eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea

Trabajo de Fin de Grado

Facultad de Derecho de la Universidad del País Vasco (UPV/EHU)

LA PRUEBA DE LA VIDEOGRABACIÓN PARA CAUSALIZAR UN DESPIDO DISCIPLINARIO: UN ANÁLISIS DESDE LA GARANTÍA DE LOS DERECHOS DE VIGILANCIA Y PROTECCIÓN DE DATOS PERSONALES DE LOS TRABAJADORES

2022

Autora: Silvia López Velasco

Directora: Miren Edurne Terradillos Ormaetxea

ÍNDICE

ABREVIATURAS

Art(s).	Artículo(s)
AEPD	Agencia Española de Protección de Datos
CE	Constitución Española
DPD	Derecho a la Protección de Datos
ET	Estatuto de los Trabajadores
FJ	Fundamento Jurídico
TC	Tribunal Constitucional
TIC	Tecnologías de la información y la comunicación
TS	Tribunal Supremo
LEC	Ley de Enjuiciamiento Civil
LOPD	Ley Orgánica de Protección de Datos
LOPDGDD	Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
LORTAD	Ley Orgánica De Regulación Del Tratamiento Automatizado De Los Datos De Carácter Personal
LRJS	Ley Reguladora de la Jurisdicción Social
p(p).	Página(s)
Rec.	Recurso
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
STC (SSTC)	Sentencia(s) de Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
STSJ	Sentencia del Tribunal Superior de Justicia
TEDH	Tribunal Europeo de Derechos Humanos

1. INTRODUCCIÓN

En la actualidad, es un hecho indudable que el continuo desarrollo de las nuevas tecnologías de la información y la comunicación (TIC) han supuesto todo un reto para el Derecho. Esto se debe a la necesidad de ofrecer una regulación actualizada y adaptada de las realidades sociales, hecho que provoca un cambio en cada una de las vertientes del Derecho. Será éste, precisamente, el ámbito de las relaciones laborales en el que nos centraremos en este trabajo.

El objeto de este Trabajo de Fin de Grado (TFG) consiste en el análisis de los conflictos que se están suscitando en las relaciones de trabajo, debido al empleo de una de las medidas que mayor auge ha tenido en la evolución de las TICs: la videovigilancia. En este sentido, es importante remarcar los derechos que entran en colisión debido al uso de los sistemas de vigilancia, esto es, el derecho de dirección empresarial y el derecho fundamental a la intimidad junto con el derecho a la protección de datos personales de los trabajadores. En ese marco, será sustancial que se respeten los derechos fundamentales de los trabajadores cuando ejercen los poderes de dirección y disciplina en la empresa, para que la prueba obtenida a través de la videovigilancia sea lícita.

Para este estudio, partiremos del marco jurídico relativo al derecho fundamental de la protección de datos personales, comenzando por el CEDH en el que haremos hincapié en el derecho a la intimidad, siguiendo por el análisis del Reglamento (UE) 2016/679. En este análisis no faltará, tampoco, la más relevante doctrina del TEDH dictada en relación con el art. 8 CEDH y su impacto en la jurisprudencia de nuestro país.

Respecto a la normativa española, haremos un breve estudio de la nueva Ley 3/2018 de protección de datos personales y derechos digitales, en concreto, acerca de los límites que establece al derecho a la intimidad y, con mayor detenimiento, el tratamiento que ofrece respecto a los datos captados por la videovigilancia. A su vez, daremos una perspectiva jurisprudencial respecto a los mismos, para conocer los criterios que siguen los órganos judiciales y cómo resuelven las controversias que surgen entre el derecho fundamental a la intimidad, el derecho a la protección de datos y el poder empresarial.

Por último, en el apartado final analizaremos la adaptación de las pruebas de videovigilancia en el proceso laboral, su calificación y, los efectos que produce la prueba ilícitamente obtenida respecto a un despido disciplinario.

Huelga apuntar que este TFG seguirá una metodología jurídica, de modo que nuestras reflexiones, desde el análisis crítico, se apoyarán en la ley, la jurisprudencia y la doctrina científica.

2. MARCO JURÍDICO DEL DERECHO A LA PROTECCIÓN DE DATOS (DPD)

a. EL DPD EN EL CONSEJO DE EUROPA: El art.8 del CEDH y su Jurisprudencia.

El desarrollo de los medios tecnológicos ha facilitado la obtención de la información respecto a las circunstancias personales tanto del ciudadano como del trabajador y, por ende, tener conocimiento de sus datos personales, por ejemplo, permitiendo que noticias anteriormente diseminadas aparezcan instantáneamente reunidas en un soporte digitalizado, posibilitando, además, métodos de recogida sin conocimiento por parte del trabajador afectado, de modo que el empresario puede acceder al contenido de los extremos personales con total ignorancia de éste[1].

Advertidos los alcances de los dispositivos electrónicos, informáticos y visuales frente a la privacidad del individuo en el marco de la relación laboral, el Derecho trata de fijar un difícil equilibrio entre la potestad empresarial a la hora de optimizar las posibilidades que le ofrecen las nuevas tecnologías, incluida la organización y el control de la mano de obra, y la preservación de los derechos y libertades fundamentales del trabajador; singularmente, el derecho a la protección de datos de carácter personal[2] (en adelante DPD).

Así pues, la doctrina constitucional ha delimitado el contenido del derecho fundamental del DPD, afirmando que "consiste en un poder de disposición y de control sobre

[1] GOÑI SEIN, J.L., "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", *Justicia Laboral,* Nº17, 2004, p.51.
[2] RODRÍGUEZ ESCANCIANO, S., "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Estudios financieros. Revista de trabajo y seguridad social,* Nº423, 2018, pp. 24-25.

los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"[3].

El derecho fundamental a la protección de datos lo encontramos reconocido, garantizado y protegido tanto en el ámbito nacional, como en el comunitario e internacional, pero son especialmente dos los preceptos más relevantes en los que nos vamos a centrar en un primer momento, para analizar el ámbito supranacional: el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea (en adelante CDFUE) y el Reglamento General de Protección de datos[4] (en adelante RGPD).

En primer lugar y en lo que al Consejo de Europa se refiere, conviene hacer hincapié en el art. 8 del Convenio Europeo de Derechos Humanos[5] relativo al derecho a la vida privada y familiar, debido a la estrecha vinculación que tiene respecto al DPD. A través del apartado primero de este art. se reconoce el "derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia", y la no injerencia por la autoridad pública salvo en los casos previstos por la ley, siempre y cuando sea una medida necesaria[6].

En lo que respecta a nuestro objeto de estudio, la videovigilancia laboral, debemos entender la videovigilancia como un instrumento que permite la captación y grabación de la imagen en un soporte físico, así como la repetición ilimitada y el análisis de las mismas, lo que faculta al empleador a la supervisión de la actividad laboral del trabajador y puede servir, bajo unas exigencias legalmente establecidas, como objeto de prueba en los casos de incumplimientos laborales. Asimismo, se trata de una herramienta que permite crear una base de datos de información personal y obtener perfiles sociales de los trabajadores afectados[7].

---

[3] Sentencia del Tribunal Constitucional (en adelante STC) 292/2000, de 30 de noviembre, Fj. 7.

[4] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

[5] Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 1950 (en adelante, CEDH)

[6] Artículo 8.2 del CEDH: *"...sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."*

[7] GOÑI SEIN, J. L., "Controles empresariales. Geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social,* Nº39, 2009, p.11.

La videovigilancia suele ser un objeto de debate por la controversia que surge entre el objetivo defensivo del empresario y su derecho a controlar la seguridad de la empresa, frente al derecho a la vida privada y el DPD. Dada la gran polémica que desencadena este conflicto de intereses, creemos oportuno analizar los distintos pronunciamientos que ha dado el TEDH. Para ello, en un primer lugar y para realizar un acercamiento a la jurisprudencia que se usa como referencia, examinaremos el asunto de López Ribalda en relación con otros supuestos similares.

Se trata de un caso sobre la instalación de cámaras de seguridad con la intención de corroborar una serie de robos de productos de un supermercado por parte del personal de la empresa. El empleador había instalado unas cámaras visibles que apuntaban hacia las entradas y salidas del supermercado, para controlar los posibles robos de los clientes, y había informado a los trabajadores de dicha instalación. A su vez, instaló cámaras ocultas para vigilar mediante un zoom la zona de trabajo de las cajas registradoras, con el fin de captar los posibles ilícitos de la plantilla tras registrar considerables pérdidas, identificando diferencias entre las ventas y el inventario de productos, todo ello sin haber informado ni a los trabajadores ni al comité de empresa.

A través de la captación de las cámaras, las sospechas recayeron sobre cinco trabajadoras a las que se les acusaba por ayudar a clientes a hurtar productos así como de hacerlo ellas directamente. Así, una vez mostradas las imágenes a las trabajadoras, éstas finalmente reconocieron los hechos que fueron objeto de despidos disciplinarios. Posteriormente, las trabajadoras recurrieron a los tribunales del orden social, cuyas sentencias consideraron legítimas las grabaciones que acreditaban los hechos fundantes del despido, lo que les permitió acudir al TEDH, basando sus pretensiones en la supuesta vulneración del art. 8 del CEDH.

La sentencia de la Gran Cámara[8], considera ilícita la prueba obtenida por vulnerar el art. 8 del CEDH, al tratarse de cámaras ocultas que vigilaban de manera continuada, considerándolo intrusivo, y sin haber proporcionado la información previa y específica exigida por la Ley de Protección de Datos de Carácter Personal (en adelante LOPD)[9].

[8] Sentencia del Tribunal Europeo de Derechos Humanos (Sección 3ª), de 9 de enero de 2018 , Caso López Ribalda y Otros v. España (en adelante STEDH).
[9] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Además, a diferencia de otros casos como el de Köpke vs. Alemania[10] en el que la vigilancia encubierta se dirigió de manera específica contra dos trabajadores y por un tiempo limitado, en este asunto no se apoyaba en una sospecha anterior sobre las afectadas, sino sobre todo el personal, siendo grabados durante todo el periodo laboral[11].

Asimismo, la sentencia destaca que en caso de haber informado a las demandantes, incluso de modo general, de la instalación de dichas cámaras y proporcionando la información exigida por la LOPD, los derechos del empleador podrían haberse visto protegidos, en cierta medida[12]. De esta forma, el pronunciamiento da a entender que, en referencia al caso Köpke, podría haberse considerado lícita la instalación de cámaras ocultas con una mínima señalización sobre su ubicación[13].

