más tiempo si sobre hechos que recogen las mismas existe procedimiento administrativo o judicial alguno. Además, importante es resaltar que no se considera fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.

Para terminar, el marco en que se mueve la presente Instrucción es claro, *"La seguridad y la vigilancia, elementos presentes en la sociedad actual, No son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, de manera que pueda mantenerse la confianza de la ciudadanía en el sistema democrático"*.

9.1.1 Modelo de cartel identificativo.

La Instrucción 1/2006 de la AEPD incluye el modelo de cartel informativo que debe utilizarse. **Ver Anexo I.**

9.2 Instrucción 1/2007, de 16 de mayo, de la agencia de protección de datos de la comunidad de Madrid: sistemas de cámaras o videocámaras en el ámbito de los órganos y administraciones públicas de la comunidad de Madrid:

La Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, elaborada al amparo del artículo 37.1.c)³⁶ de la Ley Orgánica 15/1999, para dictar, y sin perjuicio de las competencias de otros órganos, las instrucciones concretas y necesarias para adecuar los tratamientos a los principios de la presente Ley.

Fruto de un proceso y reflexión similar, reflejada en el artículo 15.d³⁷ de la Ley 8/2001, de 13 de julio, de protección de datos de carácter personal en la Comunidad de Madrid, es la *Instrucción 1/2007, de 16 de mayo, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de Datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones públicas de la Comunidad de Madrid.*

³⁶<https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf>. [Consulta:17/03/2014]. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal: Art.37.1":*Funciones: Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las Instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley"*.

³⁷ *" La Agencia de Datos de la Comunidad de Madrid ejercerá las funciones que a continuación se relacionan en el ámbito de la actuación que le atribuye el artículo 41 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: Artículo 15.d: Funciones:"Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos de datos de carácter personal a los principios contenidos en la Ley Orgánica 15/1999, de 13 de diciembre, y en la presente Ley"*.

Y como no podía ser de otro manera, la Agencia de Protección de Datos de la Comunidad de Madrid (en lo siguiente APDCM), en su Guía de Videovigilancia, nos comenta el aumento de la instalación de cámaras de videovigilancia cuya finalidad principal es la de garantizar la seguridad, aunque también se puede destinar a otros fines, entre los que se encuentran el control del tráfico, el acceso a zonas restringidas, **la vigilancia empresarial** y la asistencia sanitaria. La instalación de estos sistemas supone realizar un balance de intereses entre el derecho a la protección de datos personales y el derecho a la seguridad, pues el tratamiento de la imagen de una persona implica la aplicación de la normativa de protección de datos personales, ya que la imagen es un dato de carácter personal relativo a una persona identificada o identificable.

Además, en ocasiones, es aplicable la legislación sectorial, en función de los actores que intervengan, como puede ser el uso por parte de las Fuerzas o Cuerpos de Seguridad del Estado o por las empresas de seguridad privada, como sería la regulación en el ámbito de los bancos y las competiciones deportivas.

Por todo lo anterior, los tratamientos de datos personales de imágenes captadas a través de estos dispositivos se han hecho cada vez más comunes y debido a su especial naturaleza, que no encaja en el concepto tradicional del fichero, se hizo necesaria la publicación por parte de la APDCM de la Instrucción 1/2007 que clarificará la situación y precisará las obligaciones de las instituciones que recurran a estos dispositivos de vigilancia. Haciendo, con esta Instrucción, más racional y ordenada la captación, grabación, conservación, elaboración, modificación, bloqueo, cancelación y cesión de las imágenes de las personas físicas realizados por los Órganos y Administraciones Públicas de la Comunidad de Madrid.

9.2.1 La guía de video-vigilancia y la Instrucción 1/2007 de la APDCM en relación a la video-vigilancia empresarial.

Por su especial relevancia, la guía de video-vigilancia de la APDCM ha querido dedicar un apartado individual a la video-vigilancia empresarial. Aunque en un primer momento se puede llegar a pensar que la colocación de cámaras por parte de la empresa (Pública o Privada) con la finalidad de llevar un control de la actividad laboral del empleado sea el único sistema de control. Pues bien, en la práctica, este control empresarial puede llevarse también a través de otros instrumentos que la empresa pone a disposición del trabajador como son el correo electrónico e Internet.

