VIDEOVIGILANCIA LABORAL Y DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

Inmaculada Jiménez-Castellanos Ballesteros

Profesora Asociada de Derecho Constitucional
Universidad de sevilla

EXTRACTO **Palabras clave: protección de datos personales; intimidad; videovigilancia laboral**

La Sentencia del Tribunal Constitucional 39/2016 contiene un nuevo pronunciamiento sobre la videovigilancia en el ámbito laboral. Partiendo de esta resolución, se analiza el derecho fundamental a la protección de datos personales. En el ámbito laboral, se abandona definitivamente la doctrina de la protección de la intimidad. Sin embargo, surgen nuevas cuestiones en relación con el derecho a la protección de datos en los supuestos de videovigilancia. Esta sentencia supone un cambio en la doctrina que hasta el momento había mantenido el Tribunal Constitucional en la STC 29/2013.

ABSTRACT **Key Words: personal data protection; privacy; workplace video surveillance**

The sentence of the Spanish Constitutional Court 39/2016 contains a new pronouncement on the video surveillance at the work place. Starting from this resolution the personal data protection fundamental right is analyzed. In workplace, The Court leaves definitively the doctrine of the privacy protection. Nevertheless, new questions arise in relation with personal data protection right in workplace surveillance. This sentence supposes a change in the doctrine that up to the moment had supported the Constitutional Court in the STC 29/2013.

 Recepción del original: 07.12.2016 Aceptación original: 23.01.2017

ÍNDICE

1. LA VIDEOVIGILANCIA EN EL ÁMBITO LABORAL

En la actualidad, la aplicación de las nuevas tecnologías al ámbito laboral y la magnitud del alcance del poder de control empresarial plantean problemas jurídicos que pueden poner en cuestión valores tan importantes como la libertad y la dignidad del trabajador. No en vano, nuestra Carta Magna encabeza el Título I, dedicado a los derechos y deberes fundamentales, con el artículo 10 que consagra la dignidad humana como fundamento del orden político y de la paz social.

No es ocioso recordar cómo las nuevas tecnologías de la información y la comunicación permiten formas de control nuevas y «casi ilimitadas» que, de facto, están siendo utilizadas por los empleadores para intensificar las formas de conocimiento del comportamiento de los trabajadores, creando centros de «trabajo virtuales» en los cuales la profecía orweliana del gran hermano adquiere dimensiones laboralizadas («el inmenso poder del ojo mecánico» empresarial) en las que la realidad vuelve a superar a la ficción[1].

Del control presencial se ha pasado al tecnológico a través de los más sofisticados instrumentos de acceso y localización, mediante el empleo de datos biométricos o sistemas GPS, entre otros. Asimismo, resultan cada vez más habituales los registros del ordenador utilizado por el trabajador, su correo electrónico o el rastro de su navegación por Internet. Entre estos nuevos dispositivos de fiscalización empresarial se encuentra la videovigilancia, que podemos definir como el mecanismo de control basado en un sistema de captación de imágenes y/o grabación de sonidos en el lugar de trabajo.

Como afirma Goñi Sein, el Estado y el ciudadano recurren a la videovigilancia porque es fuente de información y porque procura una mayor seguridad (se sienten más protegidos). En efecto, no se puede negar que la vigilancia por video-

[1] Tascón López, R. "El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica", *Revista Doctrinal Aranzadi* Social, núm. 17/ 2007, p.2.

cámara puede estar justificada para la protección de las personas y de sus bienes. Incluso ha sido decisiva para la conclusión de investigaciones criminales[2]. Este argumento defensivo se viene imponiendo también en la empresa, pues en muchos casos el recurso a la videovigilancia responde a la prevención de delitos o a la verificación de una conducta ilícita por parte del trabajador.

Sin perjuicio de las ventajas que estos métodos representan para satisfacer las exigencias de seguridad, la videovigilancia contribuye a que el trabajador pierda el control de sus informaciones y datos personales.

En nuestro ordenamiento jurídico no hay ninguna normativa específica sobre el uso de videocámaras en el ámbito laboral[3]. En el marco de la libertad de empresa (art.38 de la Constitución Española, en adelante CE), el empleador, en el ejercicio de su función de control y dirección de la actividad laboral, podrá adoptar las medidas que estime más oportunas de vigilancia e inspección 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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad[4].

Esta situación de inseguridad jurídica provoca que la decisión de instalación de sistemas de videovigilancia quede al arbitrio del empresario, sin más restricción que la del respeto a la dignidad del trabajador, la cual adolece de gran vaguedad.

El poder de control empresarial debe traer aparejado el deber de utilizar medios respetuosos con los derechos fundamentales del trabajador y la necesidad de circunscribir esta actividad a la comprobación de aquellas cuestiones estrictamente vinculadas con la prestación de trabajo.

En este punto, la laguna legal ha provocado que sean los jueces y tribunales quienes asuman la misión de establecer las pautas de adecuación entre estos nuevos sistemas y los derechos fundamentales. En este sentido, «la criticable imprecisión legislativa obliga a una labor creadora, *quasi* legislativa, de los tribunales, capaz de propiciar, en ocasiones, notables contradicciones, lo cual provocará, a la postre, un evidente grado de inseguridad jurídica»[5].

[2] Goñi Sein, J.L. *La videovigilancia empresarial y la protección de datos personales*, Aranzadi, Cizur Menor (Navarra), 2007, p.16.

[3] La utilización de la videovigilancia por las Fuerzas y Cuerpos de Seguridad del Estado en lugares públicos se regula en la Ley Orgánica 4/1997 de 4 de agosto. En el ámbito privado, la Ley 5/2014, 4 de abril, de Seguridad Privada.

[4] Artículo 20.3 ET 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).

[5] Sala Franco, T. "El derecho a la intimidad y a la propia imagen y las nuevas tecnologías de control laboral", en AA VV,*Trabajo y libertades públicas* (Borrajo Dacruz, Dir.)*.,* La Ley, Ma-

En último término, ha sido la doctrina general emanada de la jurisprudencia del Tribunal Constitucional, máximo intérprete de nuestra Norma suprema, la que ha venido a aportar más dudas al problema de la colisión entre el poder de control empresarial consagrado en el art. 20.3 del Estatuto de los trabajadores (en adelante ET) y los derechos fundamentales de estos.

Precisamente, la STC 39/2016, de 3 de marzo, contiene un nuevo pronunciamiento sobre el tratamiento de imágenes obtenidas por videovigilancia en el ámbito laboral. La demanda de amparo parte de la admisión en un proceso por despido de las grabaciones presentadas por la empresa, prueba de cargo que la trabajadora estima nula al haberse obtenido vulnerando sus derechos fundamentales. El Tribunal aprecia la especial trascendencia constitucional del recurso, con la intención de perfilar y aclarar su doctrina en relación con el uso de cámaras de videovigilancia en la empresa.

El supuesto presenta similitudes con el que diera lugar tres años antes a la STC 29/2013, de 11 de febrero. Esta resolución vino a romper con la doctrina que enfocaba el debate de la videovigilancia en el ámbito laboral desde la perspectiva del derecho a la intimidad que consagra el artículo 18.1 CE. Por el contrario, el Tribunal Constitucional dirimió el asunto desde la óptica de la autodeterminación informativa. No obstante, en la sentencia de 2016, el Alto Tribunal se aparta de aquella línea jurisprudencial sin aportar argumentos que fundamenten el abandono de tal precedente.

A lo largo de estas líneas vamos a intentar abrir un dialogo entre las distintas resoluciones traídas a colación por la STC 39/2016, en relación al deber de información a los trabajadores en los supuestos de videovigilancia en el ámbito laboral.

2. LA DEFENSA DEL DERECHO A LA INTIMIDAD

La tradicional permisividad de los dispositivos de videovigilancia en el ámbito laboral quedó desautorizada por la doctrina del Tribunal Constitucional, que proclamó el respeto a la intimidad del trabajador como límite al poder de control empresarial. Ello obligó a contemplar las facultades empresariales desde la posición preeminente de los derechos fundamentales[6].