Sin embargo, el Tribunal de Estrasburgo volvió a emitir un fallo sobre el caso López Ribalda[14], como respuesta al recurso del Estado contra la sentencia de la Gran Sala de 2018, rectificando su criterio y afirmando que los tribunales españoles no habían incurrido en la violación del art. 8 del CEDH.

Esta sentencia toma como referencia la dictada por la Gran Sala en el caso Barbulescu II[15] que trataba sobre el control por el empleador del uso del correo electrónico por sus empleados, y por la cual se establecieron las reglas a seguir en materia de control laboral. Éstas se asientan en la "expectativa de privacidad" del trabajador sobre sus conversaciones, y se han considerado aplicables *mutatis mutandis* en materia de videovigilancia, y deben aplicarse en consideración a las relaciones laborales y la intrusión en la vida privada de los empleados como consecuencia del desarrollo de las nuevas tecnologías[16].

[10] STEDH de 5 de octubre de 2010, Caso Köpke v. Alemania (dec.), nº 420/07.
[11] ALTÉS TÁRREGA, J. A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la STEDH López Ribalda (II)", *Revista General de Derecho del Trabajo y de la Seguridad Social,* Nº55, 2020, p. 351.
[12] STEDH (Sección 3ª), de 9 de enero de 2018 , Caso López Ribalda y Otros v. España.
[13] GARCÍA SALAS, A. I., "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018", *Revista de Información Laboral,* Nº2, 2018, p.443.
[14] STEDH (Gran Sala), de 17 de octubre de 2019, Caso López Ribalda y Otros v. España.
[15] STEDH (Gran Sala), de 5 de septiembre de 2017, Caso Barbulescu v. Rumanía II. Esta sentencia revoca la STEDH, de 12 de enero de 1016, caso Barbulescu v. Rumanía I.
[16] ALTÉS TÁRREGA, J.A. ,"La videovigilancia encubierta…", *op.cit.*, p.353.

En este contexto, la sentencia del caso López Ribalda II, en el párrafo 116 y siguientes, relativo a la evaluación final del Tribunal, menciona los criterios que los tribunales españoles han de tener en cuenta para resolver los intereses en conflicto sentados en el caso Bârbulescu, y que proporcionan una mayor protección de los derechos fundamentales afectados. Éstos se pueden sintetizar en los siguientes parámetros: "la necesidad de analizar la legitimidad de la medida y su justificación; la información previa proporcionada; el grado de intrusión en la privacidad del trabajador y el alcance del control realizado; la existencia de medidas alternativas menos invasivas; las consecuencias derivadas para los trabajadores; y las garantías establecidas por el empresario"[17].

Finalmente, conviene traer a colación que la jurisprudencia del TEDH no ha descartado de forma absoluta la validez de la prueba de la videovigilancia, aun en ausencia de cualquier información previa, siempre que concurran circunstancias especiales como una sospecha fundada de irregularidades, grabación selectiva del trabajador afectado, no indiscriminada, corto periodo de tiempo, etc[18].

b. EL DPD EN LA UE: El art. 8 de la Carta de derechos fundamentales de la Unión Europea y el Reglamento (UE) 2016/679, relativo a la protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos.

En lo que concierne al ámbito Europeo, contiene una regulación expresa sobre el DPD en la CDFUE, mediante la cual afirma que toda persona tiene derecho al mismo, así como a acceder a los datos recogidos que la conciernan y a su rectificación. Asimismo, asegura que dichos 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[19]. Si bien este precepto contiene alguna otra previsión relativa al derecho de toda persona a acceder a los datos recogidos que la conciernan y a su rectificación, la regulación jurídica del DPD se recoge en el RGPD.

[17] *Ibídem,* p.353.
[18] STEDH (Gran Sala), de 17 de octubre de 2019, Caso López Ribalda y Otros v. España.
[19] Art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000.

En este sentido, es importante analizar el RGPD, que junto con la Directiva 2016/880[20], conforma el nuevo marco europeo de protección de datos personales, y afecta intensamente al ámbito de las relaciones laborales, siendo éste el que nos interesa estudiar.

En el RGPD se concretan los principios generales y las reglas específicas de aplicación, que limitarán los poderes tanto disciplinarios como los de dirección y control que ostentan los empresarios, frente a los derechos fundamentales de los trabajadores como son el derecho a la intimidad, privacidad, protección de datos o el secreto de las comunicaciones, que se ven afectados. En cuanto a los principios, los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado[21], los cuales analizaremos más adelante.

Asimismo, en el apartado b) y c) del precepto anteriormente citado, se concreta que los datos deben ser recogidos con fines determinados, explícitos y legítimos, sin que puedan ser tratados posteriormente de manera incompatible con dichos fines, y se introduce el principio de minimización de los datos, es decir, que los mismos deben ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Entre los principios de tutela que incorpora el reglamento, considera como pilar fundamental, el consentimiento de la persona afectada para el tratamiento de sus datos personales[22], esto es, para que el tratamiento de datos personales pueda ser considerado lícito. El mismo consentimiento se entiende como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"[23]. En este sentido, queda excluido lo que se conocía como "consentimiento tácito", pues se sustituye por una acción afirmativa y expresa del afectado, y se recoge manifiestamente el deber de confidencialidad[24].

---

[20] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
[21] Art. 5.1.a), del RGDP.
[22] Art. 6.1 a) del RGPD.
[23] Art. 4.11 del RGPD.
[24] CRISTEA UIVARU, L., "Antecedentes en la Unión Europea en el marco de la regulación de los datos personales, objetivos y nuevos retos. Futuro de la protección de datos: análisis del Reglamento (UE) 2016/679 y

Además, el legislador precisa que el responsable del tratamiento de los datos debe ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales[25], "de forma que para que el consentimiento sea válido debe dejar rastro"[26].

Respecto a la forma del mismo, el consentimiento podrá ser otorgado mediante una declaración escrita, dejando un mayor margen para su manifestación, de tal forma que se podrán utilizar medios tradicionales, electrónicos, así como la marcación de una casilla o una enunciación verbal, exigiendo en todos los métodos que se preste de forma individualizada y atendiendo a todos y cada uno de los fines perseguidos[27].

No obstante, el propio ordenamiento establece algunas excepciones de interés respecto a la necesidad de prestar consentimiento. En este aspecto, en primer lugar se legitima el tratamiento de datos sin consentimiento cuando éste sea "necesario para la ejecución de un contrato en el que el interesado sea parte"[28]. En los siguientes apartados del mismo precepto se establecen otras excepciones, por ejemplo, cuando el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, en aquellos supuestos en los que se trata de cumplir un fin de interés público o cuando se trata de facilitar el ejercicio de poderes públicos conferidos al responsable del tratamiento o, en fin, cuando el tratamiento se destine a la satisfacción de intereses legítimos, siendo necesario efectuar en todos ello una evaluación aplicando el principio de proporcionalidad[29].

Como se ha mencionado anteriormente en relación con el consentimiento como requisito fundamental, lo cierto es que debe ir acompañado de manera inescindible de la información correspondiente, surgiendo así el consentimiento informado. Por tanto, como regla, el interesado o afectado ha de prestar su consentimiento explícito para la recogida y tratamiento de sus datos y, al mismo tiempo, el responsable del tratamiento de los mismos tendrá la obligación de prestarle la debida información sobre el objeto y fines de esas

---

el nuevo modelo de privacidad", *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud,* J.M. Bosch Editor, Barcelona, 2018, p.250.

[25] Art. 7.1 del RGPD.

[26] SERRANO GARCÍA, J. Mª., "Límites de la ley de protección de datos al poder de dirección del empresario", *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia,* Editorial Bormazo, Albacete, 2019, p. 24.

[27] RODRÍGUEZ ESCANCIANO, S.,"El derecho a la protección de datos personales…", *op.cit.*, p.28.

[28] Art. 6.1 b) del RGPD.

[29] RODRÍGUEZ ESCANCIANO, S.,"El derecho a la protección de datos personales…", *op.cit.,* p.30.

operaciones, así como de los derechos subjetivos que se desprenden del tratamiento y que se encuentran a disposición del interesado[30]. Ahora bien, aún en los supuestos en que no se exija el consentimiento del trabajador, sigue siendo necesario el deber de información sobre la recogida, tratamiento, uso, plazo y conservación del tratamiento de los datos personales[31].

A su vez, este principio de transparencia requiere que toda la información y comunicación sea accesible y de fácil entendimiento, con un lenguaje sencillo y claro. Así pues, la información ha de prestarse con carácter previo y de modo expreso, de tal forma que si no se dan todos los requisitos exigidos y no es alertado de manera completa sobre las circunstancias particulares, el procedimiento deberá entenderse ilegal[32].

Finalmente, el reglamento en su art. 88, hace una pequeña mención al tratamiento de los datos personales en el ámbito laboral, respecto del cual extraemos que permite a los Estados miembros elaborar normas más específicas para garantizar la protección de los derechos y libertades en este ámbito[33]. En relación con este aspecto, es necesario señalar que dichas normas deberán preservar tanto la dignidad humana como los intereses legítimos y derechos fundamentales de los interesados, en concreto en la esfera de la transparencia del tratamiento, la transferencia de los datos personales y en los sistemas de supervisión en el lugar de trabajo[34].

---

[30] TASCÓN LÓPEZ, R., *El tratamiento por la empresa de los datos personales de los trabajadores,* Civitas/APDCM, Madrid, 2005, p.103.
[31] Arts. 13 y 14 del RGPD.
[32] THIBAULT ARANDA, J., "La vigilancia del uso de Internet en la empresa y la protección de datos personales", *Revista crítica de teoría y práctica,* Nº1, 2009, p.219.
[33] Art. 88.1 del RGPD: "*...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. "*
[34] Art. 88.2 del RGPD.

c. La Ley 3/2018, de protección de datos personales y garantía de los derechos digitales.

En lo que respecta a la normativa nacional, el DPD es un derecho fundamental, autónomo, con una regulación propia en el art. 18.4 de la CE, que permite a las personas obtener un poder de disposición sobre sus datos personales y también saber quién posee esos datos y para qué, con la facultad de oponerse a esa posesión y su uso[35].

Hoy día, la Ley de Protección de Datos de Carácter Personal y garantía de los derechos digitales (en adelante LOPDGDD)[36] es la normativa nacional que desarrolla y adapta a nuestro ordenamiento el, anteriormente estudiado, RGPD, a su vez que trata de garantizar los derechos digitales de la ciudadanía amparados en la Constitución Española (en adelante CE)[37].