Aunque la cuestión que me ocupa es el supuesto primero, donde, la Instrucción 1/2007 de la APDCM en su Norma Cuarta, contempla la posibilidad de utilizar la video-vigilancia cuando la grabación, captación, transmisión, conservación y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas, resulten necesarios para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa vinculada al ámbito competencial propio de las instituciones, órganos, organismos y demás entes y entidades que se refiere esta Instrucción.

Concretamente:

- Cuando el tratamiento de la imagen tenga por objeto el seguimiento, control y garantía del cumplimiento de la relación laboral, funcionarial o estatutaria.
- Cuando el tratamiento de la imagen se realice en el marco de una relación jurídica derivada del sometimiento del afectado a una relación administrativa de sujeción especial.
- Cuando el tratamiento de la imagen se dirija a la mejora en la calidad de la gestión de los servicios públicos.
- Cuando se realice cualquier otro tratamiento que resulte necesario para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa vinculada al ámbito de competencia del responsable del tratamiento en el ejercicio de sus funciones.

En consecuencia, si se instalan las cámaras con las finalidades anteriormente descritas, hay que cumplir con lo dispuesto en la Instrucción 1/2007.

Aunque, no hay que olvidar , que la facultad de usar la video-vigilancia con el objetivo de controlar la prestación laboral del trabajador debe ser interpretada de forma restrictiva. Y con carácter general, se utilizarán otros medios menos intrusivos para el trabajador.

También, se puede mencionar dos supuestos en los cuales sería factible la instalación:

- Control del centro de emergencias 112.
- Cámaras enfocando a una caja registradora de dinero³⁸.

³⁸http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Contentdisposition&blobheadername2=cadena&blobheadervalue1=filename%3DGU%2C3%8DA+DE+VIDEOVIGILANCIA_APDCM.pdf&blobheadervalue2=language%3Des%26site%3DPortalAPDCM&blobkey=id&blobtable=MungoBlobs&blobwhere=1310901072211&ssbinary=true. [Consulta: 25/04/2014].

9.3 Instrucción 1/2009, 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de video-vigilancia:

Hace falta reflexionar, así lo contemplaba la Agencia Catalana de Protección de Datos (en lo siguiente APDCAT), en su Memoria 2009. Donde nos decía que las innovaciones tecnológicas modifican la forma de entender las relaciones entre las personas, la forma de entender los derechos, incluyendo el Derecho a la Protección de Datos. Las nuevas tecnologías, cada vez más tienen una incidencia más directa en la vida de las personas pues están al alcance de todo el mundo. En particular, Internet nos ofrece una memoria ilimitada, una memoria sin olvidos.

Hasta hace poco, la cultura de la protección de datos personales no era una cuestión prioritaria, más bien estaba inmersa en la ignorancia, escepticismo e indiferencia. Se concebía como algo innecesario, lejano y complicado.

La APDCAT, con su empeño y compromiso ayuda a fijar una cultura seria y bien consolidada en materia de Protección de datos donde el Ciudadano sea consciente de los derechos que tiene y que los poderes públicos asuman las obligaciones de gestionar la información personal como una herramienta para obtener la confianza de los ciudadanos. Los poderes públicos deben limitar las intrusiones en la vida privada de los Ciudadanos y Ciudadanas.

La Agencia, en su tarea de Autoridad independiente para la defensa de los Derechos Fundamentales a la Protección de datos, había detectado en la práctica, que la falta de previsiones específicas en la normativa dirigidas al tratamiento concreto de datos a través de sistemas de video-vigilancia hacia necesaria una explicación y especificación sobre la conservación de imágenes, sobre el derecho de acceso, rectificación y cancelación, sobre el cumplimiento del deber de información suficiente y adecuada a los ciudadanos, sobre la inscripción de ficheros ,sobre la legitimidad y pertenencia a la hora de instalar sistemas de video-vigilancia, además de otras cuestiones enfocadas en el ámbito empresarial-laboral.

Pues bien, la APDCAT, dentro del contexto anterior ha confeccionado la **Instrucción 1/2009**, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con finalidades de video-vigilancia, que entró en vigor el 20 de febrero de 2009.

