

**EL USO DE LAS CÁMARAS DE  
VIDEOVIGILANCIA A TRAVÉS DE  
LA JURISPRUDENCIA: UNA  
SISTEMATIZACIÓN NECESARIA  
PARA DELIMITAR EL CANON  
CONSTITUCIONAL REQUERIDO  
PARA SU VALIDEZ**

JUAN PASCUAL CABALLERO

**RESUMEN:** El presente artículo se propone exponer cómo y cuándo se puede acudir a la videovigilancia en las relaciones laborales, mediante un breve estudio de las resoluciones judiciales que tratan la utilización de cámaras, fijas o móviles. Dicha exposición finalizará con una sistematización que permita identificar cuáles son las tres situaciones en las que se puede utilizar las cámaras de videovigilancia, para que fines y con qué límites.

**SUMARIO:** 1. INTRODUCCIÓN 2. EVOLUCIÓN DE LA DOCTRINA CONSTITUCIONAL PRECEDENTE. 2.1. Los pronunciamientos sobre derecho a la intimidad: Sentencias del Tribunal Constitucional 98/2000, de 10 de abril (Asunto Casino de La Toja) y 186/2000, de 10 de julio (Asunto Ensidesa) 2.2. La introducción del derecho a la protección de datos: Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero (Asunto Universidad de Sevilla) 2.3. El “giro jurisprudencial”: Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo (Asunto Bershka) 3. RECEPCIÓN POR EL TRIBUNAL SUPREMO 3.1. La Sentencia del Tribunal Supremo de 7 de julio de 2016 (RCUD 3233/14; Asunto DIA) 3.2. Sentencias del Tribunal Supremo de 31 de enero de 2017 (RCUD 3331/2015) y 1 de febrero de 2017 (RCUD 3262/2015) Asuntos: PLANA & DIEGUEZ 4.1. Sentencia del Tribunal Supremo de 2 febrero (RCUD 554/2016; Asunto DIR FITNESS) 4. CONCLUSIONES.

## 1. INTRODUCCIÓN

No es objeto del presente trabajo debido a su extensión la exposición pormenorizada de la normativa que afecta al uso de cámaras en el ámbito de las relaciones laborales. El análisis se limitará a una sucinta exposición de las resoluciones que tratan el uso de estos medios ópticos con el fin de determinar cuáles son las situaciones en las que se puede utilizar las cámaras de videovigilancia, con que fines y límites.

La normativa básica que es valorada por las resoluciones judiciales expuestas es la siguiente:

- La Constitución Española (en adelante, “CE”) prestando especial atención a los artículos 18.1 (derecho de la intimidad), 18. 4 (derecho a la protección), 33 (derecho a la propiedad privada) y 38 (libertad de empresa)<sup>1</sup>.
- Los artículos 4.2.e) y 20.3 del Estatuto de los Trabajadores (en adelante, “ET”).
- La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, “LOPD”) y la normativa de protección de datos relacionada.
- La reiterada jurisprudencia del Tribunal Constitucional (en adelante, “TC”)<sup>2</sup>, analiza el medio de control elegido por el empresario a través del principio de proporcionalidad en su triple dimensión: idoneidad, necesidad y equilibrio.

Dada la escasa regulación<sup>3</sup>, desde el punto de vista normativo surge un conflicto entre las facultades de control empresarial<sup>4</sup> y el respeto a la dignidad del trabajador<sup>5</sup>. Es más, en ningún apartado del ET se hace referencia al derecho a la protección de datos de los trabajadores, es por esta razón que,

---

<sup>1</sup> El Tribunal Constitucional ha señalado, en reiteradas ocasiones, la plena efectividad de los derechos fundamentales del trabajador en el marco de la relación laboral. Así lo recoge la STC 88/1985, de 19 de julio, FJ 2º, cuya doctrina se reitera posteriormente, entre otras, en las SSTC 186/1996, de 25 noviembre y 90/1997, de 6 de mayo. A este respecto *vid.* SANGUINITE RAYMUND W.: «Derechos fundamentales de la persona del trabajador y poderes empresariales». *Revista de Relaciones Laborales*. núm. 21-22 pág. 17. Adicionalmente, hay autores que consideran la existencia de derechos fundamentales inespecíficos laborales, que se convierten en derechos de la relación laboral por los sujetos – empresario y trabajador- y por la naturaleza de la relación en que se hacen valer. *vid.* PALOMEQUE LÓPEZ, C.: «Derechos fundamentales de la persona del trabajador y poderes empresariales», AA.VV- Dir. SEMPERE NAVARRO, A.V.: «El modelo social de la Constitución Española de 1978». *Aranzadi*. Madrid, 2003. pág. 11.

<sup>2</sup> Por todas, STC 186/2000, de 10 julio de 2000; STC 29/2013, de 11 de febrero de 2013 y STC 39/2016, de 3 marzo de 2016.

<sup>3</sup> *vid.* GOÑI SEIN, J.L.: «Los límites de las potestades empresariales vs. Derecho a la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática de las redes sociales», *Actum Social*, núm.95, 2015. pág.6; GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016», *Revista Aranzadi Doctrinal*, núm.5, 2016. pág.1.

<sup>4</sup> Estas facultades empresariales tienen su raíz en el art. 20 del Estatuto de los Trabajadores, encajándose en nuestra carta magna a través de la libertad empresa (art. 38 CE) y la propiedad privada (art. 33 CE).

<sup>5</sup> STC 151/2004, 30 de septiembre y STC 56/2008, de 14 abril.

solamente podemos encontrar soluciones a este conflicto, en las resoluciones judiciales. En este sentido es necesaria una sistematización de las sentencias que analicen este tipo de situaciones.

## **2.EVOLUCIÓN DE LA DOCTRINA CONSTITUCIONAL PRECEDENTE**

Hasta la fecha de hoy son cuatro los pronunciamientos que, en materia de videovigilancia, ha dictado nuestro TC<sup>6</sup>:

### **2.1. Los pronunciamientos sobre derecho a la intimidad: Sentencias del Tribunal Constitucional 98/2000<sup>7</sup>, de 10 de abril (Asunto Casino de La Toja) y 186/2000, de 10 de julio [Asunto Ensidesa (“STC 186/2000”)]**

En ambas sentencias la *litis* se centraba en dirimir si los medios de vigilancia y control de la actividad laboral suponían, o no, una intromisión ilegítima en la intimidad de los trabajadores (sin entrar, como sí lo harán sentencias posteriores, en el derecho a la autodeterminación informativa). Analizaremos con más detalle la STC 186/2000 por ser más interesante a los efectos del presente trabajo.

#### *(i) Supuesto de hecho*

Ante la existencia de razonables y fundadas sospechas de la comisión de graves irregularidades en un puesto de trabajo (un descuadre llamativo en el rendimiento del economato), se instaló un circuito cerrado de televisión que controlaba la zona de caja de un economato. En dicho economato prestaba servicios el recurrente en amparo.

#### *(ii) Ratio decidendi*

El TC, declaró que la instalación de estas cámaras temporales era lícita, y que no se había producido una intromisión ilegítima en el derecho a la intimidad, dado que fue una medida: (a) justificada: existían indicios de la comisión de irregularidades (descuadre contable); (b) idónea: la finalidad pretendida por la empresa fue verificar si el trabajador cometía efectivamente las irregularidades sospechadas y, en tal caso, adoptar las medidas disciplinarias correspondientes; (c)necesaria: ya que la grabación sirvió de prueba de tales irregularidades (no existía otro medio menos intrusivo) y, (d) equilibrada: la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada (suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada).

---

<sup>6</sup> Estructura apuntada por GARCÍA RUBIO, M.A.: «Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales», *Revista de Jurisprudencia El Derecho*, núm.2, 2016. pág.3.

<sup>7</sup> No se puede valorar la STC 98/2000, ello a pesar de ser la primera sentencia que entró a valorar el conflicto entre las nuevas tecnologías como medio de control empresarial y el derecho fundamental a la intimidad de los trabajadores, puesto que no analiza el buen uso o no de la videovigilancia en sentido estricto.