Si realizamos una visión desde comienzos de la aparición de la protección de datos personales en la normativa española, la CE de 1978 fue una de las primeras Constituciones europeas en introducir la protección de los datos frente al uso de la informática, encuadrándose dentro del art. 18 CE, como ya hemos mencionado[38]. En un primer momento, tal y como recoge el Preámbulo de la actual LOPDGDD[39], el desarrollo de este derecho fundamental se plasmó en la Ley Orgánica 5/1992, de 29 de octubre (en adelante LORTAD)[40], pero fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre (LOPD)[41], para adaptar el sistema jurídico español a la Directiva aprobada por la Unión Europea[42].

Entre las principales novedades que incluía la LOPD, podemos observar el objeto de la normativa, que se basaba en proteger "el control que a cada uno de nosotros nos

[35] VALLE MUÑOZ, F. A., "Control tecnológico empresarial y licitud de la prueba en el proceso laboral" desarrollado en el marco del proyecto de investigación *Nuevos retos tecnológicos del derecho probatorio* a cargo del Ministerio de Ciencia e Innovación, 2021-2024, Nº399, 2016, p.3.
[36] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
[37] Art. 1 a) y b) de la Constitución Española, de 29 de diciembre de 1978.
[38] Seminario Iberoamericano *"Nuevos retos del derecho a la intimidad",* Conclusiones finales, en Monteviedo, a fecha 15 a 18 de junio de 2015.
[39] Apartado I de la Exposición de Motivos de la LOPDGDD.
[40] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
[41] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[42] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar, en último extremo, el libre desarrollo de nuestra personalidad"[43]. En esta línea, la LOPD destaca por ser la norma que trata de impedir los menoscabos que pudieran ocasionar el uso incontrolado de los dispositivos informáticos, limitando y racionalizando la utilización de los mismos[44].

Como ya hemos analizado en otro momento, la UE aprobó el RGPD, surgiendo así incompatibilidades entre las normas de la LOPD y el reglamento, por lo que se procedió a la aprobación de la actual LOPDGDD ya que el legislador español lo consideró necesario para una adecuada adaptación al RGPD[45]. En esta línea, es importante destacar que el objeto de esta normativa española no es únicamente adaptar el ordenamiento jurídico español al reglamento, sino también garantizar los derechos digitales de la ciudadanía[46].

La ley orgánica española destaca dentro de nuestro ámbito de estudio por las novedades que incluye respecto a las relaciones laborales. Entre otras, ocupa lugar el reconocimiento del derecho a la desconexión digital (art.88 LOPDGDD), el derecho a la intimidad frente al uso de dispositivos de vigilancia y grabación de sonidos (art.89 LOPDGDD), el derecho de utilización de sistemas de geolocalización (art.90 LOPDGDD) y el derecho a la intimidad y uso de dispositivos digitales (art. 87 LOPDGDD).

[43] RAYA CABRERA, J. L., y RAYA GONZÁLEZ, L., *Instalación y Configuración de Sistemas Operativos,* RA-MA.SA, Madrid, 2011.
[44] VICENTE PARCHÉS, F., "Protección de datos personales y agentes intermediarios de colocación: la tutela de la libertad informática-intimidad del demandante de empleo", *Revista de trabajo, economía y sociedad,* Nº64, 2012, p.6
[45] MARCOS AYJÓN, M., "Cuestiones fundamentales en el derecho a la protección de los datos de carácter personal", *La protección de datos de carácter personal en la justicia penal,* J.M. Bosch editor, Barcelona, 2020, pp. 82 y 83.
[46] FERNÁNDEZ DOMINGUEZ, J. J., "El marco jurídico de la protección de datos personales: Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre", *Revista del Ministerio de Trabajo y Economía Social,* Nº.148, 2021, pp.46 y 47.

3. DERECHO A LA INTIMIDAD DEL TRABAJADOR EN LA LEY 3/2018, SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y DERECHOS DIGITALES (ART. 87 Y SS.)

a. Los límites del derecho a la intimidad

En la medida en que la relación laboral es subordinada, siendo el trabajador por cuenta ajena quien presta sus servicios al empresario dentro de su ámbito de organización y dirección[47], la postura en la que se encuentra el empresario le otorga tres tipos de poderes: directivos, de control y disciplinarios, en tanto que su ejercicio respete los derechos fundamentales y libertades públicas garantizadas por la constitución[48].

El poder de dirección de empresa se ampara en el derecho de la libertad de empresa, reconocido y garantizado en el art. 38 de la CE. Dicho control empresarial viene delimitado por el art. 20.3 del ET, que contempla la posibilidad de que el empresario "adopte medidas que estime más oportunas de vigilancia y control", en cuanto sus fines sean verificar el cumplimiento de la relación laboral, observando como límite el respeto a la dignidad de los trabajadores. En este sentido, se ha de entender que le corresponde a la empresa la selección de los medios que estime adecuados para ejercer el control, sin que la modificación de los sistemas establecidos conlleve una modificación sustancial de las condiciones de trabajo[49]. Por ello, podemos entender que el derecho a la intimidad del trabajador genera un gran límite en la facultad de control del empresario[50].

Por tanto, podemos apreciar que, junto con el DPD, otro de los principales derechos fundamentales del trabajador que se pueden ver afectados por el control empresarial es el derecho a la intimidad, previsto en el art. 18.1 de la CE. La doctrina constitucional ha desarrollado su contenido apoyando que "su función es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su

[47] Art.1.1 del texto refundido de la Ley del Estatuto de los Trabajadores, de 24 de octubre de 2015 (en adelante ET).
[48] CRUZ VILLALÓN, J., *Compendio de Derecho del Trabajo,* Tecnos, Madrid, 2021, pp. 212 y 217.
[49] SÁNCHEZ PÉREZ, J., "El conflicto entre el control empresarial y el derecho a la intimidad en la era de las nuevas tecnologías", *Revista General del Derecho del Trabajo y de la Seguridad Social,* Nº59, 2021, p. 482.
[50] FERRANDO GARCÍA, Mª. F., "Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías", *Revista de Trabajo y Seguridad Social,* p.40.

voluntad"[51]. Éste, mantiene una relación directa con el art. 18.4 de la CE, en la medida que garantiza una protección especial al derecho a la intimidad en el campo de la informática.

Es importante remarcar en este momento la diferencia entre el ya definido DPD y el derecho a la intimidad, y recordar que el Tribunal Supremo (en adelante TS) señala que "el derecho a la protección de datos atribuye a su titular un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad"[52]. A su vez, atendiendo a la doctrina del Tribunal Constitucional (en adelante TC), considera que, a diferencia del derecho a la intimidad, el DPD "no reduce su protección a los datos íntimos, sino que su objeto es más amplio, refiriéndose a cualquier tipo de dato personal".

En este punto, conviene recordar que el ET recoge expresamente el derecho a la intimidad de los trabajadores en su art. 4.2 e), y en concreto el derecho a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en materia de protección de datos personales y garantía de los derechos digitales respecto a la LOPDGDD[53].

Asimismo, la LOPDGDD le dedica al derecho a la intimidad varios preceptos respecto a los dispositivos digitales en el ámbito laboral, pues el art. 87, en su primer apartado, se limita a reconocer el derecho a la intimidad de los trabajadores en el uso de los dispositivos. El empresario sólo tendrá acceso a aquellos contenidos de los dispositivos digitales que proporcione a los trabajadores que tengan como único objetivo el de controlar el cumplimiento de las obligaciones laborales o convencionales[54]. Además, en su apartado tercero establece que para la utilización de aquellos dispositivos digitales se deberán establecer criterios de utilización, en coherencia con el derecho a la intimidad, para los cuales deberán asistir los representantes en su elaboración. Para terminar, cabe resaltar que en su último apartado admite los dispositivos digitales para fines privados, toda vez que se especifiquen los usos permitidos y se establezcan las garantías que preserven su intimidad.

Desde otra perspectiva, la LOPDGDD también contempla el derecho a la intimidad frente a los sistemas de geolocalización en el art. 90 LOPDGDD. Ésta, reconoce el derecho

[51] STC 292/2000, de 30 de noviembre, Fj. 6.
[52] STS de 7 de febrero de 2018, Rec. 78/2017
[53] Art.20. bis del ET.
[54] SÁNCHEZ PÉREZ, J., "El conflicto entre el control empresarial…", *Op.cit.,*p. 479.

del empresario al control mediante sistemas de GPS, siempre que, con carácter previo, la empresa haya informado de forma expresa, clara e inequívoca a los trabajadores (o sus representantes), para poner en conocimiento su existencia y características de los mismos[55].

En la actualidad, son varios los pronunciamientos jurisprudenciales respecto a la implantación de sistemas de geolocalización, y debe señalarse que la mayoría abordan la posible vulneración del derecho fundamental del trabajador a la intimidad, teniendo en cuenta que, en ocasiones, su uso lleva al despido del trabajador por el incumplimiento de sus obligaciones laborales[56].

En cuanto a la geolocalización fuera de la jornada laboral, es destacable la STSJ de Asturias de 27 de diciembre de 2017[57], por la que se alega la ilicitud del control de los desplazamientos por medio de dispositivos GPS en los vehículos de la empresa. En este supuesto, la empresa había cumplido con el deber de informar tanto a trabajadores como a los representantes de los mismos. Sin embargo, en tanto que el vehículo está a disposición del trabajador fuera de la jornada laboral, el sistema GPS se mantiene activo todo el tiempo sin el consentimiento de los trabajadores, por lo que su implantación es considerada no proporcional. La sentencia destaca que una vez finaliza la jornada laboral, las facultades de control y dirección del empresario desaparecen, por lo que, a partir de ese momento, es imprescindible el consentimiento de los trabajadores para mantener en funcionamiento el sistema GPS y para el análisis automatizado de los datos personales conseguidos a través del mismo[58].

En otro sentido, el Tribunal Supremo en la STS de 5 de septiembre de 2020, ha considerado lícita la aplicación de estos sistemas cuando, también cumplido el deber de información al trabajador, se haya delimitado en este caso el uso del vehículo de la empresa exclusivamente para la realización de sus labores en el marco de la relación laboral. En este caso, consta que la trabajadora utilizaba el vehículo en los periodos de descanso, así como durante su situación de baja, pese a existir una prohibición expresa. Por tanto, considera que

[55] Art. 90.2 de la LOPD.
[56] MARÍN MALO, M., "La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente", *LABOS Revista del Derecho del Trabajo y Protección Social,* Nº1, 2020, p.111.
[57] STSJ de 27 de diciembre de 2017, Asturias, Rec. 3058/2017.
[58] STSJ de 27 de diciembre de 2017, Asturias, Rec. 3058/2017, Fj. 5.

