



TRABAJO FIN DE GRADO

GRADO EN DERECHO

CURSO ACADÉMICO 2020 / 2021

TÍTULO:

Digitalización y Derechos Laborales

WORK TITLE:

Digitalization and Labour Rights

AUTOR/A: Alexandra Díaz Díaz

DIRECTOR/A: Lourdes López Cumbre

RESUMEN

El contenido de este trabajo consiste en un estudio de la facultad de vigilancia y control que ostenta el empresario que, gracias al incesante avance de las tecnologías, puede materializarse en una infinidad de mecanismos de control de la prestación laboral, pudiendo el empresario hacer uso de sistemas de control visual, como cámaras de videovigilancia, sistemas de vigilancia auditiva, como micrófonos o grabadoras de voz. También puede desplegar su facultad de control sobre las herramientas de trabajo, tales como el ordenador o el vehículo de la empresa a fin de garantizar que se está haciendo un uso adecuado de las mismas, y también cuenta con la posibilidad de controlar de la localización del trabajador a través de sistemas de geolocalización. Todos estos mecanismos de control serán objeto de estudio en este trabajo. Será también objeto de análisis la incidencia que presentan las tecnologías en el ámbito laboral y en qué medida afectan a los derechos de los trabajadores. Para ello, se expondrán cuáles son los límites y requisitos exigibles en el ejercicio legítimo de la facultad de control que ostenta el empresario y se pondrán de relieve situaciones especialmente conflictivas en esta materia. Por último, se hará un breve estudio del derecho a la desconexión digital y del teletrabajo, una modalidad de prestación laboral que está en auge y a la que han tenido que acudir muchas empresas, dada la situación de crisis sanitaria en la que estamos inmersos a causa del COVID-19.

Palabras clave: vigilancia, control, tecnologías, cámaras, micrófonos, geolocalización, digital, desconexión.

ABSTRACT

The content of this project consists of a study of employer's power of supervision and control. Thanks to the advance of the technologies, this corporate power can be materialized in a myriad of monitoring systems of labour activity. That is why the employer has numerous supervision measures, such as visual control systems, as well as security cameras. In addition, the employer also has of auditory monitoring systems, such as microphones or voice recorders. The employer can also control the working equipment, such as the computer or the company car to ensure proper use of these and the employer can also control the location of workers through geolocation systems. All these control mechanisms will be studied in this work. The impact of ICTs in the workplace will also be studied as well as the limitation produced in labour rights by the use of ICTs. For this

purpose, the limits and terms to the control power and the conflicts situations in this area will be highlighted. Finally, an analysis was carried out regarding the right to digital disconnection and the telework, which is a modality of work of growing importance, in fact, many companies have had to resort to this type of employment due to the health crisis caused by the coronavirus.

Keywords: supervision, control, technologies, cameras, microphones, geolocation, digital, disconnection.

ÍNDICE:

| | |
|---|----|
| ABREVIATURAS | 6 |
| 1. INTRODUCCIÓN | 8 |
| 2. PODER DE VIGILANCIA Y CONTROL DEL EMPRESARIO. FUNDAMENTO Y CONTENIDO | 9 |
| 2.1. Límites aplicables al poder de vigilancia y control del empresario | 11 |
| 2.2. Derechos fundamentales del trabajador en juego | 13 |
| 3. LAS DISTINTAS MODALIDADES DE VIGILANCIA Y CONTROL DEL EMPRESARIO. LA VIGILANCIA AUDIOVISUAL | 21 |
| 3.1. El deber de información previa en la instalación de sistemas de videovigilancia... .. | 25 |
| 3.2. La videovigilancia en el centro de trabajo al hilo de la STEDH en el caso López Ribalda..... | 30 |
| 3.3. Legislación en materia de protección de datos de carácter personal. Los aspectos más relevantes en relación con el poder de vigilancia y control empresarial..... | 40 |
| 4. VIGILANCIA MICROFÓNICA | 48 |
| 4.1. La vigilancia telefónica | 55 |
| 4.2. La regulación del uso del teléfono móvil en la negociación colectiva..... | 58 |
| 5. CONTROL DEL USO DE MEDIOS INFORMÁTICOS Y DEL ACCESO A INTERNET EN EL CENTRO TRABAJO | 60 |
| 5.1. Uso del correo electrónico en el ámbito laboral | 63 |
| 6. LA GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL Y EL DERECHO A LA DESCONEXIÓN DIGITAL | 72 |
| 6.1. El teletrabajo..... | 81 |
| 6.2. El derecho a la desconexión digital | 90 |

| | |
|--|-----|
| 6.3 Regulación del derecho a la desconexión digital..... | 94 |
| 7. CONCLUSIONES | 100 |
| 8. BIBLIOGRAFÍA | 104 |