### *(iii) Conclusión*

En consecuencia, se debe destacar que para poder instalar una cámara oculta se requiere acreditar no sólo un interés empresarial, sino también unos indicios que justifiquen la adopción de tales medidas. En sentido contrario, se podría afirmar, que no se puede realizar una vigilancia genérica de manera oculta<sup>8</sup>.

Hasta este momento la jurisprudencia era clara: las cámaras de videovigilancia sólo afectaban al derecho a la intimidad y era necesario aplicar el triple juicio de proporcionalidad para conocer si la medida adoptada por el empresario era vulneradora o no del derecho a la intimidad del trabajador. Aún no se había declarado por el órgano constitucional la autodeterminación informativa como un derecho autónomo<sup>9</sup>.

## **2.2. La introducción del derecho a la protección de datos: Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero [Asunto Universidad de Sevilla (“STC 29/2013”)]**

### *(i) Supuesto de hecho*

Un trabajador de la Universidad de Sevilla fue sancionado disciplinariamente por infracciones referidas al cumplimiento laboral de su horario laboral, habiéndose constatado tales ilícitos a partir de las imágenes grabadas por las cámaras de seguridad instaladas en el recinto universitario (vestíbulo y zonas de paso público). Las cámaras de seguridad disponían de la correspondiente autorización administrativa de la Agencia Española de Protección de Datos (en adelante, “AEPD”) para, entre otros fines, el control de acceso de las personas de la comunidad universitaria. En dicho recinto existían distintivos anunciando la presencia de cámaras y la captación de imágenes, si bien, el trabajador no había sido informado de que las grabaciones podrían utilizarse para supervisar el cumplimiento de sus obligaciones contractuales.

### *(ii) Ratio decidendi*

La novedad que introdujo la STC 29/2013 respecto de los anteriores pronunciamientos, radica en que añadió la necesidad de informar previamente al trabajador o, en palabras del tribunal, en que era necesaria “*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*”<sup>10</sup>.

---

<sup>8</sup> MERCADER UGUINA, J. R.: «El derecho a la intimidad del trabajador en el ámbito laboral». Ponencia impartida en el *II congreso de Actualidad Laboral* organizado por el Excelentísimo Colegio Oficial de Graduados Sociales de Madrid, 27 de noviembre de 2008.

<sup>9</sup>Por primera vez en la STC 292/2000, de 30 de noviembre.

<sup>10</sup> STC 29/2013, FJ 8º.

El TC, atendiendo al caso enjuiciado, concluyó que la conducta de la Universidad consistente en emplear grabaciones de imagen para controlar el cumplimiento del contrato por parte del trabajador, sin haber informado a este sobre su utilidad, resultaba contraria al artículo 18.4 de la CE, sin entrar a valorar si dicha medida superaba el examen o triple juicio desde la perspectiva de la proporcionalidad. Es más, añadió que la presencia de distintivos en el recinto universitario tal y como exige la normativa de protección de datos era suficiente para evitar la intromisión ilegítima en el derecho a la protección de datos del trabajador.

*(iii) Conclusión: diferencia con los supuestos anteriores*

Ahora bien, la diferencia entre las sentencias anteriores (además de la introducción de la protección de datos) son los supuestos de hecho enjuiciados. Se insiste en este extremo porque en muchas ocasiones, la doctrina científica no ha tenido en cuenta que la realidad de lo acontecido es la que marca la solución judicial. A la sazón de la publicación de la sentencia, muchos autores se centraron en señalar el cambio que suponía la introducción del derecho fundamental a la protección de datos. Sin embargo, estos célebres investigadores<sup>11</sup> no repararon en las diferencias sustanciales que se los hechos presentaban<sup>12</sup>.

¿Por qué la relevancia de los supuestos de hecho? Porque estamos ante dos casos distintos en lo que se refiere a la conducta empresarial y del trabajador.

(a) Sobre la conducta empresarial:

En la STC 186/2000 se instalaron unas cámaras con carácter puntual ante la existencia de unos indicios (alteración en las cuentas del economato), de forma excepcional y con la finalidad de comprobar si se estaba cometiendo una irregularidad por parte del trabajador. Por otro lado, en la STC 29/2013 se utiliza un sistema fijo y con vocación de permanencia, que servía para controlar el acceso de los miembros de la Universidad, del que no se había informado a los trabajadores, ni al comité de empresa, y que se utilizó como prueba en un proceso disciplinario.

(b) Sobre la conducta del trabajador:

---

<sup>11</sup> Entre los que destacan que se ha producido un cambio señalar: *Vid*, GARCÍA RUBIO, M.A.: «Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales», *Revista de Jurisprudencia El Derecho*, núm.2, 2016.pág.5, también *Vid* GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016», *Revista Aranzadi Doctrinal*, núm.5, 2016. pág.7 y, por último, ABONÉS LAPENA, H. I.: «Grabación de imagen o sonido y control de correo electrónico por el empresario», *Revista Española de Derecho del Trabajo*, núm.178. págs. 25 a 28.

<sup>12</sup>Matiz, permítase la insistencia, extremadamente relevante.

Siguiendo con el mismo orden, en el economato existían indicios de que se estaban produciendo robos, es decir, se podía estar atentando contra la seguridad empresarial. Al contrario, en la Universidad de Sevilla, el incumplimiento del trabajador consistía en que no cumplía con su jornada<sup>13</sup>.

De este fallo del órgano constitucional, se debe destacar que: (i) la instalación de cámaras permanentes, aun cuando el trabajador conozca de su existencia, genera una expectativa de confidencialidad sobre el trabajador siempre desconozca cuál es el fin de tal cámara. En segundo lugar (ii) el empresario y el trabajador están recíprocamente obligados a cumplir sus obligaciones de conformidad con las reglas de buena fe y diligencia<sup>14</sup>. En consecuencia, no se puede comunicar a los trabajadores, o a sus representantes, que un determinado sistema de cámaras es para controlar la seguridad ante robos de terceras personas, o para “*el control de acceso de las personas de la comunidad universitaria y del personal de empresas externas a sus campus y centros*” y, posteriormente, sancionarles conforme a las grabaciones obtenidas por esas mismas cámaras permanentes diciéndoles *ex post* que es un sistema de control de videovigilancia a efectos disciplinarios<sup>15</sup>. Esto es, a todas luces, una clara actuación de mala fe del empresario que genera una *expectativa de intimidad* en el trabajador para poder sancionarle con posterioridad.

La aplicación judicial de esta doctrina supuso que muchos órganos judiciales vinieran declarando el carácter lesivo del derecho a la protección de datos, cuando el empresario llevaba a cabo grabaciones para el control de la prestación laboral sin haber informado a los trabajadores de este fin<sup>16</sup>. Sin embargo, otros pronunciamientos distinguieron, como se ha señalado anteriormente, los supuestos en los que la videovigilancia, no se instalaba como medida preventiva y permanente, sino con carácter puntual ante la existencia de previas y fundadas sospechas de irregularidades en el trabajo. Los tribunales no apreciaban, en tales casos, que la ausencia de comunicación previa al trabajador comportara necesariamente vulneración del art. 18.4 CE y, aplicaban, por el contrario, el juicio de proporcionalidad<sup>17</sup>. O lo que es lo mismo, distinguían entre casos de instalación puntual de cámaras y supuestos de instalación fija o permanente.

---

<sup>13</sup> Un incumplimiento de estricto control laboral.

<sup>14</sup> Arts. 20 y 54.2.d ET y arts. 7, 1094, 1104 y 1107 del Código Civil. Concretamente el art. 20.2 señala: “(...) *En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe*”

<sup>15</sup> Un supuesto relevante en este aspecto fue la STS 13 mayo de 2014 (RCUD 1685/2013; Asunto Champion), en el que se constata que la representación legal de los trabajadores había interpelado al empresario acerca de cuáles eran los fines de utilización de las mismas. La empresa señaló que eran para evitar robos por terceros e incluso que algunas no estarían ni operativas.