Dicha Instrucción se dictó conforme a lo dispuesto en el artículo 5.1 de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, y el artículo 15.1.e) del

Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de datos.

La Instrucción, se centra en la regulación del tratamiento de las imágenes de las personas con finalidades de video-vigilancia, pero también se aplica al tratamiento de voces ligadas a la video-vigilancia³⁹ porque se considera que la utilización de dispositivos de captación de imágenes que permiten a la vez captar la voz, son cada vez más precisos gracias a la tecnología digital, lo cual, conlleva un riesgo más grave para la privacidad de las personas.

9.3.1 Ámbito de aplicación.

La Instrucción se aplicará a todos los órganos, organismos y entidades vinculadas o dependientes de las instituciones públicas de Catalunya, de la Administración de la Generalitat, de los entes locales de Catalunya, de las universidades de Catalunya y de las corporaciones de derecho público que ejerzan sus funciones exclusivamente en Catalunya.

Además, resultará de aplicación a las personas físicas o jurídicas que gestionen servicios públicos o ejerzan funciones públicas, siempre que el tratamiento se haga en Catalunya y tenga relación con materias de la competencia de la Generalitat de Catalunya o de los entes locales de Catalunya.

9.3.2 Aclaración de la Instrucción 1/2009 de la APDCAT versus Instrucción 1/2006 de la AEPD.

La Instrucción 1/2009 de la APDCAT nos aclara una cuestión que la Instrucción 1/2006 de la AEPD no tuvo en cuenta, donde el hecho de captar la apariencia o los hábitos y comportamientos de una persona que se pudieran tener la consideración de datos especialmente protegidos, no comportará la necesidad de aplicar el régimen previsto para este tipo de datos, en el caso que la captación haya sido puramente accesoria.

Además, es necesario destacar, que la Instrucción Catalana, contempla específicamente la posibilidad de captar el dato de la voz de los afectados, consiguiendo con esta especificación ajustarse a una realidad en la que concretos dispositivos de video-vigilancia posibilita esta captación de la voz.

³⁹<http://www.apd.cat/media/615.pdf>. [Consulta: 10/03/2014].

Instrucción 1/2009 APDCAT: Capítulo 1: Disposiciones generales: Artículo 1 (Objeto): *"La presente Instrucción se aplica al tratamiento de los datos personales consistentes en imágenes, y en su caso, en voces, de personas físicas identificadas o identificables con fines de video-vigilancia mediante cámaras u otros medios análogos"*.

9.3.3 Memoria de la Instrucción 1/2009.

La necesidad de elaborar una memoria ha sido una de las principales novedades incluidas en la Instrucción 1/2009. Una Memoria previa a la inscripción del correspondiente fichero, dicho de otra manera, a la captación de las imágenes, que estará a disposición de los inspectores de datos de la APDCAT, y en la que se incluirá la siguiente información:

- a) Órgano, organismo o entidad responsable: concreción de la persona responsable del fichero, de las personas operadoras del sistema de video vigilancia, y si fuera necesario, la persona responsable de la instalación y su mantenimiento.
- b) Justificación de la captación y de los tratamientos posteriores que se prevean: debe hacerse constar si se cuenta con el consentimiento de los afectados o, de no ser así, cuál de los apartados del artículo 6.2 de la LOPD⁴⁰, u otra normativa aplicable, concurre en el caso concreto, a los efectos de legitimar el tratamiento de las imágenes y las voces.
- c) Justificación de la finalidad y de la proporcionalidad del sistema, según se recoge en los arts. 6 y 7 de la Instrucción.
- d) Datos personales tratados: debe concretarse si también se captará la voz y si la finalidad conlleva, la captación de imágenes que revelen datos personales especialmente protegidos o que sea necesario la aplicación de un nivel medio o alto de seguridad.
- e) Ubicación y campo de visión de las cámaras: debe hacerse referencia a la ubicación i orientación de las cámaras.
- f) Definición de las características del sistema, donde se debe especificar:
 - Número total de cámaras que forman el sistema.
 - Condiciones técnicas de las cámaras y de otros elementos.
 - Si las cámaras son fijas o móviles.

⁴⁰ <http://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf>.

[Consulta:24/02/2014]

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Artículo.6.2: *"No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento"; "cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7.6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado"*.