ABREVIATURAS

| | |
|---------|--|
| Art. | Artículo |
| Arts. | Artículos |
| C.C | Convenio Colectivo |
| CDFUE | Carta de los Derechos Fundamentales de la Unión Europea |
| CE | Constitución Española |
| FJ | Fundamento Jurídico |
| FFJJ | Fundamentos Jurídicos |
| GPS | Sistema de posicionamiento global |
| INE | Instituto Nacional de Estadística |
| LET | Ley del Estatuto de los Trabajadores |
| LOPD | Ley Orgánica de Protección de Datos Personales |
| LOPDGDD | Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales |
| OIT | Organización Internacional del Trabajo |
| Pág. | Página |
| Págs. | Páginas |
| Rec. | Recurso |
| RGPD | Reglamento General de Protección de Datos |
| Ss. | Siguientes |
| STC | Sentencia del Tribunal Constitucional |
| STEDH | Sentencia del Tribunal Europeo de Derechos Humanos |
| STS | Sentencia del Tribunal Supremo |

| | |
|------|---|
| TC | Tribunal Constitucional |
| TEDH | Tribunal Europeo de Derechos Humanos |
| TICs | Tecnologías de la Información y la Comunicación |
| TS | Tribunal Supremo |
| TSJ | Tribunal Superior de Justicia |
| UE | Unión Europea |

1. INTRODUCCIÓN.

El poder de vigilancia y control que ostenta el empresario dentro del ámbito privado ha ido adquiriendo un protagonismo cada vez mayor como consecuencia de las modificaciones introducidas en los procesos productivos y, sobre todo, como consecuencia de la intromisión de las tecnologías en los centros de trabajo que han permitido que la facultad de control empresarial se haya visto perfeccionada hasta tal punto que puede manifestarse a través de distintos mecanismos de control, tales como la videovigilancia, la vigilancia auditiva, el control de los equipos informáticos utilizados en el centro de trabajo, la geolocalización y otras formas análogas de control. Todo ello permite que el empleador pueda efectuar un control de la actividad laboral cada vez más eficaz, pudiendo este ser efectuado prácticamente en cualquier momento y en cualquier lugar, incluso fuera del centro de trabajo, por lo que los contornos entre la vida profesional y la vida privada del trabajador se ven cada vez más difuminados.

Si bien es cierto, estos métodos de control ofrecen múltiples ventajas desde la óptica del empresario, ya que permiten controlar la prestación laboral a fin de obtener una mayor productividad en el ámbito laboral y ofrecen una mayor protección del patrimonio empresarial, evitando la comisión de irregularidades en el centro de trabajo. En contrapartida, desde la postura del trabajador, los medios tecnológicos pueden provocar afecciones en los derechos laborales y generar en el trabajador una sensación de desasosiego y de control constante. Es así como ha ido adquiriendo importancia el llamado derecho a la desconexión digital y han surgido otros términos como el denominado tecnoestrés. No obstante, pese a que estas nuevas herramientas de control ofrezcan múltiples ventajas y sean cada vez más empleadas en las diversas organizaciones empresariales, no podemos olvidar que el poder de control empresarial no es un poder omnímodo y, en cualquier caso, ha de ejercerse respetando los derechos y libertades fundamentales, tales como el derecho a la dignidad, a la igualdad y a la no discriminación, a la intimidad, al secreto de las comunicaciones y a la propia imagen entre otros, atendiendo a las eventuales vulneraciones que puedan producirse en los mismos.

2. PODER DE VIGILANCIA Y CONTROL DEL EMPRESARIO. FUNDAMENTO Y CONTENIDO

Como primera aproximación, podríamos definir el poder de vigilancia y control empresarial como el conjunto de medidas y potestades que tiene el empresario, que puede adoptar en el ámbito privado y que tienen por finalidad verificar el cumplimiento de la prestación laboral por parte del trabajador. Este conjunto de facultades y medidas que posee el empresario se encuentran incardinadas en el poder de dirección y control del empresario, el cual resulta imprescindible para la buena marcha y la productividad de la empresa.

Respecto al fundamento de las facultades de control del empresario, estas tienen su anclaje en el art. 20.3 LET, que establece que *“el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad”*.¹ Por otra parte, la facultad de control del empresario también tiene cobertura en el art. 38 CE, precepto en el que se garantiza la libertad de empresa que comprende el derecho de iniciar, desarrollar y cesar una actividad económica, lo cual implica que se atribuya al empresario la facultad de *“establecer sus propios objetivos de la empresa y dirigir y planificar su actividad en atención a sus recursos y condiciones del propio mercado”*.²

Además, el contrato de trabajo también tiene su importancia, puesto que de la relación contractual se derivan una serie de obligaciones para ambas partes del contrato y, en consecuencia, desde el momento en que es firmado, implica el sometimiento del trabajador al poder de dirección y control del empresario, por lo que no se precisa del consentimiento expreso del trabajador para que le puedan ser aplicadas estas medidas de control, ya que el consentimiento del trabajador se entiende implícito en la relación contractual. Es por ello, por lo que podríamos

¹ GARCÍA NINET, J. I. y VICENTE PACHÉS, F., “El control empresarial”, CISS, 2005, pág. 21.