Así quedó reflejado en dos sentencias cuyos supuestos de hecho pasamos a

drid, 1999, p. 205.

[6] «Estas limitaciones o modulaciones tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes» (STC 98/2000 de 10 de abril, FJ7)

exponer. En la primera resolución[7] se cuestionaba si la instalación por la empresa Casino de la Toja de un sistema de captación y grabación de sonido en determinadas zonas del centro de trabajo en concreto la caja y ruleta francesa, había vulnerado el derecho a la intimidad personal del trabajador, consagrado en el art. 18.1 CE.

El Tribunal Constitucional rebatió la tesis que limitaba apriorísticamente el alcance del derecho a la intimidad de los trabajadores a los lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos. Según su argumentación, en aquellos lugares de la empresa en los que se desarrolla la actividad laboral, pueden producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores. En tal sentido, señala como ejemplos la grabación de conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, o la captación de aquellas en las que se aborden cuestiones ajenas a la relación laboral. En definitiva, «habrá que atender no solo al lugar del centro del trabajo en que se instalan por la empresa sistemas audiovisuales de control, sino también a otros elementos de juicio (si la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticiamente, la finalidad real perseguida con la instalación de tales sistemas, si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control, etc.), para dilucidar en cada caso concreto si esos medios de vigilancia y control respetan el derecho a la intimidad de los trabajadores»(STC 98/2000, de 10 de abril, FJ 6).

En aplicación del principio de proporcionalidad, el Tribunal apreció que el sistema no superaba el criterio de la necesidad, teniendo en cuenta que la empresa ya disponía de otras medidas de seguridad por videovigilancia. Por tanto, la medida resultaba desproporcionada para el sacrificio que implica al derecho a la intimidad de los trabajadores dado que permitía captar comentarios privados, tanto de los clientes como de los trabajadores del casino, ajenos por completo al interés empresarial y por tanto irrelevantes desde una perspectiva de control del cumplimiento laboral. Todo lo cual condujo al Tribunal Constitucional al otorgamiento del amparo.

La segunda sentencia[8] de nuestro Alto Tribunal trajo causa de la admisión en un proceso por despido, como prueba de cargo, de las grabaciones de video presentadas por la empresa. Para el recurrente, esta prueba era nula de pleno derecho, al haberse obtenido vulnerando el derecho a la intimidad del trabajador (artículo 18.1 CE).

7 La STC 98/2000 de 10 de abril
8 La STC 186/200 de 10 de julio

Como consecuencia de un llamativo descuadre contable, la dirección de la empresa contrató la instalación de un circuito cerrado de televisión que enfocase únicamente las cajas y el mostrador de paso de las mercancías donde el recurrente prestaba servicios. Las cintas de vídeo grabadas revelaron que el actor sustrajo de forma reiterada diferentes cantidades de la caja. Por esta razón fue despedido.

Según el Tribunal Constitucional, la medida de instalación de un circuito cerrado de televisión estaba justificada ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo. Asimismo, era idónea para la finalidad pretendida por la empresa, esto es, verificar si el trabajador cometía efectivamente tales desviaciones de efectivo y en tal caso adoptar las medidas disciplinarias correspondientes. De igual manera era necesaria, ya que la grabación serviría de prueba de tales irregularidades. Y finalmente era equilibrada pues se limitó a la zona de la caja y a una duración temporal y determinada, suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada. Por todo lo dicho, el Tribunal Constitucional descartó que se hubiera producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE y, en consecuencia, desestimó el amparo.

El hecho de que la instalación del circuito cerrado de televisión no fuera previamente puesto en conocimiento del Comité de empresa ni de los trabajadores afectados estaba justificado por el temor de la compañía de que frustrara la finalidad perseguida y, al mismo tiempo, carecía de trascendencia desde la perspectiva constitucional. En suma, era una cuestión de legalidad ordinaria, ajena por completo al objeto del recurso de amparo.

En síntesis, no había habido vulneración del derecho a la intimidad personal del trabajador porque el empleo de las imágenes no había sobrepasado el juicio de proporcionalidad. No se hizo referencia alguna en la sentencia al derecho fundamental a la protección de datos aunque si se alegó por el recurrente la falta de información de la instalación del sistema de seguridad.

De los fundamentos jurídicos de estas sentencias podemos extraer la conclusión de que el Tribunal Constitucional confirma que el empresario no está habilitado para llevar a cabo intromisiones en la intimidad de sus empleados en los centros de trabajo, so pretexto de las facultades de vigilancia y control que le confiere el art. 20.3 ET. Y no cualquier interés empresarial es suficiente. La mera utilidad o conveniencia para la empresa no legitima la instalación de aparatos de grabación.

En la STC 98/2000, la empresa, aun existiendo un sistema de grabación de imágenes, decidió instalar un sistema de grabación de sonido para mayor seguridad. Sin embargo no se justificó que este nuevo sistema se instalase como conse-

cuencia de la detección de una quiebra en los sistemas de seguridad ya existentes. De la misma manera no resultó acreditado que el nuevo sistema, que permitiría la audición continuada e indiscriminada de todo tipo de conversaciones, resultase indispensable para la seguridad y buen funcionamiento del casino.

Por el contrario, en el caso que resuelve la STC 186/2000, la medida no obedeció al propósito de vigilar y controlar genéricamente la actividad laboral. Previamente se habían advertido irregularidades en el comportamiento de los cajeros y un acusado descuadre contable. La sentencia justifica la restricción del derecho a la intimidad mediante la utilización de las imágenes captadas en la tutela del interés empresarial de conseguir pruebas de tales irregularidades. Y se adoptó la medida de vigilancia de modo que las cámaras únicamente grabaron el ámbito físico estrictamente imprescindible, como eran las cajas registradoras.

El Tribunal llegó al convencimiento de que motivos de seguridad suficientemente graves respaldaban el interés empresarial relevante que justificaba la restricción del derecho fundamental. En consecuencia, acepta la utilización de las imágenes como prueba incriminatoria para justificar un despido disciplinario.

Por consiguiente, debe existir un interés suficientemente relevante que garantice el principio de intervención mínima cuando se trata de medidas restrictivas de los derechos fundamentales.

En cualquier caso la imposición de límites al derecho a la intimidad debe respetar el principio de proporcionalidad. Dicho principio comporta el triple juicio previo: adecuación o idoneidad, necesidad y proporcionalidad en sentido estricto.

El criterio de la idoneidad, entiende el Tribunal Constitucional, queda satisfecho porque el medio -la restricción del derecho a la intimidad- es adecuado para la consecución del fin que se persigue esto es, el interés empresarial relevante. El juicio de necesidad adolece de mayor imprecisión. Es indiscutible que las cámaras de videovigilancia son sistemas mucho más eficaces que cualquier otra vía alternativa de fiscalización porque multiplican la facultad de control del empresario. Sin embargo estas medidas solo serían constitucionales y por tanto necesarias, si el fin que se persigue con ellas no se puede lograr de otro modo menos lesivo para los derechos fundamentales.

Por último el principio que analizamos obliga a considerar el valor que se le debe dispensar desde el punto de vista constitucional al derecho fundamental limitado y al interés empresarial protegido. En tal sentido, el Tribunal no aprecia más circunstancias para ponderar la proporcionalidad de la videovigilancia que la del lugar de ubicación de las cámaras y la duración temporal limitada, «suficiente como para poder comprobar que no se trataba de un hecho aislado o de un

malentendido», sin tener en cuenta la posible intromisión en otros aspectos de la intimidad del trabajador.

3. EL CAMBIO DE ORIENTACIÓN: LA IMAGEN COMO DATO PERSONAL

Habrá que esperar una década para apreciar una mutación en la jurisprudencia constitucional expuesta. La STC 29/2013 de 11 de febrero, colmó las expectativas de un sector doctrinal que abogaba por contemplar los asuntos de videovigilancia en el ámbito laboral desde la perspectiva de la protección de datos. La relevancia que supuso este cambio de orientación exige que nos detengamos en su análisis.