"si no existe una situación de tolerancia del uso personal, tampoco existirá ya una expectativa razonable de intimidad"[59].

Al hilo de la jurisprudencia actual, el TS contempla supuestos de sistemas de geolocalización en dispositivos personales del trabajador. Éste, se ve reflejado en la STS de 8 de febrero de 2021[60], que confirma la nulidad de un nuevo proyecto de negocio denominado "proyecto Tracker", puesto en marcha por la empresa Telepizza, que consistía en incluir una cláusula en el contrato de forma unilateral, por la que les imponía a los repartidores descargarse una aplicación en su teléfono personal. La Sala considera que dicha obligación supone una vulneración al derecho de privacidad de los trabajadores y al DPD, por incumplimiento del deber de información[61].

b. Tratamiento de datos captados por la videovigilancia

En lo que respecta al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, en este epígrafe nos limitaremos a desglosar el art. 89 de la citada ley que se ocupa de regular la videovigilancia como sistema de control empresarial.

En primer lugar, el art. 89 en su primer apartado permite al empresario el uso de cámaras de videovigilancia con el fin de controlar la actividad laboral, "siempre que estas funciones se ejerzan dentro de su marco legal". Esta facultad del empresario está amparada, a su vez, en el Estatuto de los Trabajadores, permitiéndole "adoptar medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones laborales", si bien tiene como límite que ello habrá de realizarse "guardando en su adopción y aplicación la consideración debida a su dignidad"[62].

Ante estas situaciones anteriormente descritas, la LOPDGDD exige que el trabajador y, en su caso, sus representantes, sean previamente informados, de modo claro y explícito acerca de esta medida de las cámaras y sea posible salvaguardar su derecho a la intimidad[63], el cual abordaremos más adelante. De este modo, la ley admite esta forma de control a través

[59] STS de 5 de septiembre de 2020, Rec. 528/2018, Fj. 2.6.
[60] STS de 8 de febrero, Rec. 84/2019.
[61] SÁNCHEZ PÉREZ, J., "El conflicto entre el control empresarial…", *Op.cit.*, pp. 481-482.
[62] Art. 20.3 del ET.
[63] Art. 89.1 de la LOPDGDD.

de cámaras cuando se encuentren plenamente justificadas y se entienda que su colocación es razonable y proporcionada al fin perseguido[64].

Sin embargo, cuando la finalidad del uso de la videovigilancia sea captar un acto ilícito, se reduce el derecho de información sin que llegue a desaparecer, de modo que, para que se entienda cumplido el deber de informar[65], el precepto 22.4 de la propia ley exige la colocación de un dispositivo informativo en un lugar suficientemente visible identificando, como mínimo, la existencia del tratamiento, la entidad del responsable y la posibilidad de ejercitar los derechos que les proporciona el RGPD[66]. Igualmente, admite que el acceso a dicha información se haga a través de un código de conexión o dirección de internet a la misma, siendo necesario, en todo caso, que el responsable del tratamiento mantenga a disposición de los afectados la información referida[67].

En lo que al consentimiento se refiere, nada dice el art. 89 al respecto, por lo que nos remitimos al art. 6.3 de la misma ley, el cual admite el tratamiento de datos sin el consentimiento del trabajador, exigiendo únicamente la información, en los supuestos en que sea necesario para el mantenimiento, desarrollo o control de la actividad.

No obstante, la no necesidad de consentimiento no exime al empresario del deber de informar de forma expresa, precisa e inequívoca sobre la existencia del tratamiento de los datos, y proporcionar la información básica[68], porque "la información forma parte del contenido esencial del derecho y sin ella se estaría vulnerando el derecho fundamental a la protección de datos"[69].

Es de trascendental importancia señalar la prohibición respecto a la instalación de sistemas de grabación, tanto de sonidos como de videovigilancia, en los lugares destinados al descanso de los trabajadores, tales como vestuarios, aseos y comedores. No obstante, en lo referente a la grabación de sonidos, se considera factible únicamente cuando se den razones

[64] SÁNCHEZ PÉREZ, J., "El conflicto entre el control empresarial…", *Op.cit.*, p. 490.
[65] Art. 89.1,2º de la LOPD.
[66] Se trata de los derechos previstos en los arts. 15 a 22 del RGPD: Derecho de acceso, rectificación y supresión.
[67] Art. 22.4 de la LOPD.
[68] Art.11 de la LOPDGDD: *La información básica a la que se refiere el apartado anterior deberá contener, al menos: a) La identidad del responsable del tratamiento y de su representante, en su caso; b) La finalidad del tratamiento; c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.*
[69] SERRANO GARCÍA, J. Mª, "Límites de la ley de protección…" *Op.cit.,* p.25.

solventes en cuanto a la seguridad de las instalaciones empresariales, los bienes o personas, siempre y cuando se respeten los principios de proporcionalidad e intervención mínima[70], siempre y cuando respeten "el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores"[71].

Para concluir, se trata de un precepto que delimita el derecho fundamental a la protección de datos y a la intimidad, "en función de criterios relacionados con el contenido de la información captada, el espacio donde esta se obtiene y con la captación de sonido"[72].

c. El juicio de proporcionalidad

Para entender la controversia surgida a cerca de la implantación de medidas de videovigilancia en el ámbito de la relación laboral entre empresario y trabajadores, debemos recordar la doctrina del TC, que parte de la base de que los derechos fundamentales no son absolutos e ilimitados, más bien, su ejercicio está sujeto tanto a los límites fijados expresamente por la CE como a otras limitaciones que protegen o preservan otros derechos o bienes protegidos constitucionalmente[73].

Partiendo de la premisa que establece la jurisprudencia del TC, es importante recordar, por tanto, que tanto el derecho a la intimidad como el DPD no son absolutos, por lo que surge así la posibilidad de confrontamiento con otros intereses constitucionales y los derivados de la facultad de dirección de la empresa. Frente a estos enfrentamientos, cabe la cesión de derechos, y así lo señala el TC respecto al derecho a la intimidad, afirmando "que ninguno de los derechos fundamentales, y pueden ceder ante intereses constitucionalmente relevantes, siempre y cuando sea necesario para lograr un fin legítimo, que sea una medida proporcionada para su alcance y que respete el contenido esencial del derecho"[74].

[70] SÁNCHEZ PÉREZ, J., "El conflicto entre el control empresarial…", *Op.cit.*, p. 480.
[71] Art.89.3 de la LOPDGDD.
[72] LÓPEZ BALAGUER, M., "El control empresarial por videovigilancia en la LOPD", *Revista andaluza de trabajo y bienestar social,* Nº151, 2020, p.361.
[73] STC 181/1990, de 15 de noviembre, Fj.3.
[74] SSTC 143/1994, de 9 de mayo, Fj.6, y 57/1994, de 28 de febrero, Fj.5.

A este respecto, conviene señalar que ”la celebración de un contrato de trabajo no implica de modo alguno la privación de para una de las partes, el trabajador, de los derechos que la constitución que la CE le reconoce como ciudadano”[75]. Por tanto, debe existir un control sobre las limitaciones que pueden afectar a los derechos, en nuestro caso dentro de las relaciones laborales, teniendo en cuenta que estas medidas han de ser proporcionadas y necesarias. Respecto a éstas, deberán tenerse en cuenta restricciones mínimas a la hora de implantar medidas que afecten a la intimidad de los trabajadores, tratando siempre de elegir el método menos invasivo, y que no exista otra que afecte en menor grado el derecho en la medida que le proporcione los mismos o mejores resultados[76].

En el momento en que entran en colisión derechos fundamentales, deben evaluarse conforme a “los intereses en presencia, mediante una adecuada ponderación de las circunstancias concurrentes”[77]. Son los órganos judiciales los encargados de establecer estas pautas de adecuación respecto a los medios de control a los que nos referimos en el caso, las medidas de videograbación, que se reducen a dos: en una primera etapa, limitaron el derecho a la intimidad de los trabajos a los vestuarios, servicios higiénicos, taquillas, armarios y zona de descanso o esparcimientos; y más adelante, se dio a conocer el principio de proporcionalidad[78].

Además, el CEDH considera este instrumento de ponderación, el juicio de proporcionalidad, como una medida necesaria para resolver las injerencias de las libertades que consagra el convenio, como son el derecho al respeto a la vida privada y familiar, la libertad de pensamiento, conciencia, religión, expresión, reunión y asociación[79]. En esta línea, podemos extraer de las decisiones que ha tomado el TEDH, la importancia de la aplicación del principio de proporcionalidad respecto a la protección de derechos y libertades públicas y, a su vez, la influencia que determina su aplicación en los tribunales nacionales. [80].

[75] STC 151/2004, de 20 de septiembre, Fj.7.
[76] MIGUEL BARRIO, R., “El juicio de proporcionalidad en la prueba de la videograbación oculta a las personas trabajadoras”, *Revista de trabajo y seguridad social,* Nº461-462, 2021, p.128.
[77] STC 186/2000, de 10 de julio.
[78] GUDE GERNÁNDEZ, A,, “La videovigilancia en el ámbito laboral y el derecho a la intimidad”, *Revista general de derecho constitucional,* Nº20, 2015, p. 9.
[79] Arts.8-11 del CEDH.
[80] PERELLÓ DOMÉNECH, I., “El principio de proporcionalidad y la jurisprudencia constitucional”, *Jueces para la democracia,* Nº28, 1997, p.70.

El juicio de proporcionalidad exige la superación de los tres juicios, que lo integran: idoneidad, necesidad y proporcionalidad en sentido estricto, los cuales procederemos a analizar detenidamente.

Respecto al juicio de idoneidad, este examen pretende analizar si la medida utilizada es adecuada en una doble vertiente, objetiva y subjetiva. El punto de vista objetivo se centra en el descubrimiento de la irregularidad que ha provocado daños en la empresa, y el subjetivo, asociado al anterior, está enfocado en que la captación esté dirigida a descubrir quién efectúa la infracción[81].

En relación con el juicio de necesidad, en este momento se examina la medida empresarial utilizada, de tal forma que se hace una ponderación entre la misma y otras que podrían ser adoptadas, y que afecten en menor medida al derecho de la persona empleada. Este examen pregona que se debe recurrir con preferencia a los medios menos intrusivos, en la medida que existan, por lo que la utilización del medio empleado debe ser justificada[82], de tal forma que no existan otras alternativas menos intrusivas para alcanzar el mismo fin con igual eficacia[83]. Por tanto, entendemos que estos sistemas deben actuar como última ratio, ya que en caso de existir otras medidas de menor carácter lesivo y la empresa las hubiese evitado para la instalación de la videovigilancia, el órgano juzgador podría considerar como ilícita la prueba obtenida mediante las cámaras[84].