- Si las imágenes se visionan directamente o sólo se registran, con acceso limitado a determinados supuestos previstos en la Memoria.
 - Si la grabación, se realiza de forma continuada o discontinua.
 - Si las imágenes se transmiten.
 - Previsiones relativas a los mecanismos de identificación y de disociación para atender el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, conocidos también como **Derechos ARCO**.
 - Cuando se grabe la voz, también debe especificarse la distancia desde la cual ésta puede registrarse.
- g) Periodo por el cual se instala el sistema y periodo de conservación de las imágenes.
- h) Deber de información: debe incluirse una referencia al número y emplazamiento de los carteles informativos.

9.3.4 Modelo de cartel identificativo.

La Instrucción 1/2009 de la APDCAT incluye el modelo de cartel informativo que debe utilizarse. En este caso, a diferencia de la Instrucción 1/2006 de la AEPD, se incluyen dos modelos, dependiendo de si el sistema permite captar la voz de los afectados o no. **Ver Anexo II**, respectivamente.

10 El poder de organización empresarial y los derechos fundamentales del trabajador:⁴¹

Queda claro el choque de intereses que se da cuando el empresario utiliza la video-vigilancia en el lugar de trabajo. Pues aparecen enfrentados el poder de dirección del empresario (Art.20.3 ET) y los derechos fundamentales del trabajador, especialmente el de la intimidad (Art.18.1CE). Soluciones concretas al respecto poco o nada se puede determinar por la inexistencia en nuestro ordenamiento jurídico una norma que regule la instalación y utilización de mecanismos o dispositivos de control y vigilancia en el centro de trabajo (STC 57/1994, de 28 de febrero y a STC 143/1994, de 9 de mayo). Porque de existir, su finalidad principal sería la de equilibrar este choque de intereses entre el empleado y el empleador. Al no existir dicha norma, se les encomienda a los órganos jurisdiccionales, es decir, a los jueces, los que deberán dar solución al conflicto concreto.

10.1 El principio de proporcionalidad

Por tanto, si en el caso concreto se cumplen los 3 juicios del Principio de proporcionalidad⁴², la medida del empresario de instalar video-vigilancia en el centro de trabajo será justificada y no arbitraria, aunque restrinja el derecho a la intimidad del empleado. Pero está claro, que serán en todo caso, los jueces quienes deberán motivar la aplicación de estos 3 juicios o subprincipios del Principio de Proporcionalidad.

Y cuando nos encontramos ante tal situación donde se encuentran presentes derechos fundamentales como son la Libertad de empresa, intimidad del trabajador es y ha sido esencial la labor del Tribunal Constitucional.

La labor del Tribunal Constitucional ha coronado el principio de Proporcionalidad como elemento principal para decidir estos choques de intereses. Será pues el juicio de Proporcionalidad el que decida si en el caso concreto es aceptable o no la limitación o restricción de derechos fundamentales que comporta la video video-vigilancia en el centro de trabajo.

⁴¹ETXEBERRIA GURIDI, José Francisco y ORDEÑANA GEZURAGA, Ixusko. Video-vigilancia. Monografías 726.Ámbito de aplicación y derechos fundamentales afectados, Tirant lo blanch,Valencia,2010,pág. 55-56

⁴² Los tres juicios que integran el Principio de Proporcionalidad: Juicio de idoneidad; Juicio de necesidad; Juicio de proporcionalidad en sentido estricto.

10.2 ¿Qué ocurre cuando un empleador instala un sistema audiovideovisual de control sin cumplir los requisitos exigidos?

Cuando se instalan videocámaras sin cumplir los requisitos exigidos y por ello, el propio trabajador ve vulnerado sus derechos fundamentales (sobre todo el de la intimidad), puede entonces dirigirse a los tribunales, al orden social, si considera que efectivamente se le han infringido sus derechos fundamentales o incluso al orden penal, si la grabación fuese constitutiva de delito (por enfocar en lugares prohibidos: Vestidores, Aseos...). A todo ello, los trabajadores, podrán denunciarlo a su sindicato o directamente a Inspección de Trabajo. Además en relación a la Protección de sus datos personales, podrán acudir a la Agencia Española de Protección de Datos (AEPD).