Los hechos de los que trae causa la demanda en fueron los siguientes: el recurrente en amparo prestaba sus servicios en la Universidad de Sevilla. Ante las sospechas de irregularidades en el cumplimiento de su jornada laboral, el director de recursos humanos de esta institución dispuso que se emplearan las cámaras de video instaladas en la entrada del recinto para el control de acceso de personas al campus universitario con la finalidad de comprobar aquellas circunstancias. La instalación de estas cámaras estaba advertida con la debida señalización.

El sistema de videovigilancia constató unas jornadas laborales muy diferentes de los horarios consignados en las hojas de control de asistencia de la unidad administrativa. Como consecuencia, se inició la tramitación de un expediente disciplinario contra el trabajador en cuestión en el que se le impusieron por parte de la Universidad tres sanciones de suspensión de empleo y sueldo, de tres meses cada una, por varias faltas muy graves.

El recurrente manifestó ante el Juzgado de lo Social, entre otros extremos, que en el expediente disciplinario se presentaron como prueba las imágenes de las grabaciones de video, pese a no existir autorización expresa para tal control laboral, ni explicación de ese seguimiento individualizado.

Para el Juzgado, sin embargo, la Universidad tenía autorización de la Agencia Española de Protección de Datos (en adelante AEPD) para hacer uso de los ficheros grabados por sus videocámaras para el control de acceso de los miembros de la comunidad universitaria y el actor formaba parte de la misma. Añadía a lo anterior que el uso que se hizo de los medios técnicos de videograbación y de sus soportes informáticos respetó el principio de proporcionalidad exigido por la doctrina constitucional para toda medida restrictiva de los derechos fundamentales. La resolución por tanto se situó en la línea jurisprudencial defendida por el Tribunal Constitucional en la STC 186/2000, que justificaba el control oculto con el fin de comprobar unas concretas actuaciones irregulares.

La resolución de instancia fue recurrida por ambas partes ante la Sala de lo Social del Tribunal Superior de Justicia de Andalucía. La Sentencia se remitió a lo resuelto por el juzgador *a quo*, y declaró adicionalmente que la cámara utilizada se encontraba en el vestíbulo que daba acceso al puesto de trabajo del actor, sin grabar por tanto ningún aspecto íntimo que afectase a su esfera personal. Del mismo modo, la resolución puso de manifiesto que la existencia de una relación laboral justifica la obtención, cesión y tratamiento de datos personales sin necesidad de consentimiento, de conformidad con lo dispuesto en el art. 6.2 Ley Orgánica de Protección de datos (en adelante LOPD). No obstante, era obligado informar previamente a los trabajadores, lo que no se hizo, incumpliéndose con ello el deber regulado en el art. 5 LOPD, al procederse a la recogida de los datos sin proporcionar la información que ese precepto requiere. De ahí que la AEPD declarara que la Universidad de Sevilla había incumplido lo prescrito en la normativa de Protección de Datos.

En el recurso de amparo, el demandante invoca entre otros los derechos fundamentales de los arts. 18.1 y 18. 4 CE. Particularmente, el tratamiento de las imágenes obtenidas mediante las grabaciones había vulnerado su derecho fundamental a la protección de datos, ya que no se le ha facilitado información sobre la videovigilancia, lesión que apoya en la doctrina sentada en la STC 292/2000, de 30 de noviembre.

El Tribunal Constitucional viene a aclarar que pese a existir la invocación de los párrafos primero y cuarto del artículo 18 CE, la demanda se circunscribe exclusivamente a considerar si resultó vulnerado el derecho del recurrente a la protección de datos de carácter personal. Por consiguiente, no considera necesario detenerse en el derecho a la intimidad personal y, en consecuencia entiende que no resulta de aplicación la doctrina de las SSTC 186/2000 y 98/2000, en las que por otra parte, no fue objeto de alegación el derecho del art. 18.4 CE.

Asimismo, el Alto Tribunal argumenta que concurren notables diferencias entre los precedentes que desembocaron en aquellas resoluciones y los examinados ahora. En efecto, en la STC 186/2000, nos encontramos ante un caso de videovigilancia dirigida específicamente a determinadas posiciones del lugar de trabajo. La instalación del sistema no había sido comunicada a los trabajadores, pero esta cuestión no fue tenida en cuenta. El examen se centró en la proporcionalidad de la medida, cuya finalidad era la de servir de prueba para el despido del trabajador. En la STC 98/2000, se juzgaba la instalación de micrófonos en las dependencias que constituían el lugar de trabajo, con conocimiento de los trabajadores y del comité de empresa. De la vigilancia auditiva, por tanto, se había informado al trabajador pero la medida no superó el criterio de la necesidad, al existir ya cámaras de seguridad que cubrían esta finalidad.

Tal como se ha dicho, la cuestión crucial para el Tribunal será discernir si el contenido esencial del derecho fundamental a la protección de datos (art. 18.4 CE) fue vulnerado por la utilización de las grabaciones con el fin de control de la actividad laboral sin información al trabajador. Para ello tomará como punto de referencia la doctrina emanada de la STC 292/2000 de 30 de noviembre.

La primera duda que viene a resolver el Tribunal es si las imágenes grabadas constituyen un dato de carácter personal protegido por el artículo 18.4 CE. La respuesta es positiva puesto que el derecho fundamental amplía la garantía constitucional a todos aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil (ideológico, racial, sexual, económico o de cualquier otra índole) lo que «incluye también aquellos que facilitan la identidad de una persona física por medios que, a través de imágenes, permitan su representación física e identificación visual u ofrezcan una información gráfica o fotográfica sobre su identidad» (STC 292/2000, de 30 de noviembre, Fj6). En palabras del Tribunal Constitucional, «estamos, en definitiva, dentro del núcleo esencial del derecho fundamental del art. 18.4 CE» (STC 29/2013, FJ5).

En segundo lugar, se detiene en el examen de la actuación empresarial desde la perspectiva del derecho a la información del trabajador. Es aquí donde radica la *ratio decidenci* del presente caso. El tribunal vuelve a hacer hincapié en la distinción entre el derecho a la intimidad y el derecho a la protección de datos. Con referencia a las SSTC 98/2000, 186/2000 y la doctrina sentada en la 292/2000, traza las diferencias entre ambos derechos, subrayando el fundamento jurídico 6 de esta última: «La función del derecho fundamental a la intimidad del 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 las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). 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 del afectado… Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin».

Por tanto, de lo expuesto por el Tribunal Constitucional se desprende que el derecho a la información (la facultad de saber quién dispone de los datos y a que uso los está sometiendo) es un elemento caracterizador de la definición constitucional del derecho fundamental a la protección de datos personales del artículo 18.4 CE, de su núcleo esencial. Este derecho de información opera incluso cuando existe habilitación legal para recabar datos sin necesidad del consentimiento del titular.

Como todos los derechos fundamentales y este no es una excepción, tal exigencia de información no es absoluta, sino que admite límites. Sin embargo, solo por ley, que deberá respetar el contenido esencial, podrán imponerse límites a los derechos fundamentales. El tribunal reconoce que en el ámbito laboral no hay una habilitación legal que permita al empresario la omisión del derecho a la información a través de sistemas sorpresivos y no informados de tratamiento de datos. El tratamiento de los datos es legítimo porque responde a una finalidad que también lo es la vigilancia empresarial (art.20.3 ET), aun sin el consentimiento del afectado (art.6.2 LOPD). No obstante, la falta de la información exigible, vulneraría el artículo 18.4 CE.

No fue suficiente que existieran distintivos colocados en las diferentes puertas de acceso a la Universidad, anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la AEPD; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de 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 incumplimientos del contrato de trabajo.