<sup>16</sup> STSJ de Castilla -La Mancha 11 de febrero de 2016 (RSU 1714/2015; Ponente: Pedro Libran Sainz de Baranda)

<sup>17</sup> STSJ de Madrid de 9 de febrero de 2015 (RSU 886/2014; Ponente: Enrique Juanes Fraga); Castilla y León Valladolid, de 10 de octubre de 2015 (RSU 1940/2013; Susana María Molina Gutiérrez), STSJ de Cataluña, de 11 de octubre 2013 (RSU 3021/2013; Ponente Lidia Castell Valldosera); STSJ de Castilla La Mancha de 14 de enero de 2016 (RSU 1474/2015; Ponente: Luisa María Gómez Garrido)

### 2.3. El “giro jurisprudencial”: Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo (Asunto Bershka) [STC 39/2016]

#### (i) *Supuesto de hecho*

A raíz de la instalación de un nuevo sistema de control informático de caja el departamento de seguridad de Inditex detectó que en la tienda donde prestaba sus servicios la demandante existían múltiples irregularidades. Ante tales indicios, encargaron a una empresa que instalara una cámara de videovigilancia en la tienda, no comunicando a los trabajadores dicha instalación. Si bien, en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo de la existencia de cámaras que exige la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales confines de vigilancia a través de sistemas de cámaras o videocámaras (en adelante, “Instrucción 1/2006 AEPD”)<sup>18</sup>. Tras la visualización de las imágenes, se observa que una trabajadora se había venido apropiando de efectivo de la caja de la tienda, siendo despedida por este motivo.

La sentencia del TC se centra en determinar si la validez de la prueba obtenida es o no contraria a los artículos 18.4 (protección de datos) y 18.1 (derecho a la intimidad)<sup>19</sup> CE.

En lo que se refiere al derecho a la “autodeterminación informativa”, la sentencia señala que las imágenes grabadas constituyen datos de carácter personal. En este punto, señalar que sobre el derecho a la protección de datos el Tribunal, esquemáticamente, dispone que:

(a) Sobre el deber de recabar el consentimiento: en el ámbito de las relaciones laborales concurre habilitación legal para que los datos puedan ser tratados sin dicho consentimiento<sup>20</sup>.

(b) Sobre la exigencia informativa: “no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles”<sup>21</sup>:

La STC 39/2016 considera que, en este concreto caso, se cumple el deber de información porque se había colocado en el escaparate del comercio un cartel en el que se podía leer “zona videovigilada”, dando cumplimiento a lo exigido en la Instrucción 1/2006 AEPD. Es más, en materia del

---

<sup>18</sup>Vid Artículo 3.a) LOPD.

<sup>19</sup>No nos vamos a centrar en este punto, puesto que sigue la proporcionalidad en los términos que establecía la reiterada jurisprudencia del TC, entre otras, SSTC 66/1995, de 8 de mayo, FJ 5; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4, y 37/1998, de 17 de febrero, FJ 8.

<sup>20</sup>Vid. Art. 6.1 LOPD Además de la propia STC 39/2016, así también lo entiende la doctrina, entre otros, TOSCANI GIMÉNEZ, D.: «Las facultades de la empresa de videovigilancia de sus trabajadores. Comentario a la STC 39/2016». *Análisis de jurisprudencia*, Bomarzo 2016. pág.167.

<sup>21</sup>Respectos a los Derechos Fundamentales, en general, las SSTC 57/1994, de 28 de febrero; 18/1999, de 22 de febrero y en relación con el derecho a la protección de datos personales, en particular, STC 292/2000, de 30 de noviembre.



consentimiento, se señala que el empresario no tiene por qué determinar, más allá de la vigilancia, el fin exacto que se ha asignado a ese control. De este modo sólo sería necesario solicitar el consentimiento de los afectados si los datos obtenidos se utilizan para una finalidad ajena a la laboral<sup>22</sup>.

Ahora bien, en relación con esas obligaciones legales de consentimiento e información previa, el TC insiste en que el incumplimiento de dichas obligaciones sólo supondrá una vulneración del derecho a la protección de datos tras una ponderación adecuada desde el punto de vista de la proporcionalidad<sup>23</sup>. Esto supone que, sin perjuicio de las sanciones legales que pudieran derivarse, para que el incumplimiento de la obligación de información por parte del empresario implique la lesión del artículo 18.4 CE será necesario atender al principio de proporcionalidad. De tal forma que habrá que ponderar caso por caso, de un lado, el derecho a la protección de datos del trabajador, y de otro, las restricciones al mismo justificadas en el ejercicio del poder de dirección y vigilancia empresarial reconocidos en el artículo 20.3 ET, en conexión con los artículos 33 y 38 CE<sup>24</sup>. En consecuencia, no se vulnera el derecho a la protección de datos siempre que no se haya cumplido con el deber de información.

El supremo intérprete de la Constitución deja claro que, cuando se acreditan indicios de irregularidades hay que ponderar la proporcionalidad de esa falta o insuficiencia del deber de información<sup>25</sup>, entendiéndose cumplida en este caso por la existencia del distintivo informativo. O, dicho con otras palabras, que la existencia de un cartel advirtiendo el uso de las cámaras puede hacer que esa falta o insuficiencia de información, pueda ponderarse a favor de la empresa considerando legítima la medida adoptada.

Como ha señalado un sector minoritario de la doctrina<sup>26</sup>, el problema radica en que el TC no entra a valorar la distinción que supone considerar si ese sistema de videovigilancia tiene vocación de permanencia o no; o, si lo prefieren, si el sistema de videovigilancia es puntual (como reacción ante un posible ilícito por parte del trabajador), o si se trata una medida sistemática y permanente de

---

<sup>22</sup> STC 39/2016, de 3 de marzo, FJ 3º.

<sup>23</sup> STC 292/2000 de 30 noviembre, FJ 11º y STC 39/2016, de 3 de marzo, FJ 3º.

<sup>24</sup> STC 186/2000, de 10 de julio, FJ 5º y 170/2013, de 7 de octubre, FJ 3º. La STC 39/2016 señala: *“Obviamente, el sometimiento de la falta o insuficiencia de información al reiterado juicio de proporcionalidad requerirá determinar en cada supuesto, con carácter previo, si se ha producido o no la indicada omisión de la información debida (...)”*.

<sup>25</sup> La STC 39/2016 señala *“Obviamente, el sometimiento de la falta o insuficiencia de información al reiterado juicio de proporcionalidad requerirá determinar en cada supuesto, con carácter previo, si se ha producido o no la indicada omisión de la información debida”*.

<sup>26</sup> El propio Fiscal, en la STC 39/2016, de 3 de marzo, antecedente 9, señala esta diferencia; SANFULGENCIO GUTIÉRREZ, J. A.: «Cámaras de videovigilancia: más sombras que luces». *Iuris&Lex*. El economista; ARRABAL PLATERO, P.: «La videovigilancia laboral cómo prueba en el proceso». *Revista General de Derecho procesal*, núm. 37, 2015; PRECIADO DOMENECH, C.H.: «El Derecho a la Protección de datos en el Contrato de Trabajo», *Aranazadi*, Navarra. pág. 278. Asimismo, aprecian esta diferencia algunos Magistrados, como José Manuel López García de la Serrana en su voto particular a la STS de 13 mayo de 2014.

control laboral. De esta forma, se continuaría aplicando una única doctrina Constitucional, con soluciones diversas atendiendo a los supuestos de hecho enjuiciados<sup>27</sup>.

Desde la visión de quien escribe estas líneas, estamos ante una misma doctrina del TC sobre los límites de los derechos fundamentales en materia de videovigilancia. Si bien, se trata de una doctrina cuya solución diverge en función de si estamos ante cámaras ocultas o temporales; o bien, si estamos ante cámaras permanentes, fijas o sistemáticas.

Las soluciones varían puesto que en cada uno de estos supuestos concurren factores, causas, indicios, agentes, etc. que deben ser valorados judicialmente atendiendo al principio de proporcionalidad. No es lo mismo, que un empresario utilice sus cámaras permanentes para sancionar a un trabajador sin preavisarle por ausentarse de su jornada, que aquel empresario que utiliza esas cámaras de seguridad para sancionar a un trabajador que, por ejemplo, está acosando o agrediendo a otro compañero.

En consecuencia, no se ha modificado la doctrina de la STC 29/2013, sino la doctrina contenida en la STC 186/2000<sup>28</sup>, a la que se ha añadido un nuevo elemento, el derecho a la protección de datos y, además, se ha señalado que la existencia de un cartel informativo puede coadyuvar al juicio de proporcionalidad a favor del empresario, por entender cumplido de manera suficiente con el deber de información.

Una pregunta que nos debemos plantear es si el deber de información es una cuestión de legalidad, o, por el contrario, forma parte del contenido esencial del derecho y, por ende, puede conllevar la nulidad del despido.

El magistrado, D. Fernando Valdés Dal-Ré, formuló un voto particular<sup>29</sup>, señalando con acierto que, si se ha sentado por el órgano constitucional que el deber de información forma parte del contenido esencial del derecho a la protección de datos, es cuanto menos asombroso, que el mismo Tribunal afirme que el incumplimiento de tal deber no constituya su vulneración.

Ahora bien, llama poderosamente la atención, que el propio Tribunal, en el razonamiento de la Sentencia 186/2000 y ante las alegaciones del recurrente sobre el incumplimiento del artículo 64. 5. f)<sup>30</sup> ET, señaló que se trataba de una cuestión de legalidad ordinaria y ello a pesar de que el

---

<sup>27</sup> STC 39/2016 antecedente número 9.

<sup>28</sup> Último pronunciamiento del TC sobre cámaras ocultas.

<sup>29</sup> Voto particular que formula el Magistrado don Fernando Valdés Dal-Ré a la STC 39/2016, de 3 de marzo, al que se adhiere la Magistrada doña Adela Asua Batarrita.

<sup>30</sup> Dicho precepto establece: “El comité de empresa tendrá derecho a emitir informe (...) sobre las siguientes cuestiones:(...) f) La implantación y revisión de sistemas de organización y control del trabajo(...).”

legislador califica, el precitado incumplimiento, como grave<sup>31</sup>. Por lo tanto, los incumplimientos de la legalidad carecen de trascendencia desde la perspectiva del constitucional, salvo que dicho incumplimiento afecte al contenido esencial del derecho fundamental afectado. Este puede ser el caso de la sentencia *Bersbka*, al afirmar la misma, que dentro del contenido esencial del derecho a la protección de datos se encuentra el deber de información<sup>32</sup>.

Carece de toda lógica que en el derecho a la intimidad (art.18.1 CE) sea necesario acudir al juicio de proporcionalidad y en el caso del derecho la protección de datos (18.4 CE) se prescinda de la aplicación del mismo juicio, entendiéndose que la falta de información previa determina *ipso facto* su vulneración<sup>33</sup>. Es necesario tener en cuenta que hay situaciones en las que, atendiendo a la gravedad de las posibles irregularidades, no existe otro medio para poder acreditar el incumplimiento y, en consecuencia, es necesario, proporcional e idóneo que se pueda actuar a través de este tipo de medidas<sup>34</sup>.

Si admitimos con carácter absoluto la necesidad de informar a los trabajadores, no pudiendo prescindir de susodicho deber en ningún supuesto, el empresario se vería impedido de proteger sus derechos. En muchas ocasiones, la no exigencia del deber de información es el único medio posible para comprobar un incumplimiento por parte de un trabajador.

Por ello, defendiendo la reciente sentencia del TC y frente a los votos particulares que exigen el cumplimiento del deber de información en todo caso<sup>35</sup>, podemos hablar, de forma figurada, del “velo del deber de información”.

Este velo, en un principio, no permite ver o utilizar los datos personales de los trabajadores sin su previa información, protegiendo al trabajador frente a las intromisiones ilegítimas. Sin embargo, excepcionalmente, este velo puede ser levantado cuando las circunstancias lo justifiquen, de manera

---

<sup>31</sup> STC 186/2000, FJ 7º: “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 (sin duda por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida) carece de trascendencia desde la perspectiva constitucional, pues, fuese o no exigible el informe previo del Comité de empresa a la luz del art. 64.1.3 d) LET, estaríamos en todo caso ante una cuestión de mera legalidad ordinaria, ajena por completo al objeto del recurso de amparo. Este incumplimiento del deber de información del art. 64. 5.f. del ET no tienen relevancia constitucional, sin embargo, está sancionado en el art 7.7 del Texto Refundido de Infracciones y Sanciones en el Orden Social (en adelante, “LISOS”) como infracción grave.

<sup>32</sup> Acierto, por parte de D. Fernando Valdés puesto que detecta una incoherencia dentro la propia sentencia del TC. Ahora bien, hay que subrayar que con anterioridad el intérprete constitucional había señalado, sobre el derecho a la protección de datos que la “exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles” (STC 292/2000).

<sup>33</sup> CASINO RUBIO, M.: «Cámaras de seguridad y control de las obligaciones laborales. A propósito de la STC 29/2013». Disponible en (<http://www.abogacia.es/2013/03/20/camaras-de-seguridad-y-control-de-las-obligaciones-laborales-a-proposito-de-la-stc-292013-de-11-de-febrero/>)

<sup>34</sup> DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: «Control informático, videovigilancia y protección de datos en el trabajo», *Lex Nova*, Valladolid, 2012. pág. 64.

<sup>35</sup> Votos particulares de Don Fernando Valdés Ré (al que se adhiere Doña Adela Asua Batarrita) y Voto Particular de Juan Antonio Xiol Ríos.

muy similar a la doctrina del levantamiento del velo<sup>36</sup>. Con esta visión, se conseguiría que como regla general (i) el derecho a la autodeterminación informativa proteja a los trabajadores a través del deber de información y excepcionalmente (ii) evitar que ese derecho no se utilice como un velo de impunidad de aquellos que llevan a cabo comportamientos antijurídicos graves<sup>37</sup>. En mi opinión no todos los indicios de incumplimiento pueden justificar el levantamiento del “*velo de la información*”, dado que este debe tener un carácter excepcional o *última ratio*<sup>38</sup>. Sólo podría utilizarse para incumplimientos que puedan atacar la seguridad del empresario o terceros<sup>39</sup>

No podemos olvidar que, de conformidad con la doctrina del Constitucional<sup>40</sup>, el conflicto entre la intimidad del trabajador y el control empresarial se ha resuelto con la aplicación del principio de proporcionalidad. En consecuencia, ¿por qué no se va aplicar el principio de proporcionalidad en el derecho fundamental a la protección de datos, cuando este derecho no es más que un instrumento para garantizar el derecho al honor y a la intimidad personal tal y como afirma la LOPD desde su mismo pórtico<sup>41</sup>

Lo lógico, sería que el incumplimiento de esta obligación de información por parte del empresario, aunque debe sancionarse administrativamente, cómo establece la LOPD, no ha de elevarse a la categoría de conducta vulneradora del artículo 18.4 de la CE, sobre todo si tenemos en cuenta que la sanción que impone la Ley es calificada como leve<sup>42</sup>. Si la falta del deber de información “en todo caso” se elevara a conducta vulneradora del derecho a la protección de datos, los Tribunales estarían sancionando de una forma más estricta que el propio legislador, quién prevé tal conducta como una infracción leve<sup>43</sup>.

---

<sup>36</sup> El levantamiento del velo de la personalidad jurídica es una técnica jurisprudencial originaria de los Estados Unidos de América (*piercing or lifting the corporate veil*) en virtud de la cual, en determinadas situaciones, los tribunales pueden no tomar en consideración la personalidad jurídica otorgada a la sociedad para dirigirse directamente contra las personas de los socios que la componen. Definida jurisprudencialmente por primera vez por la STS de 28 de mayo de 1984 se plantea como un conflicto entre la seguridad jurídica y la justicia (arts. 1.1 y 9.3 Constitución) en el que por vía de equidad y acogiendo al principio de buena fe (art. 7.1 CC) se penetra en el *substratum* personal de las entidades a las que la ley confiere personalidad jurídica propia para evitar que a su amparo se puedan perjudicar legítimos intereses de terceros.

<sup>37</sup> ARBERAS LÓPEZ, M.: «Protección de datos de carácter personal: videovigilancia en el lugar de trabajo. Análisis sobre la instalación de sistemas de videovigilancia en el lugar de trabajo y la utilización de sus imágenes con fines disciplinarios», AA.VV- Dir. DEL REY GUANTER, S.: «2017 Práctica laboral para abogados. Los casos más relevantes en 2016 de los grandes despachos», *La Ley*, Madrid, 2017.

<sup>38</sup> *vid. op. cit.* TOSCANI GIMENÉZ, D.: «Las facultades de la empresa de videovigilancia de sus trabajadores. Comentario a la STC 39/2016».

<sup>39</sup> SANGUINETI RAYMUND, W.: «Derechos Fundamentales del trabajador y libertad de empresa: el juicio de ponderación», *Universidad Católica Andrés Bello*, 2014.

<sup>40</sup> STC 98/2000, de 18 de mayo y STC 186/2000, de 10 de julio.

<sup>41</sup> El artículo 1 de la LOPD establece: “*La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.*”

<sup>42</sup> Art. 44.2.d. LOPD.

<sup>43</sup> Cabe recordar aquí que el propio TC ha señalado que los incumplimientos de la legalidad (como el deber de información del art. 64.5.f. ET) no tienen relevancia constitucional. Sin embargo, este concreto incumplimiento está sancionado en el art 7.7 de la LISOS como infracción grave.

En consecuencia, si admitiéramos la exclusión del deber de información del contenido esencial al derecho fundamental a la protección de datos, estaríamos permitiendo una ponderación entre los derechos fundamentales en juego, el derecho a la protección de datos, y sus eventuales limitaciones justificadas por el cumplimiento de obligaciones laborales y correlativas facultades empresariales de vigilancia y control.

Lo que sí debe ser objeto del contenido esencial es el uso que *ex post* pueda llevar a cabo la empresa de los datos personales obtenidos. Si el empresario ha utilizado esos datos obtenidos para una finalidad distinta del mero control empresarial habría, por tanto vulnerado, el derecho a la protección de datos del trabajador. Parece razonable, no pudiendo ser de otra manera, que la utilización de cámaras de videovigilancia por parte de la empresa presuponga una exigencia de confidencialidad por su parte, como así se le exige también en relación con los datos que maneja de los empleados, i.e. edad, domicilio, situación familia, etc.

La parte débil de este razonamiento, estriba en que el propio legislador europeo y nacional han querido que el deber de información forme parte de los principios que inspiran el derecho a la protección de los datos<sup>44</sup>.

Por todo lo expuesto, debe estarse de acuerdo con el voto mayoritario del TC, pero no puede decirse lo mismo respecto de su razonamiento por incluir entre los elementos del contenido esencial<sup>45</sup> del derecho a la protección de datos el deber de información, a pesar de que el legislador considere que es un principio que inspira la protección de datos. Algunos autores defienden, en criterio compartido con quien escribe, que el deber de información en determinadas ocasiones puede ser exonerado<sup>46</sup>.

---

<sup>44</sup> Así recogen el deber de información: (A) A nivel Europeo los arts. 10 y 11 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 y a la libre circulación de estos datos y, en un futuro no muy lejano (entrará en vigor 25 de mayo de 2018), los arts. 13 y 14 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (B) A nivel nacional destacar el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

<sup>45</sup> Aunque por la extensión del trabajo no se puede entrar a valorar, cabe recordar aquí la STC 11/1981, de 8 abril, en su FJ 11º, dispone: *el contenido esencial es (...) una esencialidad del contenido del derecho para hacer referencia a aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos.* ¿Sin el deber de información queda totalmente desprotegida la intimidad (bien jurídico protegido) de su titular? El debate está abierto.

<sup>46</sup>ALVAREZ PADÍN, B.: «Licitud del uso empresarial de cámaras de videovigilancia ocultas con finalidad empresarial», este extracto forma parte del libro «2016 Práctica Laboral para abogados», *La Ley*, Madrid, 2016. Pág.3 (LA LEY 3448/2016).

PRECIADO DOMENECH, C.H.: «El nuevo reglamento 679/2016, de 27 de abril sobre Tratamiento de Datos personales y su incidencia en las relaciones laborales», *Actum Social*, nº121, Marzo 2017. pág.15 y FOLGUERA CRESPO, J.A.: «Videovigilancia de los trabajadores es preceptivo informarles de su finalidad disciplinaria», *La Ley*, Núm. 8365, 30 de julio de 2016.

Este último pronunciamiento del TC sigue la línea marcada por otros ordenamientos jurídicos europeos<sup>47</sup> y por otros organismos supranacionales<sup>48</sup>.

De todo lo expuesto, se puede concluir que el TC ha llegado a una conclusión jurídica acertada, aunque ha llevado a cabo un razonamiento jurídico inadecuado por (i) incluir el deber de información como parte del contenido esencial del derecho a la protección de datos, dándole un contenido mayor del que tiene el derecho a la intimidad; siendo el derecho a la autodeterminación informativa un instrumento para garantizar el derecho a la intimidad. Y, además, (ii) no ha diferenciado sobre el tratamiento que deben tener los supuestos de instalación puntual de mecanismos de captación de imágenes frente a los sistemas de seguridad o control que se presentan con cierta fijeza o permanencia en el tiempo<sup>49</sup>.

### 3. RECEPCIÓN POR EL TRIBUNAL SUPREMO

Analizada la evolución de los pronunciamientos que, en materia de cámaras de videovigilancia, ha dictado el TC procede analizar la recepción por parte del Tribunal Supremo (en adelante, “TS”) de las precitadas sentencias. Sin embargo, descartamos analizar, entre otras, las SSTS de 12 de julio de 2016 (RCUD 3314/14; Asunto Alción)<sup>50</sup>, de 21 de julio de 2016 (RCUD 318/2015; Asunto Comunidad de Bienes) y el Auto de 25 de abril de 2017 (RCUD 2204/2016; Asunto: Café Olé &

---

<sup>47</sup> La máxima instancia judicial laboral alemana, el *Bundesarbeitsgericht*, recientemente en una sentencia de 21 de mayo de 2012, consideró lícita la instalación de cámaras ocultas en un lugar de trabajo de acceso público, contradiciendo así a un sector doctrinal que interpretaba que en ningún caso debía ser admitida este tipo de videovigilancia por contradecir el § 6b 2 de la BDSG (*Bundesdatenschutzgesetz* o Ley federal de protección de datos), en donde se establece con carácter general la obligación de señalización de estos medios de control en los lugares de acceso público. A este respecto *vid.* GUDE FERNÁNDEZ, A.: «La videovigilancia laboral y el derecho a la protección de datos de carácter personal», *Revista de Derecho Político*, núm 91, septiembre-diciembre 2014, págs. 43-90.

<sup>48</sup> Cabe recordar en esta materia, por su paralelismo, la STEDH del 27 de mayo de 2014, que considera válidas las grabaciones, de un motorista con supuestas secuelas de un accidente vial obtenidas por un detective privado. La *ratio decidendi* fue que el único fin de las grabaciones es su aportación al proceso civil que persigue contribuir al debate judicial<sup>48</sup>. Esta idea también fue resaltada por alguna sentencia de nuestros tribunales que señalaban que la facultad empresarial no comprende la publicación y difusión de las imágenes captadas, ni la conversación de las mismas una vez visualizadas, salvo que se haya apreciado una infracción sancionable, en cuyo supuesto podrán ser conservadas a los solos efectos probatorios.

<sup>49</sup>En este sentido se generó cierta inseguridad jurídica. En este sentido la STSJ de Madrid de 30 de junio de 2016 (RSU 329/2016; ponente: Javier Jose Paris Marin) que señala que, ningún caso, caben controles sorpresivos con cámaras de videovigilancia; STSJ de Andalucía (Sevilla) 13 de julio de 2016 (RSU 2302/2015; ponente: Jesús Sánchez Andrada), que declara la nulidad del despido porque la cámara oculta no había sido señalizada con el correspondiente distintivo; STSJ de la Comunitat Valenciana de 7 de septiembre de 2016 (RSU 1819/2016 Ponente: Gema Palomar Chalver), que señala procedencia del despido sin la necesidad de distintivo.

<sup>50</sup> Cabe destacar que, el Tribunal *obiter dicta*, inadmite teniendo en cuenta, entre otros aspectos, la ubicación de las cámaras – FJ 3º- Está cuestión adquiere especial relevancia puesto que no todas las zonas de un centro de trabajo pueden ser ponderadas del mismo modo (aseos, baños, etc.). Un buen ejemplo, lo encontramos en la STSJ de Castilla-La Mancha de 28 de noviembre de 2015 (RSU 1040/2014; Ponente: Petra García Marquez), en la que declara vulneración del derecho fundamental a la intimidad por grabaciones efectuadas en cantinas y cafetería de la maestranza, lugares donde el derecho a la intimidad opera en su grado máximo.

Friends, S.L.)<sup>51</sup>, dado que basan su resolución en la falta de contradicción. Las restantes resoluciones que, atendiendo al orden cronológico, ha dictado el Alto Tribunal desde el 3 de marzo de 2016 en materia de Videovigilancia son:

### **3.1. La Sentencia del Tribunal Supremo de 7 de julio de 2016 (RCUD 3233/14; Asunto DIA)**

#### *(i) Supuesto de hecho*

La empresa, tras haber constatado un alto nivel pérdidas, decide instalar unas cámaras de videovigilancia en las zonas de trabajo para intentar dar solución a la irregularidad detectada. Existían carteles advirtiendo de la presencia de las cámaras. Las cámaras captaron que la trabajadora mientras llevaba a cabo sus labores extrajo un paquete de lomo que se comió y por ello fue despedida.

#### *(ii) Ratio decidendi*

- El TS declara la utilización apropiada de las grabaciones.
- Establece que las SSTC 29/2013 y 39/2016 valoran situaciones distintas aplicando la doctrina sobre el derecho a la intimidad y la protección de datos, dando como resultado distintas soluciones<sup>52</sup>.
- El empleo de las cámaras es ajustado a derecho: (i) la trabajadora actúa irregularmente “*a sabiendas de que las cámaras de vigilancia existen en ese y en otros lugares de establecimiento salvo en aseos, vestuario y oficina*”; (ii) la existencia de cámaras no era sólo de conocimiento general, sino que también existían carteles indicadores y (iii) el empleo de las cámaras, cuando se habían acreditado unos indicios, mostraba a las claras una voluntad de poner solución al problema<sup>53</sup>.

En esencia, estamos ante un supuesto en el que la empresa utiliza unas cámaras fijas con la finalidad de sancionar a los trabajadores sin haberles informado de forma clara precisa e inequívoca de que tales filmaciones pudieron ser utilizadas con efectos disciplinarios. Razón por la cual, el TS está

---

<sup>51</sup> Esta sentencia, considera que no se cumplen los requisitos del art. 219 la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social cuando: “*en el caso de contraste consta que la instalación de cámaras se debió, precisamente, a las sospechas de la empresa sobre la conducta de la actora (temporales), mientras que en el caso de autos no consta siquiera la fecha en la que el sistema de videovigilancia fue instalado (permanentes o fija)*”, FJ 2º.

<sup>52</sup> STS 7 de julio de 2017, FJ 2º. En este sentido, posteriormente, la STS 21 de julio de 2016 (RCUD 318/2015; Asunto. Comunidad de Bienes) la Sala Cuarta señala que no existe contradicción y desestima el recurso porque (i) en el caso de autos existían “*fundadas sospechas de la comisión de irregularidades por parte de la trabajadora y eso le lleva a instalar (al empresario) las cámaras con esa finalidad durante un corto periodo de tiempo*” y (ii) porque en la sentencia de contraste alegada por el recurrente las cámaras están instaladas “*de forma permanente y su objeto es la prevención de hurtos por parte de la clientela, habiéndose utilizado para una finalidad distinta cuando no existían sospechas sobre la posible actuación irregular de la trabajadora*”, FJ 3º.

<sup>53</sup> STS 7 de julio de 2017, FJ 2º.

flexibilizando *motu proprio* la doctrina recogida en la STC 29/2013 como consecuencia de la publicación de la STC 39/2016.

*(iii) Conclusión*

El TS ha legitimado el uso de cámaras fijas, previamente instaladas, para sancionar a trabajadores siempre que se constate la existencia de irregularidades previas y el conocimiento por toda la plantilla de la existencia de cámaras (sin que sea necesario avisar de la finalidad, puesto que la misma se presume de las circunstancias concurrentes).

**3.2. Sentencias del Tribunal Supremo de 31 de enero de 2017 (RCUD 3331/2015) y 1 de febrero de 2017 (RCUD 3262/2015) Asuntos: PLANA & DIEGUEZ**

*(i) Supuesto de hecho*

Dada la similitud de los hechos, se analizarán de forma conjunta.

Existen unas cámaras que ya estaban instaladas con anterioridad y cuyo fin era la seguridad. Captan a dos trabajadores manipulando tickets y hurtando diferentes cantidades de dinero. Por estos motivos son despedidos.

*(ii) Ratio decidendi*

La Sala declara la procedencia de los despidos por las siguientes razones:

- La utilización de las cámaras de seguridad era una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, clientes y terceros, así como rápida detección de siniestros), idónea para el lograr de ese fin (control de cobros y de la caja en el caso concreto) y necesaria y proporcionada al fin perseguido.
- Los trabajadores estaban informados expresamente de la instalación del sistema de vigilancia. Y, en todo caso, si se hubiera producido un defecto en el incumplimiento del deber de información, los trabajadores tendrían dos opciones: (i) requerir más información a la empresa o (ii) denunciar ante la AEPD<sup>54</sup>.
- El Tribunal define qué se entiende por seguridad en centro de trabajo, delimitando, a su vez, cuándo se pueden emplear estos medios tecnológicos en el ejercicio de la potestad sancionadora del empleador. Se trata, en palabras del propio Tribunal de: “(...) *una expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad*”

---

<sup>54</sup> Así, la sentencia analizada, señala, FJ 2º: “Y frente a los defectos informativos que alegan pudieron reclamar a la empresa más información o denunciarla ante la Agencia Española de Protección de Datos, para que la sancionara por las infracciones que hubiese podido cometer”



*del centro de trabajo pero que excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc.*<sup>55</sup>

(iii) Conclusiones

- Se excluye el uso de estas cámaras fijas o permanentes, sin avisar previamente a los trabajadores, para otro tipo de control laboral que sea ajeno a la seguridad, esto es, a título ilustrativo, la efectividad en el trabajo, las ausencias del puesto de trabajo<sup>56</sup>, las conversaciones, etc.”

Acertadamente, a pesar de que no hace referencia al mismo, el Tribunal tiene en cuenta un importante límite legal. Dicho límite se encuentra recogido en el artículo 42.4 Ley de Seguridad Privada 5/2014 (LSP), que declara que las grabaciones obtenidas por la videovigilancia de “*seguridad no pueden destinarse a uso distinto de su finalidad*”. Es más, la propia LSP define la seguridad de manera muy similar como queda establecida en esta sentencia, lo cual hace apuntar que el TS pudo<sup>57</sup> tener esta norma como criterio interpretativo.<sup>58</sup>

- Sobre la falta del deber información, la Sala invita a los trabajadores a reclamar ante la AEPD. Este es un razonamiento bastante criticable pues sería contrario al principio de responsabilidad proactiva que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuya vigencia comienza en 2018<sup>59</sup>. Sin embargo, parece que la afirmación relativa a la falta información está limitada a supuestos como el que acontece en autos: (i) se atenta contra la seguridad del centro de trabajo y (ii) los actores conocen la instalación de las cámaras. Quedarían excluido de tal afirmación los supuestos en los que, en las palabras del propio Tribunal, se realice “*otro tipo de control laboral*”, esto es, efectividad en el trabajo, ausencias del puesto de trabajo, etc.

---

<sup>55</sup> STS 31 de enero de 2017, FJ 2º.

<sup>56</sup>De esta forma logra el encaje con la STC 29/2013, debido que se trataba de un supuesto en el que se utilizó una cámara fija, sin informar al trabajador, para sancionarle por ausentarse de su puesto de trabajo.

<sup>57</sup>Digo “pudo”, porque el Alto Tribunal nada dice acerca de cómo ha obtenido esa definición de seguridad. Apunta la definición de Seguridad de centro de trabajo de una forma vaga e imprecisa y sin ninguna motivación, lo cual es en todo caso criticable.

<sup>58</sup>La LSP define seguridad privada como “*el conjunto de actividades, servicios, funciones y medidas de seguridad adoptadas, de forma voluntaria u obligatoria, por personas físicas o jurídicas, públicas o privadas, realizadas o prestadas por empresas de seguridad, despachos de detectives privados y personal de seguridad privada para hacer frente a actos deliberados o riesgos accidentales, o para realizar averiguaciones sobre personas y bienes, con la finalidad de garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades*” (Art. 2).

<sup>59</sup> Este principio obliga al responsable de la protección de datos, generalmente el empresario, a aplicar las medidas técnicas y organizativas para garantizar y demostrar la conformidad del tratamiento con la normativa de protección de datos. *vid.* PRECIADO DOMENECH, C.H.: «El nuevo reglamento 679/2016, de 27 de abril sobre Tratamiento de Datos personales y su incidencia en las relaciones laborales», *Actum Social*, núm. 121, Marzo 2017. pág.2.

### 3.3. Sentencia del Tribunal Supremo de 2 febrero (RCUD 554/2016; Asunto DIR FITNESS)

#### (i) Supuesto de hecho

Un Director Técnico de la empresa DIR FITNESS es despedido por una retahíla de importantes incumplimientos, entre los que se encuentra, dejar pasar a disfrutar de las instalaciones del gimnasio a personas que no habían pagado la cuota. Tales actuaciones fueron captadas por las cámaras de seguridad del centro de trabajo (cámaras fijas o permanentes).

#### (ii) Ratio decidendi

- Se señala la licitud de las grabaciones obtenidas en base a dos puntos (i) existían unas irregularidades<sup>60</sup>, (ii) se ha constatado que la instalación de las cámaras de videovigilancia es conocida por todo el personal que presta servicios en el gimnasio, incluido el interesado. Además, su rango de director técnico hizo que el Tribunal presumiera que debía conocer perfectamente que las cámaras estaban destinadas al control de toda irregularidad, incluida la laboral a efectos disciplinarios.
- La sala afirma que *“el trabajador conocía que en la empresa se había instalado un sistema de control por videovigilancia, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control”*<sup>61</sup>.

#### (iii) Conclusión

La acreditación de que el trabajador conoce la existencia de las cámaras de seguridad permite su uso con fines disciplinarios<sup>62</sup>.

## 4. CONCLUSIONES

En cumplimiento de lo anticipado en la introducción se va proceder a sistematizar todas las resoluciones expuestas, mediante la diferenciación de tres situaciones<sup>63</sup>: (i) Utilización de cámaras permanentes, fijas, sistemáticas o preventivas para el control laboral (ii) Utilización de cámaras

---

<sup>60</sup>HP 5º.

<sup>61</sup> STS de 2 de julio de 2017, FJ 2º.

<sup>62</sup>PURCALLA BONILLA, M.A.: «Control de las nuevas tecnologías (y algunas reflexiones sobre la protección de datos) en la relación laboral», *Actum Social*, núm 121, Marzo 2017. pág.17.

<sup>63</sup>ASPRA RODRÍGUEZ, A. y SANFULGENCIO GUTIÉRREZ, J.A.: «Las cámaras de videovigilancia y la reciente doctrina jurisprudencial». Disponible en <http://tmp.ollerosabogados.com/sites/default/files/ficheros/20161021-Alerta-Informativa-laboral-Olleros-Abogados-Laboral-Camaras-Videovigilancia.pdf>

puntuales, ocultas o represivas; (iii) Utilización de cámaras fijas en aquellos supuestos en los que se han constatado indicios de irregularidades.

(i) *Utilización de cámaras permanentes, fijas, sistemáticas o preventivas para el control laboral.*

Se trata de la regla general, esto es, cuando un empresario decide que va a proceder a controlar el cumplimiento de las obligaciones laborales de sus trabajadores a través de cámaras de videovigilancia. Ello lo hace al amparo del artículo 20.3 ET que establece, con carácter general, que el empresario podrá “adoptar las medidas de control que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales”.

En este tipo de supuestos nos encontramos con la aplicación de la doctrina fijada en la STC 29/2013 y que fue acogida por la Sala Cuarta a través de la STS de 13 de mayo de 2014 (RCUD 1685; Asunto Champion).

En estas situaciones es necesario informar previamente a los trabajadores, indicándoles cuál va a ser la finalidad de las grabaciones. De acuerdo con la Guía de Videovigilancia publicada por la AEPD<sup>64</sup>, este derecho de información previa se garantizará:

- *Con información específica a la representación sindical.* Así lo han admitido distintos órganos judiciales, que entendían salvado el deber de información previa a los trabajadores con la comunicación de instalación de las cámaras a los representantes de los trabajadores<sup>65</sup>. Destaca la STS de 12 de julio de 2016 (RCUD 3314/14; Asunto Alción).
- *Mediante el cartel anunciador y el impreso establecidos por la Instrucción 1/2006.* Este el caso de la STS de 7 de julio de 2016 (RCUD 3233/14; Asunto DIA) y existe casos en la doctrina judicial<sup>66</sup>.
- *Mediante información personalizada,* consistente en informar a los trabajadores, individualmente, en palabras del Constitucional, de forma “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”, mediante comunicación escrita( i.e. una circular<sup>67</sup> o mediante una cláusula en su contrato).

---

<sup>64</sup> Guía de videovigilancia, Agencia Española de Protección de Datos, 2014. Disponible en (<https://www.agpd.es/portales/agpd/canal/documentacion/publicaciones/comun/pdf/GuiaVideovigilancia2014.pdf>)

<sup>65</sup> STSJ de Madrid de 9 de febrero de 2015 (RSU 886/2014; Ponente: ENRIQUE JUANES FRAGA). En este sentido, Voto Particular de Juan Antonio Xiol Ríos a la STC 39/2016, de 3 de marzo, donde admite la posibilidad de admitir la ponderación del deber de información cuando se informe al comité de empresa.

<sup>66</sup> TSJ de País Vasco de 22 de noviembre de 2016 (RSU 2182/2016; Ponente: Ana Isabel Molina Castiella) STSJ de Andalucía (Sevilla) 13 de julio de 2016 (RSU 2302/2015; Ponente: Jesús Sánchez Andrada); STSJ de Andalucía (Sevilla), 21 de abril de 2016 (RSU 1237/2015; Ponente: Francisco Manuel Álvarez Domínguez).

<sup>67</sup> Tribunal Superior de Justicia de Andalucía (Sevilla), 27 de octubre de 2016 (RSU 3029/2015; Ponente: José Joaquín Pérez Benito Abad).

Una vez se haya informado el trabajador de la existencia y finalidad de las cámaras, a través de esta modalidad de control, se podrá sancionar al trabajador en todo tipo de incumplimientos: leves (falta de puntualidad, distracciones durante el trabajo, etc.), graves (embriaguez, faltas de asistencia, etc.) y muy graves (robo, acoso, etc.).

*(ii) Utilización de cámaras puntuales, ocultas o reactivas.*

Es la primera excepción a la regla general. Se trata de aquellos supuestos en los que el empleador, una vez acreditados indicios sobre un comportamiento antijurídico, está legitimado a utilizar cámaras de control siempre que ello se ajuste estrictamente a las exigencias de proporcionalidad, de manera que venga a ser una medida idónea, necesaria, proporcionada y de carácter estrictamente temporal. De esta forma, si atendemos a estos requerimientos, las medidas adoptadas por los empresarios no resultan ni arbitrarias ni caprichosas, ya que no pretenden observar con carácter general la conducta de los trabajadores en el desarrollo de las distintas funciones o cometidos, sino que se limitan a obtener un cabal conocimiento de su comportamiento en razón de detectadas irregularidades. En todo caso, la utilización de estos sistemas de control debe caracterizarse por su carácter excepcional de *última ratio* y por estar permitida sólo para incumplimientos graves y muy graves. Resultaría desmesurado instalar una cámara oculta para comprobar si un trabajador llega puntual a su puesto de trabajo, dado que este tipo de incumplimiento puede ser acreditado con un sistema de fichaje.

¿Por qué es necesario prescindir del deber de información? Porque cualquier información previa puesta en conocimiento del posible infractor o de los representantes legales de los trabajadores haría que la instalación de la cámara resultase en vano.

En este apartado se encontraría las SSTC 186/2000 y 39/2016. Dichas sentencias han sido acogidas por la Sala Cuarta a través de STS de 21 de julio de 2016 (RCUD 318/2015; Asunto. Comunidad de Bienes). Existen también numerosos ejemplos en la doctrina judicial<sup>68</sup>.

*(iii) Utilización de cámaras fijas en aquellos supuestos en los que se han constatado indicios de irregularidades.*

Es la segunda excepción que ha sido instaurada en nuestro ordenamiento a través de una flexibilización del deber de información en la doctrina de videovigilancia en supuestos de cámaras fijas.

---

<sup>68</sup>Entre otras, STSJ de la Comunidad Valenciana, 22 de septiembre 2016 (RSU 2232/2016; Ponente: Manuel José Pons Gil); TSJ de Islas Baleares, 19 de Octubre de 2016. (RSU 173/2016; Ponente: Antonio Oliver Reus) y TSJ de Islas Baleares, 19 de Octubre de 2016 (RSU 203/2016; Ponente: Ricardo Martín Martín); STSJ de Andalucía (Sevilla) 5 de octubre de 2016 (RSU 2797/2015; Ponente Jesús Sánchez Aranda); TSJ de Andalucía (Sevilla), 3 de noviembre de 2016 (RSU 3268/2015; Ponente: María Begoña García Álvarez).

Esta flexibilización ha sido llevada a cabo por la Sala Cuarta del TS en las sentencias de 7 de julio de 2016 (RCUD 3233/14; Asunto DIA); de 31 de enero de 2017 (RCUD 3331/2015) y 1 de febrero de 2017 (RCUD 3262/2015). Asuntos: PLANA & DIEGUEZ; y, por último, en la sentencia de 2 febrero (RCUD 554/2016; Asunto DIR FITNESS.).

En todas ellas, ante la existencia de indicios fundados de que un trabajador pueda estar llevando a cabo unos incumplimientos de su contrato de trabajo, se permite al empresario acudir a las grabaciones de seguridad para sancionar al trabajador. Todo independientemente de que se haya cumplimentado o no el deber de información.

En estos pronunciamientos, el TS acude a distintos criterios para “salvar” el deber de información: (i) que el trabajador actúa a sabiendas de que tales cámaras existían, o (ii) que era conocedor de que esa cámara se había colocado por razones de seguridad, interna o externa, ya sea por su posición en la empresa (directores) o porque era sobradamente conocido. En estos casos, el Alto Tribunal, llega a afirmar que no sería necesario señalar, más allá de la mera vigilancia, cuál es la finalidad exacta que se le ha asignado a ese control.

La utilización de las cámaras fijas o de seguridad, prescindiendo del deber de información sobre la finalidad, se limita a aquellos supuestos en los que existan indicios de incumplimientos que puedan atentar contra la seguridad del centro de trabajo, y queda excluido cualquier otro tipo de control laboral.

En consecuencia, la Sala Cuarta avala el uso de las cámaras fijas o permanentes, sin informar previamente a los trabajadores siempre que existan indicios fehacientes<sup>69</sup>, serían actuaciones ilícitas tales como: hurtos<sup>70</sup>, robos<sup>71</sup>, o agresiones entre compañeros de trabajo<sup>72</sup>

En la utilización de cámaras permanentes es interesante valorar la extrapolación al ordenamiento jurídico laboral de la doctrina del “hallazgo casual”, propia del Derecho Penal<sup>73</sup>. Al igual que el derecho sancionador administrativo se informa por los principios del Derecho Penal, en estos asuntos, sólo en ocasiones, puede ser aconsejable acudir a dicha rama de nuestro ordenamiento. Dicha figura jurisprudencial establece, en pocas palabras, que siempre que la instalación de los

---

<sup>69</sup> GUERRA RODRIGUEZ, L.: «Ejercicio de control a través de cámaras de videovigilancia: análisis de la doctrina constitucional», *Revista Trabajo y derecho*, núm.28, 2017.

<sup>70</sup> STJS de Andalucía (Sevilla), de 23 noviembre 2016 (RSU 159/2016; Ponente: María Begoña García Álvarez).

<sup>71</sup> STSJ de Madrid, 18 de noviembre de 2016 (RSU 975/2016; Ponente: Ignacio Moreno González Aller).

<sup>72</sup> STSJ de Cataluña, de 21 de octubre de 2016 (RSU 4374/2016; Ponente: Sara María Pose Vidal).

<sup>73</sup> MARTÍN MORALES, R.: «El derecho a la intimidad: grabaciones con videocámaras y microfonía oculta», *la ley*, núm.4, 2004.págs. 365-378.

dispositivos ópticos sea lícita, las grabaciones casualmente obtenidas podrán ser utilizadas a efectos procesales<sup>74</sup>.

Ahora bien, ¿es plausible proyectar la teoría del “hallazgo casual” al ordenamiento laboral? Algunos autores consideran que esta doctrina no tiene cabida en las relaciones laborales porque se controla una persona dentro de las exigencias de ajenidad y dependencia<sup>75</sup>. Sin embargo, el voto particular que formula el Magistrado Juan Antonio Xiol Ríos<sup>76</sup> abre la puerta a la traslación del hallazgo casual al ordenamiento laboral. Esta teoría sería plenamente válida para aquellos supuestos en los que el trabajador atenta contra la seguridad del centro de trabajo de una forma grave, supuestos como el acoso, violencia, etc. Ello se debe a que carece de coherencia que una grabación de un ilícito penal permita iniciar diligencias penales, pero, en ningún caso, permita incoar un expediente disciplinario porque se decretaría la nulidad de la prueba o despido<sup>77</sup>.

A luz de todas las resoluciones analizadas, los operadores jurídicos, empresas y trabajadores, deben tener en cuenta estas tres situaciones planteadas para realizar un uso adecuado de estos medios ópticos sin incurrir en ningún tipo de irregularidad desde la perspectiva laboral.

---

<sup>74</sup> Esta utilización viene refrendada por la utilización que el TS hace del criterio de la flagrancia, así lo señala la Sentencia del TS (Sala 2ª), de 8 de marzo de 1994.

<sup>75</sup> LAHERA FORTEZA, J.: «Nuevas jurisprudencia constitucional en la videovigilancia laboral: valoración crítica - STC 39/2016». *Derecho de las relaciones laborales*, nº5, 2016.

<sup>76</sup> Voto particular que formula el Magistrado don Juan Antonio Xiol Ríos a la STC 39/2016, de 3 de marzo dictada por el Pleno del Tribunal.

<sup>77</sup> TALENS VISCONTI, E.E.: «Video-vigilancia en el trabajo: una vuelta a la jurisprudencia clásica», *Revista Trabajo y Derecho*, Nº 21, Septiembre 2016.