² STC 96/2013, de 23 de abril, FJ 6.

situar el nacimiento del poder de control empresarial en el propio contrato de trabajo.³

En relación con esta cuestión, es importante destacar las notas caracterizadoras del contrato de trabajo, las cuales se pueden extraer del art. 1.1 LET, que regula el ámbito de aplicación de la Ley del Estatuto de los Trabajadores fijando su aplicación a *“los trabajadores que voluntariamente presten sus servicios retribuidos por cuenta ajena y dentro del ámbito de organización y dirección de otra persona, física o jurídica, denominada empleador o empresario”*. En consecuencia, el art. 1.1 LET nos permite conocer las notas definitorias del contrato de trabajo que son: la voluntariedad, la ajenidad, la dependencia y la remuneración, así como el carácter personalísimo del contrato de trabajo. Nos interesa aún más la nota de la dependencia, esto es, el sometimiento al ámbito de organización y de dirección del empresario que, además, justifica que el empresario pueda hacer uso de las facultades de control. No obstante, estos poderes de control no implican que los derechos que la constitución reconoce a los trabajadores queden vacíos de contenido, si bien es cierto pueden verse modulados al confluir con el interés empresarial.⁴

Estas facultades empresariales de vigilancia y control se han visto perfeccionadas a causa de las innovaciones tecnológicas, es más, estas medidas de control revisten múltiples modalidades, tales como la videovigilancia, la vigilancia microfónica, la vigilancia telefónica, el control de los ordenadores de la propia empresa e incluso el control a través de sistemas de geolocalización. Si bien es cierto, los múltiples mecanismos de control de los que dispone el empresario pueden provocar afecciones en los derechos del trabajador, con lo cual resulta necesario analizar cuándo los dispositivos de control implementados en el ámbito laboral son medidas legítimas y qué alcance pueden tener las mismas. La idea de la que partimos es que, si analizamos la normativa, concretamente el art 20.3 LET, podemos ver que este precepto otorga al empresario la facultad de adoptar *“las medidas que estime más oportunas de vigilancia y control”*, por lo

³ PALOMEQUE LÓPEZ, M. C. y ÁLVAREZ DE LA ROSA, M., “Derecho del Trabajo”, Editorial Universitaria Ramón Areces, 2019, pág. 591.

⁴CHARRO BAENA, P. y ESPINOZA ESCOBAR, J. H., “Cuestiones Actuales del Derecho del Trabajo. Un estudio desde las dos orillas”, Dykinson, 2014, pág. 56.

tanto, se le está otorgando un amplísimo margen de maniobra. Al mismo tiempo, no se establece ningún tipo de prohibición legal a esta tipología de medidas, por lo que se trata de una facultad discrecional, en la medida en que el empresario puede escoger los medios de control de la prestación laboral que estime más oportunos.⁵ Por lo tanto, para poder determinar la legitimidad de estos medios de control resultará necesario acudir a la ponderación casuística.

2.1. LÍMITES APLICABLES AL PODER DE VIGILANCIA Y CONTROL DEL EMPRESARIO

Se advierte, que el poder de vigilancia y control del que dispone el empresario no es un poder absoluto, en la medida en que puede resultar invasivo y atentatorio contra los derechos personalísimos del trabajador, por ende, resulta necesario analizar cuáles son las limitaciones aplicables a esta actividad de control empresarial, las cuales variarán en función de las características y circunstancias del caso concreto. Sin embargo, si acudimos a la ley y a los pronunciamientos judiciales, pueden extraerse unos límites generales que irán siendo esbozados a lo largo de este apartado.

Como límites al ejercicio de las facultades de control del empresario derivadas de las innovaciones tecnológicas, hay que señalar en primer lugar, el respeto de la dignidad personal del trabajador, ya que así lo establece el art. 20.3 LET. Como podemos observar, el art. 20.3 LET apenas contempla limitaciones al poder de vigilancia del empresario, por ello es preciso señalar que la dignidad personal no es el único derecho fundamental que puede verse conculcado con el uso de estas técnicas de control, pues también pueden resultar afectados el derecho a la no discriminación, el derecho a la intimidad personal reconocida en el art. 18.1 CE, el secreto de las comunicaciones del art. 18.3 CE y la protección de datos del art. 18.4 CE entre otros.

⁵ LLAMOSAS TRÁPAGA, A., “Relaciones laborales y nuevas tecnologías de la información y de la comunicación”, Dykinson, 2015, págs. 139-166.