Además de lo expuesto, el Tribunal añade otra precisión: tampoco había evidencia de que el control de la actividad laboral fuera el objetivo del tratamiento de las imágenes. Las cámaras no estaban instaladas en el lugar de trabajo, sino en los vestíbulos y zonas de paso públicas. Por lo tanto, la finalidad del fichero era la de controlar el acceso al recinto universitario por motivos de seguridad. Se aprecia en este caso una vulneración del principio de calidad de los datos (art.4 LOPD), puesto que se emplearon para una finalidad distinta para la que fueron recogidos, aunque aparentemente no incompatible. En cualquier caso, hubiera sido exigible el consentimiento del trabajador, a tenor del art.15 RLOPD.

En este sentido, Goñi Señi opina que la toma en consideración de imágenes o sonidos para objetivos diversos de aquellos que justificaron la medida supone una transgresión del principio de finalidad. Es más, atribuir relevancia disciplinaria a unos comportamientos irregulares conocidos de forma accidental, cuando la finalidad de la vigilancia era otra, equivaldría a asumir también entre los fines de la videovigilancia el control del comportamiento del trabajador.

A mayor abundamiento, el autor apunta que cuando la ley exige la compatibilidad, no solo está imponiendo un criterio restrictivo que alcanza a la finalidad del control perseguido sino que está además creando una «razonable expectativa

de intimidad» en los trabajadores, en el sentido de que la intromisión consentida en su ámbito reservado (imagen y sonidos) se va a limitar a la estricta satisfacción de los intereses invocados y de que todo lo que no esté orientado hacia ese fin (hechos, actos, expresiones, etc. con los que proyecta su personalidad) va a quedar a cubierto por la reserva. Al utilizar la información obtenida con fines distintos de los que justificaron la adopción, se está obligando a soportar una comprensión del ámbito de lo íntimo mayor que el acreditado y justificado por la adopción del mecanismo de control. Esa instrumentalización de la información adquirida supone en última instancia un acto lesivo para la dignidad del trabajador, pues limita su libertad[9].

El tribunal solo apunta esta cuestión para constatar que no se cumplió con el deber de información. En definitiva, concluye la sentencia, que las sanciones impuestas con base a esa única prueba, lesiva de aquel derecho fundamental, debían declararse nulas. Por consiguiente, el recurrente al haber sido privado de las facultades de disposición y control sobre sus datos personales, lo fue también de su derecho fundamental de autodeterminación informativa[10].

4. EL DEBER DE INFORMACIÓN A PROPÓSITO DE LA STC 39/2016

4.1. El fin justifica el control oculto

En términos similares a los expuestos en la STC 186/2000 de 10 de julio, y por tanto de nuevo bajo el prisma del derecho a la intimidad, se repasan en la jurisdicción ordinaria como paso previo a la interposición del recurso de amparo que daría lugar a la STC 39/2016, de 3 de marzo, los criterios que avalan la superación del juicio de proporcionalidad.

La empresa, a raíz de la instalación de un sistema de control informático de caja, había detectado irregularidades contables en la tienda donde prestaba servicios la recurrente en amparo. Ante la sospecha de una apropiación dineraria indebida por parte de alguno de los trabajadores, la entidad había encargado a

[9] Goñi Sein, J.L.*op.cit*.p.179.

[10] La sentencia no estuvo exenta de críticas. Para algunos autores resulta incomprensible por qué la utilización por el empresario de medidas de videovigilancia en condiciones como las descritas en este pronunciamiento no constituye una intromisión ilegítima en el derecho a la intimidad (SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio) y, si en cambio lo son desde la perspectiva del artículo 18.4 de la Norma suprema. Y de igual modo, les resulta inexplicable porqué la obligación de informar previamente al trabajador es una cuestión de legalidad ordinaria en el caso del derecho a la intimidad (STC 186/2000, de 10 de julio) y, en cambio, forma parte del contenido esencial de la llamada libertad informática. *Vid.* Gude Fernández,A. "La videovigilancia laboral y la protección de datos de carácter personal", *Revista de Derecho Político de la Uned*, núm.91/2014, pp..70-72.

una compañía de seguridad el establecimiento de un sistema de videovigilancia. Al comprobarse, a través de la cámara situada en la tienda y que controlaba la caja, que la trabajadora había sustraído dinero fue despedida por transgresión de la buena fe contractual.

De la instalación de la cámara había dejado constancia un distintivo informativo en un lugar visible del escaparate del establecimiento, pero no se había comunicado previamente a los trabajadores.

Esta circunstancia se puso de manifiesto por la trabajadora en la demanda solicitando la nulidad del despido por atentar contra su honor, intimidad y dignidad y subsidiariamente la declaración de improcedencia. En su argumentación sostuvo que en el centro de trabajo no existía información al público ni cartel que advirtiera de la existencia de cámaras de videovigilancia. Tampoco se había comunicado su instalación ni a la AEPD, ni al Comité de Empresa. De igual modo, no constaba que se hubiera solicitado autorización a la sección de seguridad privada de la Policía.

La sentencia del Juzgado de lo Social no atendió las pretensiones de la trabajadora. Los motivos del despido quedaron plenamente acreditados en el juicio. En lo relacionado con la instalación y grabación de la cámara de seguridad, la sentencia recalca que cumplía escrupulosamente la normativa vigente. Hecha la observación anterior, la falta de notificación de su utilización a los trabajadores, según la resolución, resultaba justificada por ser el único medio posible para satisfacer el interés del empresario en saber fehacientemente quién estaba realizando los actos defraudatorios. Para fundamentar esta necesidad de un control empresarial oculto, el fallo trae a colación la STC 186/2000 de 10 de julio.

De nuevo la doctrina constitucional de referencia se empleó como pauta interpretativa en la resolución del recurso de suplicación que la trabajadora interpuso ante la Sala de lo Social del Tribunal Superior de Justicia de Castilla y León. Para la empleada, las pruebas que justificaron su despido se obtuvieron con vulneración de su derecho fundamental a la intimidad. No obstante, a juicio de los magistrados, la decisión empresarial de colocar una cámara de videovigilancia en el centro de trabajo vino a satisfacer el juicio de proporcionalidad constitucionalmente exigido para poder afirmar su legalidad y legitimidad, en sede de tutela de los derechos fundamentales en el ámbito laboral.

En primer lugar, la actuación empresarial viene respaldada por una ley, en este caso el artículo 20.3 del ET. En segundo lugar, la medida es idónea en tanto que la misma es útil para exteriorizar, conocer e identificar al responsable de las irregularidades detectadas en la caja del centro comercial, en el que prestaba sus servicios la trabajadora despedida, irregularidades detectadas tras la implantación de un nuevo sistema de control informático; necesaria, por cuanto se trataba de probar las operaciones de apropiación dineraria y por ultimo proporcional en tan-

to que su adopción tenía como exclusivo destino las dependencias de caja de la tienda, espacio donde se llevan a cabo conductas que no exigen, según el tribunal, preservación de su conocimiento por terceras personas.

En relación a la información sobre la instalación de la cámara de seguridad, la sentencia señala que tal circunstancia vino acompañada de la colocación de un anuncio informativo de que el centro de trabajo estaba siendo videovigilado.

Por todo lo anterior, a juicio de la Sala la decisión empresarial no fue lesiva de los derechos fundamentales.

4.2. La posición mayoritaria: la conexión entre la dispensa del consentimiento al tratamiento de datos y el deber de información a los trabajadores

A partir de la interposición del recurso de amparo se procede a razonar sobre la posible lesión del derecho a la protección de datos personales como categoría autónoma del derecho a la intimidad (art.18.4 CE).

Hasta este momento no se había hecho referencia expresa a la autodeterminación informativa. Esta circunstancia será puesta de manifiesto por el Ministerio Fiscal para apoyar la inadmisión de la demanda de amparo desde el punto de vista formal. Sin embargo, el Tribunal Constitucional (STC 39/2016, FJ2) aprecia que la recurrente si había invocado el derecho fundamental vulnerado, si bien no explícitamente. Por consiguiente, sus testimonios habrían permitido desde el principio a los órganos judiciales ordinarios pronunciarse sobre el problema de la vulneración del derecho fundamental de la protección de datos.