Aunque cabe decir, que los Tribunales con sus sentencias han sentado precedentes donde en ocasiones han admitido la instalación de forma oculta de mecanismos de captación de imágenes y sonidos sin haber realizado la oportuna comunicación a los trabajadores o a sus representantes legitimados de éstos, sin cumplir por tanto el redactado del Art.64.1ET⁴³, cuando de producirse dicha comunicación pudiera poner en peligro el objetivo que persigue, en el caso que el empresario quiera comprobar el comportamiento irregular de un concreto trabajador. En tal caso, se da por buena la instalación de la video-vigilancia sin notificación previa.

⁴³ Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores: Art.64.1: "El Comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores....".

11 La imagen y sonido como dato personal y la video-vigilancia:⁴⁴

No podemos negar que la video-vigilancia, además de afectar a la intimidad y a la imagen del trabajador, en el momento que se graban imágenes y sonidos, afecta también al derecho fundamental a la protección de datos que es inherente a todos los ciudadanos. El art.2 LOPD dispone que la protección establecida en esta Ley será de aplicación *"los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento"*. Y se constituye a partir de dos conceptos básicos: El dato personal y su tratamiento:

- **Dato Personal** se entiende como art.5.1.f) RPD⁴⁵ *"cualquier información concerniente a personas físicas identificadas o identificables"* y esto comprende *" la información fotográfica, acústica o de cualquier tipo"*.
- Tratamiento se entiende como art.5.1.t) RPD⁴⁶ *"cualquier operación o procedimiento técnico sea o no automatizado, que permita la recogida , grabación, conservación, elaboración , modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión..."*.

Es evidente que la video-vigilancia es una forma de obtener y tratar la información en general y los datos personales de los trabajadores en particular. Las imágenes y sonidos que se obtienen mediante las videocámaras en las empresas y centros de trabajo para el control de la actividad laboral sólo son considerados datos de carácter personal cuándo permiten la identificación de las personas que aparecen en ellos, no aplicándose la LOPD en caso contrario y por tanto, deberán cumplir las mismas condiciones que cualquier dato⁴⁷.

⁴⁴DESDENTADO BONETE, Aurelio, MUÑOZ RUIZ, Ana Belén. Lex-Nova. Control Informático Videovigilancia y protección de Datos en el Trabajo. pág.61-62.

⁴⁵Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su Reglamento aprobado por RD 1720/2007, de 21 de diciembre (RDP).

⁴⁶ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su Reglamento aprobado por RD 1720/2007, de 21 de diciembre (RDP).

⁴⁷ Aunque la LOPD no lo dice de forma expresa, 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 relación al tratamiento de datos personales y a la libre circulación de estos datos considera dato de carácter personal la imagen, no sólo captada a través de un aparato fotográfico, sino también mediante la videocámara. De la misma forma, en nuestro ordenamiento jurídico el Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la LOPD, en su artículo.1.4: *"considera dato de carácter personal, toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión relativa a una persona física identificada o identificable"*.

Estamos ante un derecho fundamental nuevo, que ha surgido a partir de los avances de la tecnología. Así lo reconoce y lo fundamenta el TC en dos sentencias: la STC 90/2000 y la **STC 292/2000**, las dos del 30 de noviembre. En la STC 292/2000, nuestro máximo intérprete de nuestra carta magna, describe este nuevo y autónomo derecho fundamental (la protección de datos) en comparación con el derecho a la intimidad, como ya ha sido objeto de estudio en líneas anteriores, se ve especialmente afectado por el empresario cuando opta por la colocación de la video-vigilancia en el centro de trabajo. Ambos derechos fundamentales (intimidad y el de la protección de datos) comparten el mismo objetivo que es el de ofrecer una protección constitucional de la vida privada, personal y familiar. Aunque ambos derechos fundamentales compartan el mismo objetivo, éstos tienen funciones, contenido y objetos diferentes:

11.1 Funciones

- 1) **La función del derecho fundamental a la intimidad** es la de proteger frente a cualquier intromisión que pueda realizarse en el ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno de terceros en contra de nuestra voluntad⁴⁸.
- 2) **La función del derecho fundamental a la protección de datos** busca garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con la finalidad de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

11.2 Objeto

- 1) **El objeto del derecho a la intimidad** reconocido en el Art.18.1 CE es menos amplio que el derecho a la protección de datos. Pues su objeto es la de proteger la intimidad individual de la persona.
- 2) Mientras que **el objeto de protección del derecho fundamental a la protección de datos** es más amplio que el anterior puesto que no se reduce sólo a los datos íntimos de la persona, sino que se extiende a cualquier tipo de dato personal, sea o no íntimo, cuyo reconocimiento o utilización por terceros puede afectar a los derechos, sean o no fundamentales, del afectado.⁴⁹

⁴⁸ Así lo configura el propio TC en la STC 144/1999, de 22 de julio.