En último lugar, el juicio de proporcionalidad en sentido estricto implica hacer una ponderación acerca de las ventajas y los perjuicios causados que ha supuesto la implantación de la medida, lo que es generalmente un balance entre el patrimonio empresarial y la intromisión del derecho. En el momento de evaluar la vulneración de estos derechos, ambos protegidos constitucionalmente, el derecho fundamental, en este caso el de la persona empleada, debe tener preferencia frente a otros derechos como el de propiedad y patrimonio empresarial o las facultades de dirección y control del trabajo que corresponden al empresario, cuya protección es menor. Sin embargo, no se da una valoración absoluta del

[81] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.*, p.133.
[82] GARCÍA SALAS, A. I., *Necesidades empresariales y derechos fundamentales de los trabajadores,* Lex Nova, Pamplona (Navarra), 2016, p.134.
[83] GUDE FERNÁNDEZ, A., "La videovigilancia en el ámbito laboral…", *Op.cit.,* p.27.
[84] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.*, p.133.

derecho fundamental, sino que es un planteamiento a tener en cuenta en cuanto a la ponderación de intereses, siendo necesario atender a los demás requisitos[85].

Dicho esto, cabe señalar que la aplicación del principio de proporcionalidad tiene una estructura escalonada, por lo que, en primer lugar debe ser idónea, y sólo si lo es se podrá evaluar si es necesaria, de modo que si estas dos se cumplen, se podrá alcanzar la técnica de ponderación en sentido estricto[86]. Con todo ello, es relevante a tener en cuenta que han de existir sospechas razonables respecto a la comisión de infracciones, pues la mera existencia de indicios no se consideran motivos suficientes que justifiquen la adopción de este tipo de medidas[87].

De modo ejemplificativo podemos traer a colación un pronunciamiento representativo de la actuación del TS de acuerdo con este procedimiento. En esta ocasión, el TS mediante auto[88] confirmó la sentencia dictada por el TSJ de Madrid[89] que consideró ilícita la instalación del sistema de videovigilancia, por no superar el criterio de proporcionalidad. En cuanto a los hechos más relevantes a tener en cuenta de la sentencia citada, conviene destacar que la empresa había instalado una cámara de grabación de imágenes en un lugar de paso de la empresa, estando en funcionamiento durante menos de 24 horas. En esas imágenes, se apreciaba cómo el actor se acercaba a una mesa y abría varias cajas, en una de las cuales se encontraba colocado un reloj perteneciente a un cliente de la empresa y que al desconectar la cámara ya no estaba. Sin embargo, en la carta de despido no se le imputaba la usurpación del reloj, sino "su extraña actitud, removiendo una serie de enseres existentes encima de la mesa", tal y como recoge el Fj.5 de la sentencia.

La cuestión a resolver se centra en determinar la validez de la prueba de videovigilancia, para lo cual se analizó si superaba o no el test de proporcionalidad. Tal y como expresó el TSJ en el fundamento jurídico quinto de la sentencia, no cumple con los requisitos constitucionales por lo siguiente: no resulta idónea, pues la carta de despido no le imputa al trabajador la apropiación de ningún objeto y la sentencia ha considerado acreditado que el actor se llevó el reloj en cuestión; además, la medida no parece necesaria, pues al

[85] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.*, p.133.
[86] UGARTE CATALDO, J. L., *La colisión de derechos fundamentales en el contrato de trabajo y el principio de proporcionalidad,* (Tesis de doctorado), defendida en la Universidad de Salamanca (España), en 2011.
[87] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.*, p.134.
[88] ATS 1215/2013, de 9 de enero, Rec.1469/2012.
[89] STSJ de 12 de marzo de 2012, Madrid, Rec.5929/2011.

colocar objetos encima de una mesa en un lugar de paso y dentro de unas cajas con accesibilidad sin dificultad, pueden existir otros medios habituales (locales o cajas cerradas) para proteger los objetos; y por último, no se puede apreciar la proporcionalidad de la medida, pues no cumple con los requisitos informativos legales, considerado como elemento de equilibrio para preservar los derechos fundamentales.

Por último, al razonamiento anterior, el Tribunal añade la falta de justificación por no haber acreditado la existencia de desapariciones de objetos ni que el actor fuera sospechoso de ningún comportamiento relacionado.

4. EL DERECHO A LA INFORMACIÓN PREVIA Y LA DOCTRINA JUDICIAL SOBRE LAS "CÁMARAS OCULTAS"

a. El deber de información previa

Una vez centrado el tema, podemos entrar a valorar los aspectos más importantes sobre los cuales será necesario analizar la jurisprudencia actual, como son el derecho a la información previa, el consentimiento del trabajador, y los límites en el uso de sistemas de videovigilancia.

En lo que este epígrafe ocupa, el deber de información es una garantía del DPD que, a su vez, se interpretará para proteger otros intereses relacionados como el de la libertad de empresa o la propiedad[90]. A título general y conforme a la legislación actual, la LOPDGDD, conviene precisar que, dentro de las facultades de dirección y control que ostenta el empresario, debe cumplir con la exigencia del art.89 sobre el deber de informar con carácter previo. Esta información se requiere para poder proceder al tratamiento de datos por las cámaras instaladas, por lo que se deberá informar respecto a lo que se pretende llevar a cabo y las consecuencias del tratamiento.

Este deber de informar que tiene el empresario se dirige a los trabajadores y, en su caso, a los representantes. Sin embargo, a pesar de que la ley exija al empresario elaborar los

[90] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.,* p.129.

criterios respecto al tratamiento de los datos, es cierto que el art. 87 de la LOPDGDD requiere la participación de los representantes de los trabajadores en la elaboración del mismo[91].

Respecto a lo que aquí interesa y, como ya hemos mencionado en anteriores epígrafes, debemos acudir al art. 12.1 del RGPD, al cual se remite el apartado 4 del art. 22 de la LOPDGDD, destinado al deber de información. Éste proporciona el sistema informativo a seguir, y exige al empleador que tome "las medidas oportunas para facilitar al interesado toda la información indicada en los arts. 13 y 14, así como cualquier comunicación relativa al tratamiento con arreglo a los arts. 15 a 22 y 34 del RGDP". Este sistema consiste en la colocación de un dispositivo informativo en un lugar suficientemente visible, así como un código de conexión o dirección de internet a esta información[92].

Existe una tercera modalidad basada en la instalación puntual y excepcional de una cámara oculta no anunciada ni advertida, ante sospechas fundadas de un determinado acto irregular o ilícito en el ámbito del desempeño laboral por parte de un trabajador[93]. En esta línea, tanto el TS como el TC se han pronunciado acerca de cuáles son las circunstancias a valorar en el juicio de ponderación para la resolución de los casos, una línea jurisprudencial que pasaremos a analizar.

En un primer momento, la STC 186/2000, de 10 de julio, analiza la instalación de una cámara oculta que apuntaba hacia tres cajas registradoras, ante las sospechas de irregularidades en las mismas. En este caso, el TC valora la necesidad de ponderar la injerencia y el interés perseguido a través de la medida, observando el triple juicio de idoneidad, necesidad y proporcionalidad. Siguiendo este sistema, el Tribunal concluyó que no se había producido una lesión al derecho a la intimidad en la medida que la instalación de la cámara quedaba justificada por existir razonables sospechas, no encontrar otra vía más idónea para la consecución del fin, y por estar limitada a un lugar con un tiempo determinado[94]. Además, respecto a la falta de información previa, señala estar justificada por el temor de la

[91] TERRADILLOS ORMAETXEA, M. E., "El derecho de información a los trabajadores y a sus representantes resultante del deber de información previo, como garantía del derecho a la protección de datos y como límite al ejercicio de las facultades de dirección y control de la empresa en relación con la instalación y el uso de dispositivos digitales en el contexto de la relación laboral", *Revista General de Derecho del Trabajo y de la Seguridad Social,* Nº58, 2021, p.8.
[92] Art.22 de la LOPDGDD.
[93] SÁNCHEZ PÉREZ, J., "El conflicto entre el control empresarial…", *Op.cit.*, p. 490.
[94] STC 186/2000, de 10 de julio, Fj.7.

empresa a que el conocimiento del sistema frustrara la finalidad pretendida, y que adolece de trascendencia constitucional.

Posteriormente, la STC 29/2013, de 11 de febrero, genera un cambio que gira entorno a la consideración del derecho o deber de información, ya que, a diferencia del anterior pronunciamiento, "el derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, pues es patente 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"[95]. Además, en el mismo fundamento jurídico, el Tribunal protege el requisito previo de información expreso, al entender a través de la jurisprudencia, que el interés empresarial no es una causa de justificación para aplicar medidas de vigilancia sin cumplir con el requisito de la información previa.

Sin embargo, la STC 39/2016 establece un nuevo criterio en base a la interpretación del deber de información previa. El supuesto se centra en la validez de la prueba obtenida por la empresa, una grabación de vídeo, obtenida a través de una cámara instalada como consecuencia de unas sospechas de hurto, y con cartel anunciador. Sin embargo, a pesar de tener conocimiento respecto a la existencia de cámaras, no había sido informada previamente, por lo que la cuestión principal se centra en resolver si es suficiente la información general como es el cartel anunciador o, por contra, una información específica, de manera expresa, precisa, clara e inequívoca[96].

La sentencia anteriormente citada declara no haberse producido lesión alguna al derecho a la intimidad, por considerar que la medida era idónea, necesaria y equilibrada. Además, destaca haber cumplido lo exigido por el art. 3 de la instrucción de la Agencia Española de Protección de Datos[97] vigente en ese momento, esto es, haber colocado "en las zonas videovigiladas, al menos un distintivo informativo ubicado en un lugar suficientemente visible", por lo que entiende cumplida la obligación de información previa, la información general anteriormente mencionada[98]. Así, para dar respuesta a la cuestión principal acerca de

[95] STC 29/2013, de 11 de febrero, Fj.7.
[96] GOÑI SEIN, J. L., "Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información", *Ars Iuris Salmanticensis,* Nº2, 2016, p.288.
[97] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
[98] STC 39/2016, de 6 de marzo, Fj.4.

las circunstancias a tener en cuenta respecto al juicio de ponderación a través de esta sentencia y la línea jurisprudencial, se entiende que el deber de información y el principio de proporcionalidad van a acudir de manera conjunta. Además, la doctrina que desarrolla esta resolución elimina la obligatoriedad de informar a la parte trabajadora de la finalidad de la instalación de cámaras para consideración de prueba ilícita. Por tanto, se acepta la validez de la misma informando de su existencia, no de su objetivo[99].