Sobre la base de estas consideraciones, partiendo de que la sanción que se le impuso se basó en las imágenes captadas por la cámara de videovigilancia y tomando como referencia la STC 29/2013, la recurrente afirma que el derecho a la información previa al trabajador integra la cobertura ordinaria del derecho fundamental del artículo 18.4 CE, sin que sea suficiente que el tratamiento sea lícito y persiga un fin proporcionado. La necesidad de información previa, expresa, clara e inequívoca a los trabajadores debe referirse a la captación de imágenes, a su finalidad de control de la actividad laboral y a su posible utilización para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo. De no ser así, se vulnera el artículo 18.4 CE.

La demandante explica que, en lugar de esto, el tratamiento de datos se llevó a cabo sin informar al trabajador sobre su utilidad para la supervisión laboral; sin la existencia de distintivos anunciando la instalación de cámaras y la captación de imágenes; y sin comunicar a la AEPD la creación del fichero.

El recurso de amparo viene a tratar de aclarar el alcance de la información a facilitar a los trabajadores: si es suficiente una información general o si, como

se había pronunciado la STC 29/2013 de 11 de febrero, es necesaria una información específica.

Centrando la cuestión en el derecho fundamental a la protección de datos y tras recordar que la imagen se considera como dato personal, el máximo intérprete de la Constitución reitera la doctrina consagrada en la STC 292/2000 en su fundamento jurídico 7. El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos, que se concreta en la facultad de consentir la recogida, la obtención y el acceso a los datos personales. Este derecho requiere, como complemento indispensable, la facultad de saber quién los posee y para qué, pudiendo oponerse a esa posesión o uso.

Como principio general, el tratamiento de datos solamente será posible con el consentimiento de su titular, salvo que exista una habilitación legal que disponga otra cosa. Esto último ocurre en el ámbito laboral, pues, en base al art. 6.2 LOPD, el consentimiento se entiende implícito en el contrato laboral siempre que el tratamiento de datos sea necesario para su mantenimiento o cumplimiento. Esta excepción, señala el Tribunal, abarca sin duda un tratamiento de datos dirigido al control de la relación laboral, en definitiva dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los trabajadores afectados sí sería necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato.

Esto no obsta para que, como ya puso de manifiesto la anterior STC 29/2013, aunque no sea necesario el consentimiento, el deber de información siga existiendo, pues este deber permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO) y conocer la dirección del responsable del tratamiento o, en su caso, del representante (art. 5 LOPD).

Sin embargo, en palabras del Alto Tribunal, a la hora de valorar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información, la dispensa del consentimiento al tratamiento de datos en determinados supuestos debe ser un elemento a tener en cuenta, dada la estrecha vinculación entre el deber de información y el principio general de consentimiento.

Aquí es donde el Tribunal Constitucional se aparta de la doctrina recogida en la STC 29/2013, porque en aquella ocasión dejaba claro que el derecho a la información (la facultad de saber quién dispone de los datos y a que uso los está destinando) es un elemento caracterizador de la definición constitucional del derecho fundamental a la protección de datos personales del artículo 18.4 CE. Este derecho de información opera incluso cuando existe habilitación legal para recabar datos sin necesidad del consentimiento del titular.

En cambio en la STC 39/2016 después de afirmar que el deber de información previa forma parte del contenido esencial del derecho fundamental, el Tribu-

nal lo vincula estrechamente al principio general del consentimiento del afectado. En consecuencia, en aquellos supuestos en los que la ley ha excepcionado el consentimiento para el tratamiento de datos, tal circunstancia debe tenerse en cuenta a la hora de valorar si se ha vulnerado el derecho fundamental a la protección de datos por incumplimiento del deber de información.

Aplicando esta doctrina al tratamiento de datos obtenidos mediante videovigilancia en el ámbito laboral, el Tribunal deduce que el empresario no necesita el consentimiento del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o supervisión laboral (art.6.2 LOPD) ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral ex art.20.3 ET.

La relevancia constitucional de la ausencia o deficiencia de información, en los supuestos de videovigilancia laboral exige ponderar los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial, reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE.

Serán las circunstancias de cada caso las que determinen si las facultades de control empresarial han vulnerado el derecho fundamental en juego. A estos efectos el Tribunal trae a colación la jurisprudencia sobre el conflicto entre los derechos fundamentales a la intimidad y el secreto de las comunicaciones y el control empresarial del uso de los medios informáticos de la empresa por parte del trabajador.

Para estos casos, se exige eliminar la expectativa de privacidad que pudiera tener el trabajador, imponiendo a la empresa un deber información a los trabajadores sobre la existencia del control empresarial y de los medios utilizados[11].

Esta doctrina puede apreciarse en la STC 170/2013, de 7 de octubre, que resolvió el recurso de amparo interpuesto por un empleado que resultó despedido por haber proporcionado indebidamente información confidencial de la empresa a personal de otra entidad mercantil, a través del correo electrónico de aquella. En este supuesto, el convenio colectivo tipificaba como infracción la utilización de los medios informáticos propiedad de la empresa (correo electrónico, Intranet, Internet, etc.) para fines distintos de los relacionados con el contenido de la prestación laboral, con la salvedad de los derechos sindicales.

Para el Tribunal Constitucional, el derecho del empresario a vigilar la manera en que los empleados usaban los ordenadores de la empresa en el

[11] STEDH de 3 de abril de 2007, asunto *Copland vs. Reino Unido*. la expectativa de intimidad y confidencialidad de los trabajadores sólo desaparece si la empresa advierte de la fiscalización.

trabajo, formaba parte de su derecho más amplio de supervisar la forma en que efectuaban sus tareas profesionales. Por esta causa, en la STC 170/2013 lo que se planteó fue el conflicto entre esta manifestación de la libertad de empresa y los derechos a la intimidad y al secreto de las comunicaciones. Al considerar que aquella previsión del Convenio colectivo, implicaba la facultad de la intervención empresarial de las comunicaciones electrónicas sin necesidad de previa información a los trabajadores, el Tribunal Constitucional concluyó que no se vulneraron los derechos fundamentales del art.18.1 y 3 CE al no existir una expectativa de privacidad.

En términos similares se pronunció el Tribunal de Estrasburgo en la STEDH de 12 de enero de 2016, caso Barbulescu contra Rumania. En este asunto, la empresa había vigilado las comunicaciones del trabajador a través de una cuenta de correo electrónico y había descubierto que había estado utilizando internet con fines personales. Las normas internas de la compañía prohibían el uso de estos recursos empresariales para fines personales.

El tribunal de Estrasburgo sin entrar en la cuestión de si el trabajador había sido avisado o no de una posible vigilancia de su correo electrónico, dió por hecho que la empresa estaba legitimada para acceder a aquella información. Estimó que era razonable que un empresario quisiera comprobar que sus empleados estaban llevando a cabo sus tareas profesionales durante sus horarios laborales. Y, por tanto, que la vigilancia fue proporcionada y de alcance limitado.

En el marco de estas observaciones el Tribunal Constitucional se ocupa de determinar si en este supuesto se ha producido la vulneración o no del deber de información.

Según quedó acreditado, en el escaparate del establecimiento, en un lugar visible, se había colocado el distintivo informativo exigido por la Instrucción 1/2006 de 8 de noviembre de la AEPD de datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Conforme a esta normativa, el distintivo informativo deberá incluir una referencia a la «Ley orgánica 15/1999, de protección de datos» y a la finalidad para la que se tratan los datos («zona videovigilada»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

Por consiguiente, el Tribunal Constitucional afirma que el trabajador conocía que en la empresa se había instalado un sistema de control por videovigilancia, "*sin que haya que especificar, mas allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control…* En consecuencia, teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia a través

del correspondiente distintivo informativo…no puede entenderse vulnerado el artículo 18.4 CE". (STC 39/2016, FJ4, la cursiva es nuestra)

El deber informativo previo al trabajador se entiende cumplido con la colocación de los distintivos informativos. En consecuencia, no puede entenderse vulnerado el art. 18.4 CE. Para el Alto Tribunal, lo importante será determinar si se ha cumplido el principio de calidad de los datos, es decir, si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral porque solo en este caso el empresario no estaría obligado a solicitar el consentimiento de los trabajadores afectados. Al haber sido instaladas las cámaras a raíz de las sospechas de que algún trabajador se estaba apropiando del dinero de la caja, y al haber captado la apropiación de efectivo por parte de la recurrente, por lo cual fue despedida se ha cumplido plenamente el requisito de que el tratamiento de datos responda a una finalidad legítima, como ha sido en este caso el control de la relación laboral. Lo sustancial es el fin no el medio.