En segundo lugar, también funciona como límite a la facultad de control empresarial el principio de buena fe, que no solo es un deber básico que ha de respetar el trabajador (art. 5 LET), sino que, además, se configura como un deber empresarial, por lo que funciona como límite al poder de control empresarial, tal y como se desprende del art. 20.2 LET, que impone para ambas partes de la relación negocial el sometimiento recíproco en la prestación laboral a las exigencias de la buena fe. *“La buena fe es un criterio objetivo, constituido por una serie de pautas coherentes con el comportamiento de las relaciones humanas y negociales”* y el trabajador tiene una respuesta ante el quebrantamiento del principio de buena fe por parte del empleador, *“se encuentra facultado para ejercitar las acciones que procedan, incluida la solicitud de extinción del contrato de trabajo, con derecho a la indemnización señalada para el despido improcedente, por incumplimiento grave de las obligaciones del empresario, señalada en el art. 50.1 c) LET.”*⁶

Como tercera limitación a las facultades de vigilancia y control destaca el llamado *“juicio de proporcionalidad”* al que ha de someterse toda medida de control empresarial restrictiva de un derecho fundamental. Para que la medida de control empresarial cumpla el mencionado test de proporcionalidad resulta necesario superar tres estadios o exigencias: en primer lugar, será necesario superar un juicio de idoneidad que consiste en que esa medida sea susceptible de cumplir el objetivo propuesto; un juicio de necesidad, que implica que esa medida sea necesaria, o en otras palabras, que no exista otra medida menos gravosa o más moderada para la consecución del objetivo pretendido; y finalmente, hay que superar un juicio de proporcionalidad en sentido estricto, esto es, que la medida resulte ponderada o equilibrada por derivarse de la misma más beneficios que perjuicios.⁷

Además, otra limitación aplicable al ejercicio del poder de control del empresario es que, tras el empleo de estos dispositivos tecnológicos de control ha de existir un interés empresarial que justifique su uso, y además, será preciso

⁶ ARAGÓN GÓMEZ, C., “El deber de buena fe contractual” en CRUZ VILLALÓN, J., GARCÍA-PERROTE ESCARTÍN, I, GOERLICH PESET, J. M., MERCADER UGUINA, J. R., *Comentarios al estatuto de los trabajadores*, Aranzadi, 2016, págs. 304-305.

⁷ STS 594/2018 de 8 de febrero, FJ 5.

acreditar que responden a un verdadero interés empresarial, es decir, que sean medidas destinadas a garantizar la productividad y buena marcha de la empresa, de tal manera que el empresario no podrá extralimitarse, o lo que es lo mismo, el uso de estos medios de control ha de restringirse a la fiscalización por parte del empresario del correcto desempeño de la prestación laboral.⁸

2.2. Derechos fundamentales del trabajador en juego

Como ya hemos adelantado, el empleo de sistemas de control tecnológicos puede resultar una medida atentatoria contra los derechos fundamentales del trabajador, tratándose de medidas que pueden resultar intrusivas y que generan una sensación de desasosiego y de vigilancia constante en la persona del trabajador. Por todo ello, cuando existan conflictos será necesario lograr un justo equilibrio entre los bienes jurídicos que se encuentren contrapuestos, en concreto, entre el interés empresarial y los derechos fundamentales del trabajador. En este sentido, cabe tener en cuenta que los derechos fundamentales no son derechos absolutos, *“pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho”*⁹ En suma, ni el poder de control empresarial, ni los derechos fundamentales del trabajador son absolutos, por lo que tanto este como aquel, estarán sometidos a restricciones recíprocas, de tal manera que unas veces cederá el poder de dirección y control del empresario; y otras veces serán los derechos fundamentales del trabajador los que se vean modulados, siempre y cuando se respete su contenido esencial y el poder de control empresarial no constituya una intromisión ilegítima.

Procede ahora concretar cuáles son los derechos fundamentales que pueden verse limitados. Antes de examinar esta cuestión es oportuno diferenciar a efectos meramente aclaratorios entre derechos específicos y derechos

⁸RODRÍGUEZ ESCANCIANO, S., “Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores”, Tirant Lo Blanch, 2015, pág. 138.

