

**LÍMITES A LA INSTALACIÓN DE CÁMARAS DE
VIDEOVIGILANCIA EN EL ENTORNO LABORAL: LA INTIMIDAD
Y LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

HUGO IZQUIERDO ENFEDAQUE

20384851

TFG CURSO 2023-2024 (2º SEMESTRE)

ÁREA DE DERECHO LABORAL

TUTORA: RAQUEL MARÍA RODRÍGUEZ IZQUIERDO

1. INTRODUCCIÓN.....	3
2. DERECHOS EN JUEGO	6
2.1. La libertad de empresa: el poder de dirección empresarial	6
2.2. Los derechos fundamentales como límites a la instalación de cámaras de videovigilancia	8
3. LA EVOLUCIÓN DE LOS DERECHOS A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	9
3.1. El reconocimiento jurisprudencial del derecho a la intimidad en el marco de las relaciones laborales.....	9
3.2. El derecho a la protección de datos de carácter personal como derecho autónomo	12
3.3. Características esenciales de la LO 15/1999.....	13
4. INTERPRETACIÓN Y APLICACIÓN JURISPRUDENCIAL DE LA LO 15/1999	15
4.1. El cumplimiento estricto del deber de información: STC 29/2013, de 11 de febrero de 2013.....	16
4.2. La colocación del distintivo informativo como forma de cumplimiento del deber de información: El caso “Bershka”	17
4.3. Pronunciamientos judiciales significativos a partir de la doctrina jurisprudencial recaída con el caso “Bershka”	20
4.3.1. El TEDH entra en juego: el asunto López Ribalda (II).....	20
4.3.2. Matices interpretativos introducidos por el TS.....	22
5. INTERPRETACIÓN DOCTRINAL Y JURISPRUDENCIAL DE LA NUEVA LO 3/2018	24
5.1. Incidencia de la LO 3/2018 en la instalación de cámaras de videovigilancia	24
5.2. Consideraciones relevantes de la interpretación jurisprudencial recaída hasta el momento en aplicación de la nueva LO 3/2018	29
5.2.2. Decisión de la mayoría en la STC 119/2022, de 29 de setiembre de 2022 ...	29
5.2.3. El voto particular de la STC 119/2022, de 29 de setiembre de 2022	30

5.2.4. Instalación de cámaras ocultas en la nueva LO 3/2018: STS 692/2022, de 22 de julio de 2022	31
6. CONCLUSIONES	33
7. BIBLIOGRAFÍA	38
8. ANEXO JURISPRUDENCIAL	40
8.1 Tribunal Europeo de Derechos Humanos.....	40
8.2 Tribunal Constitucional.....	40
8.3 Tribunal Supremo	41

1. INTRODUCCIÓN

En el año 2018 el legislador español promulgó la nueva *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (en adelante *LO 3/2018*), que, por primera vez¹, contenía previsiones específicas en relación con la utilización de cámaras de videovigilancia en el marco de las relaciones laborales. Así, los derechos fundamentales a la intimidad y a la protección de datos de carácter personal² se situaron, normativamente hablando, como límites a la utilización de estos sistemas de videovigilancia, cuyo uso está legitimado por el poder de dirección empresarial³.

Esta nueva regulación fue aprobada después de que el Tribunal Constitucional (en adelante TC) dictase dos sentencias, en los años 2013 y 2016⁴, aparentemente contradictorias, en las que entró a valorar la validez de las pruebas obtenidas por la captación de cámaras de videovigilancia en el ámbito laboral, siendo que la validez de las mismas dependía de la posible vulneración de los derechos fundamentales a los que venimos haciendo referencia. Así, si bien la intimidad y la protección de datos de carácter personal se consolidaron, a nivel jurisprudencial, como límites a la instalación de cámaras de videovigilancia⁵, parecía que no estaba claro cuál debía ser la concreta información que el empresario debía dar a sus empleados en relación a estos sistemas de vigilancia y control. Como consecuencia, a muy grandes rasgos, por un lado, en el año 2013 el TC entendió vulnerado el derecho fundamental a la protección de datos porque el empresario no concretó que las cámaras instaladas podían utilizarse con fines disciplinarios, siendo que se consideró infringido el deber de información. En cambio, por otro lado, en el año 2016, el mismo tribunal dictaminó que el empresario había cumplido con el deber de información con la simple colocación de un distintivo informativo, el

¹ Al contrario que su predecesora, la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (en adelante *LO 15/1999*).

² Artículo 18 de la *Constitución Española* (en adelante *CE*), apartados primero y cuarto respectivamente.

³ Que tiene como último fundamento el derecho a la libertad de empresa consagrado en el artículo 38 de la *CE*.

⁴ Conocido como el caso “Bershka”.

⁵ Lo cual se constató con la nueva ley de protección de datos a la que hemos hecho referencia.

cual que avisaba de la instalación de cámaras, pero no de sus concretos usos y fines (como, por ejemplo, disciplinarios).

Asimismo, casi de forma simultánea, en los años 2017 y 2019, el Tribunal Europeo de Derecho Humanos (en adelante TEDH) se pronunció dos veces sobre el asunto López Ribalda (I y II), siendo que la decisión adaptada en primer lugar fue revocada por la gran sala, dando como consecuencia que el tribunal entendió que no se vulneró el derecho a la vida privada de las personas trabajadoras en la instalación de cámaras ocultas.

Estos tres pronunciamientos dictados sobre una misma normativa, la derogada LO 15/1999, fueron dispares, pues solo en 2013 se declaró que la prueba obtenida mediante las cámaras de videovigilancia era nula por vulneración de derechos fundamentales, mientras que en las otras dos los tribunales interpretaron que dicha instalación era ajustada a derecho. Así, siendo latente la falta de uniformidad jurisprudencial, el TS se pronunció en los años siguientes aplicando e interpretando estas doctrinas jurisprudenciales, añadiendo matices a las mismas y poniendo de manifiesto que nos situamos en un terreno notoriamente caracterizado por la casuística. De este modo, no acababa de estar claro cuál era la información que debía dar el empresario cuando instalaba esta medida de control y vigilancia, ni cuál era la consecuencia de no darla, ni si había casos donde estaba legitimado que no la diese y, con todo, cuando se debían (y se deben) considerar vulnerados los derechos a la intimidad y a la protección de datos de carácter personal.

A partir de aquí, este trabajo aborda los límites a la instalación de cámaras de videovigilancia en el marco de las relaciones laborales. Las causas que nos llevan a analizar dicha cuestión son tres. En primer lugar, la creciente proliferación de la utilización de instrumentos tecnológicos que permiten la captación de imágenes y el tratamiento de datos de carácter personal, pues esta utilización también ha aumentado en el marco de las relaciones laborales. En segundo lugar, la falta de uniformidad jurisprudencial que se ha dado en los últimos años, en atención a los pronunciamientos del TC y del TEDH, así como también del TS, en relación a los límites que debe observar el poder de dirección empresarial. De esta forma, nos ha llamado especialmente la atención: la diversidad de pronunciamientos habidos, la casuística fáctica de los mismos y la dificultad de apreciar una doctrina jurisprudencial que permitiese saber, con exactitud, qué concreta información debía dar el empresario cuando instala cámaras para el control laboral, así como también qué tipo de cámaras puede instalar, para qué finalidades y en qué ubicaciones. Por último, en tercer lugar, nos interesa conocer cuál ha sido la incidencia de la promulgación de la nueva LO 3/2018 y qué podemos esperar de la misma.

De esta forma, nuestro estudio consiste en hacer un análisis jurisprudencial, normativo y doctrinal de los límites que han supuesto el derecho a la intimidad y la protección de datos de carácter personal en la instalación de las cámaras de videovigilancia, con especial atención a los pronunciamientos del TC a lo largo de estos años y la nueva LO 3/2018. Así, por un lado, pretendemos dar respuesta a cómo se configuran estos dos derechos y cuándo se pueden considerar vulnerados en este específico ámbito. Por otro lado, queremos analizar si la nueva normativa de protección de datos recoge la jurisprudencia mayoritaria hasta el momento, si supone un avance en la determinación de los límites a la instalación de cámaras de

videovigilancia y si nos permite determinar en qué casos podremos entender vulnerados los derechos fundamentales de las personas trabajadoras.

Dicho esto, este trabajo se estructura en cuatro capítulos bien diferenciados. En primer lugar, concretamos cuáles son los derechos en juego haciendo incidencia en qué es aquello que legitima la instalación de cámaras de videovigilancia en el marco de las relaciones laborales: el poder de dirección empresarial. Este capítulo es claramente más corto, si bien entendemos que lo debemos dotar de autonomía propia. Esto es así porque nuestro estudio gira en torno a los límites que suponen los derechos fundamentales al poder de dirección empresarial. De este modo, todos los pronunciamientos judiciales tienen en cuenta dicho poder y lo ubican como punto de partida, siendo que la concepción de este no ha sufrido apenas cambios a lo largo de los años (como si lo han hecho el derecho a la intimidad y a la protección de datos de carácter personal). Asimismo, también ofrecemos una visión actual de los límites que suponen los derechos fundamentales en el marco de las relaciones laborales.

En segundo lugar, analizamos los primeros pronunciamientos del TC más relevantes para el estudio en cuestión, pues entendemos que es necesario conocer la evolución jurisprudencial que se ha dado, especialmente en lo que referente al reconocimiento de la intimidad en el marco de las relaciones laborales y a la consolidación del derecho a la protección de datos de carácter personal como derecho fundamental autónomo. También en este apartado analizamos, sucintamente, la antigua regulación de protección de datos de carácter personal.

En tercer lugar, hacemos un estudio de los pronunciamientos del TC y del TEDH a los que anteriormente hemos hecho referencia, los cuales interpretaron la posible vulneración de derechos fundamentales desde la óptica de la antigua normativa de protección de datos. También en este capítulo, se analizan algunos pronunciamientos del TS que muestran la disparidad de circunstancias que pueden darse y como este tribunal siguió e interpretó la doctrina asentada por el TEDH y el TC.

En cuarto lugar, analizamos la afectación que la nueva normativa de protección de datos de carácter personal tiene en nuestro objeto de estudio, teniendo así en cuenta cuáles son los preceptos que inciden en este. Por último, examinamos dos pronunciamientos judiciales relevantes que interpretan esta nueva legislación. Así, uno de ellos es del TC y se analiza por ser el primero que entra a valorar la nueva ley, así como por la relevancia de su voto particular. En cuanto al otro, es del TS y lo analizamos por los hechos enjuiciados, pues se trata de un caso en el que se analizan la instalación de cámaras de videovigilancia ocultas.

En cuanto la metodología utilizada, por un lado, hemos analizado especialmente los pronunciamientos del TC más destacados, si bien también algunos del TS y uno del TEDH. La elección de estos pronunciamientos es acorde con la doctrina científica mayoritaria, siendo que nos permiten ver con más claridad esta evolución, determinación y concreción de los límites en juego. Así, teniendo en cuenta la importancia que han tenido las decisiones judiciales en este ámbito, es coherente el espacio que les hemos dado y que hayamos valorado en esencia las del TC. Asimismo, en relación con los pronunciamientos judiciales examinados, hay que hacer tres consideraciones. La primera es que, además del criterio jurisprudencial aplicado, hemos expuesto los hechos más relevantes de los casos enjuiciados. Esta forma de análisis tiene como fundamento que estamos en un ámbito donde la casuística y el elemento fáctico es de especial relevancia, pues la doctrina jurisprudencial se construye

a partir de las circunstancias concurrentes en los distintos casos enjuiciados. Así, la mayoría de nuestras fuentes doctrinales también exponen los hechos que se enjuician. La segunda es que en todos los análisis hemos tenido en cuenta la opinión de la doctrina experta. Así, a lo largo del trabajo intentamos interconectar y comparar los diversos pronunciamientos judiciales con el fin de explicar cómo y porqué hemos llegado a la nueva regulación legal, siendo que pretendemos encontrar en qué extremos hay cierta uniformidad jurisprudencial (y en cuáles no los hay). En tercer lugar, todos estos pronunciamientos valoran la validez de las pruebas obtenidas a partir de la captación de imágenes por las cámaras instaladas, de modo que para el análisis de dicha validez examinan si se han vulnerado los derechos fundamentales de las personas trabajadoras. Entendemos que es relevante contextualizar esta cuestión, tanto para entender las decisiones judiciales, como para tener en cuenta que serán otros estudios (y no este) los que podrán valorar si la vulneración de derechos fundamentales conlleva o no a la validez de la prueba.

A estos pronunciamientos judiciales se suman un breve análisis de la normativa de protección de datos de carácter personal, tanto la actual como la anterior, en aquellos aspectos que inciden en nuestro estudio. Asimismo, también comentamos una instrucción de la Agencia de Protección de Datos (en adelante AEPD), de especial relevancia como se verá, y algunos artículos del *Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores* (en adelante ET). De este modo, en dicho análisis también nos guiamos de la doctrina experta, la cual hemos tratado que sea lo más variada posible

2. DERECHOS EN JUEGO

2.1. La libertad de empresa: el poder de dirección empresarial

Cuando el empresario instala cámaras de videovigilancia en el ámbito de su empresa está ejerciendo un derecho o facultad que se engloba dentro de lo que se denomina poder de dirección empresarial⁶, el cual tiene como último fundamento el artículo 38 de la CE que consagra el derecho a la libertad de empresa⁷. Esta es la base constitucional que legitima que el empresario lleve a cabo sus facultades de gestión, organización y dirección sobre los elementos de su empresa, en los que se incluyen las personas trabajadoras.

El poder de dirección empresarial tiene múltiples y diversas manifestaciones, desde el poder disciplinario⁸ hasta la modificación sustancial de las condiciones de trabajo, si bien en nuestro caso nos interesa el apartado 3 del artículo 20 del ET, donde se señala que “el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su

⁶ RAQUEL POQUET CATALÁ, “Poder de control empresarial a través de sistemas de videovigilancia: alcance y límites”, p. 3.

⁷ STC 39/2016, de 3 de marzo de 2016.

⁸ EDURNE TERRADILLOS ORMAETXEA, El poder disciplinario empresarial. E. Borrajo Dacruz (coord.), *Trabajo y libertades públicas* (p.207).

adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad”. Por ello, sobre la base del poder de dirección empresarial, y en concreto teniendo en cuenta el artículo citado, el empresario puede instalar cámaras de videovigilancia, siempre que tenga como finalidad la seguridad del centro de trabajo o el control de las obligaciones laborales, pues se trata “de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores”⁹.

Este poder de dirección empresarial implica, por un lado, que las personas trabajadoras deban asumir una serie de deberes frente el empresario, como por ejemplo “cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia” o “cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas” (artículo 5 del ET, letras a y c). Por otro lado, dicho poder conlleva que las personas trabajadoras vean modulados sus derechos, si bien “en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva”¹⁰. Esto es, “en determinadas circunstancias podrían modularse tales derechos para que pueda hacerse efectivo el poder de dirección del empresario, siempre que esa intromisión a los derechos del trabajador sea ‘razonable’”¹¹. Por ello, tal y como ha reconocido el TC de forma reiterada¹², las personas trabajadoras, antes de ello, son ciudadanos y, como tales, nuestra CE les reconoce una serie de derechos fundamentales que deben ser respetados y tenidos en consideración por cualquiera, incluida la empresa de la que forman parte.