Acercándonos a la actualidad, parecía que con la sentencia de la Gran Sala del TEDH analizada en el epígrafe primero, se asentaba una línea jurisprudencial que acababa con las distintas interpretaciones de los tribunales respecto los criterios a seguir, ya que, por un lado se encontraba el criterio en favor del juicio de proporcionalidad para la superación del deber de información y, por otro lado, el del deber de información como requisito inexcusable por parte de la empresa[100].

Actualmente, debemos diferenciar entre la videovigilancia oculta y la que se realiza con conocimiento de la persona trabajadora. Como modelo actual podemos observar la STS 21/2019, de 15 de enero, que trata de remarcar la idea de la STC 39/2016, resaltando que el deber de información previa forma parte del contenido esencial del DPD, por lo que las medidas de videovigilancia deben ser informadas con carácter previo y puestos en conocimiento a la parte trabajadora, y se mantiene en que únicamente en los sistemas de videograbación oculta es cuando hay que entrar a valorar el juicio de proporcionalidad[101].

Por último, una vez analizado el principio de proporcionalidad junto con el deber de información previa, conviene dejar claro en qué circunstancias se ha de entrar a valorar tal juicio. El deber de información, en tanto se considera contenido esencial del DPD, conlleva el deber de cumplimiento del mismo para poder entrar a valorar el principio de proporcionalidad. Este requisito lo hemos podido apreciar en actuaciones de la Sala del TEDH, que "impiden acudir al examen de la proporcionalidad a condición de que la empresa hubiera cumplido debidamente su obligación de informar previamente"[102].

---

[99] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.*, pp.113 y 119.
[100] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.,* p.119.
[101] STS 21/2019, de 15 de enero, Rec.341/2017, Fj.3.
[102] TERRADILLOS ORMAETXEA, M. E., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español", *Revista de Derecho Social,* Nº80, 2017, p.152.

b. La no necesidad del consentimiento expreso del trabajador

Como regla general, el DPD otorga "la facultad de consentir la recogida, la obtención y el acceso a los datos personales"[103], por lo que la recogida y el tratamiento de datos personales ha de llevar consigo el consentimiento del afectado, tal y como exige el art. 6 del RGPD en su primer apartado.

Sin embargo, el control empresarial dentro de las relaciones laborales es una particularidad del contenido esencial del contrato y, "el consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario"[104]. Por tanto, la no necesidad de un consentimiento expreso encuentra razón en el art. 20.3 del ET en cuanto habilita al empresario a adoptar medidas de vigilancia y control en la medida que verifique el cumplimiento de las obligaciones y deberes laborales del trabajador.

Teniendo en cuenta la jurisprudencia, podemos partir de la STC 39/2016, que entiende que el consentimiento del trabajador en la relación laboral se posiciona en un segundo plano, pues se entiende implícito, siempre y cuando el tratamiento de los datos de carácter personal sea necesario para el mantenimiento y cumplimiento del contrato. El cumplimiento de la relación laboral abarca las obligaciones derivadas del contrato, por lo que es lícito el tratamiento de datos dirigido al control de la misma, considerándolo como una excepción a la exigencia del consentimiento.

No obstante, lo que aquí interesa sería determinar la finalidad del tratamiento, ya que sólo será necesario dicho consentimiento cuando el tratamiento de datos de los trabajadores afectados no guarde una relación directa con el cumplimiento del contrato o esté dirigido a una finalidad ajena del mismo[105]. Ahora bien, a pesar de que no sea necesario el consentimiento en los casos previstos, no podemos olvidarnos de que el deber de información sigue siendo necesario.

[103] STC 292/2000, de 30 de noviembre, Fj. 7.
[104] GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J. R., "La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Barbulescu v. Rumanía; nº61496/08; Gran Sala)", *Revista de Información Laboral,* Nº10, 2017, p.1.
[105] STC 39/2016, de 6 de marzo, Fj.3.

c. Límites en el uso de sistemas de videovigilancia y de escucha en los centros de trabajo

Uno de los límites el uso de sistemas de videovigilancia que hemos abordado en el epígrafe tercero se centra en la imposibilidad de grabar en lugares de descanso o esparcimiento de los trabajadores, como los vestuarios, aseos, comedores y semejantes.

En este sentido, una de las sentencias con mayor trascendencia actual a traer a colación es la STS de 13 de octubre de 2021, que trata de un conductor de autobús de una empresa de transporte público, que fue objeto de un despido disciplinario como consecuencia de la captación de las cámaras del interior del autobús, ya que en el tiempo de parada en cabecera las cámaras de seguridad le grabaron en varias ocasiones fumando, orinando desde el vehículo y haciendo tocamientos a una pasajera a la que en repetidas ocasiones le permitía viajar sin billete. En este caso, todos los trabajadores eran conocedores de la existencia de tres cámaras de grabación de imágenes en el interior del autobús, excepto el asiento del conductor, cumpliendo con los distintos informativos que advertían de su presencia.

Sin embargo y, en lo que aquí interesa, el trabajador se encontraba en tiempo de descanso en el momento en que se grabaron varias de las conductas antijurídicas. Sobre este aspecto, el pronunciamiento del Tribunal deja claro que "ello no excluye que un conductor de autobús urbano, tras finalizar una ruta y antes de empezar la siguiente, cuando se encuentra dentro del autobús, pueda incurrir en incumplimientos contractuales graves y culpables que afecten a sus obligaciones laborales, lo que justifica que las cámaras continuaran grabando durante esos lapsos temporales"[106]. Además, el hecho de que permitiera a una pasajera viajar sin billete, se trata de incumplimientos contractuales en el momento de su horario laboral, cuando conducía el vehículo.

Por todo ello, y haciendo hincapié en la naturaleza del trabajo de transporte urbano de pasajeros en autobús y del riesgo que ello conlleva para él y para terceros, el Tribunal considera que la instalación de las cámaras de vigilancia era una medida justificada, idónea, necesaria y proporcionada.

[106] STS de 13 de octubre de 2021, Rec.3715/2018, Fj.4

Por otro lado, como último límite a analizar serían los sistemas de grabación en los centros de trabajo que, como hemos analizado en el epígrafe tercero, sólo se admiten dentro de los límites que impone el art. 89.3 de la LOPDGDD, es decir, en caso de ser "relevantes los riesgos para la seguridad de las instalaciones, bienes y personas". Además, en relación con el art. 22.3 de la misma ley, estos datos de grabación tendrán que ser suprimidos en el plazo máximo de un mes desde su captación, "salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de las personas, bienes o instalaciones, debiendo ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación".

Ya se pronunció el TC al respecto en la STC nº 98/2000, de 10 de abril, que analiza la licitud de las cámaras de videovigilancia junto con la grabación de sonido en las mismas, ya que una empresa de casino, con el fin de controlar la actividad laboral, había instalado un circuito cerrado de televisión que incorporaba unos micrófonos para la recogida de conversaciones que se pudieran efectuar en varias secciones del casino. El tribunal expresa que los micrófonos no habían sido instalados como consecuencia de la detección de una quiebra en los sistemas de seguridad y control, sino que se trataba de una medida para complementar los sistemas de seguridad ya existentes en el casino, por lo que no quedó acreditada la existencia de riesgos y que fuera indispensable para el buen funcionamiento de la empresa.

De esta forma, el Tribunal concluyó que los sistemas de grabación de sonido no superaban los principios de proporcionalidad e intervención mínima, pues la finalidad perseguida era desproporcionada para el sacrificio que implica el derecho a la intimidad de los trabajadores. A través de este sistema, se podían captar conversaciones privadas y ajenas, tanto de trabajadores como de clientes, irrelevantes para el control de la relación laboral, pudiendo acarrear consecuencias negativas a los trabajadores que, iban a estar siendo escuchados por la empresa en todo momento[107].

[107] STC 98/2000, de 10 de abril, Fj.9.

5. LA CAUSA DISCIPLINARIA DEL DESPIDO

a. La prueba de la videovigilancia en el proceso laboral

Como hemos venido analizando a lo largo de este estudio, es cierto que otro de los factores que se ve afectado por el avance de las nuevas tecnologías es la prueba en el proceso, siendo en este caso el proceso laboral el que vamos a analizar.

El avance tecnológico conlleva una adaptación constante de la normativa procesal, teniendo que ampliar los medios de prueba. En este sentido, las TICs se han convertido tanto en una herramienta de control laboral como en un medio de prueba que permite al empresario demostrar judicialmente los incumplimientos contractuales de la parte trabajadora, conocidas como prueba electrónica o digital. A su vez, ésta ha sido definida como "aquella información contenida en un dispositivo electrónico a través del cual se adquiere el conocimiento de un hecho controvertido mediante el convencimiento psicológico, o bien como consecuencia de fijar una norma legal este hecho como cierto"[108].

Concretamente, uno de estas pruebas electrónicas o digitales es la medida de la videovigilancia en la relación laboral, que podría definirse como aquel registro electrónico realizado mediante sistema de vídeo, a través del cual pueden captarse imágenes de personas, dando una idea de qué estaba ocurriendo en un momento determinado, y cuya finalidad es la de vigilancia, exactamente de prevención, verificación e identificación de posibles actos irregulares, que sirven de prueba para sancionar a los trabajadores[109].

En cuanto a su habilitación legal, haremos un breve análisis del marco jurídico en el que se encuentra la prueba electrónica y, en concreto, la prueba de la videovigilancia. En este contexto, en primer lugar se encuentra el reconocimiento de la misma en el art. 24.2 de la CE, que permite utilizar los medios de prueba pertinentes en un proceso para su defensa.

En el ámbito del proceso laboral, la Ley Reguladora de la Jurisdicción Social (en adelante LRJS)[110] en el art. 90.1, autoriza a las partes a servirse de los medios de prueba

[108] VALLE MUÑOZ, F. A., "Las cámaras de videovigilancia en la empresa como medio de prueba en el proceso laboral", *Iuslabor,* Nº3, 2021, p.33.
[109] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.*, p.107.
[110] Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.

regulados en la ley, "incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos", es decir, las pruebas digitales. En este sentido, los medios de prueba regulados en la ley y admisibles en el proceso laboral a los que se refiere el art., son los descritos en el art. 299.1 de la Ley de Enjuiciamiento Civil (en adelante LEC)[111], que es de aplicación supletoria en virtud de la Disposición Final Cuarta de la LRJS[112]. Además, respecto a las pruebas electrónicas a las que nos estamos refiriendo, el art. 299.2 de la LEC admite los medios de reproducción de palabra, sonido e imagen, así como los instrumentos que permiten archivar y conocer o reproducir datos relevantes para el proceso.