⁹ STC 186/2000, de 10 de julio, FJ 5.

inespecíficos, es decir, por una parte, están los llamados “*derechos específicamente laborales*”, que son aquellos cuya proyección se da específicamente en el ámbito laboral: el derecho a un salario, derecho a unas vacaciones, derecho a la huelga, derecho a la libre sindicalización, etc. Por otra parte, están los “*derechos inespecíficos*”, que son aquellos derechos que corresponden a todos los ciudadanos, cuya aplicación no se circunscribe únicamente al ámbito de la relación laboral, sino que son derechos con un alcance más genérico, siendo al mismo tiempo, derechos que pueden ser aplicables a los trabajadores en el propio ámbito laboral, pues es precisamente en este ámbito, donde principalmente pueden ocasionarse limitaciones en algunos de los derechos de los trabajadores al confluir con la libertad de empresa.¹⁰ Ante todo, es necesario matizar que hay derechos que se ven especialmente limitados, y que consecuentemente, gozan de un mayor protagonismo en esta materia. Estos son el derecho a la intimidad personal, el derecho al secreto de las comunicaciones o el derecho a la protección de datos, mientras que existen otros derechos que igualmente pueden verse modulados, solo que, en menor medida, como por ejemplo el derecho a la igualdad.

Dicho esto, partimos del derecho a la dignidad personal del art. 10.1 de la CE, ya que se configura como base y razón de ser de los derechos personalísimos y es un derecho que suele aparecer ligado a otros derechos, pues es fuente de otros derechos fundamentales y se concibe como “*un valor espiritual y moral inherente a la persona*” y “*ha de permanecer inalterada cualquiera que sea la situación en la que la persona se encuentre*”.¹¹

El siguiente derecho a concretar, es un derecho dotado de especial relevancia en este ámbito, dado que se trata de uno de los derechos que más limitaciones sufre frente a las medidas de vigilancia y control del empresario. Es precisamente, el derecho a la intimidad personal, un derecho derivado de la dignidad humana regulado en el art. 18.1 CE y que “*tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su*

¹⁰ PALOMEQUE LÓPEZ, M. C. y ALVAREZ DE LA ROSA, M., “Derecho del Trabajo”, Editorial Universitaria Ramon Areces, 2019, págs. 97-106.

¹¹ STC 120/1990, de 27 de junio. FJ 4.

*dignidad como persona, frente a la acción y el conocimiento de terceros, sean estos poderes públicos o simples particulares, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana”, es más, el derecho a la intimidad personal tiene una vertiente negativa, que se concreta en el “deber que se impone a terceros de abstención de intromisiones, salvo que estén fundadas en una previsión legal que tenga justificación constitucional, y que sea proporcionada, o que exista un consentimiento eficaz por parte del afectado que lo autorice, pues corresponde a cada persona acotar el ámbito de intimidad personal que reserva del conocimiento ajeno”.*¹² Una vez sentado lo anterior, cabe señalar que el derecho a la intimidad personal, del cual es titular el trabajador, es susceptible de sufrir limitaciones, ahora bien, no podrá verse limitado bajo el amparo de cualquier tipo de criterio o justificación, sino que será preciso, que se supere un juicio de proporcionalidad y que exista un necesario equilibrio entre la facultad de control del empresario y el derecho a la intimidad, pues como ya hemos mencionado anteriormente las medidas de control del empresario no pueden suponer intromisiones ilegítimas en la esfera privada del trabajador.

El siguiente derecho al que haremos alusión es el derecho a la protección de datos de carácter personal, que se trata de un derecho fundamental que ha ido adquiriendo un mayor protagonismo a consecuencia de la proliferación de las tecnologías y con el uso cada vez mayor de los medios digitales. Este derecho fundamental se encuentra regulado en el art. 18.4 CE que establece que *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*. De forma que nuestra Constitución se convirtió en pionera en el establecimiento del derecho a la protección de datos de carácter personal. Otro reconocimiento al derecho a la protección de datos lo encontramos en el art. 8 CDFUE, que dispone que *“toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan”*, asimismo, en el apartado segundo, se concreta que el derecho a la protección de datos es el derecho que tiene toda persona a que sus datos no sean tratados de manera ilícita o desleal y que en caso de que sean tratados, es necesario que el uso de estos datos responda a unos fines concretos. Además, el tratamiento

¹² STC 7/2014, de 27 de enero. FJ 3.

de datos personales ha de efectuarse con el consentimiento de la persona afectada o, en su caso, contando con una previsión legal habilitadora. Finalmente, este precepto añade que toda persona tiene derecho a acceder a los datos recogidos que la conciernen y derecho a su rectificación.

Son aplicables en esta materia, por una parte, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Reglamento que supone la derogación de la Directiva 95/46/CE. Y, por otra parte, es aplicable la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El art. 4 RGPD prevé distintas definiciones referidas a esta materia. Entre las mismas, hay que destacar la definición que se prevé de datos personales. Por datos personales se entiende *“toda información sobre una persona física identificada o identificable (“el interesado”); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona”*, a su vez, el presente artículo define tratamiento como *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”*.

Para poder ejercer el derecho a la protección de datos, se exige como presupuesto previo, la existencia de un dato de carácter personal y, además, ese dato ha de ser susceptible de poder vincularse con la persona interesada, esto es aquella a la que afectan o conciernen esos datos, la persona identificada o que

puede ser identificable. Ahora bien, el problema no viene con la existencia de datos personales, sino que el problema surge cuando esos datos son tratados. Es precisamente el “tratamiento” de datos de carácter personal el hecho que determina que el derecho a la protección de datos personales pueda ejercerse.