⁴⁹ La mencionada STC 292/2000 señala que el objeto de protección del derecho fundamental a la protección de *datos* "también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos". El TC argumenta: el hecho que se hable de datos de carácter personal no significa que sólo se protejan los relativos

11.3 Contenido

- 1) **El contenido del derecho fundamental a la intimidad personal y familiar** otorga a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido⁵⁰.
- 2) En Cambio, **el contenido del derecho a la protección de datos** atribuye a su titular una serie de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos con la finalidad de garantizar a la persona un poder de control sobre sus datos personales. Es decir, el derecho a la protección de datos otorga a la persona el poder de disposición sobre sus datos personales, y que a su vez, conlleva el derecho a que se requiera el previo consentimiento para la recogida y uso de sus datos personales, el derecho de saber y ser informado sobre el destino y uso de los datos y el derecho a acceder, rectificar y cancelar dichos datos, reconociendo a la persona el derecho de oposición.

a la vida privada o íntima de la persona. Se deben proteger todos aquellos datos que identifiquen o permitan identificar la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otro índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

⁵⁰ Este contenido se refleja en abundantes sentencias del TC. Sentencias como STC 231/1988, de 2 de diciembre, STC 110/1984, de 26 de noviembre, STC 197/1991, de 17 de octubre, STC 144/1999, de 22 de julio y STC 115/2000, de 10 de mayo.

12 Conclusiones:

A lo largo de este trabajo, hemos analizado los derechos afectados con una nueva tecnología como es la de las video-cámaras, concretamente en el ámbito laboral. Hemos visto la normativa nacional como la internacional, y la aplicación jurisprudencial de la misma. En nuestro país, las Agencias de Protección de Datos han elaborado Instrucciones al respecto. Pero sólo la APDCM (Agencia de Protección de Datos de la Comunidad de Madrid) ha considerado el ámbito de la video-gilancia empresarial. Ahora bien, como hemos comprobado, y ha señalado la APDCAT (Agencia de Protección de Datos de Cataluña), hay un vacío legal respecto a la video-vigilancia. En el ámbito laboral, son los jueces, los que ante este vacío legal, se pronuncian cuándo un sistema de video-vigilancia es conforme a ley y cuándo no lo es. Lo ponderan aplicando el principio de proporcionalidad: Los tres juicios que lo integran son: "*Juicio de idoneidad; Juicio de necesidad; Juicio de proporcionalidad en sentido estricto*", establecido por el Tribunal Constitucional. Lo cual no ha impedido que en ocasiones, teniendo en cuenta el contexto, el TC, se haya pronunciado de una forma más permisiva en unas sentencias que en otras.

La video-vigilancia como prueba procesal laboral, tampoco es una cuestión resuelta del todo, ya que unas veces la jurisprudencia social la acepta y en otros casos, como hemos visto, no. En principio, también en función del contexto, la acepta cuando su instalación ha sido imprescindible. Es por ello, en las líneas precedentes, he querido clarificar aspectos como la vaguedad del Estatuto de Trabajadores, donde una interpretación amplia del art.20.3 ET podría legitimar la adopción de cualquier dispositivo de control en el puesto de trabajo y convertir con ello, el lugar de trabajo con un espacio permanentemente vigilado. La consecuencia directa de todo sería que el trabajador se vea sometido, resignado no sólo a aceptar la discrecionalidad del empresario en la adopción de un control mediante un dispositivo de control audiovisual, sino a someterse a la incertidumbre de desconocer qué aspectos de su vida privada son conocidos, grabados y conservados por aquél. **Por tanto, dado el desarrollo tecnológico de las videocámaras aplicado en los centros de trabajo, nos preguntamos si no sería conveniente realizar una revisión y actualización del Estatuto de Trabajadores.**

En definitiva, las facultades organizativas empresariales están limitadas por los derechos fundamentales del trabajador que el empleador deberá respetar. Y por tanto, no sólo tenemos que tener en cuenta los derechos laborales clásicos del empleado (huelga, sindicación...) sino todos los derechos fundamentales como ciudadano, especialmente dado el desarrollo de las tecnologías de vigilancia que afecte el derecho a la intimidad, a la propia imagen y a la protección de datos personales.