Continuando con el reconocimiento de la prueba electrónica, a través de los arts. 382 y 383 de la LEC se reconoce el carácter autónomo de esta prueba, que incluye "los instrumentos de filmación, grabación y semejantes" y, por otro lado, el art. 384 recoge la utilización de los instrumentos y archivos informáticos[113].

Sin embargo, el ejercicio del derecho a utilizar los medios de prueba pertinentes se limita a las pruebas lícitas, que son aquellas que para su obtención no se hayan vulnerado los derechos fundamentales[114]. En este sentido, la Ley Orgánica del Poder Judicial[115] en el art. 11.1 garantiza la ineficacia de las pruebas obtenidas que, directa o indirectamente, hayan vulnerado los derechos o libertades fundamentales. Simultáneamente, también el art. 90.2 de la LRJS se pronuncia al respecto, señalando igualmente la inadmisión de las pruebas que tengan origen, directa o indirectamente, en la violación de derechos o libertades fundamentales.

Respecto a la cuestión que puede generar la ilicitud de la prueba, el art. 90.2 de la LRJS abre la vía tanto a cualquiera de las partes a suscitarla o como de oficio por el tribunal, en el momento de la proposición de la prueba. No obstante, no tendrán esta facultad de suscitar la cuestión en el caso de haberse puesto de manifiesto una vez admitida la prueba y durante su práctica, pues en este supuesto, se oirá a las partes y, en su caso, "se practicarán las

[111] Art. 299.1 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil : "*Los medios de prueba de que se podrá hacer uso en juicio son: 1.º Interrogatorio de las partes;2.º Documentos públicos; 3.º Documentos privados; 4.º Dictamen de peritos; 5.º Reconocimiento judicial; 6.º Interrogatorio de testigos*"
[112] VALLE MUÑOZ, F. A., "Control tecnológico empresarial…", *Op.cit.*, p.2.
[113] VALLE MUÑOZ, F. A., "Las cámaras de videovigilancia…" *Op.cit.,* p.47
[114] VALLE MUÑOZ, F. A., "Las cámaras de videovigilancia…" *Op.cit.,*, p.34
[115] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante LOPJ).

diligencias que se puedan practicar en el acto sobre este concreto extremo, recurriendo a las diligencias finales solamente cuando sea estrictamente imprescindible y la cuestión aparezca suficientemente fundada". Por último, el art. recoge que sólo se podrá llevar a cabo el recurso de reposición contra la resolución dictada sobre la discusión de la práctica de la prueba.

Por tanto y en base a todo lo anterior, se entiende que el juez debe inadmitir la prueba en caso de que la ilicitud de la misma resulte clara, pero es cierto que si su calificación conlleva dudas, ya que no admitirla podría vulnerar el derecho a la prueba, por lo que conviene su admisión, si bien es cierto que en cualquier caso la parte perjudicada puede realizar una protesta en el acto del juicio e interponer recurso de reposición contra la sentencia una vez dictada[116].

Son dos los requisitos necesarios para calificar la prueba como ilícita, esto es: en primer lugar, que se haya vulnerado un derecho fundamental; y en segundo y último lugar, la existencia de un vínculo funcional entre la vulneración del derecho fundamental y el resultado probatorio. De este modo, una vez declarada la ilicitud de la prueba, ésta se eliminaría del proceso sin tenerse en consideración a ningún efecto.

Con todo ello, también creemos importante matizar lo que dispone el art. 90.4 de la LRJS, pues, en los casos en los que pueda verse afectado el derecho a la intimidad u otro derecho fundamental siempre que no existan otros medios de prueba alternativos, el juez podrá autorizar el acceso a documentos o archivos en cualquier tipo de soporte, aunque previamente deberá realizar un juicio de proporcionalidad y con el mínimo sacrificio respecto a los intereses afectados. Además, terminando con el apartado 6 de este precepto, "si como resultado de las medidas anteriores se hubiesen obtenido datos innecesarios o ajenos a los fines del proceso, o aquellos que pudieran afectar de manera injustificada o desproporcionada a los derechos fundamentales o libertades públicas, se determinará lo necesario para preservar y garantizar los intereses y derechos afectados".

[116] VALLE MUÑOZ, F. A., "Las cámaras de videovigilancia…", *Op.cit.,* p. 35.

b. Los efectos de la prueba ilícitamente obtenida

Por todo lo expuesto en los anteriores epígrafes, cabe concluir que la licitud o no de las cámaras de videovigilancia como medio de prueba, dependerá en última instancia del respeto a los límites antes descritos. En un primer momento, se debe examinar si la prueba incumple alguno de los límites internos del derecho fundamental y el cumplimiento del deber de información previa en toda su extensión ya que, en caso contrario, la prueba se debería considerar ilícita. Sólo después de cumplir con estas dos fases previas podríamos pasar a los límites externos, esto es, el triple test de proporcionalidad[117]. Llegados a este punto, si el juez determina en el momento de valorar la prueba, que incumple alguno de los límites (falta de necesidad, idoneidad, proporcionalidad, utilización indiscriminada o inexistencia de sospechas razonadas que justifiquen su utilización), estaríamos ante una prueba ilícita[118].

Como consecuencia de calificar una prueba como ilícita, el juez tendría que inadmitir la prueba debido a su obtención a través de la vulneración de derechos fundamentales, por lo que, en el caso de ser la única prueba de cargo que justifique la sanción impuesta al trabajador por haber infringido la buena fe contractual, generalmente el despido, debería conllevar la declaración de nulidad de la misma[119].

Sin embargo, existen dos grandes tesis respecto a sus efectos:

Como señala el autor VALLE MUÑOZ, F.A[120], la primera tesis se basa en calificar el despido disciplinario como nulo, ya que la nulidad de la prueba tiene efectos directos en el despido u otra decisión adoptada por el empresario. Para defender esta tesis, se ha apoyado en la posición de un sector de la doctrina científica como COLAS NEILA, E., la jurisprudencia[121] y la doctrina judicial[122], que parten de la teoría de "frutos del árbol envenenado". A partir de esta idea, se entiende que no es posible calificar de diferentes maneras la prueba ilícitamente obtenida y la calificación que deba darse al despido o cualquier otra sanción, por lo que en el momento en que se vulnera un derecho fundamental

[117] TERRADILLOS ORMAETXEA, M. E., "El principio de proporcionalidad…", *Op.cit.*, p.152.
[118] MIGUEL BARRIO, R., "El juicio de proporcionalidad…", *Op.cit.*, p.134.
[119] *Ibídem*, p.134.
[120] VALLE MUÑOZ, F. A., "Las cámaras de videovigilancia…" *Op.cit.,*, p.43
[121] STS de 21 de junio de 2012, Rec. 2194/2011; STS de 13 de mayo de 2014, Rec. 1685/2013.
[122] STSJ 1532/2003, de 19 de julio, Cantabria, Rec. 909/2003; STSJ 2532/2017, de 9 de marzo, Cataluña, Rec.39/2017

que, a su vez, fundamenta los hechos que motivan el despido o sanción, la consecuencia debería ser la declaración de nulidad de ambas decisiones. De hecho, esta teoría se puede ver reflejada en algunas decisiones del TC, como la STC 196/2004, de 15 de noviembre y STC 29/2013, de 11 de febrero.

Respecto a la segunda tesis, el autor antes citado se basa en otro sector de la doctrina científica como SEMPERE NAVARRO, A. V. y GIL PLANA, J., y en la doctrina judicial[123]. Esta idea defiende que el despido o sanción impuestos por el empresario al trabajador basada en la prueba ilícita cuya obtención ha vulnerado derechos fundamentales, conlleva la improcedencia del despido o el carácter injustificado de la sanción. En este caso, sí consideran conveniente separar la calificación de la prueba ilícita con la decisión final, por lo que sería de aplicación el art. 55.2 y 4 del ET[124], es decir, declarar un despido improcedente en aquellos casos en los que el empresario no pueda acreditar el incumplimiento manifestado en la carta de despido.

Por último, conviene destacar que esta idea ha sido apoyada por el TC en la STC 61/2021, de 15 de marzo, alejándose de su jurisprudencia anterior, ya que descarta la nulidad del despido tras haber declarado nula una prueba obtenida por el empresario habiendo vulnerado el derecho a la intimidad y el secreto de las comunicaciones de un trabajador, considerando de aplicación el art. 55.5 del ET respecto al despido improcedente, aunque fuera la única prueba que fundamentaba la carta de despido.

6. CONCLUSIONES

Para concluir con este trabajo, resulta fundamental realizar una breve reflexión acerca del impacto que, desde mi punto de vista, ha generado el desarrollo de las TICs y su implantación en el ámbito del Derecho laboral.

---

[123] STSJ 5464/2009,de 17 de julio, Madrid, Rec.2831/2009; STSJ 1889/2017 de 21 de marzo, Comunidad Valenciana, Rec.3904/2016.

[124] Art.55 del ET :2.*"Si el despido se realizara inobservando lo establecido en el apartado anterior, el empresario podrá realizar un nuevo despido en el que cumpla los requisitos omitidos en el precedente. Dicho nuevo despido, que solo surtirá efectos desde su fecha, solo cabrá efectuarlo en el plazo de veinte días, a contar desde el siguiente al del primer despido…"*; 4. *"El despido se considerará procedente cuando quede acreditado el incumplimiento alegado por el empresario en su escrito de comunicación. Será improcedente en caso contrario o cuando en su forma no se ajustara a lo establecido en el apartado 1"*.

A nivel social, en primer lugar, ha quedado clara la necesidad de adaptar la legislación española a los cambios tecnológicos, y como resultado de ello, observamos la aprobación del nuevo RGPD y su desarrollo a nivel nacional por la LOPDGDD. En grandes términos y en lo que a nuestro estudio respecta, se produce un gran avance sobre la normativa de videovigilancia, proporcionando así una mayor seguridad jurídica en cuanto a los derechos de los trabajadores y los poderes empresariales que, a día de hoy, se encuentran en continuos enfrentamientos.

Adentrándonos en los aspectos importantes a destacar, es cierto que, por un lado, el trabajador mantiene el derecho a la intimidad junto con el DPD, y que, por otro, la empresa también ostenta el derecho a adoptar aquellas medidas de control y vigilancia que considere oportunas en el cumplimiento de las relaciones laborales. En el momento en que entran en colisión estos derechos, tanto las distintas normativas como los tribunales han intentado resolver esta problemática, aunque, después de haber abordado esta cuestión, considero que no han encontrado soluciones certeras, y han dejado muchas interrogantes abiertas.