Como añadido a esta cuestión, hay un conjunto de principios que son aplicables a la protección de datos personales, vienen dispuestos en el art. 5 del RGPD que tiene por rúbrica “*principios relativos al tratamiento*”. De dicho artículo se desprenden los siguientes principios: el principio de tratamiento leal y transparente, que exige que el tratamiento sea leal, lícito y transparente; como segundo principio, se prevé la limitación de la finalidad, que consiste en que para que esos datos personales puedan ser recogidos, ha de ser con arreglo a unos fines concretos, explícitos y legítimos, no pudiendo ser tratados ulteriormente de una manera incompatible a esos fines; como tercer principio, añade el principio de minimización de los datos, que establece que los datos han de ser adecuados, pertinentes y limitados a lo estrictamente necesario en relación con los fines para los que son tratados, es decir, no se podrán recoger más datos que los que sean exclusivamente necesarios para la finalidad que se pretende; el cuarto principio, es el principio de exactitud de los datos, según el cual los datos han de ser exactos y si fuera necesario, actualizados y, además, se añade que han de adoptarse todas las medidas pertinentes para que se supriman o rectifiquen los datos inexactos sin dilación; por último, se prevé el principio de integridad y confidencialidad, que supone que el tratamiento ha de efectuarse de tal forma que se garantice una seguridad adecuada de los datos personales, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Es de mayor interés, la previsión del art. 88 del RGPD, puesto que se refiere al tratamiento de datos en el ámbito laboral. Dicho artículo en su apartado primero habilita a los Estados miembros para establecer a través de disposiciones legislativas o convenios colectivos normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular, a efectos de contratación de personal, ejecución del contrato laboral, incluyendo el

cumplimiento de las obligaciones establecidas por ley o por el convenio colectivo, gestión, planificación y organización del trabajo, etc. Por otra parte, en el apartado segundo de este artículo se añade que *“dichas normas incluirán las medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo”*¹³ Este artículo es importante, dado que está dando entrada a los convenios colectivos para que estos puedan establecer previsiones normativas más específicas que garanticen una mayor protección y que otorguen unas mejores condiciones a los trabajadores en materia de protección de datos, pero, además, hemos de observar que este precepto está situando al mismo nivel los convenios colectivos y las disposiciones legislativas.

Igualmente, se ha de hacer una mención al derecho al secreto de las comunicaciones regulado en el art. 18.3 CE, que establece que *“se garantiza el secreto de las comunicaciones y, en especial, de las postales telegráficas y telefónicas, salvo resolución judicial”*. Este derecho adquiere un papel fundamental como límite al poder de vigilancia y control empresarial, siendo un derecho que puede resultar conculcado de diversas formas, entre las mismas destacan: el uso de dispositivos de captación del sonido en el centro de trabajo, la interceptación de las llamadas efectuadas en el lugar de trabajo, así como a través del control de los dispositivos digitales utilizados en el centro de trabajo, como el ordenador o el correo electrónico. Por otra parte, pese a que es un derecho que guarda cierta vinculación con el derecho a la intimidad personal, en realidad es regulado de forma autónoma con respecto de este. El fundamento de esta autonomía, así como de su específica regulación reside en la especial vulnerabilidad de la privacidad de las comunicaciones, en la medida en que estas comunicaciones son posibilitadas a partir de la intervención técnica de un tercero ajeno a la comunicación. Además, la confidencialidad de las comunicaciones ha de ser garantizada con independencia de su contenido, resultando irrelevante que

¹³ MERCADER UGUINA, J. R., “Lecciones de Derecho del Trabajo”, Tirant Lo Blanch, 2019, págs. 348-351.

estas hagan alusión a un aspecto íntimo o de otro género. En concreto, lo que se protege con el derecho al secreto de las comunicaciones es tanto el proceso de la comunicación como el contenido de la misma, pero se protege especialmente el proceso de la comunicación, pues a través de la protección del proceso de la comunicación se garantiza, a su vez, el carácter reservado de lo comunicado.¹⁴ Asimismo, resulta esencial indicar que no se puede hablar del derecho al secreto de las comunicaciones, cuando este se refiere a la propia persona que interviene en la comunicación, es decir, lo que se garantiza con la protección del secreto de las comunicaciones es, que no se permite la interferencia de terceros en una conversación. Cuestión diferente es el levantamiento del secreto de la comunicación por parte de uno de los propios partícipes, lo cual no estaría amparado dentro del art. 18.3 CE.¹⁵