El control que debe realizarse consistirá en determinar si la instalación y empleo de medios de captación y grabación de imágenes por la empresa ha respetado el derecho a la intimidad personal, de conformidad con las exigencias del principio de proporcionalidad.

En síntesis, concluye que en el caso que nos ocupa la instalación de cámaras de seguridad que controlaban la zona de caja era una medida justificada por las razonables sospechas de que alguno de los trabajadores se estaba apropiando de dinero; idónea para verificar quién cometía las irregularidades y adoptar las medidas disciplinarias; necesaria como prueba de tal circunstancia y proporcionada, pues la grabación se limitó a la zona de caja. Por todo lo dicho, no se puede hablar de vulneración del derecho a la intimidad personal (art. 18.1 CE).

4.3. El contenido esencial de los derechos fundamentales como canon de constitucionalidad frente al interés del empresario en vigilar el cumplimiento de la relación laboral

Para una acertada visión del problema del deber de información a los trabajadores en los supuestos de videovigilancia en el ámbito laboral desde la perspectiva del contenido esencial del derecho fundamental a la protección de datos es imprescindible la lectura de los votos particulares con los que cuenta esta sentencia uno del magistrado Valdés Dal-Ré al que se adhiere la magistrada Adela Asua Batarrita, y otro del magistrado Xiol Ríos.

La sentencia parte de una noción del poder de dirección empresarial que no encaja en el modelo de relaciones laborales que instaura la Constitución. De acuerdo con nuestra Norma Suprema, los poderes del empresario quedan delimitados por el contenido esencial de los derechos fundamentales de los trabajado-

res. Por consiguiente, las facultades de vigilancia y control empresarial pueden ejercitarse siempre que no se opongan a la garantía sustantiva de tales derechos.

Partiendo de esta premisa, Valdés Dal-Ré rechaza que, a los efectos de la resolución del recurso de amparo, las facultades de vigilancia y control empresarial ex art. 20.3 ET, se hayan elevado a manifestaciones de los derechos de propiedad y libertad de empresa de los arts.33 y 38 CE, para plantear así una supuesta colisión con los derechos fundamentales de los trabajadores.

De acuerdo con su razonamiento, la clave de su discrepancia reside entonces en la desviación del juicio de constitucionalidad que «sortea y da de lado» el examen del contenido esencial de los derechos fundamentales. En el enjuiciamiento de si la medida se ajusta o no a la Constitución, la facultad de control empresarial ex art.20.3 ET no puede servir de parámetro para limitar los derechos fundamentales de los trabajadores. Una argumentación de este tipo conduce a que una decisión de supervisión empresarial que no respeta el deber de información a los trabajadores (art.5 LOPD) prevalece sobre el derecho fundamental a la protección de datos del art.18.4 CE y sobre la doctrina del Tribunal Constitucional consagrada en las SSTC 292/2000 de 30 de noviembre y 29/2013 de 11 de febrero.

En el presente recurso, se parte de la base de que, en el marco de las relaciones laborales, la instalación de una cámara de videovigilancia, enfocando directamente a la caja ante la sospecha de que un trabajador se está apropiando de dinero, exige el deber de información al trabajador que establece el art.5 LOPD.

En consecuencia la cuestión es aclarar si el deber de información requiere especificar la finalidad de control de la actividad laboral como estableció la STC 29/2013 de 11 de febrero; o si por el contrario, bastaría para entender cumplido dicho deber, un anuncio hecho al público sobre la existencia de cámaras de seguridad en el establecimiento

El parámetro utilizado para decidir si ha habido o no vulneración del derecho fundamental a la autodeterminación informativa ha sido el contenido de la Instrucción 1/2006 de 8 de noviembre de la AEPD, olvidando que solo por ley se pueden fijar límites a un derecho fundamental (art. 53.1 CE).

Como afirma con claridad el voto particular de Valdés Dal-Ré, el derecho de los trabajadores a ser informados de los datos obtenidos por el empresario forma parte del núcleo fuerte del *habeas data*, que comprende entre sus contenidos el derecho a conocer el uso y destino de las imágenes captadas y la finalidad perseguida por el sistema de video-vigilancia. Así lo recuerda la primera parte de la Sentencia, cuando afirma que el deber de información forma parte del contenido esencial del derecho a la protección de datos. Pese a ello, el Tribunal Constitucional afirma a continuación que, una vez insertado el distintivo informativo

y cumplidos los anexos que exige la Instrucción de la AEPD, ya no es preciso especificar la finalidad exacta del control empresarial. Lo único importante será determinar si el dato obtenido se ha destinado a esta finalidad pues de lo contrario el empresario estaría obligado a solicitar el consentimiento de los trabajadores. A juicio de Valdés Dal- Ré se confunde el requisito del consentimiento con el deber de información.

Para Xiol Rios no se puede afirmar que la Constitución autoriza al empresario ante cualquier sospecha a instalar sistemas de videovigilancia para el control de los trabajadores, sin informarles de tal medida. Y no se puede alegar que tal deber se ha cumplido a través de un aviso al público en el entorno sobre la existencia de cámaras de seguridad. Esto, en palabras del Magistrado, «dinamita» el derecho fundamental a la protección de datos. No es aceptable que la información dirigida al público sea suficiente para entender cumplido el requisito del art.5 LOPD. A juicio de Xiol Ríos, la omisión de toda información a los trabajadores sobre la existencia de cámaras específicamente orientadas a sus puestos de trabajo supone una lesión del derecho fundamental a la autodeterminación informativa que afecta a su contenido esencial, porque lo hace ineficaz, carente de todo sentido práctico e irreconocible.

La sentencia debería haber declarado que no hay en la ley una habilitación que permita incumplir el deber de información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales. Tampoco se puede fundamentar esta omisión en el interés del empresario en controlar la actividad laboral a través de sistemas sorpresivos de tratamiento de datos. La lógica de la solución aceptada por la mayoría vulnera el derecho fundamental a la protección de datos personales del trabajador en su núcleo esencial. Confunde, como ya decía la STC 29/2013 (FJ7) y reitera Valdés Dal-Ré en su voto discrepanate, la legitimidad del fin con la constitucionalidad del acto; si bien es cierto que el objetivo del control de las obligaciones laborales a través del tratamiento de imágenes, es legítimo ex art.20.3 ET incluso sin consentimiento del trabajador (art. 6.2 LOPD). Simultáneamente, la utilización de medios que niegan al trabajador la información expresa, precisa e inequívoca que exige art. 5 LOPD lesionan el derecho a la autodeterminación informativa consagrado en el art.18.4 CE.

En resumen, según se extrae de los votos particulares, la orientación que subyace en este pronunciamiento es regresiva en la protección de los derechos fundamentales de los trabajadores. Estos derechos se ven modalizados en su efectividad cuando no suprimidos a fin de reforzar los intereses del empresario con el apoyo de los art.33 y 38 de la CE; además de evidenciar una concepción de la empresa incompatible con la definición de Estado social y democrático de derecho que consagra nuestra Carta Magna en su artículo 1.1.

5. CONCLUSIONES

La doctrina del Tribunal Constitucional ha dejado claro que el contrato de trabajo no puede considerarse un título legitimador de recortes en el ejercicio de los derechos fundamentales que incumben al trabajador. Este no pierde su condición de ciudadano por insertarse en el ámbito de una organización privada. El ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir, en ningún caso, para producir resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador, ni para sancionar el ejercicio legítimo de tales derechos por parte de aquél[12]. Los derechos fundamentales son límites al poder del empresario que tienen su fundamento último en la dignidad humana. En nuestro ordenamiento constitucional, los derechos fundamentales alcanzan una posición prevalente[13].