La doctrina jurisprudencial que han creado el TS y el TC frente a la confrontación de derechos se podría resumir en que la medida empresarial que pretenda afectar al derecho a la intimidad o al derecho a la protección de datos, por ejemplo, debe superar un triple test de idoneidad, necesidad y proporcionalidad en sentido estricto. A su vez, esa medida (una sanción o un despido disciplinario, por ejemplo) debe cumplir con los límites que presenta el DPD en la LOPDGDD que hemos analizado a lo largo del trabajo, por lo que haré una breve reflexión acerca de aquellos que he estudiado con mayor detenimiento.

En primer lugar, la normativa exige el deber de información previa por parte del empresario. Sin embargo, los tribunales, en muchas ocasiones, han desatendido ese deber que, a su vez es un derecho de los trabajadores, ya que consideran que puede ser obviado o desvirtuado en caso de sospechas de irregularidades en la empresa por razones de seguridad, o en el momento en el que captan a un trabajador cometiendo un ilícito.

Esto, a mi modo de ver, se traduce en que los tribunales apoyan la idea de los empresarios de instalar cámaras de vigilancia sin el previo requisito de información que exige la ley, con el fin de sorprender a los trabajadores hurtando o cometiendo irregularidades en su puesto de trabajo. Si bien es cierto que se trata una medida de protección para la seguridad de

la empresa, se debe tener en cuenta el derecho fundamental con el que entra en colisión, y más siendo éste el derecho a la intimidad o el DPD, que tanto han sido defendidos por la jurisprudencia del TC.

En segundo lugar, es entendible que no se exija el consentimiento expreso del trabajador para el tratamiento de datos de carácter personal, ya que dentro de las facultades del empresario se encuentra el poder de control de cumplimiento de las obligaciones laborales, la vigilancia y la disciplina, y se entiende implícito el consentimiento en la medida que la nota de subordinación característica de la relación laboral por cuenta ajena, implica el reconocimiento del poder de dirección del empresario. Sin embargo, todas estas circunstancias que estamos abordando se deben tener en cuenta de manera conjunta, por lo que al considerar que el deber de información previa forma parte del contenido esencial del DPD, no se puede entender que se puede afectar el mismo DPD y el derecho a la intimidad de cualquier forma. Si se acepta que la relación laboral rebaja la garantía que proporcionaría el consentimiento del trabajador a ser grabado, sacrificar el deber de información previa, aun en el caso de existir sospechas fundadas de la comisión de ilícitos, sería tanto como condenar el derecho fundamental del DPD en la empresa.

En tercer y último lugar, tampoco los órganos juzgadores han conseguido dar una respuesta clara acerca de los efectos que conlleva la obtención de una prueba considerada ilícita por vulnerar derechos fundamentales. Como hemos podido observar en las distintas decisiones que han tomado los órganos de última instancia, se aprecia una clara discrepancia entre los que defienden que la declaración de una prueba nula, siendo esta la única prueba que fundamente el despido disciplinario, conlleve la calificación de un despido nulo, o quienes defienden la improcedencia del mismo.

Con todo ello, podemos concluir que los derechos de los trabajadores se están viendo gravemente afectados, en mi opinión, no tanto por la regulación respecto a esta materia en concreto, sino por la falta de criterios de interpretación claros que no están ofreciendo los tribunales y que son un aspecto fundamental para poder defender los derechos de todos los trabajadores.

BIBLIOGRAFÍA

OBRAS Y ARTÍCULOS

ALTÉS TÁRREGA, J. A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la STEDH López Ribalda (II)", *Revista General de Derecho del Trabajo y de la Seguridad Social,* Nº55, 2020.

CRISTEA UIVARU, L., *"*Antecedentes en la Unión Europea en el marco de la regulación de los datos personales, objetivos y nuevos retos. Futuro de la protección de datos: análisis del Reglamento (UE) 2016/679 y el nuevo modelo de privacidad", *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud,* J.M. Bosch Editor, Barcelona, 2018.

CRUZ VILLALÓN, J., *Compendio de Derecho del Trabajo,* Tecnos, Madrid, 2021.

FERNÁNDEZ DOMINGUEZ, J. J., "El marco jurídico de la protección de datos personales: Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre", *Revista del Ministerio de Trabajo y Economía Social,* Nº.148, 2021.

GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J. R., "La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Barbulescu v. Rumanía; nº61496/08; Gran Sala)", *Revista de Información Laboral,* Nº10, 2017.

GARCÍA SALAS, A. I., "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018", *Revista de Información Laboral,* Nº2, 2018.

GARCÍA SALAS, A. I., *Necesidades empresariales y derechos fundamentales de los trabajadores,* Lex Nova, Pamplona (Navarra), 2016.

GOÑI SEIN, J. L., "Controles empresariales. Geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social,* Nº39, 2009.

GOÑI SEIN, J. L., "Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información", *Ars Iuris Salmanticensis,* Nº2, 2016.

GOÑI SEIN, J.L., "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", *Justicia Laboral,* Nº17, 2004.

GUDE GERNÁNDEZ, A., "La videovigilancia en el ámbito laboral y el derecho a la intimidad", *Revista general de derecho constitucional,* Nº20, 2015.

LÓPEZ BALAGUER, M., "El control empresarial por videovigilancia en la LOPD", *Revista andaluza de trabajo y bienestar social,* Nº151, 2020.

MARCOS AYJÓN, M., "Cuestiones fundamentales en el derecho a la protección de los datos de carácter personal", *La protección de datos de carácter personal en la justicia penal,* J.M. Bosch editor, Barcelona, 2020.

MARÍN MALO, M., "La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente", *LABOS Revista del Derecho del Trabajo y Protección Social,* Nº1, 2020.

MIGUEL BARRIO, R., "El juicio de proporcionalidad en la prueba de la videograbación oculta a las personas trabajadoras", *Revista de trabajo y seguridad social,* Nº461-462, 2021.

PERELLÓ DOMÉNECH, I., "El principio de proporcionalidad y la jurisprudencia constitucional", *Jueces para la democracia,* Nº28, 1997.

RAYA CABRERA, J. L., y RAYA GONZÁLEZ, L., *Instalación y Configuración de Sistemas Operativos,* RA-MA.SA, Madrid, 2011.

RODRÍGUEZ ESCANCIANO, Susana, "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Estudios financieros. Revista de trabajo y seguridad social,* Nº423, 2018.

SÁNCHEZ PÉREZ, J., "El conflicto entre el control empresarial y el derecho a la intimidad en la era de las nuevas tecnologías", *Revista General del Derecho del Trabajo y de la Seguridad Social,* Nº59, 2021.

Seminario Iberoamericano *"Nuevos retos del derecho a la intimidad",* Conclusiones finales, en Monteviedo, a fecha 15 a 18 de junio de 2015.

SERRANO GARCÍA, J. Mª., "Límites de la ley de protección de datos al poder de dirección del empresario", *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia,* Editorial Bormazo, Albacete, 2019.

TASCÓN LÓPEZ, R., *El tratamiento por la empresa de los datos personales de los trabajadores,*Civitas/APDCM, Madrid, 2005.

TERRADILLOS ORMAETXEA, M. E., "El derecho de información a los trabajadores y a sus representantes resultante del deber de información previo, como garantía del derecho a la protección de datos y como límite al ejercicio de las facultades de dirección y control de la empresa en relación con la instalación y el uso de dispositivos digitales en el contexto de la relación laboral", *Revista General de Derecho del Trabajo y de la Seguridad Social,* Nº58, 2021.

TERRADILLOS ORMAETXEA, M. E., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español", *Revista de Derecho Social,* Nº80, 2017, p.152.

THIBAULT ARANDA, J., "La vigilancia del uso de Internet en la empresa y la protección de datos personales", *Revista crítica de teoría y práctica,* Nº1, 2009.

UGARTE CATALDO, J. L., *La colisión de derechos fundamentales en el contrato de trabajo y el principio de proporcionalidad,* (Tésis de doctorado), defendida en la Universidad de Salamanca (España), en 2011.

VALLE MUÑOZ, F. A.,"Control tecnológico empresarial y licitud de la prueba en el proceso laboral" desarrollado en el marco del proyecto de investigación *Nuevos retos tecnológicos del derecho probatorio* a cargo del Ministerio de Ciencia e Innovación, 2021-2024, Nº399, 2016.

VALLE MUÑOZ, F. A., "Las cámaras de videovigilancia en la empresa como medio de prueba en el proceso laboral", *Iuslabor,* Nº3, 2021.

VICENTE PARCHÉS, F., "Protección de datos personales y agentes intermediarios de colocación: la tutela de la libertad informática-intimidad del demandante de empleo", *Revista de trabajo, economía y sociedad,* Nº64, 2012.

JURISPRUDENCIA

Tribunal Europeo de Derechos Humanos

STEDH (Gran Sala), de 17 de octubre de 2019, Caso López Ribalda y Otros v. España.

STEDH (Sección 3ª), de 9 de enero de 2018 , Caso López Ribalda y Otros v. España.

STEDH (Gran Sala), de 5 de septiembre de 2017, Caso Barbulescu v. Rumanía II

STEDH de 5 de octubre de 2010, Caso Köpke v. Alemania (dec.), nº 420/07.

Tribunal Constitucional

STC 39/2016, de 6 de marzo.

STC 29/2013, de 11 de febrero.

STC 151/2004, de 20 de septiembre.

STC 292/2000, de 30 de noviembre.

STC 186/2000, de 10 de julio.

STC 98/2000, de 10 de abril.

STC 143/1994, de 9 de mayo.

STC 57/1994, de 28 de febrero.

STC 181/1990, de 15 de noviembre.

Tribunal Supremo

STS de 13 de octubre de 2021, Rec.3715/2018.

STS de 8 de febrero de 2021, Rec. 84/2019.

STS de 5 de septiembre de 2020, Rec. 528/2018

STS de 15 de enero de 2019, Rec.341/2017.

STS de 7 de febrero de 2018, Rec. 78/2017.

ATS de 9 de enero de 2013, Rec.1469/2012.

Tribunal Superior de Justicia

STSJ de 27 de diciembre de 2017, Asturias, Rec. 3058/2017

STSJ de 12 de marzo de 2012, Madrid, Rec.5929/2011.

LEGISLACIÓN

Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000.

Constitución Española, de 29 de diciembre de 1978.

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 1950.

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

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.

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

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.