Por otra parte, también es de interés, aunque en menor medida, el derecho a la igualdad y a la no discriminación, derecho que es contemplado en el art. 14 CE, que establece que *“los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social”* El derecho a la igualdad en el ámbito laboral ha de entenderse en dos sentidos, por un lado, la igualdad ante la ley, y, por otro lado, la no discriminación por cualquier circunstancia o condición personal o social. Es de mayor interés y presenta una mayor relación con el tema que estamos tratando el derecho a la no discriminación, más concretamente, la no discriminación en la relación laboral. El art. 4.2 c) LET especifica aún más, y establece que *“los trabajadores tienen derecho a no ser discriminados directa o indirectamente para el empleo, o una vez empleados”* y, seguidamente, menciona una serie de razones por las cuales puede producirse una discriminación en la relación laboral. Por lo tanto, según este precepto está vedada la discriminación, tanto en la selección para el contrato de trabajo como durante el tiempo en el cual se está desarrollando la prestación laboral. Ahora bien, hay que matizar que no se trata de un derecho absoluto y que en función de las circunstancias que concurran en el caso concreto pueden darse

¹⁴ STC 123/2002, de 20 de mayo, FFJJ 4 y 5.

¹⁵ FERRER SERRANO, R. L., “Guía de protección de datos de los trabajadores”, Tirant Lo Blanch, Valencia, 2019, págs. 144 y ss.

ciertas desigualdades, ya que, aunque en situaciones idénticas en principio ha de existir una igualdad de trato. Sin embargo, pueden darse desigualdades, siempre que el trato desigual esté adecuadamente justificado, por lo tanto, pueden existir desigualdades en las condiciones de trabajo, por ejemplo, en la jornada o en el salario y no por ello, se estará vulnerando el derecho a la igualdad. Además, el derecho a la igualdad y a la no discriminación se proyecta en el ámbito del poder de control que ostenta el empresario, ya que no se pueden utilizar medidas de control de forma discriminatoria, por ejemplo, no se pueden instalar cámaras de videovigilancia para controlar a un trabajador o a una trabajadora en concreto por razones arbitrarias e ilegítimas, ya que esta actuación comportaría una clara vulneración al derecho a la igualdad y a la no discriminación del art. 14 CE.¹⁶

En relación con el derecho a la igualdad y a la no discriminación, podemos traer a colación la Sentencia del Tribunal Superior de Justicia de Madrid núm. 75/2019, de 25 de enero (rec. 971/2018), ya que en esta sentencia el actor alega no solo que se ha producido una vulneración en su derecho a la intimidad al no ser informado de la existencia de cámaras de videovigilancia, sino que también alega que se ha vulnerado su derecho a la igualdad al ser objeto de un despido discriminatorio, concretamente expone que se ha producido una infracción del principio de igualdad de trato del art. 14 CE, así como una infracción del art. 55.5 LET, y que su despido es discriminatorio, ya que inicialmente solo se despide al recurrente, y no se despide a otros dos trabajadores, el Sr. Augusto y el Sr. Pascual, que también habían realizado ventas o compras irregulares adquiriendo los productos a un precio inferior o sin que estos sean abonados.

No obstante, el tribunal determina que no existe discriminación alguna, ya que, aunque en un momento inicial solo es despedido el recurrente, con posterioridad también se despide al Sr. Augusto, no considerándose significativo el hecho de que su despido se produzca un mes después, por lo que este hecho resulta intrascendente, ya que la empresa pudo haber precisado de un tiempo mayor para determinar la conducta ilícita del otro trabajador. Lo que sí que se considera relevante para determinar la inexistencia de un trato desigual, es que

¹⁶ PALOMEQUE LÓPEZ, M. C. y ÁLVAREZ DE LA ROSA, M., "Derecho del Trabajo", Editorial Universitaria Ramón Areces, 2019, págs. 107-113.

ambos trabajadores son sancionados igualmente. Y respecto al otro trabajador, el Sr. Pascual, nada consta en el relato fáctico respecto a los hechos que pudieran habersele imputado, por lo que no puede establecerse comparación alguna, ni apreciarse trato discriminatorio alguno con respecto a este último trabajador.

En lo que respecta a la posible vulneración del derecho a la intimidad del recurrente, el tribunal determina la inexistencia de vulneración alguna y, para ello, se basa en que la medida de control empleada cumple con el triple juicio de proporcionalidad exigido persistentemente en la jurisprudencia del Tribunal Constitucional, asimismo, se cumple con el deber de información, ya que la representación legal de los trabajadores tenía pleno conocimiento de la instalación del sistema de videovigilancia y, además, dicha información también es facilitada a toda la plantilla. Por último, el Tribunal esgrime como argumento adicional que, en el ámbito laboral, el derecho a la intimidad queda circunscrito a determinados espacios o “zonas de reserva” situadas dentro de la empresa, en las que el trabajador tiene una alta o total expectativa de privacidad, es decir, son zonas en las que empleado tiene una confianza plena de que su imagen o conducta no va a ser observada, tratándose de zonas en las que el empleador tiene vedada su intromisión. No ocurre así en el presente caso, ya que las cámaras de videovigilancia no se sitúan en estas zonas de reserva, sino que son colocadas en espacios públicos en los que se conocía la existencia de las cámaras, por lo que, basándose en todas estas razones, el tribunal no aprecia vulneración alguna en el derecho a la intimidad personal del art. 18.1 CE, ni en el derecho a la igualdad del art. 14 CE.¹⁷