El empresario en el ejercicio del poder de dirección que tiene su fundamento en el artículo 20 ET, puede adoptar las medidas que estime oportunas para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. La instalación de cámaras de videovigilancia para el control empresarial de la relación laboral aporta indudables ventajas al poder de vigilancia del empresario pero al propio tiempo supone un riesgo para los derechos fundamentales del trabajador, ya que implica la sumisión de ciertos aspectos de su vida privada a las necesidades de la organización productiva. El alcance de la videovigilancia supera con creces la simple verificación del cumplimiento de los deberes derivados de la prestación laboral, pues la intensidad de este control tecnológico invade la privacidad del sujeto y supone la obtención de información estimable sobre su persona.

Desde esta perspectiva, la jurisprudencia constitucional había asumido inicialmente que los problemas jurídicos derivados del control audiovisual de la prestación laboral debían analizarse desde la óptica de la protección del derecho fundamental a la intimidad del trabajador. Entre los motivos que justifican tal proceder se encuentra el hecho de que el reconocimiento jurisprudencial del derecho a la protección de datos personales ha sido muy reciente. El contenido esencial del derecho fundamental a la protección de datos fue delimitado definitivamente por el Tribunal Constitucional a partir de las SSTC 290 y 292/2000, de 30 de noviembre. De ahí que los amparos, resueltos con anterioridad a esta fecha, se fundaran primordialmente en el derecho a la intimidad. Sin embargo, el derecho a la protección de datos es un derecho fundamental autónomo e independiente del derecho a la intimidad. De ahí la importancia de la jurisprudencia que puso de manifiesto que los avances tecnológicos han puesto en riesgo no ya nuestra intimidad, sino

[12] STC 39/2016, de 3 de marzo, FJ 5.
[13] STC 99/1994 de 11 de abril, FJ 7.

nuestra propia identidad y libertad. Derivado del artículo 18.4 CE, este precepto constitucional es la base sobre la que el legislador construyó su régimen jurídico. Nos encontramos por tanto ante un derecho fundamental nuevo y de configuración legal. Por ello, su tutela a través del recurso de amparo supone que el juicio de constitucionalidad de cualquier medida que suponga tratamiento de datos personales del trabajador se transforma inevitablemente en un juicio de legalidad.

Hay que tener en cuenta esta idea para desligar la resolución de los supuestos de videovigilancia en el ámbito laboral de la esfera del derecho a la intimidad. Las imágenes grabadas constituyen «datos personales» que pueden servir para deducir perfiles del trabajador. La función del derecho fundamental a la protección de datos no es la de proteger un ámbito propio y reservado, libre de intromisiones ajenas, sino la de que el empleado pueda ejercer un control jurídico pleno sobre el uso y destino de su información personal, evitando que se emplee para fines distintos de los que motivaron su obtención. Además, a diferencia del derecho a la intimidad, el derecho a la autodeterminación informativa reclama específicos deberes jurídicos derivados de los principios del consentimiento para la recogida de los datos y de la información sobre el uso y destino de los mismos. Estos deberes son imprescindibles para que el afectado pueda ejercer los derechos ARCO que la ley le reconoce. Cualquier medida que restrinja estas facultades hasta hacerlas irreconocibles devalúa el contenido esencial del derecho fundamental a la protección de datos.

La información es un derecho del interesado que se regula como una obligación del responsable del tratamiento. En relación con el modo de suministrar esa información esta ha de ser expresa, precisa e inequívoca. Y debe precisar el objeto y la finalidad de la recogida de los datos.

El derecho del trabajador a la información previa actúa como garantía del control y la disposición de los propios datos personales. Con este derecho, se salvaguarda la libertad y la autodeterminación del trabajador, evitando un potencial uso ilegítimo de sus datos personales. El empresario debe asumir la obligación de informar, tendente a facilitar al trabajador el ejercicio de sus derechos.

Solo cuando el trabajador sea informado previamente de los datos personales que se intentan recabar o de los obtenidos por el empresario, podrá valorar la repercusión del sistema de videovigilancia respecto de su vida privada y ejercer un control sobre su información personal, de conformidad con lo previsto en la normativa sobre protección de datos.

La importancia del principio de transparencia ha sido puesta de manifiesto por el recién aprobado Reglamento de la Unión Europea 2016/679, que ha resaltado entre los deberes del responsable del tratamiento la transparencia en la infor-

mación y comunicación al interesado[14]. Esta obligación se concreta en el artículo 5.1 LOPD: «Los interesados a los que se soliciten los datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante».

Por su parte, la obligación general de recabar el consentimiento del afectado para el tratamiento de los datos personales tiene, entre otras excepciones la de que esta operación se lleve a cabo con ocasión de una relación laboral de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento. Esta singularidad no puede implicar una renuncia por parte del trabajador al derecho a ser informado del tratamiento de sus datos personales, pues quedaría al arbitrio del empresario decidir cuándo habría información por tratarse de un control rutinario y cuando por tratarse de un control oculto sería oportuna una información al público en general.

Por el contrario, el deber de información persiste aunque no haya obligación de solicitar el consentimiento del trabajador, pues como puso de manifiesto la STC 39/2016 «este deber permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o, en su caso, del representante (…) El deber de información previa forma parte del contenido esencial del derecho a la protección de datos». De no cumplirse, se está vulnerando no ya la ley, sino el derecho fundamental que esta ha venido a desarrollar. El artículo 18.4 CE asegura a la persona un poder de control sobre sus datos, su uso y destino. Sin embargo «ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin»[15].

[14] Artículo 88.

[15] STC 29/2013 de 11 de febrero, FJ 6.

La cuestión objeto de debate en la STC 39/2016 ha sido la de aclarar el alcance de la información a los trabajadores en los supuestos de control audiovisual de la prestación laboral. La posición que el Alto Tribunal había defendido en la STC 29/2013 puede resumirse en que la omisión del deber de información previa al trabajador supone una lesión del contenido esencial del derecho fundamental a la protección de datos pues restringe el ejercicio de las facultades que lo conforman. Por el contrario en la STC 39/2016 el máximo intérprete de nuestra Carta Magna parece dejarse llevar por la postura de quienes entienden que una información expresa, precisa e inequívoca que contemple la finalidad del tratamiento, las consecuencias de su obtención y la posibilidad de ejercitar los derechos ARCO, frustraría el interés del empresario en la obtención de un medio de prueba de conductas ilícitas.

La videovigilancia en el recurso de amparo resuelto por esta sentencia tenía el propósito de controlar el cumplimiento de la relación laboral ante las sospechas del empresario por las irregularidades contables que había detectado un nuevo sistema informático. Con el pretexto de no frustrar la obtención de un medio de prueba de tales desviaciones, no se informó a los trabajadores de la instalación de la cámara. En su lugar se cumplieron las exigencias de la Instrucción 1/2006 de la Agencia Española de Protección de Datos. En el escaparate del establecimiento, en un lugar visible, se colocó un distintivo informativo. La intención última de este rótulo era la de informar al público en general que el establecimiento estaba siendo videovigilado.

Esta circunstancia, sin embargo, es apreciada por el Tribunal Constitucional como suficiente para considerar cumplido el deber de información que impone el derecho fundamental a la protección de datos. El trabajador conocía la existencia de las cámaras y, por lo tanto, no podía tener una «expectativa de privacidad». El trabajador podía advertir que la zona estaba sometida a videovigilancia, y podía dirigirse a la entidad responsable identificada también en el distintivo, para solicitar la información necesaria sobre el destino, el uso y el tratamiento de los datos. Pero en ningún caso se le había informado que sus imágenes podían ser utilizadas con la finalidad del control de la prestación laboral. En consecuencia el distintivo convierte el derecho del trabajador a la información sobre el tratamiento de datos personales y el correlativo deber del empresario a proporcionarla en la obligación del trabajador de ser lo suficientemente diligente como para deducir que sus datos están siendo objeto de tratamiento, eso sí, ignorando con qué finalidad.