Como bien indica POQUET CATALÀ, “este poder empresarial puede vulnerar determinados derechos de las personas trabajadoras, entre ellos, derechos fundamentales y libertades públicas (...). De ahí, la necesidad de establecer unos límites que claramente delimiten hasta qué punto puede llegar la empresa en el ejercicio de su poder de control y vigilancia”¹³.

Teniendo en cuenta lo que hemos expuesto, en los siguientes apartados nos centraremos en los límites a la instalación de cámaras de videovigilancia en el trabajo¹⁴. Si bien del mencionado artículo 20.3 del ET se pueden deducir dos expresos (“la dignidad de la persona y, en su caso, la capacidad real de las personas trabajadoras con discapacidad”¹⁵) nuestro estudio girará en torno a los límites que suponen los derechos a la intimidad y a la protección de datos de carácter personal, consagrados en el artículo 18, apartados 1 y 4 respectivamente, de nuestra carta magna.

⁹ STC 39/2016, de 3 de marzo.

¹⁰ STC 99/1994, de 11 de abril de 1994.

¹¹ FEDERICO JAVIER FERNÁNDEZ ORRICO, “Protección de la intimidad del trabajador”, p.7.

¹² A modo de ejemplo, en la STC 106/1996, de 12 de junio.

¹³ POQUET, p.2.

¹⁴ Como bien señala el GORDO GONZÁLEZ, “los límites sobre los medios tecnológicos de control de la actividad de los trabajadores también son objeto de controversia permanente. Las nuevas tecnologías facilitan que los trabajadores puedan desarrollar su actividad (...). No obstante, esa misma tecnología permite que el empleador pueda llevar a cabo un control más exhaustivo de las funciones desarrolladas por sus empleados, que suele entrar en conflicto con los derechos a la intimidad, a la propia imagen o al secreto de las comunicaciones de los trabajadores” (Luis Gordo González, “El Derecho del Trabajo 2.0”, p.3)

¹⁵ Artículo 20.3 del ET.

2.2. Los derechos fundamentales como límites a la instalación de cámaras de videovigilancia

Lo primero que debemos de tener en cuenta es que el alcance y concepción del derecho a la intimidad y del derecho a la protección de datos de carácter personal, como límites a la instalación de medios de videovigilancia por parte del empresario, ha ido cambiando y evolucionando con los años. Por ello, analizaremos paulatinamente, en los próximos capítulos, cuál ha sido la evolución jurisprudencial, doctrinal y normativa que se ha dado desde finales del siglo pasado y principios del presente, hasta finalizar con la promulgación de la nueva normativa de protección de datos de carácter personal y su interpretación (escasa) jurisprudencial hasta el momento.

Así, con carácter previo, debemos exponer, brevemente, unos parámetros generales de la concepción actual de los derechos fundamentales como límites al poder de dirección empresarial. Esto es, mostrar una fotografía actual de la cuestión que acabaremos de completar al final de este trabajo.

Como hemos mencionado *ad supra*, las personas trabajadoras son ante todo personas titulares de los derechos fundamentales reconocidos por nuestra CE. Por ello, “la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano”¹⁶. El contenido de dichos derechos, tal y como emana de la doctrina del TC¹⁷, no es ilimitado y absoluto, sino que está configurado por límites intrínsecos y extrínsecos, esto es, por su propia naturaleza y por la existencia de otros derechos constitucionales reconocidos. Por tanto, el derecho a la libertad de empresa consagrado en el artículo 38 de la CE, que sirve como fundamento a la instalación de cámaras de videovigilancia, modula dichos derechos, y estos a su vez suponen un límite a este poder empresarial. En palabras del TC: “es en aplicación de esta necesaria adaptabilidad de los derechos del trabajador a los requerimientos de la organización productiva en que se integra, y en la apreciada razonabilidad de éstos, como se ha afirmado que manifestaciones del ejercicio de aquéllos que en otro contexto serían legítimas, no lo son, cuando su ejercicio se valora en el marco de la relación laboral”¹⁸.

Por último, habrá que tener en cuenta que nos movemos en un ámbito que se caracteriza por la escasez normativa, así como por el rápido desarrollo de los medios e instrumentos tecnológicos, por lo que ambos factores han provocado que hayan sido en gran parte los tribunales, de la mano del TC, quienes hayan tenido que interpretar y delimitar los límites a la instalación de sistemas de videovigilancia en el marco de una relación laboral¹⁹. De esta forma, “la criticable imprecisión legislativa obliga a una labor creadora, cuasi legislativa, de los tribunales, capaz de propiciar, en ocasiones, notables contradicciones, lo cual provocará, a la postre, un notable grado de inseguridad jurídica”²⁰, como veremos cuando analicemos las sentencias del TC recaídas a partir del año 2013.

¹⁶ STC 88/1985, de 19 de julio (F2).

¹⁷ A modo de ejemplo, en la STC 11/1981, de 8 de abril.

¹⁸ STC 99/1994, de 11 de abril.

¹⁹ RODRIGO TASCÓN LÓPEZ, *El Tratamiento por la Empresa de Datos Personales*, p. 138.

²⁰ TOMAS SALA FRANCO, *El derecho a la intimidad y a la propia imagen*, pág. 205.

3. LA EVOLUCIÓN DE LOS DERECHOS A LA INTIMIDAD Y A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

En este capítulo explicaremos cuáles fueron los antecedentes jurisprudenciales de principios de siglo que supusieron un cambio de paradigma en la concepción del ejercicio del derecho a intimidad en el marco de una relación laboral. De este modo, estudiaremos la progresiva concepción del TC acerca de la instalación de cámaras de videovigilancia, viendo como al principio la cuestión solo se circunscribía al derecho a la intimidad, de manera que, posteriormente, entró en juego el derecho a la protección de datos de carácter personal con la STC 292/2000, de 30 de noviembre del año 2000 y la promulgación de la citada LO de 15/1999.

3.1. El reconocimiento jurisprudencial del derecho a la intimidad en el marco de las relaciones laborales

Un buen punto de partida para analizar cómo ha sido tratada la cuestión de la instalación de cámaras de videovigilancia por el TC son las sentencias 98/2000, de 10 de abril del año 2000 y 186/2000, de 10 de julio del año 2000. Estas sentencias fueron dictadas sin tener en cuenta la LO 15/1999 (pues los hechos enjuiciados fueron anteriores a su promulgación) y, si bien solo resuelven la cuestión desde la perspectiva de la posible vulneración del derecho a la intimidad, suponen un importante avance al considerar que el ejercicio del derecho a la intimidad está presente en el ámbito de una relación laboral.

La STC 98/2000, de 10 de abril, enjuició un caso en el que la empresa, un casino, decidió instalar unos micrófonos que permitían recoger y grabar las conversaciones, tanto de las personas trabajadoras como de los clientes, que se producían en la zona de caja y en la zona donde se hallaba la ruleta. Dicho sistema de captación de sonido complementaba otro sistema de seguridad que consistía en un circuito de televisión cerrado, a lo que hay que añadir que se probó que las personas trabajadoras conocían de su existencia²¹. El asunto llegó al TC después de que el TJG de Galicia negase que se había vulnerado el derecho a la intimidad de las personas trabajadoras²², de manera que el alto tribunal señaló que “tal afirmación resulta rechazable, pues no puede descartarse que también en aquellos lugares de la empresa en los que se desarrolla la actividad laboral puedan producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores (...) en las que se aborden

²¹ STC 98/2000, de 10 de abril, antecedente de hecho segundo.

²² Dicho tribunal afirmó que el centro de trabajo no era un lugar donde las personas trabajadoras ejercían su derecho a la intimidad, de modo que la captación de las conversaciones mantenidas por las personas trabajadoras no podía suponer una vulneración de dicho derecho.

cuestiones ajenas a la relación laboral que se integran en lo que hemos denominado propia esfera de desenvolvimiento del individuo”²³.

Así, el TC dispuso que hay que tener en cuenta tanto el lugar donde se instalaban estos sistemas de control, como otros elementos, tales como “si la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticamente, 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.”. Asimismo, el TC señaló que, en todo caso, hay espacios que *per se* comportan una vulneración del derecho a la intimidad, como los aseos, las zonas de descanso o esparcimiento, vestuarios o análogos²⁴.

Por tanto, a modo de resumen, el TC dictaminó, en primer lugar, que el empresario debe respetar el derecho a la intimidad de las personas trabajadoras, pues como derecho fundamental debe partirse de su prevalencia, de tal forma que “su limitación por parte de las facultades empresariales sólo puede derivar bien del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho (...), bien de una acreditada necesidad o interés empresarial, sin que sea suficiente su mera invocación para sacrificar el derecho fundamental del trabajador”. En segundo lugar, reafirmó “que el ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador”, por lo que los juzgadores deben proceder “a una ponderación adecuada (...) que respete la correcta definición y valoración constitucional del derecho fundamental en juego y de las obligaciones laborales que pueden modularlo”. Así, por este motivo los tribunales deben tener en cuenta **el principio de proporcionalidad**, esto es, que las medidas de control llevadas a cabo por el empresario sean “las indispensables y estrictamente necesarias” para satisfacer la necesidad empresarial que se trate, de modo que, si existen medidas menos restrictivas del derecho, deban ser estas últimas las que se adopten. Con todo, si bien el TC entendió que había un interés legítimo por parte de la empresa en la instalación del sistema de micrófonos, este no era “indispensable para la seguridad y buen funcionamiento del casino”, por lo que “la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores, como de los clientes del casino, constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el art. 20.3 LET (...)”. Por ende, la doctrina entiende que “la sentencia consideró que esas grabaciones vulneraron el derecho fundamental a la intimidad de los afectados y ello a pesar de que habían sido efectuadas en el centro de trabajo, de forma abierta, con la información previa y existiendo un interés empresarial en el conocimiento de los hechos”²⁵.

Poco después de este pronunciamiento, el TC se pronunció nuevamente en un caso parecido en su sentencia 186/2000, de 10 de julio del año 2000. En este caso, el recurso se interpuso a raíz de un despido disciplinario que se había basado en las grabaciones obtenidas por la empresa, quien había instalado un circuito cerrado de televisión que solo enfocaba las cajas registradoras, de modo que dicha instalación vino motivada por **sospechas fundadas de**

²³ Señalamos que, de ahora en adelante y salvo afirmación en contra, todas las citas textuales se han extraído de la STC 98/2000, de 10 de abril del año 2000.

²⁴ Previsión que recoge la actual LO 3/2018 en su artículo 89.2.

²⁵ ANA GUDE FERNÁNDEZ, “La videovigilancia en el ámbito laboral”, p.11.

irregularidades en dichas cajas. Así, las grabaciones mostraron como algunos empleados sustraían prendas y enseres vendidos por la empresa, siendo que la instalación de dichas cámaras no fue comunicada ni a las personas trabajadoras ni al comité de empresa.

El alto tribunal vuelve a tener en cuenta las anteriores consideraciones en relación a la STC 98/2000, de 10 de abril del año 2000, si bien se aportan algunas cuestiones relevantes que debemos comentar. Por un lado, como bien indica el GONZÁLEZ GONZÁLEZ²⁶, lo más destacado es que **excluye la necesidad de informar a las personas trabajadoras** y al comité de empresa de la instalación de las cámaras, en tanto que el TC entiende que “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”²⁷. Por ello, dicha exigencia de información no viene “derivada del contenido esencial de los derechos a la intimidad y a la propia imagen”²⁸. Esta es, como se irá viendo más adelante, una cuestión relevante, pues en las posteriores sentencias del TC²⁹ sí que tendrá en cuenta este deber de información, de manera que en algunos supuestos la infracción de este deber implicará que se vulnere el derecho a la protección de datos de carácter personal³⁰.

Por otro lado, el TC profundizó acerca del principio de proporcionalidad, por lo que señaló que cualquier medida restrictiva de derechos fundamentales, como lo es la instalación de cámaras de videovigilancia, debe superar el juicio de proporcionalidad. Por tanto, se deben comprobar el cumplimiento de tres requisitos (la negrita es nuestra):

Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)³¹.

A partir de aquí, en este caso el alto tribunal desestimó el recurso y entendió que la medida empresarial no vulneró el derecho a la intimidad, pues la medida era justificada (teniendo en cuenta las previas sospechas que habían³²), necesaria (en cuanto el fin perseguido: la averiguación de dichas irregularidades) y proporcionada (pues las cámaras se dirigían solo a las cajas y la medida era temporal).

A raíz de ambas sentencias extraemos tres conclusiones muy importantes para nuestro estudio. La primera es que ambas “niegan una premisa mantenida por la jurisprudencia durante mucho tiempo: la de que el centro de trabajo no puede constituir, por definición, un espacio en el que se ejerce el derecho a la intimidad”³³. La segunda es que, los tribunales, a partir de las citadas sentencias, someterán las medidas de vigilancia y control empresarial

²⁶CARLOS GONZÁLEZ GONZÁLEZ, “Novedades de la Ley Orgánica 3/2018”, p.5.

²⁷ STC 98/2000, de 10 de abril del año 2000.

²⁸ GONZÁLEZ, “Novedades de la Ley Orgánica 3/2018”, p.6.

²⁹ Esto es, en la STC 29/2013, de 11 de febrero de 2013.

³⁰ A lo largo del trabajo veremos que no toda infracción del deber de información supondrá que se produzca una vulneración al derecho de protección de datos de carácter personal, tal y como ocurre, por ejemplo, en la STEDH de 17 de octubre de 2019 (asunto *López Ribalda y otros c. España*).

³¹ STC 98/2000, de 10 de abril del año 2000.

³² Este aspecto es de suma trascendencia, pues como veremos, el TEDH, el TC y el TS lo han tenido en cuenta en reiteradas ocasiones.

³³ GUDE, p.12.

basadas en cámaras de videovigilancia a la observancia del principio de proporcionalidad³⁴, de manera que “el criterio jurisprudencial anterior, centrado en la consideración del lugar y tiempo de trabajo como un ámbito extraño a la intimidad fue desplazado a partir de estas decisiones jurisprudenciales por la técnica de la ponderación”³⁵. Por último, la tercera conclusión que se extrae es que hasta el momento no se había valorado la instalación de cámaras de videovigilancia teniendo en cuenta el derecho a la protección de datos de carácter personal, pues se estudiaba la cuestión sobre “la base de la colisión de las facultades de control con el derecho a la intimidad de los trabajadores, sin ninguna referencia al derecho de autodeterminación informativa que consagra el artículo 18.4 CE”³⁶.

3.2. El derecho a la protección de datos de carácter personal como derecho autónomo

También en el año 2000, a raíz de los recursos de inconstitucionalidad de algunos artículos de la LO 15/1999³⁷, el TC dictó la sentencia 292/2000, de 30 de noviembre, la cual es relevante por dos cuestiones. Por un lado, está mencionada en el preámbulo de la actual LO 3/2018, pues es una de las sentencias pioneras que entró a definir el derecho a la protección de datos de carácter personal, consagrado en el artículo 18.4 de la CE, de manera que se dispone que es “un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso”³⁸. Por otro lado, dicha sentencia es tenida especialmente en cuenta en la STC 29/2013, de 11 de febrero de 2013, siendo que esta última tiene especial relevancia en nuestro objeto de estudio, pues traza como límites independientes y autónomos, a la instalación de cámaras de videovigilancia, los derechos a la intimidad y a la protección de datos de carácter personal.

Como indica DESEDENTADO BONTE “la construcción de ese derecho autónomo —derecho a la protección de datos personales, libertad informática o derecho a la autodeterminación informativa— ha sido obra del Tribunal Constitucional (...)”³⁹, de modo que “en las sentencias de la primera etapa (...) la protección de datos se concibe todavía como una función de garantía del derecho de la intimidad (...)”⁴⁰. De esta forma, afirma este mismo autor (como lo hace la doctrina en general) que “el proceso de reconocimiento se cierra con las SSTC 290 y 292/2000 (3), sobre todo con esta última” pues esta “afirma con claridad la existencia de un derecho fundamental a la protección de datos personales frente a la informática”⁴¹.

³⁴ AURELIO DESDENTADO BONETE, ANA BELÉN MUÑOZ RUIZ, *Control informático, videovigilancia y protección de datos*, pag.25.

³⁵ GUDE, p.13.

³⁶ GÓNZALEZ, “Novedades de la Ley Orgánica 3/2018”, p.8.

³⁷ En concreto, los artículos 21.1 y 24.1 y 2 de la citada ley.

³⁸ LO 3/2018, I preámbulo.

³⁹ DESDENTADO, MUÑOZ, p.2.

⁴⁰ *Ibidem*.

⁴¹ *Ibidem*, p.4.

Así las cosas, en la citada sentencia el TC desvinculó el derecho a la protección de datos de carácter personal del derecho a la intimidad, pues mientras que este último tiene por objeto “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”⁴², el derecho a la protección de datos tiene como finalidad “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”, esto es, pretende que las personas puedan disponer de dichos datos. Así, este poder de disposición no solo se refiere a datos íntimos e implica que la persona titular del derecho pueda conocer quién tiene esos datos, pues no se puede disponer de los mismos si no se tiene conocimiento de quién, cómo y para qué los trata. Por consiguiente, es “el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. Esto es, en definitiva, es el poder de disposición sobre los datos personales”.

3.3. Características esenciales de la LO 15/1999

El 14 de enero del año 2000 se promulgó la LO 15/1999⁴³, de manera que aquella fue aprobada “principalmente para hacer frente a la necesidad de trasponer las exigencias derivadas de la Directiva 95/46, de 24 de octubre de 1995”⁴⁴. Así, el objeto de la ley era “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”⁴⁵. Hay que tener en cuenta que dicha ley no contemplaba disposiciones específicas en materia laboral, por lo que contenía “regulaciones generales (...) dirigidas a ordenar todos los sectores de la vida social”⁴⁶. Si bien esto era así, se entendió que sus disposiciones eran “plenamente aplicables también al ámbito de las relaciones de trabajo”⁴⁷, como se deriva de la doctrina jurisprudencial del TC⁴⁸ y del TS⁴⁹ posterior a la promulgación aquella.

En su ámbito de aplicación, se disponía que sería de “aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos”⁵⁰, de forma que por datos de carácter personal se entendió “cualquier información concerniente a personas físicas identificadas o

⁴² STC 292/2000, de 30 de noviembre. Señalamos que de ahora en adelante todas las citas textuales son de dicha sentencia.

⁴³ Que derogó a la *Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*.

⁴⁴ RODRIGO, TASCÓN LÓPEZ, *El tratamiento por la empresa de los datos personales*, p.9

⁴⁵ LO 15/1999, artículo 1.

⁴⁶TASCÓN, p.13.

⁴⁷Ibidem, p.13.

⁴⁸ Por ejemplo, en la STC 29/2013, de 11 de febrero de 2013 o en la STC 39/2016, de 3 de marzo de 2016.

⁴⁹ A modo de ejemplo, en la STS 77/2017, 31 de enero de 2017 o la STS 1003/2021, 13 de Octubre de 2021.

⁵⁰ LO 15/1999, artículo 2.1.

identificables”⁵¹. Por lo que se refiere al tratamiento de datos, se estipuló que serían “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación”⁵², definición que permite incluir a las grabaciones captadas por cámaras de videovigilancia en el ámbito laboral. Asimismo, cabe destacar que el responsable del tratamiento (el empresario en nuestro caso) podía ser una “persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento”⁵³, mientras que el afectado (las personas trabajadoras) debía ser la “persona física titular de los datos que sean objeto del tratamiento (...)”⁵⁴. Es destacable señalar que por consentimiento se entendió “toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”⁵⁵.

A partir de aquí, hemos de destacar tres cuestiones. En primer lugar, la ley establecía que los datos de carácter personal se podían recoger para su tratamiento cuando fueran “adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas (...)”⁵⁶, de manera que no podían “usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”⁵⁷. A raíz de esto, la doctrina entendió que mientras “la adecuación y la pertinencia se refieren a la idoneidad del dato para lograr la finalidad de la que deriva su justificación en atención a las exigencias de la relación laboral (...) La proporcionalidad se vincula a la exigencia de que los datos, aun siendo idóneos, no deben ser excesivos en orden al cumplimiento de su finalidad”⁵⁸. En segundo lugar, se estableció que los interesados a los que se solicitasen los datos debían “ser previamente informados de modo expreso, preciso e inequívoco: (...) de la existencia de un fichero o tratamiento de datos de carácter personal (...) de las consecuencias de la obtención de los datos (...) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición (...) de la identidad y dirección del responsable del tratamiento”⁵⁹. En tercer lugar, quizás lo más relevante, era que se establecía como regla general que “el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado”⁶⁰, si bien, como indicó la doctrina, “dicho régimen se caracteriza, más que por la regla general, por sus continuas excepciones”⁶¹. Así, la ley señalaba que no era preciso el consentimiento cuando se tratase de “las partes de un contrato o precontrato de una relación negocial, laboral o administrativa”⁶² y fuesen “necesarios para su mantenimiento o cumplimiento (...)”⁶³. Por ello, se entiende que “la prestación del consentimiento para estos negocios jurídicos lleva consigo la presunción de que el afectado ha consentido asimismo la recogida y el tratamiento de sus datos dentro del

⁵¹ Íbidem, artículo 3 letra a.

⁵² Ídem, letra c.

⁵³ ídem, letra d.

⁵⁴ ídem, letra e.

⁵⁵ Íbidem, letra f.

⁵⁶ ídem, artículo 4 apartado 1.

⁵⁷ ídem, apartado 2.

⁵⁸ DESDENTADO, MUÑOZ, “Protección de datos y contrato de trabajo”, p.29.

⁵⁹ Íbidem, artículo 5 apartado primero.

⁶⁰ Íbidem, artículo 6 apartado primero.

⁶¹ FRANCISCA GARCÍA-NÚÑEZ SERRANO, “La regulación sobre protección de datos personales”, p.9.

⁶² LO 15/1999, artículo 6 apartado segundo.

⁶³ Íbidem.

marco de las relaciones jurídicas mencionadas”⁶⁴, por lo que “en el ámbito laboral el consentimiento del trabajador pasa, como regla general, a segundo plano y cobra más fuerza el cumplimiento de otros deberes como el deber de información”⁶⁵.

Además de la LO 15/1999, hay que destacar la *Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras*⁶⁶. Esta instrucción se dictó como consecuencia de la creciente proliferación de los sistemas de videovigilancia, lo cual generó “numerosas dudas en lo relativo al tratamiento de las imágenes”⁶⁷. Así, dicha normativa es tenida en cuenta en los pronunciamientos jurisdiccionales que analizaremos posteriormente, de forma que esta era aplicable al tratamiento de datos de carácter personal en el ámbito laboral. En ella, se señalaba que los responsables de dicho tratamiento, en nuestro caso los empresarios, debían cumplir con el deber de información al que hemos hecho referencia *ad supra*, por lo que habían de “colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y (...) tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999”⁶⁸.

4. INTERPRETACIÓN Y APLICACIÓN JURISPRUDENCIAL DE LA LO 15/1999

Teniendo en cuenta la concepción jurisprudencial que había del derecho a la intimidad y a la protección de datos de carácter personal a partir de las sentencias del TC que hemos comentado anteriormente, así como la normativa específica relativa al segundo de los derechos, los tribunales se enfrentaron a múltiples casos en los que la instalación de cámaras de videovigilancia colisionaba con tales derechos. Así, de la casuística jurisprudencial que desarrollaremos a continuación, observamos que los criterios no son del todo uniformes. Como bien fue indicando la doctrina durante esos años, hasta la promulgación de LO 3/2018, “los tribunales laborales han sido los que, en ausencia de una regulación normativa expresa en la materia, se han ocupado de resolver las diferentes cuestiones surgidas por el empleo de la videovigilancia”⁶⁹. Así, es un ámbito en el que la doctrina y la jurisprudencia han señalado reiteradamente la conflictividad que han producido estas medidas de vigilancia y control, pues “no ha existido una norma que contemplara una respuesta a tales situaciones. Por ello, esta falta de regulación del choque entre derechos de una y otra parte, se ha visto compensada por la jurisprudencia y por la abundantísima doctrina científica”⁷⁰.

Así las cosas, no eran pocas las voces que ya desde el inicio de siglo señalaban que “sería conveniente que el legislador tomara cartas en el asunto y no dejara a la interpretación de los Tribunales la escasa regulación laboral existente sobre este asunto, estableciendo una serie

⁶⁴ GARCÍA-NÚÑEZ, p.10.

⁶⁵ DESDENTADO, MUÑOZ, “Protección de datos”, p.32.

⁶⁶ De ahora en adelante Instrucción 1/2006.

⁶⁷ Instrucción 1/2006, preámbulo.

⁶⁸ *Ibidem*, artículo 3.

⁶⁹ GUDE, p.24.

⁷⁰ FÉRNANDEZ, p.5.

de (...) reglas básicas de coordinación y de equilibrio entre el poder de vigilancia empresarial y el derecho fundamental del trabajador”⁷¹. En la misma línea, en el año 2005 se señalaba que “son numerosas las voces alzadas para reclamar una regulación propia y específica que atienda las múltiples y variadas peculiaridades existentes en el marco laboral”⁷².

4.1. El cumplimiento estricto del deber de información: STC 29/2013, de 11 de febrero de 2013

En primer lugar, hay que tener en cuenta la STC 29/2013, de 11 de febrero del 2013. Parte de la doctrina ha señalado que esta sentencia es sumamente relevante, pues es la primera⁷³ en la que se traza una distinción clara y nítida entre el derecho a la intimidad y el derecho a la protección de datos de carácter personal, siendo que resuelve la cuestión atendiendo únicamente a este último derecho. Así, se “establece condiciones adicionales para la validez de la utilización de las cámaras de vigilancia en los centros de trabajo, exigiendo con rigor el cumplimiento del deber de información previo a los trabajadores para admitir las grabaciones como prueba del comportamiento del trabajador”⁷⁴. Vemos por tanto como el elemento central es el deber de información previo, de manera que como bien indica la doctrina mayoritaria (por ejemplo, POQUET⁷⁵, GONZÁLEZ GONZÁLEZ⁷⁶ o HENRÍQUEZ TILLERÍA⁷⁷) esta interpretación constituye una primera fase en la que el TC exigió un deber de información en sentido estricto, esto es, “considera que existe un claro deber de información previa a los trabajadores, por parte de la empresa, respecto a la puesta en práctica de controles laborales”⁷⁸.

Así las cosas, los hechos enjuiciados fueron la impugnación de unas sanciones, de empleo y sueldo, que se impusieron a un trabajador de la universidad de Sevilla. Dichas sanciones lo fueron a partir de la captación de imágenes por las cámaras de videovigilancia instaladas en los accesos del lugar de trabajo, de forma que ante las sospechas de que el trabajador no cumplía con su horario laboral, se utilizaron dichas grabaciones. Si bien los trabajadores tenían conocimiento de la instalación de las cámaras, pues había carteles informativos de las mismas, aquellos no habían sido informados previamente de las concretas finalidades que podían tener la captación de imágenes.

A partir de aquí, el TC entendió que la captación de dichas imágenes constituye un dato de carácter personal que tenía encaje en el artículo 18.4 de la CE, pues entra dentro del contenido de dicho derecho “aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil”⁷⁹. De esta forma, el alto tribunal

⁷¹ FERNÁNDEZ, p.9.

⁷² TASCÓN, p.13.

⁷³ En el mismo sentido, se dictó la STC 1685/2013, de 13 de mayo de 2014.

⁷⁴ GÓZALEZ, p.8.

⁷⁵ POQUET, p.9.

⁷⁶ GÓZALEZ, Control empresarial de la actividad laboral, p.8.

⁷⁷ SEBASTIÁN HENRÍQUEZ TILLERÍA, *Protección de datos, videovigilancia laboral*, p.63.

⁷⁸ JAVIER ÁLVAREZ HERNANDO, “Relaciones laborales y protección de datos”, p.43

⁷⁹ STC 29/2013, de 11 de febrero (F5).

tuvo en cuenta la doctrina de la STC 292/2000, de 30 de noviembre del año 2000⁸⁰, entendiendo que el contenido esencial del derecho proclamado en el artículo 18.4 de la CE era, en este caso, el derecho del trabajador a conocer quién posee la información y con qué fin lo hace. Así, este derecho de información también entra en juego aun cuando no es necesario el consentimiento del afectado⁸¹, por lo que “no hay una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales”⁸². De este modo, el TC concluyó que “por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa”. Por todo ello, el alto tribunal constató que se había vulnerado el artículo 18.4 de la CE, pues por mucho de que se advirtiese de las cámaras con los distintivos, era necesario proporcionar al trabajador la información previa y expresa, precisa, clara e inequívoca de la finalidad del tratamiento de datos. Se debía así “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”. Por último, cabe destacar que el tribunal no somete la medida empresarial al test de proporcionalidad, como si lo hizo anteriormente en las STC 8/2000, de 10 de abril del año 2000 y 186/2000, de 10 de julio del año 2000, si bien el objeto de estudio también era la vulneración de un derecho fundamental⁸³.

4.2. La colocación del distintivo informativo como forma de cumplimiento del deber de información: El caso “Bershka”

En el año 2016 se dictó la STC 39/2016, de 3 de marzo de 2016 (caso “Bershka”), donde el TC se reunió en pleno por la captación de imágenes de una trabajadora que alegó la vulneración de su derecho a la intimidad y a la protección de datos de carácter personal. Así, para gran parte de la doctrina este pronunciamiento supuso un cambio jurisprudencial del TC en la concepción del deber de información exigido al empresario cuando instala cámaras de videovigilancia, pues si bien el alto tribunal no expone tal cosa en el texto de la sentencia⁸⁴,

⁸⁰ Hay que recordar que esta sentencia era la que consagra y define el derecho a la protección de datos de carácter personal, de manera que señala como indispensable el conocer quién trata nuestros datos, cómo lo hace y con qué fin. Esto es, dicha sentencia exigía de forma estricta cumplir con el deber de información en sentido amplio.

⁸¹ Pues, tal y como hemos expuesto, la propia LO 15/1999 lo dispensa en el marco de una relación laboral.

⁸² STC 29/2013, de 11 de febrero de 2013. Señalamos que las próximas citas literales, salvo afirmación en contra, corresponden a dicha sentencia.

⁸³ Esto confronta con la jurisprudencia más reciente que, por regla general, aun incumplido el deber de información, sí que somete la medida al test de proporcionalidad, de forma que no todo incumplimiento del deber de información comporta, *per se*, una vulneración del derecho a la protección de datos de carácter personal.

⁸⁴ Como bien indica GÓNZALEZ: “parece evidente que el Pleno del TC ha cambiado la doctrina de la STC 29/2013. Sin embargo, resulta sorprendente que no se mencione ese trascendente cambio, a pesar de que la recurrente en amparo fundada gran parte de su recurso precisamente en el deber informativo al trabajador que resulta del art. 18.4 CE, tal y como había sido interpretado por la sentencia citada” (GÓNZALEZ, Control empresarial de la actividad laboral, p.13). En la misma línea, se emitió un voto particular por parte del Magistrado don Fernando Valdés Dal-Réal, al que se adhirió la Magistrada doña Adela Asua Batarrita.

este consideró que el incumplimiento del deber de información no implica, *per se*, que se vulnere el derecho del artículo 18.4 de la CE, pues más allá de las posibles sanciones en materia de protección de datos que pudiese haber^{85 86}, la medida debe someterse al principio de proporcionalidad.

Los hechos enjuiciados, de forma sucinta, fueron los siguientes. La empresa tenía evidencias de que en la zona de caja se cometían irregularidades, siendo que de estas últimas podía “desprenderse una apropiación dineraria por parte de alguno de los trabajadores que trabajaban en dicha caja”⁸⁷. Por ello, el empleador instaló cámaras de videovigilancia que enfocaban las cajas y colocó el correspondiente distintivo informativo (que exigía la Instrucción 1/2006), por lo que si bien este se colocó en un lugar visible (el escaparate de la tienda), no se avisó a las personas trabajadoras de la instalación de dichas cámaras. De este modo, como consecuencia de la captación de imágenes de esas cámaras, se comprobó que una trabajadora se apropiaba indebidamente de cantidades dinerarias de la caja sometida a grabación, por lo que se procedió a su despido (el cual fue impugnado y dio lugar al pronunciamiento del alto tribunal).

Dicho esto, las ideas más relevantes son las siguientes. En primer lugar, el TC ratificó que el empresario no necesita del consentimiento expreso “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 control laboral”, pues el consentimiento se entiende implícito. En segundo lugar, señaló que el deber de información debe cumplirse, si bien “para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad”. Por tanto, lo que debe hacerse es un **juicio de ponderación** entre el derecho a la protección de datos de carácter personal y el poder de dirección empresarial⁸⁸. De esta forma, como es obvio, en primer lugar, habrá que determinar si se ha dado esa insuficiencia informativa. En tercer lugar, el TC, entrando a valorar los hechos, indicó que el hecho de colocar el distintivo informativo de las cámaras permitió a la empresa cumplir con el deber de información pues se adecuaba al artículo 3 de la Instrucción 1/2006 citada *ad supra*⁸⁹. Así, entendió el tribunal que la trabajadora podía

⁸⁵ El TC, cuando se está refiriendo al deber de información, señala que “sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad” (STC 39/2016, de 3 de marzo de 2016).

⁸⁶ En cuanto este inciso, si bien esta sentencia no entra a valorar dicha cuestión en profundidad, los posteriores pronunciamientos sí que fueron más claros. Por ejemplo, en la STJUE de 17 de octubre de 2019 (*asunto Lopez Ribalda y otros c. España*) se establece que ante un incumplimiento del deber de información los afectados tienen otros mecanismos como acudir a la AEPD (135).

⁸⁷ STC 39/2016, de 3 de marzo de 2016, antecedente segundo. Señalamos que las siguientes citas literales, salvo afirmación en contra, pertenecen a dicha sentencia.

⁸⁸ Que como indicábamos al principio de nuestro estudio, trae causa del artículo 38 de la CE y se plasma en el artículo 20.3 del ET.

⁸⁹ Recordemos que en su artículo tres la Instrucción 1/2006 señalaba que: “los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán: a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados”. Es curioso que el TC realice tal interpretación, pues de una lectura literal podemos extraer que se deben cumplir con las exigencias del artículo 5 de LO 15/1999, además de colocar el distintivo. Es decir, cabe la posibilidad de interpretar que los requisitos son cumulativos, en tanto que el artículo 5 señalaba que: “los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: (...) De

”conocer la existencia de las cámaras y la finalidad para la que habían sido instaladas”⁹⁰, por lo que sabía de la instalación de las cámaras ”sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control”⁹¹. De este modo, lo relevante es ”si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento”.

A partir del anterior razonamiento el TC resolvió que no se había vulnerado el artículo 18.4 de la CE, pues no se incumplió con el deber de información. Así, seguidamente, el tribunal aplicó el test de proporcionalidad a la instalación de dichas cámaras en relación con el derecho a la intimidad, por lo que hizo uso de la doctrina emanada en la STC 186/2000, de 10 de julio del año 2000 que ya hemos comentado anteriormente⁹². Como consecuencia de dicha aplicación, el alto tribunal entendió que la medida empresarial estaba justificada a raíz de las serias sospechas de apropiación de dinero por alguno de sus empleados, de manera que era idónea para la finalidad que se buscaba (el averiguar dichas irregularidades), necesaria (pues las imágenes permitirían dictaminar que se cometían dichas irregularidades) y proporcionada (en tanto las cámaras solo enfocaban a las cajas, siendo que no se vulneraba el derecho a la intimidad).

Así, se puede decir que, en primer lugar, “no es preciso constitucionalmente (aunque pudiera conllevar una infracción legal) proporcionar la información exacta sobre la finalidad de los datos recabados, cuando esté sobradamente justificado por las necesidades empresariales; así como, en segundo lugar, que la información dirigida al público, y no directamente al trabajador, sea suficiente para cumplir el requisito informativo a estos efectos”⁹³.

A raíz de este pronunciamiento no fueron pocas las voces críticas, dado que “se crea una nueva jurisprudencia constitucional a la establecida desde 2013, siendo más sencillo superar el juicio de contradicción, pues se amplían considerablemente las posibilidades empresariales de utilización de sistemas de videovigilancia sin lesión de derechos fundamentales a la

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”. En cambio, el TC opta por entender que el deber de información se entiende cumplido con el simple distintivo informativo sin más argumentación.

⁹⁰ En este punto, FERRER SERRANO señala que ”no es cierto es que dicha pegatina colocada en el escaparate permita conocer la finalidad de control de la actividad laboral para la que se instalan las cámaras, máxime cuando se encuentra oculta, deducción que surge del hecho de que los trabajadores no fueron capaces de verla al menos hasta que se produjo el despido. (...) Los trabajadores de un comercio relacionan una pegatina de videovigilancia con la actividad de la empresa de proteger su patrimonio empresarial de eventuales robos de productos, pero ello nada tiene que ver con la finalidad de control de la actividad laboral de los trabajadores”. (ROBERTO LUIS FERRER SERRANO. ”Videovigilancia e información personal de los trabajadores”, p.11).

⁹¹ Si tenemos en cuenta la doctrina sentada en la sentencia del TC del año 2013 dicha afirmación es, al menos, cuestionable, pues la máxima era, precisamente, que las personas trabajadoras pudieran conocer la concreta finalidad del tratamiento de sus datos de carácter personal.

⁹² Esta es, en esencia, que ”el empresario no queda apoderado para llevar a cabo, so pretexto de las facultades de vigilancia y control que le confiere el art. 20.3 LET, intromisiones ilegítimas en la intimidad de sus empleados en los centros de trabajo. Los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo suponen, por lo que ahora interesa, que también las facultades organizativas empresariales se encuentran limitadas por los derechos fundamentales del trabajador” (STC 186, de 10 de julio del año 2000).

⁹³ ANA ISABEL GARCÍA SALAS, ”El deber empresarial de informar acerca de la videovigilancia”, p.7.

intimidad (art. 18 CE), y a la autodeterminación informativa y derecho a la privacidad (art. 18.4 CE)”⁹⁴⁹⁵. En la misma línea, como bien indica GOÑI SEIN:

La nueva orientación que emerge (...) flexibiliza el requisito esencial del deber de información previa del derecho fundamental del artículo 18.4 ce hasta el punto de convertirlo en una exigencia meramente formal (...). Sin embargo, la consecuencia que deriva es que el derecho a la protección de datos se hace ahora ineficaz, (...) porque la colocación de un cartel distintivo habilita a la empresa para tomar imágenes del trabajador y servirse de las grabadas cuando, como y para lo que convenga con tal de que su uso guarde alguna relación con el contrato.⁹⁶

Si bien a partir de esta sentencia hubo cierta unificación jurisprudencial⁹⁷, en el año 2018 GARCÍA SALAS ya señalaba que “hasta que no haya cierto consenso sobre algunos de los puntos básicos en que se sustenta la videovigilancia (...), se continuará con la montaña rusa de pronunciamientos judiciales”⁹⁸, haciendo latente esta falta de normativa específica laboral en este ámbito.

Con todo, la interpretación dada por el TC en el año 2013 y 2016 tiene cuestiones comunes que se han consolidado desde entonces. Por un lado, ambas trazan de forma clara y nítida los dos derechos fundamentales en juego que limitan el poder empresarial, de manera que en el ámbito de un contrato de trabajo se circunscribe al derecho de protección de datos de carácter personal el deber de información (si bien su cumplimiento es interpretado de dos formas distintas), siempre y cuando la captación de las imágenes tenga por objeto la seguridad o el control laboral. Por otro lado, mantienen la doctrina constitucional de que cualquier medida restrictiva de derechos fundamentales tiene que observar el principio de proporcionalidad, si bien parece que su aplicación solo recae cuando se analiza el derecho a la intimidad.

4.3. Pronunciamientos judiciales significativos a partir de la doctrina jurisprudencial recaída con el caso “Bershka”

4.3.1. El TEDH entra en juego: el asunto López Ribalda (II)

Uno de los pronunciamientos más significativos es la STEDH de 17 de octubre de 2019 (asunto *López Ribalda y otros c. España*)⁹⁹. En este caso los hechos enjuiciados más

⁹⁴ JOSÉ ANTONIO, GONZÁLEZ MARTÍNEZ, “La videovigilancia empresarial en la industria 4.0”, p.21.

⁹⁵ En el mismo sentido, FERRER SERRANO señala que con esta sentencia: “se ha ampliado la posibilidad de introducir estos sistemas de control de la actividad laboral, incluso de forma permanente, bastando una información genérica previa, aun inespecífica, por la que los trabajadores puedan conocer la existencia de este control”. (Videovigilancia e información personal de los trabajadores, p.2).

⁹⁶ JOSÉ LUIS GOÑI SEIN, “Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información previa”, p.2.

⁹⁷ Seguida por el TS.

⁹⁸ GARCÍA SALAS, p.9.

⁹⁹ A partir de ahora nos referiremos como asunto López Ribalda (II). Cabe decir que este asunto tuvo un primer pronunciamiento por parte de la Tercera Sección del TEDH en el que se entendió vulnerado el artículo 8 del CEDH, este es, el derecho a la vida privada.

relevantes fueron que la empresa (un supermercado), a raíz de observar pérdidas de existencias y ventas, instaló cámaras de videovigilancia. Por un lado, unas eran visibles, enfocaban en los accesos del supermercado y fueron informadas a las personas trabajadoras. En cambio, por otro lado, las otras cámaras eran ocultas y enfocaban a las cajas. Así, a partir de las imágenes obtenidas de estas últimas, varias personas trabajadoras fueron despedidas por la perpetración de una serie de robos, de manera que impugnaron la validez de dichas grabaciones por haber vulnerado su derecho “a la protección de su privacidad”¹⁰⁰.

De dicha sentencia extraemos tres consideraciones importantes. En primer lugar, el TEDH señala una serie de circunstancias que se deben tener en cuenta a fin de garantizar el principio de proporcionalidad en la instalación de las cámaras de videovigilancia: si se ha notificado la instalación; “el alcance de la vigilancia por el empleador y el grado de intrusión en la vida privada del empleado (...), así como las limitaciones de tiempo y espacio y el número de personas que tienen acceso a los resultados”¹⁰¹; las razones legítimas de la medida¹⁰²; la posibilidad de haber utilizado medios menos lesivos; cuáles son las consecuencias de la medida; y, por último, si se han ofrecido medidas pertinentes a los empleados teniendo en cuenta el grado de intrusión. En línea con esto, “para resolver la cuestión (...) resulta necesario valorar específicamente el lugar donde las grabaciones fueron tomadas”¹⁰³. Por tanto, el TEDH entiende que la expectativa de privacidad en los lugares gravados (un supermercado abierto al público) era limitada, en contraposición con otros lugares de “carácter privado, como los aseos o los vestuarios, en los que se justifica una mayor protección, o incluso la prohibición total de la videovigilancia”. De esta forma, entiende que “es manifiestamente inferior en los lugares visibles o accesibles a los compañeros o, como en el presente caso, al público en general”.

En segundo lugar, el TEDH, teniendo en cuenta las cuestiones anteriores, entiende que la medida estaba legitimada por razones legítimas y que el grado de intrusión en la vida privada de las personas trabajadora fue proporcionado. De este modo, el tribunal entiende que no cualquier sospecha de un acto ilícito podrá justificar la instalación de cámaras ocultas, si bien “la existencia de una sospecha razonable de que se ha cometido una falta grave y la magnitud de las pérdidas identificadas (...) pueden parecer una justificación de peso”. Asimismo, el tribunal tiene en cuenta que las sospechas se referían a varias personas trabajadoras, de manera que “esto crea una atmósfera general de desconfianza en el lugar de trabajo”.

En tercer lugar, quizás lo más relevante para nuestro caso, es que el TEDH señala que el deber de información se incumplió respecto las cámaras ocultas, si bien es una cuestión que debe tenerse en cuenta al someter la medida al test de proporcionalidad. En palabras del tribunal “el suministro de información a la persona objeto de la vigilancia y su alcance constituyen sólo uno de los criterios que deben tenerse en cuenta para evaluar la proporcionalidad de una medida (...). Sin embargo, si no se dispone de esa información, las medidas derivadas de los demás criterios serán aún más importantes”. Por tanto, vemos como

¹⁰⁰ Asunto López Ribalda II (20). De ahora en adelante, salvo afirmación en contra, las citas textuales corresponden a dicha sentencia.

¹⁰¹ En este punto el TEDH entiende que es relevante que las cámaras solo enfocasen las cajas y que la medida fuese temporal, pues apenas duró unos días.

¹⁰² El TEDH tiene muy en cuenta las evidencias previas de irregularidades en las cajas derivadas de la pérdida de existencias

¹⁰³ JAVIER IGNACIO ZARAGOZA TEJADA, La prueba obtenida por videocámaras de seguridad, p.14

se introduce un importante matiz, pues el TEDH considera que este incumplimiento del deber de información es un elemento más a tener en cuenta al valorar la proporcionalidad de la medida, por lo que vuelve a situarlo íntimamente relacionado con el derecho a la intimidad (a la vida privada) y no tanto a la posible vulneración de un derecho fundamental. Como señala Zaragoza, el TEDH entiende, en relación con el deber de información, que "dicha exigencia constituye solo un criterio a tener en cuenta más para evaluar la proporcionalidad de la adopción de la medida de control"¹⁰⁴¹⁰⁵. Por todo ello, el tribunal señala que "las demandantes podrían haber denunciado ante el Organismo de Protección de Datos el incumplimiento por parte del empleador de su obligación de proporcionar información previa, como se exige en el artículo 5 de esa Ley (...). Así pues, el derecho interno había puesto a disposición de las demandantes otros recursos para garantizar la protección específica de los datos personales"¹⁰⁶. Hay que remarcar que esta última aclaración del TEDH no es baladí, pues se hará eco el TS en sentencias posteriores¹⁰⁷¹⁰⁸.

3.3.2. Matices interpretativos introducidos por el TS

Por lo que se refiere al TS, este tiene diversos pronunciamientos que van en la misma línea de los que hemos ido comentando¹⁰⁹, si bien algunos de ellos introducen algunos matices que nos permiten ver la falta de uniformidad jurisprudencial¹¹⁰. En primer lugar, la STS 71/2017, de 31 de enero del año 2017 (antes de que se dictase el asunto López Ribalda II), el tribunal enjuició un asunto en el que, a partir de la grabación de unas cámaras instaladas en un supermercado por motivos de seguridad (que enfocaban a las cajas), un trabajador fue despedido por hurtar *tickets*, siendo que el trabajador conocía de la existencia de las cámaras, si bien no su finalidad exacta, pues no sabía del destino que se podía dar a las grabaciones¹¹¹. En este caso, la empresa no tenía sospechas previas de irregularidades¹¹². Así, el TS, brevemente, concluye que la instalación cumplía con el principio de proporcionalidad pues, entre otras cosas, "los

¹⁰⁴ ZARAGOZA, p.16

¹⁰⁵ En esta línea, el TEDH llega a afirmar que "la facilitación de información a cualquier empleado podría muy bien haber desvirtuado el objetivo de la videovigilancia, que era, como señalaron esos tribunales, descubrir a los responsables de los robos, pero también obtener pruebas para utilizarlas en los procedimientos disciplinarios contra ellos" (Asunto López Ribalda II (131)).

¹⁰⁶ Asunto López Ribalda II (135 y 136).

¹⁰⁷ Por ejemplo, en la STS 1003/2021, 13 de octubre del año 2021.

¹⁰⁸ Como se deduce de lo que hemos expuesto, el TEDH entendió que no se vulneró el derecho a la privacidad que alegaban los demandantes, pues la medida era legítima y cumplía con el test de proporcionalidad. De esta forma, las grabaciones no vulneraron los derechos de las personas trabajadoras despedidas.

¹⁰⁹ Esto es, nos referimos a las sentencias que son posteriores a la STC 39/2016 de 3 de marzo del año 2016 y que se hacen eco de la misma.

¹¹⁰ Aparte de las tres sentencias que comentaremos, hay otros pronunciamientos, tales como la STS 630/2016, 7 de Julio de 2016, la STS 86/2017, 1 de febrero de 2017 o la STS 817/2021, 21 de Julio de 2021. Cabe hacer hincapié en esta última, pues tiene en cuenta el artículo 105 de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social, el cual establece que corresponde al empresario la carga de la prueba de los hechos imputados en la carta de despido. Así, el TS pone dicho precepto en relación con el artículo 24.2 de la CE que consagra el derecho a utilizar los medios de prueba pertinentes.

¹¹¹ En todo caso, el TS afirma que el caso "Bershka", al que venimos haciendo referencia, "ha rebajado las exigencias informativas que debe facilitar la empresa al trabajador cuando instala un sistema de video-vigilancia" (STS 71/2017, de 31 de enero de 2017).

¹¹² Recordemos que en el asunto "Bershka" o el Asunto López Ribalda II se tenía muy en cuenta el hecho de que hubiesen indicios previos de irregularidades, siendo que reforzaba la legitimidad de la medida empresarial adoptada.

trabajadores estaban informados (...) de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad, expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo”¹¹³. En este punto, el TS hace una precisión relevante pues indica que no hubiese sido lícito utilizar las grabaciones para otros fines que no fuesen la seguridad (como la efectividad en el desempeño de las labores, la asistencia o las conversaciones con otros trabajadores¹¹⁴). Esta última consideración introduce matices respecto la sentencia del TC 39/2016, de 3 de marzo de 2016, pues el alto tribunal señaló entonces que lo importante era si el dato se recogía para “el mantenimiento, desarrollo o control de la relación contractual”¹¹⁵. En esta línea, el TS señala que “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”¹¹⁶, por lo que vemos que sigue la misma línea que el TEDH, cuya puerta había dejado abierta la STC 39/2016, de 3 de marzo de 2016.

En segundo lugar, la STS 96/2017, de 2 de febrero de 2017, enjuició un asunto en el que el trabajador de un gimnasio fue despedido como consecuencia de la captación de imágenes, de manera que las cámaras estaban “instaladas en la entrada y en los espacios públicos del gimnasio”¹¹⁷, de forma que las personas trabajadoras conocían de su existencia. Las causas del despido fueron varias, de modo que las imágenes captadas por las cámaras permitieron, por ejemplo, demostrar que incumplía con su jornada laboral o que dejaba pasar a personas que no eran del club. En este caso la empresa tenía sospechas de irregularidades previas y el TS entiende relevante el hecho de que años antes una persona había sido despedida como consecuencia de las grabaciones, de manera que el trabajador despedido conocía esta circunstancia, por lo que el tribunal dictaminó que era conocedor de que las imágenes podían ser utilizadas con fines disciplinarios y por ello su utilización no tuvo carácter sorpresivo¹¹⁸. Así, haciéndose eco de la sentencia del TC de 2016, el TS entiende que no se incumplió con el deber de información (y por ende con el artículo 18.4 de la CE) ni con el derecho a la intimidad, pues la medida era proporcionada. Por tanto, vemos como se vuelve a ir más allá de la seguridad *strictu sensu*¹¹⁹, pues no se hace alusión a la comisión de posibles ilícitos, sino que se hace un control de sus obligaciones laborales (su jornada, por ejemplo).

En tercer lugar, por último en este apartado, debemos comentar la STS 1003/2021, de 13 de octubre de 2021, donde los hechos enjuiciados versan entorno a el despido por motivos disciplinarios de un conductor de autobús, de modo que fueron las imágenes de dichas cámaras las que probaron los incumplimientos contractuales. En este caso, el conductor conocía de la existencia de las cámaras, pues había el correspondiente distintivo informativo y se había comunicado que eran para la seguridad de los conductores, por lo que desconocía que pudiesen ser utilizadas con motivos disciplinarios. Los hechos imputados, entre otros,

¹¹³ STS 71/2017, de 31 de enero del año 2017.

¹¹⁴ *Ibidem*.

¹¹⁵ STC 39/2016, de 3 de marzo de 2016 (F4). Parece claro que el TC fue más flexible en su interpretación, pues el mantenimiento o el control laboral va más allá de la seguridad en las cosas o elementos de la empresa.

¹¹⁶ *Ibidem*.

¹¹⁷ STS 96/2017, de 2 de febrero de 2017 (antecedente de hecho segundo).

¹¹⁸ *Ibidem*, (F2)

¹¹⁹ Al contrario de la STS 71/2017, de 31 de enero de 2017.

fueron fumar en el autobús, dejar pasar gratuitamente a mujeres, intimar con ellas, orinar por la ventana, etc. A partir de aquí, remarcamos esta sentencia por 2 motivos. El primero es que, sin haber sospechas de irregularidades, el TS entiende que la instalación de las cámaras es adecuada en atención a la actividad laboral desarrollada (el transporte de pasajeros), de manera que “con el riesgo que supone para él y para terceros: tanto los pasajeros del vehículo como otros usuarios de las vías públicas, la instalación de esas cámaras de vigilancia en el autobús era una medida justificada por razones de seguridad en sentido amplio, que incluye el control de la actividad laboral”¹²⁰¹²¹. La segunda cuestión es que algunas imágenes fueron captadas en tiempo de descanso, pues el conductor se quedaba dentro del autobús entre ruta y ruta, a lo que el TS razona que eso no es óbice de que “pueda incurrir en incumplimientos contractuales graves y culpables que afecten a sus obligaciones laborales, lo que justifica que las cámaras continuaran grabando durante esos lapsos temporales”¹²²¹²³. Con todo, entiende el TS que el trabajador podría haberse dirigido al organismo competente de protección de datos por lo que se refiere al posible incumplimiento del deber de información¹²⁴.

5. INTERPRETACIÓN DOCTRINAL Y JURISPRUDENCIAL DE LA NUEVA LO 3/2018

5.1. Incidencia de la LO 3/2018 en la instalación de cámaras de videovigilancia

Una vez hemos expuesto la evolución normativa y jurisprudencial de la instalación de cámaras de videovigilancia desde finales del siglo pasado, podemos comentar la nueva legislación de protección de datos que entró en vigor en el 7 de diciembre de 2018. De esta forma, el análisis de la misma será solo en relación con aquellos preceptos que tienen incidencia en la instalación de cámaras de videovigilancia en el marco de una relación laboral¹²⁵. Asimismo, debemos de tener en cuenta las consideraciones que hemos ido apuntando por parte de la doctrina, quien reclamaba desde hacía años una regulación más específica del asunto en cuestión, así como los apuntes realizados acerca de la casuística jurisprudencial recaída a

¹²⁰ STS 1003/2021, de 13 de octubre de 2021.

¹²¹ Por tanto, el TS vuelve a abalar que se lleve a cabo un control laboral cuando la finalidad de la cámara era la seguridad del autobús.

¹²² STS 1003/2021, de 13 de octubre de 2021.

¹²³ El tribunal no dedica más de dos frases a razonar esta cuestión, de modo que parece huir de la misma al afirmar que “en cualquier caso, el actor permitió que una pasajera viajara sin el correspondiente título en el autobús en varias ocasiones. Se trata de incumplimientos contractuales que se produjeron cuando estaba conduciendo el vehículo” (STS 1003/2021, de 13 de octubre de 2021).

¹²⁴ Cabe puntualizar que, más allá del repaso jurisprudencial que hace el TS en gran parte de su sentencia, no se detiene a valorar en profundidad si se ha vulnerado el derecho a la intimidad del conductor.

¹²⁵ Hay que tener en cuenta que el concepto de “tratamiento” y “datos de carácter personal”, así como las partes implicadas (en este caso se habla de destinatario en vez de interesado de acuerdo con el artículo 4 del Reglamento 2016/679 de 27 de abril de 2016 al que haremos referencia), son prácticamente lo mismo que lo dispuesto en la ley 15/1999. En todo caso, está fuera de dudas que la captación de imágenes mediante cámaras de videovigilancia en el marco de una relación laboral está dentro del ámbito de aplicación de la ley y son aplicables los preceptos que exponremos.

partir de la STC 29/2013, de 11 de febrero del 2013, que como se ha evidenciado dista de ser uniforme.

Con carácter previo, debemos remarcar que la nueva legislación ha introducido¹²⁶ el artículo 20 bis del ET, el cual establece que (la negrita es nuestra) “los trabajadores tienen derecho (...) a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales”. De esta forma, el ET hace “una remisión expresa (...) a la regulación que sobre los «derechos digitales» proporciona la propia LO 3/2018”¹²⁷.

En primer lugar, a efectos generales, la LO 3/2018 se ha promulgado como consecuencia del Reglamento (UE) 2016/679¹²⁸, siendo que, tal y como indica GONZÁLEZ GONZÁLEZ¹²⁹, es de aplicación directa y tiene primacía frente las normas internas de los estados miembros que lo contradigan. De esta forma, el artículo 1 de la LO 3/2018 establece que el “derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica”¹³⁰. En todo caso, ambas regulaciones son aplicables en el marco de una relación laboral y, si bien no aportan una “regulación especializada para las relaciones de trabajo”¹³¹, tienen preceptos que de forma expresa las contemplan (al contrario de lo que pasaba con la LO 15/1999 que hemos comentado *ad supra*). Así, “por primera vez en nuestro ordenamiento jurídico se regula el control empresarial de la actividad de los trabajadores cuando colisiona con los derechos fundamentales a la intimidad y a la protección de los datos personales”¹³².

Así las cosas, la ley contiene dos partes diferenciadas por lo que se refiere al impacto en las relaciones laborales: “por un lado, la regulación propiamente dicha de protección de datos personales (títulos I a IX), que guarda bastante paralelismo con la estructura del Reglamento 2016/679 (...); por otro, la regulación de los llamados derechos digitales (título X), una parte (...) que en cualquier caso, proporciona nuevas garantías para los ciudadanos y conecta como ya hemos dicho con antiguas exigencias del artículo 18.4 CE”¹³³. A estas dos partes debemos señalar de forma específica el artículo 22 (que tiene incidencia laboral directa, pero está situado en el título IV).

Por lo que se refiere a la primera parte, hay que prestar atención principalmente a tres cuestiones. La primera es que el consentimiento sigue siendo el eje central de la normativa de acuerdo con el artículo 6 del Reglamento 2016/679, pero el mismo “experimenta alguna modulación importante en el ámbito de la relación de trabajo”¹³⁴, de manera que sigue sin ser

¹²⁶ Disposición final decimotercera de la LO 3/2018.

¹²⁷ JOAQUÍN GARCÍA MURCIA, IVÁN ANTONIO RODRÍGUEZ CARDO, “La protección de datos personales en el ámbito de trabajo”, p.21

¹²⁸ *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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*. De ahora en adelante nos referiremos al mismo de forma abreviada como hemos hecho en el texto.

¹²⁹ GONZÁLEZ, “Novedades de la Ley Orgánica 3/2018”, p.24.

¹³⁰ Artículo 1 de LO 3/2018.

¹³¹ GARCÍA, RODRÍGUEZ, p.20.

¹³² GÓNZALEZ, p.28.

¹³³ GARCÍA, RODRÍGUEZ, p.22.

¹³⁴ *Ibidem*.

necesario cuando “el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte”¹³⁵, por lo que no es necesario que las personas trabajadoras presten su consentimiento cuando estamos ante cámaras de videovigilancia con fines de vigilancia o control laboral¹³⁶. La segunda cuestión es que los principios aplicables al tratamiento de datos se amplían a los ya establecidos en la ley 15/1999, de acuerdo con el artículo 5 del reglamento que, entre otras cuestiones, señala que los datos deben ser tratados de forma lícita, pertinente, adecuada y limitada a los fines perseguidos (que han ser explícitos y legítimos), así como mantenidos durante el tiempo que sea necesario. La tercera cuestión que debemos comentar es la relativa a los derechos del interesado (la persona trabajadora), en concreto el deber de transparencia e información contemplado en los artículos 12 de la LO 3/2018 y 12, 13 y 14 del Reglamento 2016/679, pues “se hace más exigente el deber informativo”¹³⁷, de forma que “el responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden”¹³⁸. Así, “se establece una lista exhaustiva de la información que debe proporcionarse a los interesados (...) y que comprende: la información sobre el responsable del tratamiento; la finalidad del tratamiento; la legitimación o título que legitima el tratamiento; los destinatarios de las cesiones o transferencias de los datos; los derechos de las personas; los datos del Delegado de Protección de Datos y la procedencia o fuente de los datos”¹³⁹.

Teniendo en cuenta las tres cuestiones comentadas, el artículo 22 de la LO 3/2018 señala que cuando la finalidad del tratamiento de las imágenes captadas sea la de “preservar la seguridad de las personas y bienes, así como de sus instalaciones”¹⁴⁰, el deber informativo “previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679”¹⁴¹. Así, el artículo prosigue señalando que: “el tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica”¹⁴². Vemos, por tanto, que dicho artículo se está refiriendo a la seguridad y no al control de la relación laboral, por lo que a priori excluiría utilizar este tipo de cámaras para fines disciplinarios (si bien seguidamente matizaremos esta afirmación).

Dicho esto, debemos hacer mención del artículo 89¹⁴³ de la LO 3/2018 que regula el “derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el

¹³⁵ Reglamento 2016/679, artículo 6.1 letra b.

¹³⁶ Como bien indican GARCÍA MURCIA e RODRÍGUEZ CARDO, se sigue la línea establecida por nuestro TC en cuanto que el consentimiento se entiende implícito en una relación laboral cuando sea necesario para mantener y cumplir el contrato (GARCÍA, RODRÍGUEZ, p.22).

¹³⁷ GONZÁLEZ, *Novedades de la Ley Orgánica 3/2018*, p.26.

¹³⁸ Artículo 12.1 de la LO 3/2018.

¹³⁹ GONZÁLEZ, “Novedades de la Ley Orgánica 3/2018”, p.26.

¹⁴⁰ Artículo 22.1 de la LO 3/2018.

¹⁴¹ Artículo 22.4 de la LO 3/2018.

¹⁴² Artículo 22.8 de la LO 3/2018.

¹⁴³ Tal y como dice QUÍLEZ MORENO, “resulta de agradecer el dictado de este artículo, que en principio parece despejar algunas dudas y nos clarifica varias cuestiones sobre las que la jurisprudencia, como hemos visto, ha titubeado en ocasiones.” (JOSÉ MARIA QUÍLEZ MORENO, “La garantía de Derechos Digitales en el ámbito laboral”, p.11).

lugar de trabajo”¹⁴⁴. Así, con carácter previo, hay que tener en cuenta la observación que señala GÓNZALEZ GONZÁLEZ, pues llama la atención “que sólo mencione el derecho a la intimidad, obviando la estrecha vinculación de la videovigilancia con el derecho a la protección de datos”¹⁴⁵, de manera que tampoco la exposición de motivos da una justificación de esta cuestión. Si bien esto es cierto, en dicha regulación “se procede, por definición, a la captación de datos personales, con vistas, en su caso, a su conservación y tratamiento”¹⁴⁶, de modo que el derecho a la protección de datos opera también como límite (pues así lo ha reconocido la doctrina y el propio TC, por ejemplo, en la sentencia 119/2022, de 29 de septiembre de 2022, que comentaremos más adelante). Así, en el primer párrafo de su apartado primero, el artículo citado señala que (la negrita es nuestra):

Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida¹⁴⁷.

Como vemos, el artículo parte del poder de dirección empresarial que legitima la instalación de sistemas de videovigilancia para el control de las personas trabajadoras¹⁴⁸, si bien dicho poder ha de estar “sometido siempre a dos límites concurrentes, que derivan de sendos derechos fundamentales: la intimidad y la protección de datos personales”¹⁴⁹. A partir de aquí, la norma general es que el empresario debe cumplir con un deber de información amplio, previo al tratamiento de datos, donde informe de forma clara, expresa y concisa de la medida empresarial. Por tanto, no bastaría con el simple distintivo informativo de la existencia de cámaras de videovigilancia, de modo que se deduce que cuando las cámaras pueden servir para el control laboral, será necesario informar del concreto uso que puede darse. Se entiende que el precepto “exige una redacción (...) clara y concisa, entendible para cualquier trabajador, de la existencia de dicho sistema de grabación de imágenes, y que tales imágenes no solo tienen la finalidad de preservar la seguridad de las personas, bienes o instalaciones, sino que pueden ser tratadas para controlar el correcto desempeño de la actividad laboral de los trabajadores”¹⁵⁰¹⁵¹. Así, el hecho de informar comporta que se dé “información de la finalidad del sistema instalado”¹⁵² de forma que, por ejemplo, “debe concretarse por el empleador que incluye la finalidad sancionadora si se captan incumplimientos laborales de los trabajadores”¹⁵³.

¹⁴⁴ Artículo 89 LO 3/2018.

¹⁴⁵ GÓNZALEZ, “Novedades de la Ley Orgánica 3/2018”, p.28.

¹⁴⁶ GARCÍA, RODRÍGUEZ, p.38.

¹⁴⁷ Artículo 89.1 (primer párrafo) de la LO 3/2018.

¹⁴⁸ Al igual que hemos comenzado nuestro estudio explicando tal cuestión.

¹⁴⁹ GARCÍA, RODRÍGUEZ, p.38.

¹⁵⁰ MORENO, p.12.

¹⁵¹ En la misma línea, con matices, se pronuncian GONZÁLEZ GONZÁLEZ (GÓNZALEZ, “Novedades de la Ley Orgánica 3/2018”, p.32), FERNÁNDEZ ORRICO (ORRICO, p.25) o QUÍLEZ MORENO (MORENO, p.12)

¹⁵² GONZÁLEZ, “Novedades de la Ley Orgánica 3/2018”, p.32.

¹⁵³ Ibidem.

Siguiendo con el apartado uno del artículo 89 de la LO 3/2018, se dispone que (la negrita es nuestra): “en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica”. Así, “esta previsión legal parece recoger el criterio de la STC 39/2016, 3 de marzo”¹⁵⁴, pues bastará con el distintivo informativo colocado en lugar suficientemente visible para entender cumplido el deber de información. Como vemos, la redacción es bastante vaga e inexacta, pues no se nos dice cuál es el concreto alcance de la expresión “acto ilícito”¹⁵⁵, de manera que, por ejemplo, el magistrado GONZÁLEZ GONZÁLEZ entiende que se deben incluir los delitos, las infracciones administrativas y los incumplimientos de obligaciones laborales¹⁵⁶. En la misma línea QUÍLEZ MORENO entiende que, además, debemos incluir aquellas faltas contempladas en el convenio colectivo aplicable, si bien se pregunta si también se incluyen los códigos internos de buenas prácticas o los Manuales del *Compliance*. Con todo, afirma que ampliar el concepto de ilícitos comporta apartarse de la regla general que el legislador establece en el párrafo primero del artículo 89.1 de la lo 3/2018¹⁵⁷. Asimismo, el precepto nos dice que se tiene que captar la comisión de un acto ilícito de forma flagrante, por lo que parece que es una previsión a la comisión de unos hechos que ya han pasado. Así, “no afronta el problema de manera abstracta y anticipada, de modo que el empleador se ha de seguir enfrentando al dilema de dar la información previa, expresa, clara y concisa (...) con la dificultad que ello supone para registrar actos ilícitos ante una sospecha, o de llevar a cabo controles sorpresivos a riesgo de que se le impute un incumplimiento de sus deberes informativos”¹⁵⁸.

Así las cosas, el artículo 89 tiene otra previsión que nos interesa en nuestro estudio, pues señala que “en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos”¹⁵⁹. Como vemos, esta es una previsión que se ha venido haciendo por la doctrina del TC desde hace años, pues ya estaba presente en su sentencia 98/2000, de 10 de abril del año 2000¹⁶⁰. De esta forma, “son espacios donde de manera natural se producirán manifestaciones de la vida íntima de los trabajadores, por lo que siempre resulta lesiva del derecho a la intimidad de los trabajadores la instalación de medios audiovisuales en tales lugares”¹⁶¹. En estos espacios no se desarrollan funciones laborales, por lo que por su propia naturaleza el empresario no puede llevar a cabo funciones de control de las personas trabajadoras a su cargo.

¹⁵⁴ POQUET, p.15.

¹⁵⁵ Como señala GONZÁLEZ GONZÁLEZ: “No podemos conocer la razón que determinó que de la redacción inicial – captación de un delito - se haya pasado en el informe de la ponencia del proyecto de la ley orgánica y en el texto definitivo a hacer mención al “acto ilícito”. La redacción actual es consecuencia de una enmienda del PP, pero, por desgracia, en la justificación de la enmienda no se ofrecen argumentos que sirvan al intérprete para orientarle y poder dar una respuesta más segura”. (GONZÁLEZ, Novedades de la Ley Orgánica 3/2018, p.33).

¹⁵⁶ Ibidem, p.33.

¹⁵⁷ QUÍLEZ, p.13.

¹⁵⁸ GARCÍA, RODRÍGUEZ, p.39.

¹⁵⁹ Artículo 89.2 de la LO 3/2018.

¹⁶⁰ Ver capítulo 1.

¹⁶¹ *Practicum Social 2020*, p.105

5.2. Consideraciones relevantes de la interpretación jurisprudencial recaída hasta el momento en aplicación de la nueva LO 3/2018

5.2.2. Decisión de la mayoría en la STC 119/2022, de 29 de setiembre de 2022

Habiendo expuesto los extremos más relevantes de la nueva normativa de protección de datos de carácter personal, debemos comentar dos sentencias (una del TC y otra del TS) que han sido especialmente relevantes y que nos ayudan a comprender la interpretación jurisprudencial dado hasta la fecha en base a la nueva normativa.

La primera de ellas es la STC 119/2022, de 29 de septiembre de 2022, donde se señala que se “trata de valorar la repercusión que la entrada en vigor de la Ley Orgánica 3/2018 pueda tener en nuestra doctrina sobre las imágenes captadas por una cámara de seguridad instalada en una empresa para su utilización en el marco de un despido disciplinario”¹⁶². Así, los hechos destacados son los siguientes. Un trabajador fue despedido por entregar productos de su empresa a cambio de dinero en metálico a un tercero, sin entrega de factura o albarán, de forma que la prueba se fundamentó en las imágenes captadas por cámaras de vigilancia del sistema de seguridad de la empresa. Así, estas cámaras eran visibles y conocidas, se había colocado el correspondiente distintivo informativo de las mismas y estaban instaladas como una medida más de seguridad de las instalaciones de la empresa. Hay que tener en cuenta, además, dos cuestiones destacadas: las imágenes se visionaron porque se descubrió una bolsa de una empresa de la competencia con un producto de la empresa litigante, de manera que al día siguiente la bolsa no estaba (lo cual generó sospechas); años antes se había despedido un trabajador por la utilización de las mismas cámaras con la misma finalidad.

A partir de aquí, en primer lugar, en relación con el derecho de protección de datos de carácter personal, el TC hace una precisión relevante, pues afirma con rotundidad “que el incumplimiento del deber de información afectaría, en esencia, al derecho a la protección de datos de carácter personal, no a la intimidad”. A partir de aquí, el alto tribunal entiende que las cámaras son conforme a la normativa, pues la empresa colocó las cámaras en lugar visible y con el correspondiente distintivo informativo, de modo que “se utilizaron para comprobar un hecho concreto, que resultó flagrante, y sobre la base de una sospecha indiciaria concreta, como era la irregularidad manifiesta de guardar un producto de la empresa dentro de una bolsa con el logotipo de una empresa de la competencia, en un lugar no habilitado a tal efecto”¹⁶³. Vemos, por tanto, como interpreta el concepto de “ilícito” en sentido amplio. En cuanto el hecho de que un trabajador fuese despedido años antes por la captación de imágenes de las mismas cámaras, entiende el tribunal que ratifica que el trabajador despedido-litigante era conocedor de que las cámaras se podían utilizar con fines disciplinarios. Así, el TC concluye que el derecho a la protección de datos de carácter personal no se ha visto vulnerado.

¹⁶² STC 119/2022, de 29 de septiembre de 2022. Señalamos que, a partir de aquí, todas las citas textuales corresponden a dicha sentencia, salvo afirmación en contra.

¹⁶³ Ibidem.

En segundo lugar, el alto tribunal entra a valorar la posible vulneración del derecho a la intimidad, de modo que somete la medida empresarial al principio de proporcionalidad. Así, tiene en cuenta, entre otras cosas, que las cámaras estaban en un lugar de atención al público y que eran visibles, así como que no fueron utilizadas con carácter “generalizado o indefinido, o para realizar una investigación de carácter prospectivo, sino para verificar la posible existencia de una conducta irregular detectada el día anterior”. Por ello, concluye que dicho vulnerado tampoco se ha visto vulnerado (y como consecuencia declara la validez de la prueba).

5.2.3. El voto particular de la STC 119/2022, de 29 de setiembre de 2022

En relación con esta sentencia, cabe comentar que hubo cinco magistrados que emitieron un voto particular, de modo que entendemos que es un dato relevante debido al número de magistrados no conformes con la mayoría (siete a cinco). Así, hay dos cuestiones relevantes que debemos comentar para nuestro análisis. Por un lado, el voto particular sigue la misma línea que hemos seguido en este trabajo, al afirmar que entre 2013 y 2019 hubo tres decisiones judiciales sobre la incidencia del deber de información que, dictadas en base a una misma normativa (la LO 15/1999), fueron divergentes. Así, dispone que:

La “STC 29/2013 sustenta que ese deber forma parte esencial del derecho fundamental del art. 18.4 CE y que no cabe ser suplido en ningún caso por la información genérica dirigida al público en general (...). La STC 39/2016 sostiene que existe un deber de información a los trabajadores pero que no es específico y puede ser cumplido con la información genérica dirigida al público. La STEDH de 17 de octubre de 2019 (...) se inclina por considerar que (...) el deber de información, aun siendo un elemento de relevancia en la tutela del derecho, cabe que sea omitido en determinadas circunstancias¹⁶⁴.

A partir de aquí, por otro lado, los magistrados señalan que la LO 3/2018, que irrumpe en esta situación de divergencia jurisprudencial, “no puede ser ignorada e impone una reevaluación tanto de la jurisprudencia del Tribunal Europeo de Derechos Humanos como la de este tribunal para establecer el actual estándar de tutela del derecho”. De esta forma, entienden que la opinión mayoritaria del TC no recoge la voluntad del legislador cuando redactó el artículo 89 de la LO 3/2018, pues aquel configuró una regla general (apartado primero, párrafo primero) que pretende que el empresario informe de manera amplia a las personas trabajadoras, esto es, que lo haga “de manera específica y diferenciada a la del público en general sobre la existencia de un sistema de control videográfico y de los eventuales fines disciplinarios de las imágenes captadas, en atención a la singularidad de las relaciones de trabajo”. Entienden, por ello, que este deber de información se configura como una garantía del derecho de protección de datos de carácter personal, pues estamos ante relaciones laborales donde el empresario ejerce sus facultades de control. Es la observación de esta regla general la que permite la injerencia en el derecho que conlleva la instalación de cámaras de videovigilancia, de modo que dicha regla sirve como una garantía para evitar posibles

¹⁶⁴ Voto particular de la STC 119/2022, de 29 de septiembre de 2022. Señalamos que, a partir de aquí, todas las citas textuales corresponden a dicho voto particular, salvo afirmación en contra.

abusos por parte del empresario. Así, no se puede consentir “una dejación o desatención continuada en su estricto cumplimiento por parte del empleador cuyos posibles abusos tiene por objeto contener”.

De este modo, la excepción relativa a la captación flagrante de un ilícito debe operar de forma muy limitada, pues no basta con la simple captación de aquel, sino que además se debe exigir que “se den cumplidas razones por parte del empleador respecto de su incumplimiento”. Por tanto, los magistrados señalan que, si no, se estaría “propiciando que el empleador optara por el incumplimiento continuado de la regla general del deber específico de información a sus trabajadores fiándolo todo, ante la existencia de carteles genéricos informativos, a la eventual concurrencia de la flagrancia en la captación para legitimar el uso disciplinario de las imágenes obtenidas”. Hay que tener en cuenta que este deber de información específico es parte del contenido esencial del derecho y se constituye como una garantía del mismo, por lo que no es un simple formalismo.

Teniendo en cuenta lo expuesto, el voto particular concluye que, en casos donde se capten ilícitos flagrantes, además del correspondiente distintivo informativo, es necesario que el empleador exponga cuáles son las razones que le han llevado a incumplir con el deber de información que exige la regla general. Si esto no es así, “el razonamiento de que la existencia de una sospecha razonable de que se ha cometido una falta grave pueda resultar una justificación de peso para modular las exigencias del deber de información puede dar lugar a investigaciones privadas y podría utilizarse como justificación en un número inaceptablemente elevado de casos”. Por ende, la interpretación que hace la opción mayoritaria del TC desvirtuaría las garantías que ofrece el artículo 89.1, pues supone situar la excepción y la norma general al mismo nivel¹⁶⁵ como consecuencia de “la desmesurada extensión que se da a las posibilidades excepcionales de su modulación en caso de flagrancia”.

5.2.4. Instalación de cámaras ocultas en la nueva LO 3/2018: STS 692/2022, de 22 de julio de 2022

En segundo lugar, por último, debemos comentar la STS 692/2022, de 22 de julio de 2022 para unificación de doctrina, la cual permite preguntarnos si en la nueva legislación de protección de datos de carácter personal tiene cabida la instalación de cámaras de videovigilancia ocultas. En este caso, los hechos afectaban a una empleada del hogar. Así, la empresaria se percató de que alguien había sustraído una cantidad de dinero importante de su caja fuerte, de manera que procedió a instalar una cámara oculta que enfocaba al armario donde se ubicaba la caja fuerte. En las grabaciones visualizó, después de haber transcurrido más de un mes desde la sustracción de dinero, a la trabajadora intentado abrir la caja fuerte. Si bien a la casa acudían dos personas más a limpiar, la trabajadora-litigante era la única que tenía llaves y se quedaba sola limpiando en más de una ocasión. Hay que tener en cuenta que la empleadora iba en silla de ruedas.

¹⁶⁵ Dice el voto particular que “sitúa a ambas en un mismo nivel axiológico”.

A partir de aquí, el TS entra a valorar la validez de la prueba por una posible vulneración de derechos fundamentales, de manera que lo primero que hace es hacerse eco del asunto López Ribalda II, pues entiende que por aquel entonces la normativa de protección de datos vigente también exigía, en principio, informar de la existencia de cámaras de videovigilancia. Así, recuerda que el TEDH consideró que la existencia de sospechas razonables de posibles ilícitos graves puede justificar la instalación de cámaras ocultas, de manera que señala el TS (siguiendo la doctrina expuesta por el TEDH) “que solo una imperativa protección de intereses públicos o privados importantes puede justificar la ausencia de información previa”¹⁶⁶. Asimismo, el TS entiende que también es aplicable el razonamiento del TEDH de que los demandantes tienen a su disposición otros medios (por ejemplo, el acudir a la AEPD), así como el hecho que tuvo en cuenta la STS 817/2021, 21 de Julio de 2021.

Teniendo en cuenta las anteriores consideraciones, en primer lugar, el TS afirma que la instalación de la cámara estaba justificada por la importante sustracción de dinero, porque solo enfocaba al armario donde se ubicaba la caja fuerte y por la situación de la empleadora, especialmente vulnerable. Entiende, por ello, que la medida era “justificada e idónea para el fin perseguido”¹⁶⁷, así como necesaria, pues no había otras medidas menos restrictivas. Así, señala que el hecho de declarar nula la prueba deja a la empleadora sin posibilidad de probar el incumplimiento laboral, de manera que aquella (especialmente vulnerable) es quien está obligada a demostrar los hechos que imputa a su trabajadora.

Por lo que se refiere al derecho a la protección de datos de carácter personal, haciéndose eco del caso “Bershka”, el TS afirma que (la negrita es nuestra): “no todo incumplimiento del deber de información previa, en nuestro caso, del artículo 89.1 de la Ley Orgánica 3/2018, conlleva una vulneración del derecho fundamental a la protección de datos del artículo 18.4 CE”, pues considera que la medida debe someterse al principio de proporcionalidad. Con todo, afirma además que “el posible incumplimiento de la legislación de protección de datos tiene otras consecuencias y otras posibles protecciones, ya señaladas, que no se agotan en el debate sobre la validez de la prueba de videovigilancia en un proceso por despido”.

En tercer lugar, para apoyar sus pretensiones, señala que en este caso concurrían una imperativa protección de intereses privados que justificaban la falta de información previa, así como que “en el caso pudo existir un ilícito penal, ámbito en el que caben espacios de videovigilancia judicialmente autorizada sin información a la persona afectada”. Asimismo, por último, tiene en cuenta que el “es un bien específico y singular desde la perspectiva de la protección de datos personales”.

Con todo, el tribunal concluye que en el presente caso era difícil la colación del distintivo informativo al que hace alusión la instrucción 1/2006, porque de haberlo colocado se hubiese frustrado la posibilidad de demostrar el incumplimiento laboral. Asimismo, señala que hay diferencias entre un sistema de videovigilancia *ad hoc* que trae causa de la existencia de sospechas fundadas y de un sistema que sea permanente, de modo que en este último caso se debe cumplir con el deber de información del artículo 89.1 de la LO 3/2018. Así, la obligación de información podrá “excepcionalmente modularse en supuestos tan especiales

¹⁶⁶ STS 692/2022, de 22 de julio de 2022 (F4).

¹⁶⁷ STS 817/2021, 21 de Julio de 2022. Señalamos que, a partir de aquí, todas las citas textuales corresponden a dicha sentencia salvo afirmación en contra.

como el presente, en el que, por lo demás, un sistema de videovigilancia permanente, sobre el que desde luego habría que proporcionar la información previa mencionada, podría estar difícilmente justificado y resultar desproporcionado”.

Por último, cabe señalar que el TS insiste, de manera reiterada, que estamos ante un caso excepcional en el que se valora la validez de una prueba, por lo que “solo excepcionalmente -y si se dan circunstancias similares a las aquí concurrentes- se podrá prescindir del distintivo informativo mencionado”. Así, lo que se está decidiendo es la validez o no de la prueba en un supuesto especial en el que falta el deber de información, “y no de otras consecuencias que la conducta empresarial puede tener desde la perspectiva más amplia de la legislación de protección de datos en su conjunto”. Por ello, una cosa es que se valore la prueba, y otra que “la empresa no pueda ser declarada responsable de un posible incumplimiento de la legislación de protección de datos con las posibles consecuencias administrativas o civiles, o de otra naturaleza, que ello pueda conllevar”.

6. CONCLUSIONES

Llegados a este punto, me propongo formular las conclusiones de este estudio, por lo que haré referencia a las cuestiones principales que se han ido tratando, cuáles son las certezas que se pueden extraer y cuáles son las preguntas o dudas que quedan.

I. En ejercicio de su poder de dirección empresarial, el empresario puede instalar cámaras de videovigilancia en su empresa, ya sea para garantizar la seguridad de sus bienes, de sus instalaciones o de las personas, o bien para llevar a cabo el control de las obligaciones laborales de las personas a su cargo. Así, cuando se lleve a cabo la instalación de dichas cámaras, se deben tener en cuenta los derechos fundamentales constitucionalmente reconocidos a todas las personas, incluidas las trabajadoras. De esta forma, estos derechos se verán modulados por el mismo contrato de trabajo y, a su vez, servirán como límite a la instalación de dichas cámaras. Así, dos derechos destacan especialmente: el derecho a la intimidad y el derecho a la protección de datos de carácter personal, si bien su evolución, reconocimiento e interpretación no han ido de la mano.

II. En el año 2000, el TC señaló que en el marco de una relación laboral las personas trabajadoras siguen siendo titulares del derecho a la intimidad y que este debe ser respetado. Por consiguiente, el TC determinó, por un lado, que hay espacios donde nunca cabe instalar cámaras de videovigilancia: aseos, vestuarios, lugares de descanso o análogos. Por otro lado, y por lo que se refiere a los demás lugares del entorno laboral, el tribunal dictaminó que se habían de tener en cuenta las circunstancias concurrentes, tales como la existencia de sospechas previas de irregularidades, si se avisó a las personas afectadas, la ubicación de las cámaras o la temporalidad de la medida. En suma, exigió que se cumpliese con el principio de proporcionalidad, el cual conlleva que la medida empresarial adoptada tenga como fundamento un fin legítimo, además de que sea idónea para conseguir dicho fin, necesaria y proporcionada. Es decir, debe realizarse una ponderación de los derechos en juego. A partir de este razonamiento, el derecho a la intimidad no ha sufrido apenas cambios interpretativos

(como sí lo ha hecho la protección de datos de carácter personal), pues siempre se ha sometido al principio de proporcionalidad. De este modo, se configura como aquel derecho que permite protegerse de las injerencias externas que puedan producirse en la esfera privada de una persona, esto es, permite el poder excluir del conocimiento de terceras personas aquellas parcelas de la vida personal y familiar reservadas a la privacidad de uno mismo.

III. En ese mismo año el TC reconoció el derecho a la protección de datos como derecho fundamental autónomo, el cual implica el poder decidir quién utiliza nuestros datos, cómo lo hace y con qué finalidad, siendo que la captación de imágenes por cámaras de videovigilancia en el entorno laboral se encuentra dentro del ámbito de dicho derecho (independientemente del grado de intrusión en la esfera personal que pueda darse). A partir de aquí, como norma general, la LO 15/1999 exigía la necesidad de que el afectado consintiese el tratamiento de sus datos, si bien tal cosa se excepcionaba en el marco de las relaciones laborales (como lo hace la actual normativa), siempre, eso sí, que el tratamiento sea necesario para la ejecución del contrato o la seguridad de las cosas o las personas. Así, desde entonces, el TC ha venido señalando que el consentimiento de la persona trabajadora está implícito. Con todo, de esa primera sentencia parecía desprenderse que el deber de información previo, acerca de cómo se iba a llevar a cabo el tratamiento y con qué fines, formaba parte del contenido esencial del derecho.

IV. Las STC 29/2013, de 11 de febrero de 2013 y 39/2016, de 3 de marzo de 2016 (caso *Bershka*) consolidaron como límites a la instalación de cámaras de videovigilancia el derecho a la intimidad y a la protección de datos de carácter personal. De esta forma, por un lado, la primera sentencia consideró que se debe cumplir con el deber de información de manera estricta, que consiste en que la persona trabajadora tenga, con carácter previo, conocimiento de la instalación de cámaras de videovigilancia, del tratamiento de sus datos y de las concretas finalidades, especialmente, si las imágenes se pueden utilizarse con fines disciplinarios. Así, el deber de información se configuró como parte del contenido esencial del derecho a la protección de datos de carácter personal, de manera que incumplir con ese deber conllevaba vulnerar dicho derecho. Por otro lado, entiendo (y así lo hace parte de la doctrina y el voto particular) que en el año 2016 el TC cambió radicalmente su posición (sin reconocerlo). De este modo, al interpretar el artículo 3 de la Instrucción 1/2006, señaló que se cumplía con el deber de información con la colocación de un distintivo informativo, en un lugar suficientemente visible, de la instalación de cámaras de videovigilancia, sin que hiciese falta informar de sus concretos usos y finalidades. Por ello, para el tribunal lo importante era si los datos se recogían para el mantenimiento, desarrollo o control de la relación laboral. En cuanto a esto último, entiendo que, si bien tuvieron especial incidencia las sospechas previas y que estas eran de un atentado contra la seguridad (una apropiación dineraria), la expresión dada por el TC (mantenimiento, desarrollo o control de la relación laboral) dio pie a que los tribunales pudiesen hacer una interpretación cada vez más expansiva, propiciando que las cámaras de seguridad pudiesen utilizarse para la captación de ilícitos de todo tipo, incluso, para fines disciplinarios no relacionados directamente con la seguridad de las cosas o las personas. De esta forma, creo que vació el contenido el derecho a la protección de datos de carácter personal, pues con un deber de información tan amplio las personas trabajadoras no

podían saber qué usos concretos se les daría a sus imágenes, siendo que este conocimiento forma parte del contenido esencial del derecho.

En cuanto a la interpretación dada por el tribunal de la Instrucción 1/2006, entiendo que es cuestionable, pues su artículo 3 señalaba que debía cumplirse con el deber de información que dictaba la LO 15/1999 y (punto y seguido) se decía que, a tal fin, debería colocarse el correspondiente distintivo. Creo que se podía hacer una interpretación literal de este precepto y que ambos requisitos fuesen cumulativos, conllevado que se exigiese colocar el distintivo y, además, informar de las concretas finalidades que se podían dar a las cámaras.

Con todo, el TC señaló que incumplir con el deber de información no suponía, *per se*, vulnerar el derecho a la protección de datos dado que la medida debía someterse al test de proporcionalidad en cuanto el derecho a la intimidad, por lo que el alto tribunal tuvo especialmente en cuenta la existencia de la sospecha previa de apropiación dineraria. Entiendo que este argumento es discutible, porque un derecho se vulnera o no se vulnera, y si el deber de información forma parte del contenido esencial de dicho derecho, incumplir con el mismo debería conllevar vulnerar el derecho. De esta forma, el TC de facto relegó el deber de información a una cuestión de legalidad ordinaria (y así lo hizo el TS en sus pronunciamientos al indicar que, ante un incumplimiento del deber de información, la persona afectada puede dirigirse ante la AEPD), además de flexibilizarlo hasta tal punto que lo desnaturalizó.

Tres años más tarde, la Gran Sala del TEDH avaló la instalación de cámaras de videovigilancia ocultas en el asunto López Ribalda (II), si bien no libre de polémica, pues dos años antes la Sala de la Sección Tercera consideró que se había vulnerado el derecho a la vida privada de las personas trabajadoras. Así, en la segunda sentencia, el TEDH señaló que, si bien la empresa incumplía con el deber de información, las personas trabajadoras tenían otros medios a su disposición, como acudir a la AEPD. Por tanto, como he comentado *ad supra*, siguió la línea de excluir el deber de información del contenido esencial del derecho. Así, determinó que el incumplir con dicho deber se debía tener en cuenta al someter la medida empresarial al test de proporcionalidad, conllevando que este debía ser más exigente. Si bien es cierto que el TEDH solo estaba valorando si se había vulnerado el derecho a la vida privada, creo que no delimitó bien ambos derechos, de forma que parece que el deber informativo pasa a ser una de las circunstancias a tener en cuenta cuando se valora el derecho a la intimidad, dándose pasos atrás en la delimitación autónoma e independiente de los dos derechos que se han estudiado.

Además, el TEDH señaló que la instalación de cámaras ocultas puede estar legitimada en ciertos casos, siendo que la existencia de sospechas previas de irregularidades puede justificar la medida, siempre atendiendo a la gravedad de aquellas y al grado de intrusión de la medida. Así, el TEDH volvió a tener en cuenta las circunstancias concurrentes (la temporalidad de la medida, la ubicación de las cámaras y la existencia de sospechas previas de irregularidades) y entendió que no fue vulnerado el derecho a la vida privada. Por tanto, se dio un paso más en la pérdida de garantías de las personas trabajadoras, pues avaló las cámaras ocultas.

Entre el caso *Bershka* y la proliferación de casos en los que fuera aplicable la nueva LO 3/2018, el TS se pronunció en diversas ocasiones haciendo uso de la interpretación dada por

el TC y por el TEDH. Así, consolidó la idea de que la colocación del distintivo informativo (en lugar visible) era suficiente para entender que no se vulneraba el derecho a la protección de datos, pues en todo caso había otros medios para denunciar esta cuestión. Aun así, la doctrina distaba de ser meridianamente clara y aun dependía de las circunstancias concurrentes. De este modo, en un pronunciamiento de 2017 el TS entendió que las cámaras instaladas en un supermercado para la seguridad de las cosas y personas no podían ser utilizadas con fines disciplinarios si este fin se desconocía. En cambio, en ese mismo año, avaló que se utilizasen con fines disciplinarios las imágenes captadas por las cámaras que controlaban los accesos de un gimnasio, si bien existían sospechas previas de conductas reprochables y se tuvo en cuenta que años antes se despidió a otra persona trabajadora a partir de la utilización de esas mismas cámaras, interpretando (de forma muy cuestionable) que el trabajador sabía que se podían utilizar con fines disciplinarios. Asimismo, en el año 2021, se valoraron las imágenes captadas, entre otras cosas, durante los tiempos de descanso de un autobusero y, si bien la cuestión no fue abordada por el tribunal, creo que la intimidad de dicho trabajador pudo ser vulnerada. Con todo, como he venido diciendo, nos movíamos en un terreno marcado en gran parte por las circunstancias del caso concreto al que se enfrentaban los tribunales.

V. La incidencia de la LO 3/2018 en la instalación de cámaras de videovigilancia es clara y manifiesta, pues introduce por primera vez disposiciones específicas en el marco de una relación laboral. Así, el artículo 22 dispone que cuando la instalación responde a la seguridad de las cosas, bienes o instalaciones de la empresa, el deber de información se entiende cumplido con la colocación del correspondiente distintivo informativo, recogiendo así la interpretación jurisprudencial del TC en el caso *Bershka* (en relación con el artículo 3 de la instrucción 1/2006).

Asimismo, el artículo 89 introduce como norma general la exigencia de cumplir con el deber de información de manera estricta, por lo que debe informarse de forma previa, expresa, clara y concisa de la medida empresarial. Por tanto, hay que avisar a las personas trabajadoras, con carácter previo, de los concretos fines para los que podrán ser utilizadas las cámaras (incluidos los disciplinarios). Además, sitúa la intimidad como límite explícito a la medida.

A partir de aquí, se excepciona este deber de información amplio cuando se capte la comisión flagrante de un ilícito por parte de las personas empleadas, por lo que dicho deber se entenderá cumplido con la colocación del correspondiente distintivo informativo. Parte de la doctrina considera que debe interpretarse el concepto de ilícito de manera amplia, por lo que se incluirán los delitos penales, las infracciones administrativas y los incumplimientos laborales (si bien hay más dudas respecto a los códigos de conducta o manuales de *compliance*). Cabe señalar que la redacción original del artículo concretaba que debía tratarse de ilícitos penales, pero una enmienda de un grupo parlamentario suprimió el “penales” (sin señalar cuáles fueron las causas).

A partir de aquí, entiendo que el artículo es demasiado genérico y ambiguo, porque no indica cuando ni cuándo debe captarse el ilícito, ni qué tipo de ilícito se entiende incluido. De este modo, si se hace una interpretación expansiva de esta excepción, se permitirá cumplir con el deber de información solo con el correspondiente distintivo en multitud de casos, lo que conlleva que se puede producir una desprotección de las personas trabajadoras. Esto es así porque bastará con que el empresario examine, justificándose en la seguridad de las cosas o

las personas, las grabaciones hasta encontrarse con un incumplimiento laboral (por ejemplo, no cumplir con la jornada), para así ampararse en la excepción y justificar el no cumplimiento del deber de información de forma clara, expresa y concisa. Ciertamente es que un control tan exhaustivo, de demostrarse, no cumpliría con la exigencia de la temporalidad de la medida, pero creo que la interpretación de la norma que se haga debe proporcionar garantías previas y suficientes a las personas trabajadoras. Nada impide, de hecho, que el empresario haga un control desproporcionado, pero teniendo en cuenta la desigualdad de las partes en el contrato laboral, considero que debe exigirse siempre un deber de información amplio (relegando la excepción a casos muy extremos). Si lo que se pretende es que las personas trabajadoras cumplan con las prestaciones del contrato de trabajo, no debería haber problema con que tengan toda la información posible de cuál puede ser el tratamiento de las imágenes que se captan.

Hay que tener en cuenta que hablamos de derechos fundamentales y que las personas no saben cuándo el empresario puede estar examinando las grabaciones ni con qué habitualidad lo hace. Asimismo, si se considera que el derecho a la protección de datos de carácter personal consiste en saber quién trata tus datos, cómo lo hace y con qué fines, el deber de información es, indudablemente, parte de su contenido esencial, y este deber ser amplio, claro y expreso (al menos en la mayoría de los casos). De esta forma, cumplido con el deber de información, deberá examinarse caso a caso cuál ha sido la injerencia que ha tenido la captación de imágenes en la vida privada (intimidad) de las personas porque, como he dicho, no cabe hacer una investigación exhaustiva y desproporcionada, de modo que se deberá tener en cuenta la ubicación de las cámaras, las sospechas previas o la temporalidad de la medida.

Por ello, creo que la excepción debería referirse solo a los ilícitos penales (que atentarían contra la seguridad de las cosas y las personas) y debería concretarse que las sospechas previas deben ser anteriores (al visualizado de las cámaras) y fundadas, siendo que el empresario debe probar cuáles eran los indicios de dichos ilícitos, por ejemplo, que de forma reiterada la contabilidad de una caja no cuadrara. Asimismo, creo que debería modificarse el precepto y tener en cuenta cuál puede ser la consecuencia del hallazgo casual.

Por último, el precepto deja claro que en los lugares dedicados al descanso, al esparcimiento de trabajadores, baños, vestuarios y análogos, queda totalmente prohibida la videovigilancia. De este modo, ante un caso concreto, sí que es cierto que hay ciertas cosas que están claras, como la prohibición de cámaras en lugares de esparcimiento y descanso; que es válida la simple pegatina que informe sobre cámaras para la vigilancia de las cosas o las personas; y, a fin de cuentas, si el empresario no quiere tener problemas, lo más práctico es informar de los concretos usos que se darán a las cámaras en caso de que estas sirvan para el control laboral.

VI. En la primera sentencia que aplicó la nueva normativa, la opinión mayoritaria del TC, compuesta por siete magistrados (de doce), siguió la doctrina recaída en el caso *Bershka* y asunto López Ribalda (II), por lo que ante la existencia de meras sospechas de un incumplimiento contractual que atentaba contra la seguridad de las cosas, se permitió la visualización de las cámaras de vigilancia con fines disciplinarios, siendo que se entendió cumplido el deber de información con el correspondiente distintivo al ampararse la medida

empresarial en la excepción que vengo comentando. Personalmente creo que la doctrina del voto particular es la más correcta y la más garantista, pues las meras sospechas de un incumplimiento laboral justificaron que el TC avalase que se pudiesen visualizar las cámaras y descubrir el ilícito. Hay que recordar que la única evidencia era que se había encontrado una bolsa de la empresa con productos de la competencia. Así, en línea con el voto particular, creo que la regla general del deber de información del artículo 89.1 de la LO 3/2018 operará en pocos casos, pues las empresas se ampararán en la existencia de sospechas previas para analizar las imágenes captadas y que estas tengan consecuencias disciplinarias ante el desconocimiento de las personas trabajadoras. Con todo, creo que la posición de los magistrados está muy ajustada, cinco votos a siete, por lo que en el futuro podría cambiar la interpretación dada. En todo caso, es evidente que es una cuestión que admite interpretaciones y que la nueva normativa, si bien despeja algunas dudas, deja grandes vacíos que los tribunales deberán colmar.

Por lo que se refiere a las cámaras ocultas, la STS 692/2022, de 22 de julio, las avala en un supuesto muy excepcional, pero eso no quita que entienda que no se vulneran derechos fundamentales. Considero que no deberían permitirse este tipo de cámaras de acuerdo con la nueva normativa, pues dicho supuesto no está contemplado, además de que se establece como regla general el deber de información en sentido amplio. Por ello, creo que se puede entender que esta sentencia aumenta la inseguridad jurídica y puede dar pie a que los empleadores hagan uso de estas cámaras en la creencia de que, quizás, los tribunales las avalaran según las circunstancias concurrentes, por lo que dicha sentencia no tiene, a mi entender, efectos disuasorios.

7. BIBLIOGRAFÍA

ÁLVAREZ HERNANDO, J. (2014). *Practicum Protección de Datos 2015*. Editorial Aranzadi, S.A.U.

ARANZADI THOMSON REUTERS (2020). *Practicum Social 2020*, Editorial Aranzadi, S.A.U.

DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B. (2011). “Protección de datos y contrato de trabajo”. *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social*, 46/2011, 13-66.

DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B (2012). *Control informático, videovigilancia y protección de datos*. Lex Nova.

- FERNÁNDEZ ORRICO, F.J. (2019). "Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre". *Revista Española de Derecho del Trabajo*, 222/2019, 31-76.
- FERRER SERRANO, R.L (2017). "Videovigilancia e información personal de los trabajadores. A propósito de los criterios fijados por la sentencia del Tribunal Constitucional de fecha 3 de marzo de 2016 y su reciente recepción jurisprudencial". *Revista de Información Laboral*, 12/2017, 51-65.
- GARCÍA SALAS, A.I. (2018). "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018". *Revista de Información Laboral*, 2/2018, 117-147.
- GARCÍA-NÚÑEZ SERRANO, F. (2000). "La regulación sobre protección de datos personales y su incidencia en el ámbito laboral". *Revista Doctrinal Aranzadi Social*, 21/2000, 1105-1118.
- GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I.A. (2019). "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo". *Revista Española de Derecho del Trabajo*, 216/2019, 19-64.
- GUDE FERNÁNDEZ, A. (2014). "La videovigilancia en el ámbito laboral y el derecho a la intimidad". *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 35/2014, 109-134.
- LUIS GOÑI SEIN, J. (2016). "Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información previa". *AIS: Ars Iuris Salmanticensis*, 4 (2), 288-291.
- GORDO GONZALEZ, L. (2018). "El Derecho del Trabajo 2.0: la necesidad de actualizar el marco de las relaciones laborales a las nuevas tecnologías". *Revista de Información Laboral*, 12/2017, 171-182.
- GONZÁLEZ GONZÁLEZ, C. (2016). "Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016". *Revista Aranzadi Doctrinal*, 5/2016, 129-148.
- GONZÁLEZ GONZÁLEZ, C. (2018). "Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales". *Aranzadi digital*, 1/2018, 1-48.
- GONZÁLEZ MARTÍNEZ, J.A (2021). "La videovigilancia empresarial en la industria 4.0: la salvaguarda de la intimidad informática del trabajador". *Revista Aranzadi Doctrinal*, 10/2021.

HENRÍQUEZ TILLERÍA, S. (2019). "Protección de datos, videovigilancia laboral y doctrina de la sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información". *Iuslabor*, 3/2019, 55-80.

POQUET CATALÁ, R. (2022). "Poder de control empresarial a través de sistemas de videovigilancia: alcance y límites". *Revista Aranzadi Doctrinal*, 5/2022, 105-126.

QUÍLEZ MORENO, J.M. (2019). "La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores". *Revista Española de Derecho del Trabajo*, 217/2019, 127-152.

SALA FRANCO, T. (1999). El derecho a la intimidad y a la propia imagen. En E. Borrajo Dacruz (coord.), *Trabajo y libertades públicas* (p.201-230). Wolters Kluwer España.

TASCÓN LÓPEZ, R. (2005). *EL TRATAMIENTO POR LA EMPRESA DE DATOS PERSONALES DE LOS TRABAJADORES: ANÁLISIS DEL ESTADO DE LA CUESTIÓN*. Civitas.

TASCÓN LÓPEZ, R. (2005) "El tratamiento por la empresa de los datos personales de los trabajadores ¿un problema resuelto o caído en el olvido?". *Revista Doctrinal Aranzadi Social*, 16/2005, 10-52.

TERRADILLOS ORMAETXEA, E. (2004). *El poder disciplinario empresarial. Principios y Garantías*. Tirant lo Blanch.

ZARAGOZA TEJADA, J.I. (2020). "La prueba obtenida por videocámaras de seguridad tras la STEDH del 17 de octubre del 2019. Caso López Ribalda vs España". *Revista Aranzadi Doctrinal*, 2/2020, 32-51.

8. ANEXO JURISPRUDENCIAL

8.1 Tribunal Europeo de Derechos Humanos

STEDH Asunto López Ribalda y otros contra España (demandas nº 1874/13 y 8567/13) de 17 de octubre de 2019.

8.2 Tribunal Constitucional

STC 11/1981, de 8 de abril de 1981.

STC 88/1985, de 19 de julio de 1985.

STC 99/1994, de 11 de abril de 1994.

STC 106/1996, de 12 de junio de 1996.

STC 98/2000, de 10 de abril del 2000.

STC 186/2000, de 10 de julio del 2000.

STC 292/2000, de 30 de noviembre del 2000.

STC 29/2013, de 11 de febrero de 2013.

STC 39/2016, de 3 de marzo de 2016.

STC 119/2022, de 29 de setiembre 2022.

8.3 Tribunal Supremo

STS 630/2016, de 7 de julio de 2016.

STS 77/2017, de 31 de enero de 2017.

STS 86/2017, 1 de febrero de 2017.

STS 96/2017, de 2 de febrero de 2017.

STS 817/2021, de 21 de julio de 2021.

STS 1003/2021, de 13 de octubre de 2021.

STS 692/2022, de 22 de julio de 2022.