13 BIBLIOGRAFIA

- MONOGRAFÍAS CONSULTADAS

- DESDENTADO BONETE, Aurelio; MUÑOZ RUIZ, Ana Belén. *Control Informático, videovigilancia y protección de datos en el trabajo*. Editorial Lex Nova, S.A.U. 1ª Edición. Valladolid,2012.
- ETXEBERRIA GURIDI, José Francisco; ORDEÑANA GEZURAGA, Ixusko; ARZOZ SANTISTEBAN, Xabier; CALONGE CRESPO, Iñaki; ESPARZA LEIBAR, Iñaki; GONZÁLEZ LÓPEZ, Juan José; PECHARROMÁN FERRER, Begoña; PÉREZ GIL, Julio. Tirant Monografías 726. *Videovigilancia. Ámbito de aplicación y derechos fundamentales afectados. En particular la protección de datos personales*, Editorial Tirant Lo Blanch, edita Tirant Lo Blanch. Valencia, 2010.
- GOÑI SEIN, José Luis. *La Videovigilancia empresarial y la Protección de Datos Personales*. Editorial Aranzadi, SA. 1ª Edición. Navarra, 2007.
- SÁNCHEZ-RODAS NAVARRO, Cristina. Videocámaras y poder de vigilancia, Editorial Aranzadi Social núm.5, Tomo IX, 1999.

- PÁGINAS WEBS CONSULTADAS

- <<http://www.boe.es/buscar/pdf/1992/BOE-A-1992-18489-consolidado.pdf>> [Consulta: 26 mayo 2014].
- <<http://www.boe.es/buscar/pdf/1982/BOE-A-1982-11196-consolidado.pdf>>. [consulta: 24/03/2014].
- <http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf>. [Consulta: 20/03/2014].
- <https://www.apda.ad/system/files/wp67_es.pdf>.[Consulta: 14/04/2014].
- <https://www.apda.ad/system/files/wp89_es.pdf>.[Consulta: 14/04/2014].
- <<http://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf>> [Consulta:24/02/2014]
- <http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/Instruccion_1_2006_videovigilancia.pdf>. [Consulta:17/03/2014].
- <<http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=ContentDisposition&blobheadername2=cadena&blobheadername3=filename%3D%26site%3DPortalAPDCM&blobkey=id&blobtable=MungoBlobs&blobwhere=1310901072211&ssbinary=true>>. [Consulta: 25/04/2014].
- <<http://www.apd.cat/media/615.pdf>>.[Consulta:10/03/2014].

ANEXO I

Modelo de cartel indicativo según Instrucción 1/2006 de la AEPD:



ANEXO II

Modelos de carteles indicativos según instrucción 1/2009 de ADPCAT:



ANEXO III

- JURISPRUDENCIA

- Sentencia STC 98/2000, 10 Abril. Recurso de amparo núm.4015/1996. Ponente el Magistrado don Fernando Garrido Falla.
- Sentencia STC 186/2000, 10 de Julio. Recurso de amparo núm.2.662/1997.
- Sentencia STC 29/2013, 11 Febrero. Recurso de amparo núm.10522-2009. Ponente el Magistrado don Fernando Valdés Dal-Ré.

- NORMATIVA CONSULTADA

- Directiva 95/46/CE
- Constitución Española (CE).
- OIT: Repertorio de Recomendaciones Prácticas de la OIT de octubre de 1996, Protección de los datos personales de los trabajadores.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen (LO 1/1982).
- Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido del Estatuto de los Trabajadores.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- Instrucción 1/2007, de 16 de mayo, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid.
- Instrucción 1/2009, de 10 de febrero, de la Agencia Catalana de Protección de Datos, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia.