

FACULTAD
DE CIENCIAS
JURÍDICAS



ZIENTZIA
JURIDIKOEN
FAKULTATEA

TRABAJO FIN DE ESTUDIOS / IKASGAIEN AMAIERAKO LANA
GRADO EN RELACIONES LABORALES Y RECURSOS HUMANOS

.....

**LA VIDEOVIGILANCIA COMO INSTRUMENTO DE CONTROL EN LAS
RELACIONES LABORALES.**

Fátima Ouahhadi Escudero

DIRECTOR / ZUZENDARIA

Julen Llorens Espada

Pamplona / Iruñea

14 de junio de 2020

Resumen

Las facultades de verificación y control empresarial mediante sistemas de videovigilancia en el ámbito de las relaciones laborales han suscitado grandes debates en relación con su posible incidencia en los derechos fundamentales de los trabajadores.

Este tema ha sido abordado en varias ocasiones por el Tribunal Constitucional, así como por el Tribunal Europeo de Derechos Humanos; con el objetivo de delimitar cuáles son las consideraciones que deben atenderse en materia de videovigilancia dentro del ámbito que nos ocupa. De esta manera, en el presente estudio se analiza la doctrina judicial más relevante en la materia, desde la perspectiva de la salvaguarda de los derechos fundamentales y, concretamente el derecho a la protección de datos.

Palabras clave

Videovigilancia, control, protección de datos, intimidad, privacidad.

Abstract

The faculty of verification and business control by systems of video vigilance in the labour relationships area, have provoked huge debates regarding their possible influence in fundamental human rights of workers.

This matter has been tackled in several occasions by Constitutional Court, such as the European Court of Human Rights; With the aim of delimit which are the considerations that must be attended to in matters of video vigilance in the area which spend us. In this way, in this study is analysed the most relevant judicial doctrine in this area, since the perspective of protect the fundamental human rights and specifically the right of the protection of data.

Key word

Video vigilance, control, protection of data, privacy.

Índice de abreviaturas:

AEPD	Agencia Española de Protección de Datos.
Art./ Arts.	Artículo/ Artículos.
CE	Constitución Española de 1978, Cortes Generales «BOE» núm. 311, de 29 de diciembre de 1978.
CEDH	Resolución de 5 de abril de 1999, de la Secretaría General Técnica, por la que se hacen públicos los textos refundidos del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983.
ET/ LET	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.
FJ	Fundamento Jurídico.
LO	Ley Orgánica.
LOPD	Ley Orgánica de Protección de Datos.
LOPDPGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.
Núm.	Número.
Rec.	Recurso.
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y el consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
STC/ SSTC	Sentencia del Tribunal Constitucional/ Sentencias del Tribunal Constitucional.
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos.
STS/ SSTS	Sentencia del Tribunal Supremo/ Sentencias del Tribunal Supremo.
STSJ	Sentencia del Tribunal Superior de Justicia.

TC	Tribunal Constitucional.
TEDH	Tribunal Europeo de Derechos Humanos.
TS	Tribunal Supremo.
TSJ	Tribunal Superior de Justicia.
UE	Unión Europea

Índice

1. MARCO GENERAL DE LA VIDEOVIGILANCIA EN LAS RELACIONES LABORALES.....	1
1.1. Retos, peligros y virtudes de la videovigilancia	1
1.2. El derecho a la intimidad ante la videovigilancia	5
1.3. La privacidad ante la videovigilancia	8
1.4. El derecho a la protección de datos ante la videovigilancia	11
2. PONDERACIÓN DE DERECHOS CONSTITUCIONALES.....	17
2.1. El Triple Test de Proporcionalidad.	17
2.2. El Test Barbulescu.	18
3. EVOLUCIÓN DOCTRINAL EN MATERIA DE VIDEOVIGILANCIA EN LAS RELACIONES LABORALES.....	20
3.1. Precedentes jurisprudenciales tendentes a permisibilidad de control y vigilancia empresarial.	20
3.2. Rectificación de doctrina y aplicación del principio de proporcionalidad: las SSTC 98/2000 y 186/2000.	21
3.3. Introducción doctrinal del derecho a la protección de datos personales como límite a las facultades de control y vigilancia empresarial y a la videovigilancia.	24
3.4. La STC 29/2013 y el nivel de exigencia informativo en la videovigilancia en el ámbito laboral.	27
3.5. La STC 39/2016 y la flexibilización del principio de transparencia.	30
3.6. Barbulescu II.	33
3.7. López Ribalda II.	36
4. CONCLUSIONES.....	42
5. BIBLIOGRAFÍA CONSULTADA.....	45
6. JURISPRUDENCIA CONSULTADA.....	49
STEDH Barthold vs Alemania, de 25 de marzo de 1985.....	49

1. MARCO GENERAL DE LA VIDEOVIGILANCIA EN LAS RELACIONES LABORALES

1.1. Retos, peligros y virtudes de la videovigilancia

La evolución tecnológica ocurrida en las últimas décadas ha supuesto una auténtica revolución en las diferentes esferas que componen la sociedad.

Estos avances se han implantado en la cotidianidad, que ha visto como la tecnología se ponía al servicio de los particulares, así como de las entidades públicas y privadas; permitiendo que utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades”¹.

En definitiva, se puede afirmar que “la digitalización constituye una ‘nueva forma de vivir, de trabajar y de relacionarse que ofrece enormes oportunidades de progreso, de mejoras económicas y de beneficios sociales”².

Sin embargo, aunque es cierto que esta realidad conlleva innumerables ventajas para los usuarios; también deriva en una serie de inconvenientes que deben ser valorados a fin de acotar los escenarios donde va a desarrollarse, con el objetivo de minimizar en la medida de lo posible la inseguridad jurídica que pueda conllevar su rápido desarrollo.

En el ámbito de las relaciones laborales también ha tenido una gran incidencia, donde los dispositivos digitales se han impuesto por las ventajas que presentan en relación con una eficaz gestión de la actividad productiva.

Entre las facultades que normativamente³ se le conceden al empleador, se encuentra la posibilidad de adoptar las medidas que estime más oportunas en relación con la vigilancia y control de la actividad productiva, con el objetivo de verificar el

¹REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

² CEOE. *Plan Digital 2020 - La digitalización de la sociedad española*, 2016.

³ El artículo 20 de la Ley del Estatuto de los Trabajadores indica en su tercer apartado 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 adopción y aplicación la consideración debida a su dignidad.

cumplimiento de las obligaciones contractuales; siempre y cuando estas medidas no deriven en una vulneración de la dignidad del trabajador⁴.

Por tanto, “se reconoce al empresario la posibilidad de adoptar las medidas que estime oportunas de vigilancia y control, pero no ya ante circunstancias especiales, sino para realizar la mera comprobación ordinaria de que el trabajador cumple con sus obligaciones laborales o, según reza el precepto, ‘para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales’”⁵.

Esta potestad se ha visto favorecida por el creciente desarrollo de la tecnología disponible, pues posibilita que se instalen sistemas de videovigilancia en el ámbito de la empresa con la argumentación defensiva basada en la “detección y verificación de la realización por parte del trabajador o de terceros (usuarios, clientes, etc.) de una conducta ilícita o de prevención de delitos”⁶.

La instalación de un sistema de videovigilancia se justifica, por lo tanto, en ese contexto de seguridad y protección de personas y bienes; sin embargo, tiene un alcance mucho mayor del que, a priori, pueda o pudiera preverse, “provocando una disrupción notable en los modelos de negocio y comportando nuevos retos para la protección de los derechos fundamentales de los trabajadores”⁷.

Los sistemas tecnológicos de videovigilancia, mediante la captación de imagen y sonido, suponen grandes ventajas en relación con la verificación que habitualmente se realizaba mediante la observancia de la actividad laboral por personal específico, por lo que resulta indudable que esta herramienta conlleva una reducción del coste que implicaba la vigilancia tradicional. Actualmente es posible vigilar un área más amplia, de una manera ininterrumpida, permitiendo un control más intenso.

⁴ Así mismo, el artículo 20.bis del ET recoge como límite a la potestad de control y verificación empresarial el derecho a la intimidad del trabajador frente al uso de dispositivos de videovigilancia.

⁵ MIÑARRO YANINI, M. “Impacto del reglamento comunitario de protección de datos en las relaciones laborales. Un –pretendido– ‘cambio cultural’”, en *Revista mensual núm. 423, CEF – Trabajo y Seguridad Social*. ISSN: 1138 – 9532, 2018. Pág. 7.

⁶ GOÑI SEIN, J.L. “El poder del ojo mecánico y la determinación de los límites de la libertad de vigilancia empresarial”, en *Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, 2007. Pág. 16.

⁷ GOÑI SEIN, J.L. “Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del reglamento europeo de protección de datos de 2016”, En *Revista de derecho social*, ISSN 1138-8692. Núm 78, 2017. Págs. 15 – 42.

Este medio, por lo tanto, permite una mayor precisión a la hora de identificar actos ilícitos; siendo además un medio probatorio muy eficaz ya que permite el mantenimiento, conservación y recuperación de imágenes y sonidos; permitiendo acreditar el incumplimiento de sus obligaciones laborales por el trabajador en el proceso laboral⁸.

Así mismo, diferentes autores defienden que la mera instalación de un sistema de videovigilancia constituye un medio disuasorio de conductas contrarias a lo que se entiende como un comportamiento diligente en los trabajadores.

Sin embargo, aunque la finalidad sea la única y exclusiva constatación de que se están cumpliendo las obligaciones contractuales por parte de los trabajadores filmados, la salvaguarda de los bienes patrimoniales o la voluntad de disuadir a los empleados de cometer actos ilícitos; las grabaciones permiten captar aspectos relativos a su comportamiento y esfera privada, limitando así su libertad.

Esta situación, en consecuencia, conlleva una mayor desprotección para los trabajadores; puesto que, como advierte Goñi Sein, este escenario puede contribuir a que “su privacidad quede tremendamente atenuada o que prácticamente no haya espacio alguno para la libertad, (...) de tal manera que el empresario termine por adueñarse por entero del comportamiento de las personas en el lugar de trabajo”⁹.

El efecto de la revolución tecnológica, en definitiva, repercute en el desvanecimiento de los límites que permiten la conceptualización de la vida privada del trabajador en el contexto de la actividad profesional, en la medida en que los nuevos sistemas tecnológicos posibilitan una vigilancia continua mientras dura la prestación y a veces después, lo que hace que el trabajador caiga en un estado de visibilidad permanente¹⁰.

⁸ GOÑI SEIN, J.L. “Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del reglamento europeo de protección de datos de 2016”, En *Revista de derecho social*, ISSN 1138-8692. Núm 78, 2017. Págs. 15 – 42.

⁹ GOÑI SEIN, J.L. “El poder del ojo mecánico y la determinación de los límites de la libertad de vigilancia empresarial”, en *Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, 2007. Pág. 18.

¹⁰ MERCADER UGUINA, J., “Les libertés individuelles dans l’entreprise à l’épreuve des nouvelles technologies. Observations à partir de la situation espagnole”, AA. VV. (Dir. AUVERGNON, Ph.) *Les libertés individuelles et relations de travail: le possible, le permis et l’interdit*. Presses Universitaires de Bordeaux, 2011, p. 148; COELHO MOREIRA, T., “A privacidade dos trabalhadores e a utilização de redes sociais online: algumas questões”, *Questões Laborais*. Núm. 41, 2013. Pág. 46.

Rodríguez Escanciano, expresó que “el ojo mecánico contribuye de esta manera a la gobernabilidad, al control social de los trabajadores, ampliando la esfera de poder del empresario”¹¹.

En este contexto, la videovigilancia incide en el núcleo más sagrado de la vida privada, ya sea de manera indirecta o de manera directa con total intencionalidad¹². De modo que es preciso valorar las posibles consecuencias que pueda ocasionar esta revolución tecnológica, y en concreto la videovigilancia, en relación con su incidencia en la vida privada de los trabajadores; ya que no cabe asumir que el empresario quede “apoderado para llevar a cabo, so pretexto de las facultades de vigilancia y control que le confiere el art. 20.3 ET, intromisiones ilegítimas en la intimidad de sus empleados en los centros de trabajo”¹³.

Es por eso por lo que la legislación vigente debe garantizar que la aplicación de estas nuevas herramientas en el ámbito de la esfera laboral no suponga una vulneración de los derechos reconocidos a los ciudadanos, aun cuando existe relación de dependencia profesional; pues no cabe olvidar que “la tecnología debe convivir con los valores democráticos y el respeto a los derechos fundamentales de la persona”¹⁴, “por lo que resulta imprescindible establecer límites y garantías para salvaguardar los derechos de los trabajadores”¹⁵.

Con ese fin, se procede a realizar un análisis de cuales son los derechos fundamentales individuales de los trabajadores que puedan verse afectados por la instalación de sistemas de videovigilancia en el centro de trabajo; así como de los

¹¹ RODRIGUEZ ESCANCIANO, S. “Vigilancia y control en la relación de trabajo: la incidencia de las nuevas tecnologías”, en *La protección de datos de carácter personal en los centros de trabajo*, F. Largo Caballero, CLI – CINCA, Madrid, 2006. Pág. 88.

¹² GOÑI SEIN, J.L. “Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del reglamento europeo de protección de datos de 2016”, En *Revista de derecho social*, ISSN 1138-8692. Núm 78, 2017. Págs. 15 y ss.

¹³ GONZALEZ GONZALEZ, C. “Control empresarial de la actividad laboral mediante video vigilancia y colisión con los derechos fundamentales del trabajador. Novedades del Proyecto de la Ley Orgánica de protección de datos y derechos digitales” en *Revista Aranzadi Doctrinal*, ISSN 1889-4380, Núm. 4, 2019. Pág. 7

¹⁴ GOÑI SEIN, J.L. “El poder del ojo mecánico y la determinación de los límites de la libertad de vigilancia empresarial”, en *Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, 2007. Pág. 20.

¹⁵ VILLALBA CANO, L. *La videovigilancia laboral y su incidencia en el derecho de protección de datos a la luz de la jurisprudencia constitucional y del reglamento europeo 2016/679*; en FODERTICS 7.0 Estudios sobre derecho digital, BUENO DE MATA, F. (DIR), Editorial Comares, ISBN: 9788490457658, 2019. Pág. 206.

derechos constitucionales en los que se justifica la facultad de vigilancia y control empresarial.

Una vez identificados los derechos afectos resulta imprescindible ponderarlos y determinar en qué situaciones estos pueden verse limitados o modulados para ceder ante otros bienes jurídicos protegidos.

1.2.El derecho a la intimidad ante la videovigilancia

El derecho a la intimidad se encuentra recogido en la Sección 1ª del Capítulo II del Título I de la Constitución Española de 1978 (CE), concretamente, en el artículo 18.1 CE, que establece:

“1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”¹⁶.

A pesar de que se contemplen tres derechos en un mismo artículo, no deben entenderse como un mismo derecho o facetas de este; pues cada uno de ellos es autónomo e independiente, con contenido y entidad propia; y todos ellos forman parte de los denominados *derechos de la personalidad*¹⁷.

Los derechos de la personalidad, y, en consecuencia, el derecho a la intimidad personal, se configuran como derechos irrenunciables, inalienables e imprescriptibles. Estos derechos son inherentes a la dignidad humana¹⁸, por lo que todas las personas son titulares de derecho por el simple hecho de serlo.

El derecho a la intimidad, sin embargo, no se encuentra específicamente definido en la normativa vigente; por lo que es preciso realizar un análisis doctrinal a fin de entender qué comprende.

La sentencia del Tribunal Constitucional 156/2001, de 26 de julio – entre otras –, en su fundamento jurídico cuarto, delimita el concepto vinculándolo a la personalidad y afirmando que deriva de la dignidad de la persona humana. El Tribunal, además, establece

¹⁶ Constitución Española de 1978, Cortes Generales «BOE» núm. 311, de 29 de diciembre de 1978.

¹⁷ SERVICIO DE ESTUDIOS DEL PARLAMENTO EUROPEO, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado. España*, en Unidad de Biblioteca de Derecho Comparado. Octubre, 2018. Pág. 29.

¹⁸ El artículo art. 10.1 de Constitución Española de 1978 establece que:

“La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social”.

que la intimidad personal constitucionalmente garantizada en el artículo 18.1 CE, entraña la existencia de “un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario – según las pautas de nuestra cultura – para mantener una calidad mínima de vida humana”¹⁹.

El TC también aclaró esta cuestión aseverando que “lo que el art. 18.1 CE garantiza es el secreto sobre nuestra propia esfera de vida personal y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los contornos de nuestra vida privada”²⁰.

Por lo tanto, es posible afirmar que el derecho a la intimidad implica la potestad individual para determinar qué aspectos se desean compartir y cuales se prefieren reservar de conocimiento ajeno en las diferentes esferas que componen la vida del individuo.

De igual modo, diferentes autores y entidades han intentado aportar claridad a la conceptualización de este derecho. Entre ellos Valdés de la Vega, afirma que “el derecho a la intimidad tiene que ver, en su aspecto externo, con un espacio en el cual la persona deposita sus elementos privados, un espacio en el cual desarrolla su esfera privada”²¹.

Por su parte, Carrillo, delimita su conceptualización como “el derecho del ciudadano no sólo a reservarse una esfera de la vida propia como secreta e intangible a los demás, sino también a ostentar la capacidad para evitar su manipulación o instrumentalización [...]. Actualmente, la intimidad más que un derecho a no ser molestado (que persiste) es un derecho de participación y control de las informaciones que afecten a la persona y sobre los que el interesado está legitimado para incidir en la forma y contenido de su divulgación, ámbito éste en el que se suelen producir un gran porcentaje de las intromisiones ilegítimas”²².

En la misma línea, el Servicio de Estudios del Parlamento Europeo declara que este derecho tiene una vertiente negativa que faculta al titular de derecho a excluir a

¹⁹ SSTC 156/2001, de 2 de julio de 2001. Rec. 4641/98. FJ 4; 57/1994, de 28 de febrero de 1994. Rec. 1.445/91 FJ 5; 143/1994, de 9 de mayo de 1994. Rec. 3.192/1992 FJ 6; 179/1991, de 19 de septiembre de 1991. Rec. 184/1989 FJ 3; y 231/1988, de 23 de diciembre de 1988. Rec. 1.247/1986 FJ 3.

²⁰ STC 176/2013, de 21 de octubre de 2013. Rec. 1.783/2010 FJ 7.

²¹ VALDÉS DE LA VEGA, B.: “El derecho a la intimidad y su expectativa de respeto en el uso personal de las tecnologías de la información y comunicación en el trabajo. Un comentario a la sentencia del Tribunal Supremo de 26 de septiembre de 2007 y a la doctrina del Tribunal Europeo de Derechos Humanos”, en *Revista de Derecho Social*, núm.42, 2008. Pág. 145.

²² CARRILLO, M. *Los límites a la libertad de prensa en la constitución española de 1978*, Barcelona, 1987. SBN 13: 9788476650400. Pág. 58.

terceros de cualquier intromisión ilegítima, y una vertiente positiva que “se concreta en la potestad de su titular para ejercer un poder soberano sobre su vida privada, que impide que los terceros puedan revelar, divulgar o, en suma, servirse de su intimidad sin consentimiento o autorización de aquél; y ello con independencia de que se haya accedido a la privacidad ajena de manera legítima”²³.

Por lo tanto, el derecho a la intimidad personal abarca tanto la potestad para excluir a terceros de cualquier intromisión ilegítima; así como la facultad para decidir y controlar quien dispone de información relativa a su persona, el alcance de su contenido y su posible divulgación.

Tras analizar las posibles implicaciones del contenido de este derecho fundamental, es posible afirmar que el derecho a la intimidad no se encuentra excluido del ámbito de las relaciones laborales donde, el “efecto de la revolución digital estriba en el desvanecimiento de las fronteras entre la actividad profesional y la vida privada del trabajador”²⁴.

En consecuencia, este derecho también se encuentra “garantizado” en la Ley del Estatuto de los Trabajadores²⁵, en el artículo 4.2.e), donde se delimitan sus derechos básicos²⁶; determinándose, además, en el artículo 20.bis el derecho de los trabajadores a la intimidad frente al uso de dispositivos de videovigilancia. De igual modo, el artículo 18 ET precisa el escenario en que pueden realizarse registros sobre la persona del trabajador, concretando que debe atenderse a la posibilidad de asistencia de un representante legal y otorgando especial relevancia al respeto máximo de la dignidad e intimidad del trabajador. Así mismo, la infracción de este derecho se encuentra tipificado legalmente, correspondiendo la consideración de muy graves a los “actos del empresario

²³ Servicio de Estudios del Parlamento Europeo, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado. España*, en Unidad de Biblioteca de Derecho Comparado. Octubre, 2018. Pág. 30

²⁴ RODRÍGUEZ-PIÑERO ROYO, M., *Las nuevas tecnologías en la empresa*, Consejo de Relaciones Laborales, Sevilla, 2006. Pág. 14.

²⁵ 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.

²⁶ El apartado segundo, letra e), de este artículo establece que los trabajadores tendrán derecho al “respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo”.

que fueren contrarios al respeto a la intimidad y consideración debida a la dignidad del trabajador”²⁷.

Este derecho, sin embargo, no es un derecho absoluto; “pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el límite que aquel haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho”²⁸.

1.3.La privacidad ante la videovigilancia

Otro de los bienes jurídicos que pueden verse afectados a raíz de la instalación de videovigilancia en el ámbito empresarial, es el derecho a la privacidad, que también se encuentra regulado en el artículo 18 CE anteriormente mencionado.

En su apartado cuarto, establece:

“La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”²⁹.

De esta definición se desprende un estrecho vínculo entre el derecho a intimidad, el derecho a la privacidad y el derecho a la protección de datos y al secreto en las comunicaciones.

En primer lugar, es preciso recordar que en el segundo apartado del artículo 10 CE³⁰ se señala que las normas relativas a los derechos fundamentales y a las libertades públicas contenidas en la Carta Magna deben interpretarse de conformidad a lo establecido en la Declaración Universal de Derechos Humanos, los Tratados y acuerdos internacionales ratificados por España.

En consecuencia, es ineludible hacer referencia a la Declaración Universal de Derechos Humanos³¹ para tratar de comprender el alcance de este derecho. En el artículo 12 del documento, se especifica que “nadie será objeto de injerencias arbitrarias en su

²⁷ Artículo 8.11 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social.

²⁸ STC 57/1994, 28 de febrero de 1994 .Rec. 2302/1990.

²⁹ Constitución Española de 1978, Cortes Generales «BOE» núm. 311, de 29 de diciembre de 1978.

³⁰ Constitución Española de 1978, Cortes Generales «BOE» núm. 311, de 29 de diciembre de 1978.

³¹Declaración Universal de Derechos Humanos. Adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948.

vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

La Carta de Derechos Fundamentales de la Unión Europea³² – en su séptimo artículo – así como el Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales³³ – en el primer apartado de su octavo artículo –, también reconocen este derecho, indicando que “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”³⁴.

El derecho a la vida privada, por lo tanto, tiene un alcance superior al que puede derivar del derecho a la intimidad. Los aspectos que comprende el derecho a la vida privada pueden no tener excesiva relevancia al observarse de manera independiente; sin embargo, si se valoran en conjunto podrían dar información vital para el sujeto, pudiendo incluso configurar el perfil completo del individuo.

El Tribunal Europeo de Derechos Humanos determina que la noción de vida privada incluye el derecho a establecer y desarrollar relaciones con otros seres humanos, y el derecho a la identidad y al desarrollo personal³⁵. Así mismo, recuerda que el concepto de privacidad “incluye los elementos de identificación de la persona”³⁶; no limitándose al círculo íntimo y englobando el derecho a “llevar una ‘vida privada social’, es decir, la posibilidad de que una persona se vincule y desarrolle relaciones con sus semejantes y con el mundo exterior”³⁷, existiendo además una zona de interacción entre los individuos que, incluso estando en un contexto público, puede pertenecer a la vida privada³⁸.

El Tribunal de Estrasburgo defiende que el derecho al respeto de la vida privada no comprende únicamente facultades de exclusión frente al conocimiento y difusión de

³² Carta de Derechos Fundamentales de la Unión Europea 2010/C 83/02.

³³ BOE» núm. 108, de 6 de mayo de 1999. Resolución de 5 de abril de 1999, de la Secretaría General Técnica, por la que se hacen públicos los textos refundidos del Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983.

³⁴ El artículo 8.1 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, de 1950; así como el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966; consagraron el reconocimiento del derecho a la intimidad como derecho fundamental en el ámbito internacional.

³⁵ Fernández Martínez vs España, STEDH de 12 de junio de 2014.

³⁶ Von Hannover vs Alemania, STEDH de 7 de febrero de 2012.

³⁷ Barbulescu vs Rumania, STEDH de 5 de septiembre de 2017.

³⁸ Von Hannover vs Alemania, STEDH de 7 de febrero de 2012.

datos relativos a la vida íntima³⁹, sino también obligaciones a cargo del Estado a fin de garantizar el efectivo respeto de la vida privada, incluso en las relaciones entre particulares⁴⁰.

Así mismo, se ha considerado relevante mencionar un aspecto importante en relación con la efectividad en la protección de estos derechos en el ámbito laboral, atendiendo a lo que la jurisprudencia ha conceptualizado como *expectativa razonable de privacidad*.

Ésta podría darse, según ha señalado el Tribunal Constitucional, cuando el interesado, o cualquier otra persona encontrándose en las mismas circunstancias, puede albergar expectativas razonables “de encontrarse al resguardo de la observación o del escrutinio ajeno. Así por ejemplo cuando se encuentra en un paraje inaccesible o en un lugar solitario debido a la hora del día, puede conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores. Por el contrario, no pueden abrigarse expectativas razonables al respecto cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean, claramente pueden ser objeto de registro o de información pública”⁴¹.

Por lo tanto, aunque puede darse en diferentes esferas, quizás pueda resultar más identificable tal intromisión a la intimidad cuando esta se produce en lugares excluidos de publicidad, como el ámbito doméstico o privado. Sin embargo, como se ha indicado, el ámbito de protección del derecho a la intimidad “trasciende el círculo íntimo en el que el individuo puede desarrollar su actividad personal y excluir plenamente a terceros”⁴², por lo que resulta ineludible determinar cuando puede albergarse tal expectativa de privacidad en el ámbito de las relaciones laborales.

En este sentido, el máximo intérprete de la Constitución⁴³ dictamina que basta con que el empresario, de acuerdo con las exigencias de buena fe, prohíba expresamente – ya sea de manera absoluta o parcial – aquellas conductas que considere que exceden de

³⁹ Barthold vs Alemania, STEDH de 25 de marzo de 1985

⁴⁰ SERRANO OLIVARES, R., “El derecho a la intimidad como derecho de autonomía personal en la relación laboral”, en *Civitas. Revista española de derecho del trabajo*, núm. 103, 2001. ISSN 0212-6095. Pág. 108.

⁴¹ STC 12/2012, de 30 de enero de 2012. Rec. 4829/2009.

⁴² Servicio de Estudios del Parlamento Europeo, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado. España*. En Unidad de Biblioteca de Derecho Comparado. Octubre, 2018. Pág. 30 y ss.

⁴³ STC 241/2012, de 17 de diciembre de 2012. Rec. 7304/2007.

lo que considera un comportamiento diligente por parte de los trabajadores; pues estableciendo las reglas de uso de los medios proporcionados no cabe albergar expectativa razonable de privacidad y, como sentencia el TC, si no existe tal expectativa no puede entenderse lesionado el derecho a la intimidad.

Sin embargo, según señala Baz Rodríguez⁴⁴, la tolerancia generalizada de ciertas actuaciones en el lugar de trabajo genera una expectativa para el trabajador. Por lo que resulta necesario imponer a la empresa un deber informativo hacia los trabajadores acerca de la existencia del control empresarial, así como de los medios utilizados.

1.4. El derecho a la protección de datos ante la videovigilancia

Actualmente, “la obtención, conservación y tratamiento de datos personales cobra una especial relevancia en el seno de la relación laboral”⁴⁵.

Las organizaciones empresariales cuentan con grandes cantidades de información relativa al personal que tienen contratado, como pueden ser los datos de carácter personal referidos a la situación familiar o económica de los trabajadores.

Una eficaz gestión de la plantilla, así como de la actividad productiva, hace necesaria la obtención y la conservación de datos que, de no asegurar un tratamiento basado en las exigencias normativas, supondría un grave riesgo en cuanto a la vulneración de los derechos de los trabajadores.

Es por ello que, “en lo relativo al derecho de protección de datos, resulta patente la dificultad de conciliar las distintas facultades y derechos que la normativa sobre la materia atribuye a los titulares de los datos personales, con los intereses del empresario, ya que en ocasiones estos pueden ir en detrimento de aquéllos”⁴⁶.

⁴⁴ BAZ RODRÍGUEZ, J.: “Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre [BOE n. o 267, de 7-XI-2013]”, en *Revista Ars Iuris Salmanticensis*, Vol. 2, núm. 1, 2014. Pág. 365.

⁴⁵ VALVERDE ASENSIO, A.J., “Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores”, en *Revista andaluza de trabajo y bienestar social*, núm. 119, 2013. Pág. 14.

⁴⁶ VILLALBA CANO, L. “Jurisprudencia constitucional. La contradicción entre las SSTC 29/2013, de 11 de febrero y 39/2016, de 3 de marzo”, en FODERTICS 7.0 Estudios sobre derecho digital, BUENO DE MATA, F. (DIR); en *La videovigilancia laboral y su incidencia en el derecho de protección de datos a la luz de la jurisprudencia constitucional y del reglamento europeo 2016/679*, Editorial Comares, ISBN: 9788490457658, 2019. Pág. 206.

El artículo 18.4 CE delimita el derecho a la autodeterminación informativa⁴⁷, estableciendo que “la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”⁴⁸.

Este derecho permite a los titulares de los datos controlar la información relativa a su persona; ya sea en una vertiente negativa – negar la cesión de la información – o positiva, en “la llamada ‘libertad informática’, es también el derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*)”⁴⁹.

A nivel supranacional también se encuentra protegido este derecho.

El artículo 16 del Tratado de Funcionamiento de la Unión Europea establece, en su primer apartado, que todas las personas tienen derecho a la protección de datos de carácter personal que le conciernan. De igual modo, lo hace el artículo octavo de la Carta de Derechos Fundamentales de la UE⁵⁰.

Así mismo, la relevancia de este derecho y las posibles intromisiones en las diferentes esferas, han llevado a la Unión Europea a desarrollar y actualizar normativa al respecto. De esta manera, el Reglamento 2016/679⁵¹ pretende actualizar la legislación a la evolución tecnológica y la globalización, pues – según considera el propio RGPD – se “requiere un marco más sólido y coherente para la protección de datos en la UE” puesto que “las personas deben tener el control de sus propios datos personales”⁵².

⁴⁷ El derecho a la autodeterminación informativa se configura a raíz de las manifestaciones normativas internacionales y europeas, siendo equiparable al concepto “privacy”, proveniente del Derecho Anglosajón.

⁴⁸ Apartado cuarto del artículo 18 de la Constitución Española de 1978.

⁴⁹ STC 254/1993, de 20 de julio de 1993. Rec. 1.827/1990, FJ 7. Esta sentencia, evalúa una posible vulneración del derecho a la intimidad personal; y es la que reconoce y dota de sustantividad propia al derecho a la protección de datos; separándolo del derecho a la intimidad (18.1 CE).

Sin embargo, es la STC 292/2000, de 30 de noviembre (Rec. 1463/2000, FJ 7) la que delimita el contenido esencial del derecho fundamental a la protección de datos personales, entendiéndolo como el derecho a consentir el tratamiento de los datos, conocer quién tiene acceso a la información proporcionada y la facultad para oponerte a la posesión y los usos que se hagan de ella.

⁵⁰ La Carta de los Derechos Fundamentales de la Unión Europea, en el Capítulo I referido a la Dignidad, establece en su octavo artículo, relativo al derecho a la Protección de Datos de carácter personal:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

⁵¹ Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

⁵² Considerando séptimo del Reglamento (UE) 2016/679.

Este Reglamento tiene alcance general, es obligatorio en todos sus elementos y de obligado cumplimiento para los Estados Miembros de la UE⁵³; sin embargo, en el considerando 11 del RGPD se advierte que “la protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes”.

Así mismo, se considera relevante señalar que el ámbito de aplicación de este Reglamento no es exclusivo a las relaciones laborales, por lo que se debe acudir a su artículo 88 para encontrar una referencia específica.

En este artículo, que consta de tres apartados, se señala la necesidad de que sean los Estados Miembros quienes elaboren “normas específicas con el objeto de garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores”⁵⁴, indicando además que se deben elaborar preservando la dignidad humana de los individuos interesados, así como sus intereses legítimos y derechos fundamentales.

En definitiva, el artículo 88 del RGPD, así como el Considerando 155, no regulan “propriadamente la protección de datos en el ámbito laboral, si no que ordena a los Estados miembros que lo hagan a través de varias vías”⁵⁵. Sin embargo, aun no siendo su ámbito

⁵³ El artículo 288 del Tratado de Funcionamiento de la UE señala el alcance general, la obligatoriedad en todos sus elementos y la aplicabilidad directa sobre todos los Estados que formen parte de la Unión Europea.

⁵⁴ Artículo 88 RGPD indica establece que:

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.
2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

⁵⁵ MIÑARRO YANINI, M. “Impacto del reglamento comunitario de protección de datos en las relaciones laborales. Un – pretendido – ‘cambio cultural’”. *Revista mensual CEF – Trabajo y Seguridad Social*. Núm. 423, ISSN: 1138 – 9532, 2018. Pág. 10.

de aplicación exclusivamente laboral, no se debe pasar por alto que las relaciones laborales no quedan al margen de esta normativa, puesto que la transversalidad de la protección de datos implica que resulta plenamente aplicable en cualquier ámbito donde se traten los datos personales, incluidas las relaciones de trabajo.

Encontramos, así mismo, que a nivel nacional se ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que tiene por objeto adaptar al ordenamiento jurídico español el RGPD, garantizando los derechos digitales de la ciudadanía respetando el mandato del artículo 18.4 CE.

A lo largo del segundo y tercer capítulo de la LO 3/2018 se detallan cuáles son los principios relativos al tratamiento de los datos personales, que requieren de especial atención para adecuar medidas que garanticen el ejercicio del derecho de protección de datos.

Sin perder de vista este propósito, debe tenerse en cuenta el *Principio de calidad de los datos*, en base al cual los datos recogidos deben ser adecuados, pertinentes y no excesivos en relación con la finalidad perseguida.

Muy estrechamente relacionado, se encuentra el *principio de finalidad legítima*, cuya relevancia es esencial en relación con la posible adopción de medidas de videovigilancia en el ámbito empresarial. El reglamento señala que los datos deberán ser recogidos para unos fines determinados, explícitos y legítimos; sin que puedan ser posteriormente tratados de modo incompatible.

De gran relevancia es también el *principio de consentimiento*⁵⁶, pues constituye un elemento esencial en relación con la legitimidad de la obtención de los datos personales. Sin embargo, a pesar de tratarse de un elemento indisponible a la hora de garantizar este derecho, es preciso señalar que, en el ámbito laboral, “el consentimiento pasa, en principio, a un ‘segundo plano’, ya que se entiende implícito en el contrato de trabajo, siempre y cuando el tratamiento de los datos personales sea necesario para el

⁵⁶ El Informe *Article 29 Working Party Guidelines on consent under Regulation 2016/679: The Working Party On The Protection Of Individuals With Regard To The Processing Of Personal Data*, de 28 de noviembre de 2017, pág. 5; señala las consideraciones que deben tenerse en cuenta a fin de determinar si el consentimiento es válido. En este mismo sentido, se señala en el Dictamen 2/2017, de 8 de junio, de este mismo órgano consultivo de la UE, que, dada la relación de dependencia existente entre trabajador y empresario, no debería considerarse prestado válidamente el consentimiento por no existir una verdadera libertad de escoger; por lo que afirma que no debe considerarse este principio como base jurídica de la protección de datos cuando se dé en el ámbito de la relación laboral.

mantenimiento y cumplimiento de éste⁵⁷”. En consecuencia, sí existirá la obligación de obtener el consentimiento del interesado en aquellas situaciones en las que los datos se empleen para fines ajenos al cumplimiento del contrato de trabajo.

Otro de los elementos que configuran el derecho a la protección de datos es el *principio de transparencia*, en virtud del cual los afectados por el tratamiento de los datos deben ser informados de manera expresa, precisa e inequívoca acerca de la forma y finalidad del tratamiento, así como de las consecuencias que puedan derivar de prestar o no consentimiento⁵⁸.

Por último, el *principio de accesibilidad, cancelación y descontextualización* de los datos, que debe entenderse como la posibilidad de acceso del interesado a los datos recogidos, así como a solicitar su modificación o cancelación.

En relación con estos principios y su aplicabilidad en la videovigilancia, es destacable el artículo 22 de la Ley, que regula el tratamiento de imágenes a través de cámaras o videocámaras con el objetivo de preservar la seguridad de las personas, bienes e instalaciones, así como el plazo de conservación de las grabaciones⁵⁹. Este artículo señala que el deber de información se entenderá cumplido mediante la colocación de un dispositivo informativo en un lugar lo suficientemente visible⁶⁰, manteniendo el responsable del tratamiento a disposición de los afectados la información pertinente para hacer efectivos los derechos contenidos en la protección de datos.

Así mismo, hace referencia al artículo 89 de la Ley, relativo al derecho a la intimidad frente al uso de dispositivos de videovigilancia en el ámbito de trabajo. Este

⁵⁷ VILLALBA CANO, L. “Jurisprudencia constitucional. La contradicción entre las SSTC 29/2013, de 11 de febrero y 39/2016, de 3 de marzo”, en FODERTICS 7.0 Estudios sobre derecho digital, BUENO DE MATA, F. (DIR); en *La videovigilancia laboral y su incidencia en el derecho de protección de datos a la luz de la jurisprudencia constitucional y del reglamento europeo 2016/679*. Editorial Comares, ISBN: 9788490457658, 2019. Pág. 207.

⁵⁸ El quinto apartado del preámbulo de la LO 3/2018 señala que el principio de transparencia reconoce la denominada “información por capas”, generalmente aceptada en ámbitos como el de la videovigilancia; donde se facilita que el interesado disponga de la información básica e indicándole un medio que le permita acceder de manera sencilla e inmediata a la información completa.

⁵⁹ El artículo también delimita el plazo de conservación de estas grabaciones, indicando que deben eliminarse los datos obtenidos en el plazo máximo de un mes desde su captación; salvo que estos pudieran ser empleados para acreditar la comisión de actos contrarios a la integridad de los bienes, personas o instalaciones en cuyo caso deberá ponerse a disposición de la autoridad competente en el plazo de setenta y dos horas desde que se tenga conocimiento.

⁶⁰ Este dispositivo informativo debe identificar la existencia del tratamiento de los datos, así como la identidad del responsable y la posibilidad de ejercitar los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición al tratamiento de los datos.

precepto, en su primer apartado, recoge la facultad reconocida al empresario para proceder al tratamiento de las imágenes obtenidas a través de sistemas de videocámaras con el objeto de ejercitar las funciones de control y verificación que se le conceden a través el artículo 20.3 del Estatuto de los Trabajadores, para así establecer mayores garantías en relación con el derecho de información en el tratamiento de los datos dentro del ámbito laboral.

En este sentido, el artículo impone la obligación de informar con carácter previo, de manera expresa, clara y concisa, a los trabajadores afectados y a sus representantes, sobre el uso de dispositivos de videovigilancia. Sin embargo, incluye la salvedad de que en el caso de que se haya captado “la comisión flagrante de un acto ilícito por los trabajadores” se entenderá cumplido el deber de información mediante la colocación de un dispositivo, atendiendo a los requisitos previstos en el anteriormente citado artículo 22 de la Ley.

Esta salvedad, según expresa Serrano Olivares, “se trata de una excepción expresada en términos poco claros” puesto que “genera la duda de si el legislador se refiere a cualquier acto ilícito – ilícito laboral – o solamente a actos que pudieran reputarse como delictivos”⁶¹. De esta manera, el legislador deja abierta una vía que, en la práctica, ha suscitado varios conflictos que debe resolver necesariamente la jurisprudencia.

De igual modo, los tribunales deben dar respuesta a varias cuestiones que se plantean en relación con la garantía del ejercicio del derecho a la protección de datos cuando se dan situaciones de videovigilancia en el ámbito laboral, pues, como sentencia el Tribunal Europeo de Derechos Humanos, la imagen, el nombre y la identidad personal forman parte del concepto de vida privada; por lo que en él también se incluye el tratamiento de los datos cuando se obtengan través de un sistema de videocámaras⁶².

Por ende, la posibilidad de no advertir acerca del tratamiento de los datos amparándose en la exclusión de información prevista legalmente, puede suponer una injerencia en el respeto a la vida privada – recogido en el artículo 8 del Convenio – así como una intromisión en su derecho a la autodeterminación informativa y a su intimidad.

⁶¹SERRANO OLIVARES, R. “Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales”. *Revista IUSLabor 3/2018*, ISSN 1699-2938, 2018. Pág. 223.

⁶²López Ribalda y otros vs España, STEDH de 9 de enero de 2018.

De igual modo, no debe pasarse por alto que en ningún caso podrá realizarse dicho control de una manera arbitraria o ilimitada puesto que, aunque el artículo 20.3 ET – que faculta la vigilancia empresarial – desarrolle un bien jurídico reconocido constitucionalmente con origen en los artículos 33 y 38 CE; el derecho a la intimidad, a la vida y privada y a la protección de datos son derechos fundamentales que deben ser igualmente observados.

2. PONDERACIÓN DE DERECHOS CONSTITUCIONALES

2.1.El Triple Test de Proporcionalidad.

Aun no existiendo derechos fundamentales absolutos, debiendo matizarse cuando surge una confrontación entre ellos, la limitación debe realizarse poniendo en relación los bienes protegidos por nuestro ordenamiento jurídico. En este sentido, el Tribunal Constitucional ha delimitado el modo en que debe valorarse una posible vulneración de estos derechos elaborando una extensa doctrina acerca del modo de proceder para garantizar un punto de equilibrio prudencial, sentenciando que debe realizarse un *triple test de proporcionalidad* para considerarse aceptable la limitación.

Sin embargo, no es hasta el año 2000 cuando el TC dicta una sentencia acerca de la legalidad de un circuito cerrado de televisión, momento en que aplica por primera vez este juicio ponderativo en la cuestión objeto de estudio. De esta manera, la STC 186/2000⁶³, de 10 de julio, señala que “la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad”, por lo que es necesario constatar si se cumplen tres condiciones. Para ello, debe valorarse, en primer lugar, si la medida es susceptible de alcanzar el objetivo perseguido (juicio de idoneidad); en segundo lugar cabría determinar si la medida es necesaria, en el sentido de que no exista otra medida menos intrusiva e igualmente eficaz para la consecución del mismo propósito (juicio de necesidad); y, por último, si la medida es equilibrada o ponderada, para lo que habrá que atender a si de ella derivan más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

De esta manera, si la medida adoptada por la empresa para garantizar el cumplimiento de las obligaciones derivadas de la relación laboral supera el triple juicio de proporcionalidad, podrá considerarse que se ha realizado con las exigencias necesarias

⁶³ STC 186/2000, de 10 de julio de 2000. Rec. 2662/1997. FJ 6.

para garantizar la no vulneración del derecho fundamental ponderado. Sin embargo, en este supuesto concreto, el principio de proporcionalidad es aplicado a vistas de salvaguardar el derecho a la intimidad; sin valorar las consideraciones relativas a la protección de datos.

En relación con esto, Goñi Sein señala que “respecto al primer requisito (...) de acuerdo con la normativa de protección de datos, no basta con analizar la simple adecuación entre la medida de videovigilancia y el interés perseguido” si no que éste “hay que ponerlo en relación con fines que realmente justifiquen el recurso de la videovigilancia”; puesto que “requiere una valoración minuciosa de si existe realmente interés empresarial legítimo que justifique el emplazamiento de los dispositivos de captación de imágenes de los trabajadores, aun cuando una superficial consideración de la doctrina constitucional sobre el principio de idoneidad, pueda conllevar a interpretar que es suficiente un juicio exclusivo sobre la mera adecuación”⁶⁴.

2.2. El Test Barbulescu.

En este mismo sentido, el TEDH matizó las consideraciones que debían tenerse en cuenta con el objetivo de valorar si las medidas de verificación y control empresariales a través de medios tecnológicos suponen una intromisión en la vida privada de los empleados. De esta manera, el caso de Barbulescu⁶⁵ contiene los criterios⁶⁶ que deben atenderse para no infringir el artículo octavo del Convenio, habiendo sido posteriormente aplicados en el caso López Ribalda; indicando que “los órganos jurisdiccionales nacionales, a la hora de ponderar los distintos intereses en juego”⁶⁷, deben tener en cuenta, en primer lugar, si los empleados han sido previamente informados de las medidas que pretenden instaurarse, así como de la aplicación y naturaleza de estas.

En segundo lugar, el Tribunal de Estrasburgo considera que debe valorarse el alcance de la medida, así como el grado de intrusión que esta ha supuesto en la privacidad del empleado. En este sentido señala que es importante determinar el carácter más o menos privado del lugar donde tenga lugar la videovigilancia, los límites espaciales y

⁶⁴ GOÑI SEIN, J.L. “Principios de protección de datos aplicables en el momento de la adopción del sistema de videovigilancia empresarial”, en *Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, 2007. Págs. 119 y 120.

⁶⁵ Barbulescu vs Rumania. STEDH, Gran Sala, de 5 de septiembre de 2017.

⁶⁶ Estos criterios posteriormente fueron aplicados específicamente a supuestos de videovigilancia en el ámbito laboral a través del caso López Ribalda y otros vs España; puesto que el Tribunal consideró que estos principios eran transferibles (*mutatis mutandi*).

⁶⁷ López Ribalda y otros vs España, STEDH, Gran Sala, de 17 de octubre de 2019.

temporales de las grabaciones y el número de personas que tendrán acceso al visionado o tratamiento de los resultados.

El Tribunal indica que otro requisito que debe tomarse en consideración es si los motivos justifican la captación de imágenes mediante videocámaras y el alcance de estas pueden considerarse legítimos. Otro criterio a valorar es si hubiese podido emplearse la videovigilancia de un modo menos intrusivo, por lo que es determinante atender a la legitimidad de la finalidad perseguida por el empleador.

Como quinto criterio, se atiende a la relevancia de las posibles consecuencias que haya podido ocasionar la medida en los trabajadores afectados, para ello no debe pasarse por alto el modo en que el empresario utilizó los resultados obtenidos de la grabación y si esta realmente sirvió para alcanzar la finalidad perseguida. En sexto y último lugar, el TEDH insta a confirmar si las garantías que se ofrecieron al trabajador eran adecuadas en relación con el grado de intrusión al que se haya visto sometido por la videovigilancia⁶⁸.

En definitiva, es indudable que los criterios delimitados por el Tribunal se corresponden con una valoración más restrictiva a la hora de establecer los parámetros requeridos para un adecuado uso de la videovigilancia en el ámbito laboral, reduciendo en mayor medida las posibles intromisiones en los “derechos fundamentales inespecíficos del trabajador”⁶⁹.

A pesar de ello, los conflictos surgidos en relación con la eficaz protección de estos derechos y las facultades de control empresarial no han sido más que incrementadas en los últimos años; puesto que, como señala Villalba Sánchez⁷⁰, la fiscalización empresarial a través de las nuevas tecnologías comporta dos peligros: de un lado su carácter invasivo, cuyo límite se encuentra en el derecho a la intimidad; y de otro su “memoria ilimitada” – en relación con su capacidad para captar, conservar, transmitir y

⁶⁸ En relación con la salvaguarda de estas garantías, la Gran Sala del Tribunal de Estrasburgo, en la posterior sentencia relativa al caso López Ribalda, asevera que debe valorarse la posibilidad de informar de la instalación y el alcance de las medidas que se pretendan adoptar al trabajador afectado, a sus representantes o a un organismo independiente.

⁶⁹ PALOMEQUE LOPEZ, M.C., *Los derechos laborales en la Constitución Española*. CES, Madrid, 1991. Pág. 31. Esta denominación fue acuñada para referirse a aquellos derechos de los cuales todo ciudadano es titular, y por ende, también lo son los trabajadores.

⁷⁰ VILLALBA SANCHEZ, A. “El derecho fundamental a la protección de datos del trabajador frente a los poderes del empresario, con especial referencia al consentimiento del trabajador”, en CASTRO MARQUES, E. (coord.): *Digital work and personal data protection: key issues for the labour of the 21st century*. Cambridge Scholars Publishing, Cambridge, 2018. Págs. 473-493

reproducir los aspectos objeto de registro – cuya trasgresión incide en el derecho a la protección de datos.

En relación con esto, resulta ineludible determinar cuáles son los límites de la videovigilancia y cuándo se está haciendo un uso legítimo de estas tecnologías. Esta cuestión ha suscitado numerosos conflictos en el ámbito que nos ocupa, requiriendo una gran labor de integración jurisprudencial por parte de los tribunales; por lo que se debe acudir a la jurisprudencia constitucional, así como a la jurisprudencia ordinaria, para dar solución a algunas cuestiones claves que se han ido dejando entreabiertas a lo largo de este estudio de investigación.

3. EVOLUCIÓN DOCTRINAL EN MATERIA DE VIDEOVIGILANCIA EN LAS RELACIONES LABORALES.

3.1. Precedentes jurisprudenciales tendentes a permisibilidad de control y vigilancia empresarial.

La vigilancia y control en las relaciones laborales no es una novedad, por lo que los Tribunales ordinarios del orden social han venido tratando la videovigilancia de manera habitual. Sin embargo, inicialmente únicamente se invocaba la protección del derecho a la intimidad en su vertiente negativa; de esta manera, habitualmente se permitía una práctica tolerada de estos medios de verificación, bajo la argumentación de que el centro de trabajo no es un lugar público en el que opere la intimidad, por lo que la eficacia de este derecho quedaría reducida a los lugares de descanso, aseo⁷¹ o comedores reservados al uso de los empleados.

En este sentido, es bastante reveladora la STSJ de Galicia, de 25 de enero de 1996, que parte de la premisa de que el centro de trabajo no constituye un espacio donde los trabajadores puedan ejercer el derecho a la intimidad, puesto que el desarrollo del cometido profesional supone abarcar las conversaciones del personal y de clientes, por lo que el Tribunal sentencia no haber razón para que la empresa no pueda conocerlas; argumentando, además, que el derecho a la intimidad se ejercita en la esfera privada del trabajador, por lo que en la empresa debe entenderse limitado a aquellos “lugares de

⁷¹ Es posible, sin embargo, hallar sentencias – como la STSJ de Galicia de 1995 – donde se permite que la cámara enfoque las puertas de los aseos pues se considera que no filman el interior, respetando la limitación de la filmación a lugares ajenos al espacio de protección de la intimidad del trabajador.

descanso o esparcimiento, vestuarios, servicios y otros análogos, pero no en aquellos lugares donde se desarrolla la actividad laboral”⁷².

De esta manera, la jurisprudencia venía considerando que las facultades dimanadas del artículo 20.3 del Estatuto de los trabajadores, permitían que el empresario emplease cuantos medios considerase oportunos para asegurar el control y la vigilancia de la actividad laboral; guardando la consideración debida a la dignidad humana, que no se entendía vulnerada si el control se restringía al estricto ámbito laboral, el cual se consideraba ajeno a la esfera de intimidad personal.

3.2. Rectificación de doctrina y aplicación del principio de proporcionalidad: las SSTC 98/2000 y 186/2000.

Esta afirmación fue más tarde rectificada por el Tribunal Constitucional en la STC 98/2000, recordando que desde la perspectiva constitucional no puede aceptarse que la prestación de una actividad en el marco de la relación laboral implique la privación de los derechos fundamentales a quienes dan servicio en las organizaciones productivas, puesto que estas no son ajenas a los principios y derechos constitucionales⁷³. Por lo tanto, el máximo interprete de la Constitución, rechaza la premisa de que el centro de trabajo no constituya por definición un espacio donde se pueda ejercerse el derecho a la intimidad por parte de los empleados; debiendo atenderse a un “necesario equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito – modulado por el contrato, pero en todo caso subsistente – de su libertad constitucional”⁷⁴; resultando indispensable, tal y como señala el TC, advertir los principios de proporcionalidad e intervención mínima que rigen en la modulación de los derechos fundamentales.

De esta manera, el Tribunal sentencia que es posible que pueda producirse una vulneración del derecho a la intimidad, aun en el desempeño de tareas profesionales; siendo esta una matización de gran relevancia puesto que al reconocer tal posibilidad, las limitaciones o modulaciones a las que pueda someterse este derecho fundamental deben resultar ser indispensables y estrictamente necesarias para satisfacer el interés empresarial tutelado – el cual emana del artículos 33 y 38 de la Constitución –, de modo que se debe valorar si existen otros medios para alcanzar el objetivo perseguido que resulten menos intrusivos.

⁷² STSJ de Galicia, de 25 de enero de 1996. Rec. 3/1996.

⁷³ STC 98/2000, de 10 de abril de 2000. Rec. 4.015/1996, FJ 6.

⁷⁴ STC 98/2000, de 10 de abril de 2000. Rec. 4.015/1996, FJ 7.

En relación con esta afirmación, resulta ineludible atender a la necesidad expresada por el TC de evaluar adecuadamente si la finalidad que persigue el empleador es legítima, señalando que “la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación”⁷⁵, debiendo tratarse de una medida “indispensable para la seguridad y el buen funcionamiento”⁷⁶ de la empresa.

A pesar de que esta sentencia introduce la indispensabilidad de ponderar la medida atendiendo los derechos fundamentales de los trabajadores, observando razones de necesidad y finalidad, no es hasta la STC 186/2000, de 10 de julio, cuando se aplica de manera expresa el triple juicio de proporcionalidad exigido para valorar la legitimidad de una posible modulación o limitación del derecho a la intimidad. Sin perder de vista este objetivo, la sentencia precisa que “los equilibrios y limitaciones recíprocos que se derivan para ambas partes del contrato de trabajo suponen (...) que también las facultades organizativas empresariales se encuentran limitadas por los derechos fundamentales del trabajador; quedando obligado el empleador a respetar aquellos”⁷⁷. Además, el Tribunal señala que la limitación de tales derechos “por parte de las facultades empresariales solo puede derivar del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho”⁷⁸.

De esta manera, el máximo interprete de la Constitución, precisa qué aspectos deben tenerse en cuenta para una correcta aplicación del triple test de proporcionalidad, atendiendo a los criterios previamente mencionados de idoneidad, necesidad y proporcionalidad en sentido estricto⁷⁹.

En este sentido, el TC considera que la medida era ajustada al principio de proporcionalidad, y, por lo tanto, legítima. Para ello basa su argumentación en que la medida estaba justificada, puesto que el empresario tenía sospechas fundadas de graves irregularidades por parte de un trabajador en concreto; en que era la medida idónea para la finalidad pretendida, ya que permitía comprobar si tales sospechas estaban justificadas

⁷⁵ STC 98/2000, de 10 de abril de 2000. Rec. 4.015/1996, FJ 9.

⁷⁶ STC 98/2000, de 10 de abril de 2000. Rec. 4.015/1996, FJ 9.

⁷⁷ STC 186/2000, de 10 de julio. Rec. 2.662/1997, FJ. 6.

⁷⁸ STC 186/2000, de 10 de julio. Rec. 2.662/1997, FJ. 6.

⁷⁹ Como se ha mencionado anteriormente, el triple juicio de proporcionalidad atiende, en primer lugar, al juicio de idoneidad entrando a valorar si la medida empleada es susceptible de alcanzar el objetivo propuesto; el segundo juicio aplicativo relativo a la necesidad se refiere a la posibilidad de existir una medida más moderada pero igualmente eficaz para conseguir el propósito empresarial; y por último, el juicio de proporcionalidad en sentido estricto enjuicia si la medida es la más equilibrada o ponderada, en el sentido de que deriven de ella más ventajas o beneficios para el interés general, que perjuicio sobre otros bienes o valores en conflicto.

y, en consecuencia, emplear las grabaciones como medio probatorio para, así, poder emprender medidas disciplinarias contra el trabajador en cuestión; entendiendo el Tribunal que era también necesaria por los mismos motivos probatorios de irregularidades y, en último lugar, que la medida estaba equilibrada puesto que únicamente filmaba la zona necesaria para despejar las sospechas y durante el tiempo imprescindible para comprobar que “no se trataba de un hecho aislado o confusión, si no de una conducta ilícita reiterada”⁸⁰. De esta manera el Tribunal argumenta que la medida no ha lesionado el derecho a la intimidad consagrado en el artículo 18.1 CE.

En relación con esta sentencia, se ha considerado relevante además destacar que, como se viene adelantando, únicamente se atiende a la posible injerencia en el derecho a la intimidad, de manera que, aunque se pone de manifiesto que la empresa no informó al trabajador ni a sus representantes acerca de la instalación de sistemas de videovigilancia – amparándose en el temor a frustrar la finalidad perseguida de corroborar las sospechas de irregularidades graves – el Tribunal considera que esta cuestión “carece de trascendencia desde la perspectiva constitucional”⁸¹, puesto que, según argumenta, se trata de una mera legalidad ordinaria exigible en base al artículo 64.1.3.d) ET⁸².

En definitiva, es posible extraer algunas conclusiones que determinan el marco doctrinal resultante de ambas sentencias en relación con la videovigilancia en el ámbito empresarial, cuando esta se plantea con una finalidad de control de la actividad. Así mismo, en primer lugar, cabe diferenciar entre dos escenarios diferentes cuando se trata de un control genérico e ilimitado de la actividad laboral o cuando, por el contrario, se corresponde a un control limitado a una zona concreta y durante un espacio temporal indispensable para llevar a cabo las verificaciones. En este sentido, en la STC 186/2000 el Tribunal Constitucional reconoce que la videovigilancia no constituye un método de control selectivo en cuanto a las imágenes que capta, por lo que es posible que resulte invasivo en relación con aspectos inherentes a la vida personal del trabajador⁸³. De esta

⁸⁰ STC 186/2000, de 10 de julio. Rec. 2.662/1997, FJ. 7.

⁸¹ STC 186/2000, de 10 de julio. Rec. 2.662/1997, FJ. 7.

⁸² Actualmente, los Derechos de información y consulta y competencias de los representantes de los trabajadores se encuentran regulados en el artículo 64 del Estatuto de los Trabajadores, sin embargo es en el apartado quinto donde debe acudir para encontrar para la mención expresa relativa al derecho de los representantes de los trabajadores a ser informados, con carácter previo, acerca de la finalidad del control laboral, posibilitando así que elaboren un informe previo a la adopción de tales medidas.

⁸³ STC 186/2000, de 10 de julio. Rec. 2.662/1997, FJ. 5.

manera se deduce ineludible atender a la zona de ubicación de las cámaras, así como al alcance temporal de las grabaciones.

Por lo tanto, resulta esencial discernir entre la instalación de una cámara de videovigilancia fija y la videovigilancia *ad hoc*, puesto que se tendrá en consideración la existencia de serias sospechas previas a la instalación de estos sistemas, con el objeto de determinar si la finalidad perseguida por el empleador es legítima. En consecuencia, se destaca también la necesidad de contemplar la existencia de sospechas fundadas sobre posibles irregularidades. Esto, sin embargo, no implica que la captación mediante sistemas de videovigilancia no pueda ser permanente y/o tener un alcance general; no obstante, para determinar la legitimidad de la decisión deberá atenderse a si está lo suficientemente justificada.

Es posible, de igual modo, concluir que la valoración de las sospechas previas de irregularidades, así como la consideración de la pretensión como legítima; está estrechamente ligada con la obligación de información requerida al empresario para con los trabajadores afectados y sus representantes, puesto que este deber puede no tener cabida de estimarse que la advertencia previa pudiera frustrar la finalidad perseguida.

De esta manera, en palabras de Rojas Rosco, “la falta de información previa y de proporcionalidad de la medida de control determinará la ilicitud o nulidad de la actuación empresarial y la nulidad de la medida disciplinaria adoptada con base en dichas pruebas (doctrina del fruto envenenado). Es decir, puede faltar información previa, pero solo en aquellos casos en que sea estrictamente justificado”⁸⁴.

3.3. Introducción doctrinal del derecho a la protección de datos personales como límite a las facultades de control y vigilancia empresarial y a la videovigilancia.

Es en la STC 292/2000, de 30 de noviembre, cuando se introduce un importante matiz doctrinal que servirá posteriormente como base para la importantísima STC 29/2013⁸⁵. En este sentido, el Tribunal aborda el litigio atendiendo a la posible vulneración de los artículos 18.1 CE y 18.4 CE, “al no respetar el contenido esencial del derecho fundamental al honor y a la intimidad personal y familiar” así como el

⁸⁴ ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., “El impacto del RGPD en el ámbito del control laboral y la era de la innovación”, en *Actualidad Civil*, No 5, 2018. Pág. 6.

⁸⁵ STC 29/2013, de 11 de febrero de 2013. Rec. 10.522/2009.

derecho fundamental delimitado por su propia doctrina como “libertad informática”⁸⁶. De esta manera, el TC señala cuáles son los “requisitos o garantías del derecho a la información en la recogida de datos”, contenidos en la Ley Orgánica de Protección de Datos de Carácter Personal⁸⁷.

Así mismo, teniendo en cuenta su propia doctrina, recuerda que ya la STC 254/1993⁸⁸ señaló que “la garantía de la vida privada de la persona y de su reputación poseen (...) una dimensión positiva que excede del ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona”⁸⁹, atribuyendo a su titular el “poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos”.

El TC señala, al mismo tiempo, que las imágenes que sean captadas por un soporte físico constituyen un dato de carácter personal⁹⁰ y, por ende, están bajo el amparo de protección constitucional aquellos datos que “identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo”⁹¹.

De esta manera, el máximo interprete de la Constitución conceptualiza el contenido del derecho fundamental a la protección de datos, delimitando que “consiste en un poder de disposición y de control sobre los datos personales, que faculta a la persona a decidir cuáles de esos datos proporcionar a un tercero (...) o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee estos datos personales y para qué, pudiendo oponerse a esa posesión o uso”⁹². Así mismo, argumenta que el contenido esencial del derecho a la protección de datos se concreta jurídicamente en la

⁸⁶ STC 292/2000, de 30 de noviembre de 2000. Rec. 1.463/2000. FJ. 1.

⁸⁷ Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de carácter Personal. BOE núm. 298. Actualmente derogada – con efectos desde el 7 de diciembre de 2018 – por la disposición derogatoria única de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

⁸⁸ STC 254/1993, de 20 de julio. BOE núm. 197 de 18 de agosto de 1993.

⁸⁹ STC 254/1993, de 20 de julio. BOE núm. 197 de 18 de agosto de 1993. FJ. 4.

⁹⁰ El artículo cuarto del Reglamento (UE) 2016/679, de 27 de abril, define los datos personales como “ toda información sobre una persona física identificada o identificable («el interesado»)”; así mismo concreta que “se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”.

⁹¹ STC 292/2000, de 30 de noviembre de 2000. Rec.1.463/2000. FJ. 6.

⁹² STC 292/2000, de 30 de noviembre de 2000. Rec.1.463/2000. FJ. 7.

facultad de “consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero”⁹³.

En definitiva, esta sentencia define cuál es el contenido esencial del derecho a la protección de datos personales, teniendo especial relevancia la mención al consentimiento del trabajador, así como a la obligación de información previa que debe proporcionarle el empleador, con el objeto de garantizar que puedan ejercerse plenamente las facultades emanadas del artículo 18.4 CE, pues tal y como indica el TC “ese derecho a consentir el conocimiento y el tratamiento (...) de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro, el poder de oponerse a esa posesión y usos”⁹⁴.

Mediante estas delimitaciones, el Tribunal pone en el centro de la valoración jurídica el deber de información a los trabajadores, considerando que, de no respetarse este precepto, incluso aun cuando el fin perseguido sea legítimo, se estaría vulnerando el derecho a la intimidad⁹⁵. En consecuencia, como explica Henríquez Tillería, “establece dos escenarios de análisis: primero, el cumplimiento del deber informativo previo – el que debe ser expreso –, y pasado este requisito, se pasa a un segundo nivel de análisis, en base al principio de proporcionalidad”⁹⁶; considerando vulnerado el derecho a la protección de datos en caso de no cumplir cualquiera de estos “dos estadios de valoración”⁹⁷.

⁹³ STC 292/2000, de 30 de noviembre de 2000. Rec.1.463/2000. FJ. 7.

⁹⁴ STC 292/2000, de 30 de noviembre de 2000. Rec.1.463/2000. FJ. 7.

⁹⁵ Textualmente, la STC 292/2000, de 30 de noviembre, en su fundamento jurídico décimo, sentencia que si no se incluyen las garantías adecuadas frente al uso potencial invasor de la vida privada del ciudadano a través de su tratamiento informático, se vulneraría el derecho a la intimidad, al igual que lo harían las intromisiones directas en el contenido nuclear de esta. De manera, continúa, que “estas facultades legalmente atribuidas y concernientes a sus posibilidades de actuación son necesarias para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos”.

⁹⁶ HENRÍQUEZ TILLERÍA, S. “Transición de la doctrina del Tribunal Constitucional en materia de videovigilancia laboral y el derecho a la protección de datos personales”, en *Protección de Datos, videovigilancia labora y doctrina de la Sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información*. IUSLABOR 3/2019, ISSN 1699 – 2938. Pág. 62.

⁹⁷ HENRÍQUEZ TILLERÍA, S. “Transición de la doctrina del Tribunal Constitucional en materia de videovigilancia laboral y el derecho a la protección de datos personales”, en *Protección de Datos, videovigilancia labora y doctrina de la Sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información*. IUSLABOR 3/2019, ISSN 1699 – 2938. Pág. 62.

3.4. La STC 29/2013 y el nivel de exigencia informativo en la videovigilancia en el ámbito laboral.

Como se ha adelantado, esta sentencia⁹⁸ del Tribunal Constitucional sirvió posteriormente para invocar la lesión de los derechos fundamentales contenidos en el artículo 18.1 y 18.4 CE en la STC 29/2013⁹⁹. Este litigio versa sobre la posible vulneración de derechos en el supuesto de un trabajador que es sancionado con suspensión de empleo y sueldo por incumplir el horario de trabajo que tenía establecido, así como su jornada laboral; justificado la sanción en base a imágenes recabadas mediante grabaciones captadas a través de un sistema de videovigilancia instaladas previamente en el centro de trabajo bajo el pretexto de seguridad.

De este pronunciamiento, resulta relevante en relación con los hechos acontecidos, por un lado, que, pese a que la finalidad para la que fueron instaladas las cámaras de videovigilancia fuera en inicio la pretensión de garantizar la seguridad; el empleador tomó la determinación de emplear dichas imágenes para acreditar posibles irregularidades en base a previas sospechas de incumplimiento de las obligaciones contractuales por parte del trabajador. Y, de otro lado, es destacable también que el convenio colectivo de aplicación preveía explícitamente la posibilidad de emplear tales medios audiovisuales con finalidades de control y verificación de la actividad productiva; sin embargo, no existió comunicación de información expresa acerca de esta finalidad del tratamiento de los datos personales recogidos de los trabajadores, aunque sí se contaba con un distintivo informativo en las instalaciones que advertía de la existencia de sistemas de videovigilancia.

En base a estos datos, el TC se distancia de la jurisprudencia constitucional recogida en las SSTC 98/2000 y 186/2000; señalando que en estas sentencias se trata la posible vulneración del artículo 18 CE desde la perspectiva única del derecho a la intimidad, justificando que el derecho de información dimana del artículo 64.1.3.d) ET, por lo que, como se ha visto, se argumenta que la obligación de informar a los representantes únicamente contiene una previsión legal – no constitucional –, considerándolo un aspecto residual.

⁹⁸ Refiriéndonos a la STC 292/2000, de 30 de noviembre; citada previamente.

⁹⁹ STC 29/2013, de 11 de febrero de 2013. Rec. 10.522/2009.

Este distanciamiento por parte del Tribunal tiene gran relevancia, puesto que atendiendo a las indicaciones proporcionadas por la Agencia Española de Protección de Datos – en base a la anterior doctrina¹⁰⁰ –, el distintivo informativo al que se hace alusión en la sentencia resultaría conforme a lo establecido en la Instrucción 1/2006¹⁰¹ que contempla en su artículo tercero que el cumplimiento del deber de información por los responsables del tratamiento se entenderá atendido mediante la colocación de un distintivo informativo lo suficientemente visible en la zona video vigilada, siempre y cuando se tenga a disposición de los interesados un impreso con la información prevista en el artículo quinto de la LO 15/1999.

En este sentido, el TC sentencia que “una interpretación restrictiva del derecho a la información (...) no podrá operar en un juicio relativo al art. 18.4 CE”¹⁰², recordando además que, aun cuando en el ámbito empresarial existe habilitación legal para recabar los datos sin necesidad de consentimiento – cuando estos resulten necesarios para el desarrollo de la relacional laboral – el derecho de información opera igualmente, argumentando que “una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento”¹⁰³. En este sentido, es posible afirmar, por tanto, que “el deber de informar constituye (...) un deber autónomo del consentimiento del trabajador, que procederá en todo caso”¹⁰⁴.

Así mismo, el Tribunal reconoce que “la exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles y legalmente previstas”¹⁰⁵, no existiendo, continúa, tal habilitación legal expresa para su omisión en el ámbito de las relaciones laborales, y no pudiendo “situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados”¹⁰⁶, puesto que “se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través

¹⁰⁰ Emanada de las SSTC 98/2000 y 186/2000

¹⁰¹ Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras, que impone la obligación de instalar distintivos con el deber de información del art. 5 de la L.O. 15/1999.

Esta Instrucción actualmente se encuentra derogada en su totalidad a raíz de la publicación de la LOPDPGDD 3/2018.

¹⁰² STC 29/2013, de 11 de febrero de 2013. Rec. 10522/2009. FJ. 6.

¹⁰³ STC 29/2013, de 11 de febrero de 2013. Rec. 10522/2009. FJ. 7.

¹⁰⁴ LAHERA FORTEZA, J. “Nueva jurisprudencia constitucional en la videovigilancia laboral. Valoración crítica (STC 39/2016, 3 de marzo)”, en *Derecho de las relaciones laborales*, núm. 5, 2016. Pág. 497.

¹⁰⁵ STC 29/2013, de 11 de febrero de 2013. Rec. 10522/2009. FJ. 7.

¹⁰⁶ STC 29/2013, de 11 de febrero de 2013. Rec. 10522/2009. FJ. 7.

del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que lesiona el art. 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible”¹⁰⁷.

De esta manera, el máximo intérprete de la Constitución sentencia que el artículo 18.4 CE ha sido vulnerado al no informar previamente al trabajador acerca de la utilidad de supervisión laboral asociada a las imágenes capturadas, no pudiéndose entender lo contrario por constatare existente el distintivo informativo de la instalación en el recinto, o la notificación de la creación del fichero a la AEPD; puesto que “era necesaria una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida”¹⁰⁸, concretando además las características y el alcance¹⁰⁹ del tratamiento de los datos.

En base a estas puntualizaciones, el Tribunal no estima relevante el testimonio de previas sospechas fundadas, ni entra a valorar la adecuación de la medida, no atendiendo al triple test de proporcionalidad; en su lugar, declara nulas¹¹⁰ las sanciones impuestas al trabajador, por estar justificadas en base a una única prueba obtenida a través de un medio que lesionaba el derecho fundamental a la protección de datos.

Tras esta sentencia, cabe cuestionarse qué ocurre en aquellos supuestos en los que – como señalaban la STC 186/2000 – la información previa a los trabajadores en caso de sospechas fundadas de incumplimientos laborales pueda frustrar la finalidad de verificación y comprobación perseguida por el empleador. En este sentido, Villalba Sánchez señala que no se trata de permitir que el empresario lleve a cabo un control a través de sistemas sorpresivos o no informados que aseguren la máxima eficacia de la videovigilancia, “se trata (...) de establecer un sistema de control que opere de forma

¹⁰⁷ STC 29/2013, de 11 de febrero de 2013. Rec. 10.522/2009. FJ. 7.

¹⁰⁸ STC 29/2013, de 11 de febrero de 2013. Rec. 10.522/2009. FJ. 8.

¹⁰⁹ Las características y el alcance, según recuerda el TC en esta sentencia, abarcan la comunicación relativa a en qué casos podrán examinarse las grabaciones, durante cuánto tiempo y con qué propósitos.

¹¹⁰ El artículo 90 de del Real Decreto Legislativo 2/1995, de 7 de abril, por el que se aprueba el texto refundido de la Ley de Procedimiento Laboral, establecía que “las partes podrán valerse de cuantos medios de prueba resulten regulados por la Ley (...) salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas”.

Esta Ley, sin embargo, se encuentra actualmente derogada por la Disposición Derogatoria Única de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social; aunque es posible encontrar la misma precisión en el artículo 90.2 de la Ley 36/2011.

preventiva (...) por considerarse más acorde con la buena fe que ha de presidir el ejercicio de derechos y obligaciones de las partes del contrato”¹¹¹.

Esta posición doctrinal se aproxima a la precisión señalada por el Grupo de Trabajo del artículo 29 de la UE, que indica que “los sistemas de vigilancia por videocámara cuyo objetivo directo es controlar, desde una situación remota, la calidad y la cantidad de las actividades laborales y, por lo tanto, implican el tratamiento de datos personales en este contexto, por regla general no deberán estar permitidos”¹¹². Sin embargo, diferencia tal situación de la sucedida en el uso de sistemas de videovigilancia por videocámara cuando se utilizan para verificar el cumplimiento de requisitos productivos o de seguridad laboral, pues – aun cumpliendo con las garantías pertinentes – pueden implicar, directa o indirectamente, el control remoto de los trabajadores. A pesar de la diferenciación en relación con el contexto, el Dictamen 4/2004 expresa la obligación de informar a quien trabaje en el lugar de prestación y pueda verse afectado por el tratamiento de datos personales, incluyendo en ese deber de información datos relativos a la identidad del responsable y el objetivo de la videovigilancia; “así como cualquier otra información necesaria para garantizar que el tratamiento es justo en lo que respecta al interesado”. Así mismo, señala que en el contexto laboral la información facilitada no podrá considerarse suficiente si se facilita en forma de símbolo; debiendo, por lo tanto, ser específica, tal y como señala el Tribunal Constitucional en la STC 29/2013.

3.5. La STC 39/2016 y la flexibilización del principio de transparencia.

Aludiendo esta sentencia¹¹³ recurre en amparo una trabajadora que considera que la empresa ha vulnerado su derecho a la protección de datos personales a través de la captación de imágenes mediante un sistema de videovigilancia del cual, a pesar de admitir conocer su existencia, no había sido informada previamente – tal y como señala la doctrina derivada de la STC 29/2013 – de manera expresa, precisa, clara e inequívoca sobre la captación de tales imágenes, así como de la finalidad de control de la actividad

¹¹¹ VILLALBA SANCHEZ, A. “El derecho fundamental a la protección de datos del trabajador frente a los poderes del empresario, con especial referencia al consentimiento del trabajador”, en CASTRO MARQUES, E. (coord.): *Digital work and personal data protection: key issues for the labour of the 21st century*. Cambridge Scholars Publishing, Cambridge, 2018. Pág. 489.

¹¹² Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara; adoptado el 11 de febrero de 2004 por el Grupo de trabajo creado en virtud del artículo 29 de la Directiva 95/46/CE. Como el mismo Dictamen indica, “se trata de un organismo de la UE, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad”.

¹¹³ STC 29/2013, de 11 de febrero de 2013

laboral y su posible utilización para la imposición de sanciones disciplinarias por incumplimiento de las obligaciones dimanantes del contrato laboral.

De esta manera, resulta destacable reseñar que la empleada trabajaba para una empresa dedicada a la atención y venta al público, por lo que existía información genérica mediante un distintivo informativo – en un lugar lo suficientemente visible – acerca de la existencia de sistemas de videovigilancia en el recinto. Sin embargo, ante la apreciación de múltiples irregularidades y sospechas fundadas de apropiación dineraria por parte de los trabajadores; la empresa decide instalar otra cámara de videovigilancia enfocando directamente a la caja registradora con el objetivo de verificar tales sospechas previas; sin comunicarlo previamente a los trabajadores. A raíz de esta instalación, la trabajadora recurrente en amparo es despedida disciplinariamente.

En base a los hechos acontecidos, el máximo intérprete de la Constitución considera que las especificidades derivadas de los supuestos concretos acerca de la posible vulneración del derecho a la protección de datos requieren perfilar o aclarar su propia doctrina en relación con el uso de cámaras de videovigilancia. En consecuencia, manifiesta la necesidad de determinar el “alcance de la información a facilitar a los trabajadores sobre la finalidad del uso de la videovigilancia en la empresa: si es suficiente la información general o, por el contrario, debe existir una información específica”¹¹⁴

Por ende, el Tribunal Constitucional realiza un recorrido sobre los elementos definidores del derecho a la protección de datos personales, indicando además que la no exigencia de consentimiento en los datos necesarios para el mantenimiento de la relación laboral se traduce en la indispensabilidad del deber de información previa como complemento esencial a la dispensa de consentimiento. En añadido, el Tribunal señala que la falta de exigencia de consentimiento también repercute de manera directa en el principio de calidad de los datos, debiendo corresponder “la causa que justifica el fichero y los datos personales que se recaban y que afectan a los derechos de las personas”¹¹⁵. Sin embargo, el TC sentencia que, en cualquier caso, “el incumplimiento del deber de requerir el consentimiento del afectado para el tratamiento de datos o del deber de información previa sólo supondrá una vulneración del derecho fundamental a la

¹¹⁴ STC 39/2016, de 3 de marzo. Rec. 7.222/2013. FJ 1.

¹¹⁵ STC 39/2016, de 3 de marzo. Rec. 7.222/2013. FJ 1.

protección de datos tras una ponderación de la proporcionalidad de la medida adoptada”¹¹⁶.

De esta manera, donde el mismo Tribunal señaló en la STC 29/2013 la necesidad de atender adecuadamente al deber de información previa específica para así considerar la licitud de la prueba obtenida y, posteriormente, valorar la proporcionalidad de la medida empleada para controlar la actividad laboral; en esta STC 39/2016 se rebaja esta exigencia dando paso directamente a la valoración de la legitimidad de la finalidad perseguida y su ponderación a través del triple test de proporcionalidad, volviendo, por ende, a la doctrina constitucional emanada de la STC 186/2000.

De esta manera, el TC argumenta no haberse producido injerencia en el derecho a la protección de datos personales, puesto que considera cumplido el deber de exigencia informativa, atendiendo al conocimiento de la trabajadora de la existencia de sistemas de videovigilancia en el centro de trabajo por medio del distintivo informativo colocado en un lugar lo suficientemente visible, “sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control”¹¹⁷. Esta argumentación encuentra su justificación en la ya mencionada Instrucción 1/2006 de la AEPD.

Así mismo, argumenta que lo importante es discernir si el tratamiento de los datos obtenidos mediante la captación de imágenes se ha empleado con la finalidad de control de la relación laboral, puesto que es la única manera de eludir la exigencia de consentimiento previo; siendo este el supuesto enjuiciado, según considera el TC. Por lo tanto, aplica el principio de proporcionalidad para analizar si la modulación de los derechos fundamentales de la trabajadora se ha producido con el máximo respeto y en la medida en que ha resultado imprescindible. De esta manera, se considera que no se ha producido lesión en el derecho a la intimidad al valorar la medida justificada por existir razonables sospechas previas de irregularidades e idónea para la finalidad pretendida puesto que permitía llevar a cabo la verificación de ilícitos y posibles sanciones. Además, se estima la medida como necesaria, atendiendo a la posibilidad de posterior aportación como prueba; y equilibrada, ya que únicamente se filmó la zona necesaria para la comprobación de las sospechas.

¹¹⁶ STC 39/2016, de 3 de marzo. Rec. 7.222/2013. FJ. 3.

¹¹⁷ STC 39/2016, de 3 de marzo. Rec. 7.222/2013. FJ. 4.

En definitiva, esta sentencia introduce “importantes cambios en lo que respecta al deber de información y su concreto alcance, relajando las exigencias de una información más específica y con mayor rigor”¹¹⁸, hasta el punto de convertirlo en un requisito meramente formal.

Así, en palabras de Goñi Sein, “esta última doctrina ha propiciado un complemento devaluado de los presupuestos formales del deber de transparencia”; de manera que “la falta de una información específica sobre la finalidad de control de la actividad laboral y su posible uso con fines disciplinarios, ya no comporta la invalidez de la prueba, ni excluye la validez del procedimiento sancionador, siempre que el empleado haya tenido conocimiento de la existencia de las cámaras”¹¹⁹.

Así mismo, el autor considera que la consecuencia de esta nueva orientación doctrinal deriva en que “el derecho a la protección de datos se hace ahora ineficaz, carente de sentido práctico e irreconocible, (...) 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 relación con el contrato”¹²⁰.

Así mismo, Villalba Sánchez expresa que “el intérprete del derecho pasa por alto la abismal diferencia que media entre un dato necesario para el ‘cumplimiento’ de las obligaciones derivadas del contrato y un dato necesario para el ‘control del cumplimiento’ de dichas obligaciones”, confundiendo necesidad con conveniencia.

3.6. Barbulescu II.

A pesar de que pueda parecer que la doctrina constitucional ha terminado por delimitar el contenido esencial, así como el alcance, del derecho a la protección de datos, estos vaivenes jurisprudenciales no encuentran su fin con esta sentencia; por lo que resulta ineludible destacar varios pronunciamientos proporcionados en los últimos años por el TEDH en relación con la materia.

¹¹⁸ ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., “El impacto del RGPD en el ámbito del control laboral y la era de la innovación”, en *Actualidad Civil*, Núm. 5, 2018. Pág. 9.

¹¹⁹ GOÑI SEIN, J.L., “Vigilancia empresarial y protección de datos: Doctrina Jurisprudencial”, en *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*. núm. 143, 2019, Pág. 202.

¹²⁰ GOÑI SEIN, J.L. “Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo [BOE nº.85, de 8-IV-2016]. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información”, en *Reseñas de Jurisprudencia (Enero – Junio 2016) Trabajo y Seguridad Social*. En *Ars Juris Salmanticensis*, vol. 4. eISSN: 2340 – 5155. Universidad de Salamanca, 2016. Pág. 289.

En este sentido se ha considerado relevante mencionar la sentencia de 5 de septiembre de 2017 relativa al caso *Barbulescu contra Rumanía*¹²¹. En esta sentencia la Gran Sala del TEDH trata un conflicto relativo al secreto de las comunicaciones¹²², aludiendo el demandante vulneración del artículo 8 del Convenio¹²³ el cual contiene el derecho al respeto a la vida privada. A pesar de que no se trata de un supuesto referido a la instalación de sistemas videovigilancia en el ámbito laboral, el TEDH valora la posible injerencia en la vida privada del trabajador, delimitando – en consecuencia – una serie de criterios que deben atenderse con el objeto de garantizar el derecho a la protección de datos en el ámbito laboral.

Con el objeto de destacar las similitudes y extraer las conclusiones que se han estimado relevantes por su aplicabilidad en el caso que nos ocupa – la videovigilancia en el contexto empresarial –, se ha determinado ineludible reseñar algunos acontecimientos. Como hechos probados, destaca que el reglamento interno de la empresa establecía expresamente la prohibición del uso por parte de los empleados de los recursos de la empresa para fines personales; sin embargo, no se menciona la posibilidad de control empresarial para verificar el cumplimiento de estos preceptos. En añadido, a raíz de la constatación de incumplimiento por parte de otro empleado, se había distribuido una nota informativa que recordaba tal prohibición, y avisaba de que se llevaría a cabo vigilancia empresarial con posibles sanciones ante infracciones contractuales; nota que la empresa asegura que había sido firmada por el trabajador demandante, por lo que podría entenderse posible asumir su conocimiento de las consecuencias que podían derivarse.

En base a las comprobaciones efectuadas, la empresa solicita explicaciones al trabajador tras la constatación de irregularidades en el cumplimiento de sus obligaciones laborales; advirtiendo de que se ha procedido a la supervisión de sus comunicaciones. Ante tal afirmación, el trabajador asegura que el uso se correspondía con fines laborales,

¹²¹ *Barbulescu vs Rumania*. STEDH, Gran Sala, de 5 de septiembre de 2017.

¹²² El derecho al secreto de las comunicaciones es un derecho fundamental constitucionalmente protegido a través del artículo 18.3 CE. Así mismo, la intromisión por parte de terceros no autorizados a comunicaciones personales implica un tratamiento de datos no consentido por el titular. De esta manera, una injerencia en las comunicaciones de un trabajador deriva en una posible vulneración del derecho a la protección de datos.

¹²³ Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales.

por lo que la empresa presenta como medio probatorio la transcripción de las conversaciones aludidas, derivando en última instancia en la rescisión contractual¹²⁴.

Tras realizar un análisis de los hechos, el TEDH señala las consideraciones que deben atenderse para eliminar cualquier posible expectativa razonable de intimidad por parte del trabajador, y recuerda cuáles son los principios de protección de datos, atendiendo a la necesidad, finalidad, transparencia, legitimidad, proporcionalidad y seguridad de la medida¹²⁵; para posteriormente delimitar la normativa aplicable al caso, sentenciando se aprecia vulneración del artículo 8 del CEDH. Para realizar esta afirmación, el Tribunal de Estrasburgo argumenta que “los órganos jurisdiccionales nacionales no determinaron si el demandante había sido previamente notificado de la posibilidad de que el empresario pudiera establecer medidas de vigilancia y del alcance y la naturaleza de dichas medidas”¹²⁶, así como “tampoco se valoró el alcance y carácter intrusivo del control”¹²⁷. El Tribunal señala además que no “se examinó la gravedad de las consecuencias de la medida de control y el procedimiento disciplinario”.

De esta manera, el caso *Barbulescu* delimita las directrices que deben seguirse para una adecuada consideración de la vida privada de los trabajadores, poniendo el énfasis en la necesidad de realizar una advertencia clara y previa acerca de la prohibición expresa de la conducta que se pretende controlar, de modo que se elimine la expectativa razonable de intimidad; así como en la indispensabilidad de informar también previa y claramente acerca del establecimiento de las medidas de vigilancia y control. Una vez se haya podido constatar que se han tenido en consideración estos requerimientos, el TEDH insta a someter la medida al juicio de ponderación para valorar su proporcionalidad.

¹²⁴ A pesar de que no guarda relación directa con la pretensión alegada, se ha considerado importante mencionar que Sr. *Barbulescu* insta la nulidad del despido ante diversas instancias judiciales de su país – Rumanía – siendo estas desatendidas por no valorar una posible vulneración del artículo 8 del Convenio. De esta manera, el TEDH también valora la vulneración de este derecho en su vertiente positiva, es decir, la obligación de actuación de los Estados miembros para permitir que los ciudadanos vean garantizado este derecho y protegerlo frente a actuaciones de otros sujetos; por lo que señala que las autoridades públicas deberán asegurarse de que las facultades de vigilancia empresarial se acompañen de garantías adecuadas y suficientes para prevenir un uso abusivo.

¹²⁵ Como se viene señalando, los principios de protección de datos deben valorarse atendiendo a la necesidad de la medida para alcanzar el objetivo pretendido, a la finalidad específica, explícita y legítima para la que deben recogerse los datos, a la finalidad legítima necesaria para realizar operaciones de tratamiento de datos, a la proporcionalidad en el sentido de que los datos objeto de vigilancia deben ser pertinentes y adecuados a la finalidad perseguida y a la seguridad que debe garantizarse mediante medidas que aseguren que los datos recogidos no sean accesibles a terceros.

¹²⁶ *Barbulescu vs Rumania*. STEDH, Gran Sala, de 5 de septiembre de 2017 (132).

¹²⁷ *Barbulescu vs Rumania*. STEDH, Gran Sala, de 5 de septiembre de 2017 (133).

Esta sentencia, según expresa Ruíz González, “viene (...) a elevar el listón de exigencia en materia de transparencia en la información previa, lo cual hace necesario su confrontación con los últimos planteamientos de nuestros tribunales españoles”¹²⁸. Sin embargo, como se ha mencionado, esta sentencia sirve también como fundamento justificativo en el reciente caso López Ribalda¹²⁹, donde la Gran Sala del TEDH vuelve a realizar algunas matizaciones de gran relevancia, aplicándolas en materia de videovigilancia en el ámbito laboral.

3.7. López Ribalda II.

El litigio tiene su origen en una empresa dedicada a la venta de alimentación, habiendo observado el gerente de la tienda graves irregularidades entre las cifras de venta y los niveles de stock en el almacén, identificando también grandes pérdidas económicas durante varios meses consecutivos. Ante la constatación de estas incidencias, se decide iniciar una investigación interna destinada a esclarecer lo ocurrido, instalando cámaras de videovigilancia visibles – enfocando la entrada y salida del supermercado – y ocultas, que grababan directamente a las cajas. La empresa reunió a los trabajadores para comunicarles las sospechas de robo y trasladarles la información de la instalación de videocámaras en la entrada y salida; ocultando la instalación de videovigilancia encubierta tanto a los trabajadores como a sus representantes¹³⁰.

Las grabaciones obtenidas constataron las sospechas previas acerca de irregularidades, y permitieron identificar a los catorce empleados implicados. La empresa permitió que la delegada sindical visionase las grabaciones y se citó individualmente a los catorce trabajadores – junto con el gerente, la delegada sindical y el representante legal – con el objetivo de comunicarles su despido disciplinario con causa en un incumplimiento grave de las obligaciones de buena fe y lealtad exigidas en una relación laboral que, según alega el empresario, justifican la ruptura del contrato con efectos inmediatos. En base a estas acusaciones, cinco de los catorce trabajadores despedidos deciden interponer una demanda ante la jurisdicción social solicitando que no fuesen

¹²⁸ RUÍZ GONZÁLEZ, C.M., “Las nuevas propuestas interpretativas del Tribunal Europeo de Derechos Humanos sobre el control del uso laboral de la tecnología de la empresa: Barbulescu y López Ribalda”. En *Cuadernos de Derecho Transnacional*, Vol. 10, núm. 2º. ISSN 1989-4570, 2018. Pág. 925.

¹²⁹ López Ribalda y otros vs España. STEDH, Gran Sala, de 17 de octubre de 2019.

¹³⁰ Consta en los hechos de la sentencia que dos años antes de lo acontecido, la empresa notificó la instalación de videocámaras a la Agencia Española de Protección de Datos, quien le señaló la obligatoriedad de información; en consecuencia, la empresa instaló en ese momento un distintivo informativo sobre la instalación de cámaras de videovigilancia en el recinto empresarial.

admitidas las pruebas obtenidas mediante el recurso de videovigilancia encubierta por vulnerar su derecho a la protección de la vida privada.

El Juzgado de lo Social consideró que, amparándose en las facultades de control emanadas del artículo 20 ET, el empresario puede ejercer funciones de verificación de la actividad laboral por lo que, basándose en la doctrina emanada del TC – prestando especial relevancia a la STC 186/2000 – determinó que la finalidad perseguida era legítima y aplicó el triple juicio de proporcionalidad; estimando que la medida había sido proporcionada y no vulneraba el derecho a la intimidad de las trabajadoras; por tanto, sentenció que tampoco podía entenderse que las grabaciones no constituyesen una prueba válida¹³¹.

Las trabajadoras recurrieron ante el Tribunal Superior de Justicia denunciando que no había sido atendido el cumplimiento de la obligación de información previa dimanado del artículo 5 de la LOPD, por lo que no consideraban que la medida pudiera entenderse proporcionada sin atender a ese criterio. El Tribunal Superior, sin embargo, confirmó las sentencias de primera instancia alegando que el control no había sido realizado de manera desproporcionada y que se trataba de un medio difícilmente reemplazable para alcanzar la finalidad pretendida. Así mismo, el TSJ estimó que la falta de información a los trabajadores, así como a los delegados de personal y a la representación sindical, estaba fundada razonablemente en el temor empresarial a que el conocimiento de la instalación de videovigilancia frustrase su objetivo. Igualmente, el Tribunal señala que en cualquier caso esta falta de información podrá derivar en una sanción administrativa, sin que sea relevante en relación con la admisibilidad de la prueba. Los empleados, no conformes con el fallo, recurren en casación al Tribunal Supremo, declarándose inadmisibles; así como al Tribunal Constitucional en recurso de amparo, declarándose también inadmisibles por estimarse inexistencia de violación de un derecho fundamental.

De esta manera, los demandantes acuden ante el TEDH alegando vulneración del artículo 8 CEDH a raíz de la videovigilancia encubierta instalada en la empresa, sin información previa, expresa, precisa e inequívoca a las trabajadoras acerca la existencia

¹³¹ En relación con las pruebas aportadas, es destacable que la sanción de despido no se basa únicamente en las imágenes obtenidas mediante la videovigilancia. La empresa aporta como pruebas presentadas en el expediente las grabaciones de video, el testimonio de la gerente y la delegada sindical, así como de otros empleados que admiten haber participado en el robo a raíz de las grabaciones, y un informe pericial realizado durante el proceso penal abierto sobre los hechos, en los que se compara las imágenes de las cámaras y los tickets de caja relativos a las compras filmadas.

del sistema y sus características, y que estas no fueron limitadas en el tiempo si no que filmaba permanentemente a todos los trabajadores durante la jornada laboral. Así mismo, alegan que la licitud del uso de las grabaciones como medio probatorio interfiere en su derecho a la intimidad.

El Tribunal de Estrasburgo valora las quejas declaradas como admisibles y, tras analizar la expectativa razonable de privacidad de los empleados, atendiendo a la obligatoriedad de información en base a los criterios establecidos en los principios del derecho de protección de datos; determina que los trabajadores podían albergar tal expectativa razonable. Así mismo, el Tribunal considera que, puesto que no se conocía la identidad del comitente de actos ilícitos – no pudiendo entenderse motivada la medida en base sospechas previas – las grabaciones se dirigían “contra todo el personal, sin límite de tiempo y durante todo el horario laboral”¹³².

De igual modo, el TEDH evalúa la proporcionalidad de la medida, concluyendo que “si bien se había aplicado debido a sospechas legítimas de robo, su alcance era amplio (...) e incumplía la obligación de la legislación nacional de informar previamente a los afectados por la recogida y tratamiento de sus datos personales de la existencia, finalidad y modalidades de estas medidas”¹³³. Por ende, sentenció que no se alcanza por parte de los órganos jurisdiccionales nacionales un equilibrio equitativo entre los derechos de los empleados y el interés del empleador; alegando que “los derechos del empresario podían haberse salvaguardado, al menos hasta cierto punto, por otros medios”¹³⁴. De esta manera, “no solo no se habría superado el juicio de transparencia, sino que tampoco se habría superado el juicio de proporcionalidad”¹³⁵.

En consecuencia, el Tribunal considera vulnerado el derecho al respeto a la vida privada de las trabajadoras al infringir los principios exigibles según la normativa contenida en el RGPD. No estando conforme con la conclusión alcanzada, el Gobierno español recurre la sentencia ante la Gran Sala del Tribunal de Estrasburgo en base a la naturaleza de la obligación contenida en el artículo octavo del CEDH para los Estados miembros; aludiendo que la vulneración de la privacidad de los trabajadores fue

¹³² López Ribalda y otros vs España, STEDH de 9 de enero de 2018.

¹³³ López Ribalda y otros vs España. STEDH, Gran Sala, de 17 de octubre de 2019.

¹³⁴ López Ribalda y otros vs España, STEDH de 9 de enero de 2018.

¹³⁵ Servicio de Estudios del Parlamento Europeo, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado. Consejo de Europa*, en Unidad de Biblioteca de Derecho Comparado. Octubre, 2018. Pág. 32.

consecuencia de una actuación privada, compitiéndole a la jurisprudencia española únicamente el cometido de analizar el justo equilibrio entre los derechos de ambas partes.

De esta manera, se verifica por la Gran Sala si las decisiones emanadas de los órganos jurisdiccionales nacionales se corresponden con las disposiciones aplicables, señalando, en primer lugar, los criterios aplicables para garantizar la proporcionalidad de las medidas de videovigilancia en el ámbito de las relaciones laborales. Estos principios, definidos por la doctrina como *Test Barbulescu* son, en palabras del Tribunal, “transferibles, *mutatis mutandi*”, a estas circunstancias; por lo que se procede a valorar la correcta aplicación por parte de los Tribunales nacionales.

Sin embargo, la Gran Sala del TEDH debe estimar si los Tribunales internos realizaron una correcta ponderación de los intereses en juego, por lo que – aun mencionando los principios del Test Barbulescu – debe atender a la legislación y doctrina constitucional existente en el momento en que se juzgaron los hechos; debiendo realizar el triple juicio de proporcionalidad constitucional, en base al principio de adecuación, necesidad y proporcionalidad en sentido estricto. En este sentido, se afirma que los Tribunales ponderaron de manera adecuada la instalación de videovigilancia, considerando la medida justificada por razones legítimas de sospechas de irregularidades, atendiendo de igual modo al interés legítimo del empleador en verificar los ilícitos, así como identificar a los infractores con el objeto de sancionarles. En añadido, el TEDH confirma que se examinó el alcance de la medida y el grado de intrusismo en la intimidad de los trabajadores, puesto que se limitó la grabación a la zona necesaria, así como al tiempo indispensable para constatar las sospechas de robo.

Así mismo, se atiende a la expectativa de privacidad que podían albergar los trabajadores, delimitando que ésta es de gran importancia en lugares reservados a la privacidad – como aseos o vestuarios –, siendo todavía fuerte la expectativa razonable en aquellos espacios de trabajo cerrados – como las oficinas –, y reduciéndose claramente en “lugares visibles o accesibles para los compañeros o, como en el caso, el gran público”¹³⁶. Y, finalmente, la Gran Sala determina que la medida fue necesaria puesto que permitió identificar a los trabajadores implicados y, aunque sí reconoce que los órganos jurisdiccionales internos podían haber valorado en profundidad la posibilidad de emplear medidas menos intrusivas, admite que “el alcance de las pérdidas constatadas

¹³⁶ López Ribalda y otros vs España. STEDH, Gran Sala, de 17 de octubre de 2019 (126).

por el empleador podía hacer pensar que los robos habían sido cometidos por varias personas, y que de informar a cualquier de los miembros del personal podía poner en riesgo la finalidad de la videovigilancia”¹³⁷. En consecuencia, se estiman suficientes las comprobaciones efectuadas por el Estado español, considerando proporcionada la medida empleada por el empresario.

Por otro lado, se atiende al cumplimiento de las obligaciones derivadas del deber de información, estimando que la legislación aplicable al caso concreto no requiere del consentimiento del trabajador, aunque sí resulta necesario informar previa y claramente de la existencia y modalidades de la recogida de los datos, “aunque sólo sea de manera general”¹³⁸. De esta manera, a pesar de que el Tribunal afirma que “la exigencia de transparencia y el derecho a la información que resulta de ello son fundamentales, especialmente en el contexto de las relaciones laborales, donde el empleador tiene poderes importantes sobre los trabajadores y cuyo abuso debe evitarse”, también afirma que “la información proporcionada a la persona objeto de vigilancia y su alcance son sólo uno de los criterios a considerar a la hora de valorar la proporcionalidad de tal medida (...). Sin embargo, si falta esa información, las garantías derivadas de los demás criterios serán aún más importantes”¹³⁹.

En consecuencia, el TEDH sentencia que, aun siendo cierto que los tribunales españoles no tuvieron en consideración la falta de información previa por considerarlo irrelevante, “las particulares circunstancias del presente asunto, en especial con respecto al grado de intromisión en la vida privada de las demandantes (...) y las legítimas razones que motivaron la puesta en marcha de la videovigilancia, (...) el Tribunal estima que los órganos jurisdiccionales de lo social pudieron (...) considerar que la injerencia en la vida privada de las demandantes era proporcionada”¹⁴⁰. Sin embargo, matiza que no es posible aceptar que la mínima sospecha de irregularidades justifique la instalación de un sistema de videovigilancia encubierta.

De esta manera, donde los últimos pronunciamientos¹⁴¹ del TEDH en relación con el derecho a la protección de datos podían derivar en la conclusión de que las medidas de control y verificación de la actividad laboral mediante el uso de videovigilancia debían

¹³⁷ López Ribalda y otros vs España. STEDH, Gran Sala, de 17 de octubre de 2019. (128)

¹³⁸ López Ribalda y otros vs España. STEDH, Gran Sala, de 17 de octubre de 2019 (131).

¹³⁹ López Ribalda y otros vs España. STEDH, Gran Sala, de 17 de octubre de 2019 (131).

¹⁴⁰ López Ribalda y otros vs España. STEDH, Gran Sala, de 17 de octubre de 2019 (134).

¹⁴¹ Refiriéndonos al caso Barbulescu II y a López Ribalda I.

ser previamente informadas a los trabajadores y sus representantes, de manera expresa, precisa e inequívoca sobre la existencia y particularidades de la recogida de datos personales; puesto que sin este requerimiento no cabe ponderar los intereses contrapuestos, sin que fuese suficiente que el tratamiento resulte lícito o proporcionado al fin perseguido; tras el pronunciamiento de la Gran Sala en el caso López Ribalda se flexibiliza esta obligación legal permitiendo la exención cuando se tengan sospechas razonables, implicando una ponderación más estricta del principio de proporcionalidad.

En definitiva, expresado en palabras de Henríquez Tillería, “esto acarrea una importante carga de incertidumbre jurídica, por tratarse de una ponderación *ex post* de la proporcionalidad de la medida, obligando a una necesaria apreciación judicial de los hechos, en desmedro de la garantía legal concreta entregada al trabajador consistente en el cumplimiento irrestricto del derecho de ser informado. En otras palabras, se abre una peligrosa puerta a la legitimación de videovigilancia oculta condicionada”¹⁴².

¹⁴² HENRÍQUEZ TILLERÍA, S. “Transición de la doctrina del Tribunal Constitucional en materia de videovigilancia laboral y el derecho a la protección de datos personales”, en *Protección de Datos, videovigilancia labora y doctrina de la Sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información*. IUSLABOR 3/2019, ISSN 1699 – 2938. Pág. 73.

4. CONCLUSIONES.

- i. La introducción de las nuevas tecnologías en el ámbito de las relaciones laborales ha supuesto una auténtica revolución digital, quedando patente las virtudes y peligros que derivan de su aplicación durante la actividad laboral. Así mismo, se ha evidenciado la existencia de posibles consecuencias – tanto negativas como positivas – que pueden resultar de su uso mediante la instalación de sistemas de videovigilancia.
- ii. El uso de la videovigilancia en el ámbito empresarial puede emplearse en base a las facultades de control y verificación atribuidas al empresario, con fines de salvaguarda de patrimonio empresarial; así como para constatar el cumplimiento de las obligaciones contractuales por parte de los trabajadores.
- iii. La obtención, conservación y tratamiento de los datos personales de los empleados a través de sistemas de videovigilancia en el ámbito laboral puede derivar en una vulneración de su derecho a la privacidad; pudiendo incidir, así mismo, en su derecho a la intimidad y en el derecho a la protección de datos personales.
- iv. La posible vulneración de los derechos fundamentales reconocidos a los trabajadores debe entenderse atendiendo a la consideración de que no son derechos absolutos, así como tampoco lo son los derechos constitucionales de los que emana la facultad de control empresarial. En consecuencia, deben ponderarse los intereses en juego con el objeto de valorar la constitucionalidad de cualquier medida restrictiva de derechos fundamentales.

Esta ponderación se realiza, en base a la doctrina constitucional, atendiendo al triple test de proporcionalidad. Sin embargo, la Gran Sala del Tribunal Europeo de Derechos Humanos ha matizado algunas cuestiones que deben tenerse en cuenta además de estos principios, señalando una valoración más restrictiva a la que se venía realizando en los Tribunales españoles.
- v. La legislación comunitaria y nacional, así como los Informes, Dictámenes, Recomendaciones y demás textos elaborados para salvaguardar el adecuado uso de la videovigilancia en este ámbito, contienen amplias

referencias a los principios que deben atenderse con el objeto de garantizar el derecho a la protección de datos; teniendo especial relevancia, en el ámbito de las relaciones laborales, el principio de transparencia.

- vi. Puesto que la obligación de consentimiento expreso se entiende que no tiene cabida en el ámbito laboral, el deber de información resulta – a priori – ineludible.

El alcance de este deber informativo ante la instalación de sistemas de videovigilancia determina que debe realizarse previamente a la instalación, de manera expresa, clara y concisa; a todos los trabajadores afectados por las filmaciones, así como a sus representantes legales.

Sin embargo, esta obligación de información específica prevé la salvedad del supuesto en que se capte la “comisión flagrante de un acto ilícito”, determinando que en este escenario será suficiente con transmitir la información de manera genérica, con las garantías del art. 22 L O3/2018.

- vii. En base a la doctrina emanada del TC, así como del TEDH, cabe entender que, de manera excepcional, podrá prescindirse del deber de información cuando existan razonables sospechas sobre la comisión de actos ilícitos – siempre y cuando resulte una medida proporcionada – cuando se considere que de haberse cumplido con las exigencias informativas, se hubiese frustrado la finalidad pretendida de verificación de irregularidades contractuales, así como la posibilidad de usar las filmaciones como medio probatorio.

En consecuencia, se abre una vía de excepcionalidad para la videovigilancia oculta, si bien, debiendo en estos casos guardarse, más si cabe, un estricto cumplimiento del resto de exigencias recogidas en el test *Barbulescu*.

- viii. A pesar del deber de sigilo que deben atender los representantes de los trabajadores en relación con las comunicaciones que reciban por parte del empresario, la doctrina considera que el deber información en materia de protección de datos personales también puede excluir a los representantes cuando esto pueda derivar en la frustración su interés legítimo.
- ix. Atendiendo a la legitimidad de la finalidad perseguida, no debe confundirse la mera utilidad o conveniencia empresarial, con la

indispensabilidad de la medida para garantizar la seguridad y el correcto funcionamiento de la actividad laboral.

- x. Según la última sentencia emanada del TEDH enjuiciando el caso López Ribalda, no cabe entender que pueda existir expectativa razonable de privacidad en lugares visibles o accesibles al gran público o en aquellos espacios donde tengan pleno acceso otros compañeros.

5. BIBLIOGRAFÍA CONSULTADA.

CEOE. Plan Digital 2020 - La digitalización de la sociedad española, 2016.

MIÑARRO YANINI, M. “Impacto del reglamento comunitario de protección de datos en las relaciones laborales. Un – pretendido – ‘cambio cultural’”, en *Revista mensual núm. 423, CEF – Trabajo y Seguridad Social*. ISSN: 1138 – 9532, 2018. Págs. 5 – 15.

GOÑI SEIN, J.L. “El poder del ojo mecánico y la determinación de los límites de la libertad de vigilancia empresarial”, en *Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, 2007. Págs. 15 – 50.

GOÑI SEIN, J.L. “Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del reglamento europeo de protección de datos de 2016”, en *Revista de derecho social*, ISSN 1138-8692. Núm 78, 2017. Págs. 15 – 42.

MERCADER UGUINA, J., “Les libertés individuelles dans l’entreprise à l’épreuve des nouvelles technologies. Observations à partir de la situation espagnole”, AA. VV. (Dir. AUVERGNON, Ph.) *Les libertés individuelles et relations de travail: le possible, le permis et l’interdit*. Presses Universitaires de Bordeaux, 2011, p. 148; COELHO MOREIRA, T., “A privacidade dos trabalhadores e a utilização de redes sociais online: algumas questões”, *Questões Laborais*. Núm. 41, 2013.

RODRIGUEZ ESCANCIANO, S. “Vigilancia y control en la relación de trabajo: la incidencia de las nuevas tecnologías”, en *La protección de datos de carácter personal en los centros de trabajo*, F. Largo Caballero, CLI – CINCA, Madrid, 2006.

GONZALEZ GONZALEZ, C. “Control empresarial de la actividad laboral mediante video vigilancia y colisión con los derechos fundamentales del trabajador. Novedades del Proyecto de la Ley Orgánica de protección de datos y derechos digitales” en *Revista Aranzadi Doctrinal*, ISSN 1889-4380, Núm. 4, 2019.

VILLALBA CANO, L. *La videovigilancia laboral y su incidencia en el derecho de protección de datos a la luz de la jurisprudencia constitucional y del reglamento europeo 2016/679*; en FODERTICS 7.0 Estudios sobre derecho digital, BUENO DE MATA, F. (DIR), Editorial Comares, ISBN: 9788490457658, 2019. Págs. 205 – 214.

SERVICIO DE ESTUDIOS DEL PARLAMENTO EUROPEO, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado. España*, en Unidad de Biblioteca de Derecho Comparado. Octubre, 2018.

- VALDÉS DE LA VEGA, B.: “El derecho a la intimidad y su expectativa de respeto en el uso personal de las tecnologías de la información y comunicación en el trabajo. Un comentario a la sentencia del Tribunal Supremo de 26 de septiembre de 2007 y a la doctrina del Tribunal Europeo de Derechos Humanos”, en *Revista de Derecho Social*, núm.42, 2008. Págs. 143 – 157.
- CARRILLO, M. *Los límites a la libertad de prensa en la constitución española de 1978*, Barcelona, 1987. ISBN 13: 9788476650400.
- RODÍGUEZ-PIÑERO ROYO, M., *Las nuevas tecnologías en la empresa*, Consejo Andaluz de Relaciones Laborales, Sevilla, 2006. ISBN: 846894677X.
- SERRANO OLIVARES, R., “El derecho a la intimidad como derecho de autonomía personal en la relación laboral”, en *Civitas. Revista española de derecho del trabajo*. Núm. 103, 2001. ISSN 0212-6095. Págs. 97 – 124.
- BAZ RODRÍGUEZ, J.: “Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre [BOE n. o 267, de 7-XI-2013]”, en *Revista Ars Iuris Salmanticensis*, Vol. 2. Núm 1. ISSN-e 2340-5155 2014. Pág. 364 – 367.
- VALVERDE ASECIO, A.J.,”Protección de datos de carácter personal y derechos de información de los representantes de los trabajadores”, en *Revista andaluza de trabajo y bienestar social*. Núm. 118/ 2013. Págs. 13 – 54.
- VILLALBA CANO, L. “Jurisprudencia constitucional. La contradicción entre las SSTC 29/2013, de 11 de febrero y 39/2016, de 3 de marzo”, en FODERTICS 7.0 Estudios sobre derecho digital, BUENO DE MATA, F. (DIR); en *La videovigilancia laboral y su incidencia en el derecho de protección de datos a la luz de la jurisprudencia constitucional y del reglamento europeo 2016/679*, Editorial Comares, ISBN: 9788490457658, 2019.
- MIÑARRO YANINI, M. “Impacto del reglamento comunitario de protección de datos en las relaciones laborales. Un – pretendido – ‘cambio cultural’”. *Revista mensual CEF – Trabajo y Seguridad Social*. Núm. 423, ISSN: 1138 – 9532, 2018. Págs. 5 – 15.
- SERRANO OLIVARES, R. “Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales” en *Revista IUSLabor 3/2018*, ISSN 1699-2938, 2018.

- GOÑI SEIN, J.L. “Principios de protección de datos aplicables en el momento de la adopción del sistema de videovigilancia empresarial”, en *Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson Civitas, 2007. Págs. 106 – 136.
- PALOMEQUE LOPEZ, M.C., *Los derechos laborales en la Constitución Española*. CES, Madrid, 1991.
- VILLALBA SANCHEZ, A. “El derecho fundamental a la protección de datos del trabajador frente a los poderes del empresario, con especial referencia al consentimiento del trabajador”, en CASTRO MARQUES, E. (coord.): *Digital work and personal data protection: key issues for the labour of the 21st century*. Cambridge Scholars Publishing, Cambridge, 2018. Págs. 473 – 493.
- ROJAS ROSCO, R., Y LÓPEZ CARBALLO, D., “El impacto del RGPD en el ámbito del control laboral y la era de la innovación”, en *Actualidad Civil*. Núm. 5, 2018.
- HENRÍQUEZ TILLERÍA, S. “Transición de la doctrina del Tribunal Constitucional en materia de videovigilancia laboral y el derecho a la protección de datos personales”, en *Protección de Datos, videovigilancia laboral y doctrina de la Sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información*, en *IUSLABOR 3/2019*, ISSN 1699 – 2938. Págs. 55 – 80.
- LAHERA FORTEZA, J. “Nueva jurisprudencia constitucional en la videovigilancia laboral. Valoración crítica (STC 39/2016, 3 de marzo)”, en *Derecho de las relaciones laborales*, núm. 5, 2016. Págs. 494 – 499.
- GOÑI SEIN, J.L., “Vigilancia empresarial y protección de datos: Doctrina Jurisprudencial”, en *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*. GOÑI SEIN, J.L., “Vigilancia empresarial y protección de datos: Doctrina Jurisprudencial”, en *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*. Núm. 143, 2019, págs. 191-216.
- GOÑI SEIN, J.L. “Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo [BOE nº.85, de 8-IV-2016]. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información”, en *Reseñas de Jurisprudencia (Enero – Junio 2016) Trabajo y Seguridad Social. Ars Iuris Salmanticensis*, Vol. 4. eISSN: 2340 – 5155. Universidad de Salamanca, 2016. Págs. 288 – 291.
- RUÍZ GONZÁLEZ, C.M., “Las nuevas propuestas interpretativas del Tribunal Europeo de Derechos Humanos sobre el control del uso laboral de la tecnología de la empresa:

Barbulescu y López Ribalda”, en *Cuadernos de Derecho Transnacional*, Vol. 10, núm. 2º. ISSN 1989-4570, 2018. Págs. 915 – 930.

Servicio de Estudios del Parlamento Europeo, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado*. Consejo de Europa, en Unidad de Biblioteca de Derecho Comparado. Octubre, 2018.

6. JURISPRUDENCIA CONSULTADA.

STEDH Barthold vs Alemania, de 25 de marzo de 1985.

STEDH Von Hannover vs Alemania, de 7 de febrero de 2012.

STEDH Fernández Martínez vs España, de 12 de junio de 2014.

STEDH Barbulescu vs Rumania, de 5 de septiembre de 2017.

STEDH López Ribalda y otros vs España, de 9 de enero de 2018.

STEDH, Gran Sala, López Ribalda y otros vs España, de 17 de octubre de 2019.

STC 231/1988, de 23 de diciembre de 1988. Rec. 1.247/1986.

STC 179/1991, de 19 de septiembre de 1991. Rec. 184/1989.

STC 254/1993, de 20 de julio de 1993. Rec. 1.827/1990.

STC 57/1994, de 28 de febrero de 1994. Rec. 1.445/1991; 2.302/1990.

STC 143/1994, de 9 de mayo de 1994. Rec. 3.192/1992.

STC 98/2000, de 10 de abril de 2000. Rec. 4.015/1996.

STC 186/2000, de 10 de julio de 2000. Rec. 2662/1997.

STC 292/2000, de 30 de noviembre de 2000. Rec. 1.463/2000.

STC 156/2001, de 2 de julio de 2001. Rec. 4641/1998.

STC 12/2012, de 30 de enero de 2012. Rec. 4.829/2009.

STC 241/2012, de 17 de diciembre de 2012. Rec. 7.304/2007.

STC 29/2013, de 11 de febrero de 2013. Rec. 10.522/2009.

STC 176/2013, de 21 de octubre de 2013. Rec. 1.783/2010.

STC 39/2016, de 3 de marzo. Rec. 7.222/2013.

STSJ de Galicia, de 25 de enero de 1996. Rec. 3/1996.