En este supuesto, las cámaras sirvieron para la constatación de un incumplimiento de la relación laboral. La pregunta es si el interés del empresario de sorprender *in fraganti* al empleado justifica el recurrir a un sistema de videovigilancia que no garantiza la finalidad última para la que puedan ser empleadas las imágenes en el futuro. Los datos de carácter personal solo pueden ser recogidos

para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento, como establece el principio de calidad de los datos[16]. No serían válidas finalidades tan generales que admitieran cualquier propósito, aunque fuera legítimo, pues con ello se frustraría el poder del afectado de controlar la recopilación, archivo y tratamiento de su información personal.

La sentencia no tiene en cuenta que el principio de transparencia y el de calidad de los datos forman parte del contenido esencial del derecho fundamental a la protección de datos, y no solo para que el interesado preste su consentimiento sino especialmente cuando este no es necesario como ocurre en las relaciones laborales. El deber de información previa al trabajador o si se quiere al Comité de Empresa, con indicación de la finalidad del tratamiento, es un requisito de inexcusable legitimidad de cualquier sistema de videovigilancia, porque garantiza el poder de disposición del empleado sobre sus datos personales, en este caso sus imágenes. El uso de las videocámaras para controlar el cumplimiento de la relación laboral no se ve satisfecho con la existencia de rótulos indicativos anunciando la instalación de cámaras y la captación de imágenes. Es necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida.

Con este fallo, el Tribunal va a apartarse de su jurisprudencia anterior, al diferenciar los supuestos del empleo de la videovigilancia para control específico de la actividad laboral, siempre que el empresario tenga sospecha de irregularidades, de los hallazgos casuales derivados de grabaciones de cámaras orientadas al control de la seguridad en la STC 29/2013. No obstante, en ambos casos, había indicios de quebrantamiento de los deberes laborales. En un supuesto se emplearon las cámaras previamente instaladas que vigilaban el acceso al recinto universitario, para el control de la jornada laboral y en el otro, se instalaron con ocasión de la apreciación de las irregularidades contables. El fin común era la obtención de una prueba que justificase la sanción o el despido. No obstante la solución dada por el Tribunal Constitucional es distinta. En la STC 29/2013, el objetivo de obtener una prueba del incumplimiento de la jornada laboral no es excusa de la falta de información previa al trabajador de que las imágenes se iban a utilizar para la supervisión laboral. En la STC 39/2016, el fin de comprobar y obtener prueba de una apropiación indebida, justifica la sustitución de la obligación previa de informar al trabajador por la colocación de un distintivo informativo que, sin embargo, a la luz del derecho fundamental a la protección de datos es manifiestamente inconstitucional pues la información forma parte de su contenido esencial.

[16] Artículo 4 de la LOPD.

En mi opinión, el fin de comprobar y obtener prueba de una apropiación indebida no puede justificar el medio, la falta de información previa al trabajador. La vulneración del derecho a la autodeterminación informativa del trabajador resultó de la privación de las facultades y principios que conforman el poder de control sobre sus datos personales. El deber de información no está vinculado al consentimiento, sino que es imprescindible para el ejercicio de los derechos ARCO. En consecuencia, si falta la información, se corre el riesgo de que los datos personales del trabajador se destinen a una finalidad distinta de aquella para la que fueron recabados, con lo que se frustraría del derecho de oposición; puede incluso que sean incorrectos y, en consecuencia, el trabajador, al desconocerlos, no podría rectificarlos. Incluso podría el empresario cederlos sin que se informe al trabajador sobre su cesión y por tanto de forma irregular. Los sistemas de videovigilancia ofrecen posibilidades de mantenimiento, conservación y recuperación en cualquier momento de las imágenes y sonidos. Estos tratamientos de datos permiten la elaboración de perfiles del trabajador, con el riesgo que supone no saber qué aspectos de su vida privada son conocidos, conservados y grabados por el empresario, sin tener en cuenta su relevancia con las obligaciones derivadas de la prestación laboral con total ignorancia por parte del trabajador afectado. Las imágenes tratadas y grabadas pueden servir para confeccionar perfiles ideológicos raciales, sexuales y económicos o para discriminar al trabajador.

En consecuencia, la obligación del empresario de informar a los trabajadores del tratamiento de sus datos personales debe determinar la finalidad de control de la actividad laboral a la que esa captación podría ser dirigida; una información que concrete las características y el alcance del tratamiento de datos que va a realizarse, esto es, en qué casos las grabaciones podrían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podrían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

Lo importante es que el empresario no posea más datos de los estrictamente necesarios para su derecho de defensa, que sean veraces y que se facilite la identidad de los responsables del tratamiento, con restricciones en cuanto al modo, tiempo y forma de conservación, así como que se guarde la debida proporcionalidad.

No obstante lo dicho, como los derechos fundamentales no son absolutos, no me parece desacertada la opinión de Xiol Ríos, en el segundo voto particular, cuando afirma que podría justificarse una restricción del derecho a la información si la instalación de la cámara se notificase únicamente al Comité de Empresa, para evitar la frustración de la finalidad de la videovigilancia. Lo cual debería limitarse, en mi opinión, a aquellos supuestos en los que se trata de la comprobación de ilícitos penales especialmente graves, como el acoso sexual y para la ob-

tención de pruebas. Una interpretación semejante debería exigir que, en cualquier caso, se garantizara el ejercicio de los derechos ARCO por parte del trabajador. Una medida de este tipo exigiría que la empresa que quiera instalar videocámaras informase a los representantes de los trabajadores sobre 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 y sobre el acceso a las mismas, su conservación y cancelación.

En relación con el deber de información sobre la instalación de las videocámaras, la buena fe contractual vendría a avalar estas conclusiones, lo cual se refleja en el Estatuto de los Trabajadores, que regula en su artículo 64 los derechos de información y consulta y competencias del Comité de Empresa. Este derecho es 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.

En cualquier caso, los límites al deber de información deben respetar siempre el contenido esencial del derecho fundamental a la protección de datos. De lo contrario, si se restringe de tal manera que se impida el derecho a la información del trabajador, se estaría denegando el derecho de acceso a los propios datos. El derecho a la información es el núcleo del *habeas data*.

La Sentencia analiza el supuesto desde la perspectiva del derecho a la intimidad. Equipara el deber de información que pesa sobre el empresario para eliminar la expectativa de confidencialidad, en el ámbito del derecho a la intimidad en el control del uso de los medios informáticos de la empresa, con el derecho del trabajador a ser informado como presupuesto del ejercicio de las facultades ARCO, contenido esencial de la autodeterminación informativa.

La Constitución exige que la ley sea la que fije los límites a un derecho fundamental. Como pusieron de manifiesto las SSTC 292/2000 y 29/2013, no hay habilitación legal expresa para limitar el derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales. El deber de información al trabajador debe ser previo al tratamiento de datos. No se puede fundamentar el incumplimiento de esta obligación de informar en el interés empresarial de controlar la actividad laboral, a través de sistemas sorpresivos de tratamiento de datos. La lógica de la argumentación de la mayoría de los Magistrados en la STC 39/2016 ha sido la conveniencia empresarial del uso estos sistemas de videovigilancia. Pero esa interpretación no puede sostenerse a costa de quebrantar el derecho fundamental del 18.4 CE.

En resumen, la doctrina constitucional que se extrae de este pronunciamiento olvida el contenido esencial del derecho fundamental a la protección de datos. Asimismo, el pronunciamiento desorienta, por cuanto no deja clara las diferencias entre el derecho a la intimidad y el de autodeterminación informativa. Y por

último, resaltaría, dada su trascendencia, que la resolución desconoce los graves riesgos que para la privacidad se derivan de los avances tecnológicos de nuestro tiempo con medios y sistemas de control empresarial que se perfeccionan a un ritmo vertiginoso.