3. LAS DISTINTAS MODALIDADES DE VIGILANCIA Y CONTROL DEL EMPRESARIO. LA VIGILANCIA AUDIOVISUAL

A causa de la irrupción de las herramientas tecnológicas en el ámbito laboral, el empresario dispone de infinidad de alternativas a fin de controlar el correcto

¹⁷ STSJ de Madrid núm. 75/2019, de 25 de enero (rec. 971/2018), FFJJ 1 y 4.

desenvolvimiento de la prestación laboral. Dentro de las diferentes modalidades de control empresarial, el empleador puede monitorizar la actividad laboral a través de la supervisión visual por medio de la instalación de sistemas de videovigilancia en el centro de trabajo, la cual es una de las medidas más utilizadas y, quizás, por esta misma razón, es una de las medidas de control que más controversias suscita en el ámbito laboral. Asimismo, el empleador puede hacer uso de otros medios de control, tales como los sistemas de captación del sonido, dentro de los cuales cabe mencionar: la vigilancia microfónica y la vigilancia telefónica, esto es la intervención de las llamadas realizadas en el centro de trabajo por el propio trabajador, igualmente el empresario dispone de sistemas de geolocalización y también puede controlar los propios medios utilizados en el centro del trabajo, como el propio ordenador de la empresa, el acceso a internet y el uso de los medios de comunicación.

En lo que respecta a la vigilancia empresarial a través de sistemas de captación de la imagen y de la voz, que es la primera manifestación de control que trataremos en el presente trabajo, como ya se ha indicado en líneas anteriores, la instalación de sistemas de videovigilancia es una de las medidas más utilizadas en el centro de trabajo y, por lo tanto, se trata de una modalidad de control que adquiere un papel destacable. Nos referimos con ello a la instalación de cámaras que pueden ser fijas o móviles y que sirven para la captación de imágenes con el propósito de visualizar o reproducir las imágenes captadas. Asimismo, el empleador puede querer añadir un plus de seguridad, instalando cámaras de seguridad que no solo sirvan para la captación de imágenes, sino que además tengan integrado un sistema de captación del sonido, siendo, en este caso, una medida mucho más invasiva, por lo que deberá estar sometida a mayores limitaciones.

Principalmente, es preciso analizar una serie de aspectos acerca de la videovigilancia empresarial, tales como si es necesario informar al trabajador de la instalación de sistemas de videovigilancia en el centro de trabajo o si, por el contrario, se puede prescindir de este deber de información. En definitiva, se concretará en qué consiste este derecho de información y cómo se articula. Asimismo, se analizará en qué lugar del centro de trabajo pueden ser implantados los sistemas de videovigilancia, así como otras limitaciones y garantías que han de ser respetadas por el empleador en el ejercicio de su potestad de control a través de la instalación de sistemas de videovigilancia.

Partimos de la premisa de que la instalación de cámaras de videovigilancia en el centro de trabajo es una potestad ajustada a derecho reconocida en el art. 20.3 LET. No obstante, esta facultad se encuentra sometida a algunas limitaciones, tales como el cumplimiento del deber de información previa que analizaremos más adelante, la observancia de una finalidad concreta, la superación de un juicio de proporcionalidad, etc.

Como ya hemos adelantado, la instalación de sistemas de videovigilancia en el centro de trabajo ha de estar condicionada a la observancia de una finalidad concreta, en otras palabras, el empresario no puede actuar de forma arbitraria, ni puede instalar sistemas de videovigilancia de forma indiscriminada, sino que, el uso de las medidas de control en el ámbito laboral ha de estar enfocado estrictamente a la garantía de un correcto desenvolvimiento de la actividad laboral. Esta finalidad que ha de dar cobertura a la potestad de control empresarial puede consistir en una finalidad protectora del patrimonio empresarial, tal y como ocurre en la STS 630/2016, de 7 de julio de 2016, en la que se determinó la validez de la prueba obtenida a través de la implantación de medidas de videovigilancia en el centro de trabajo, medidas que se instalaron tras las múltiples pérdidas acaecidas en la empresa. En el presente caso los empleados eran conocedores de la existencia de las cámaras de videovigilancia, no solo porque era un hecho de común conocimiento, sino también porque estaban colocadas a la vista. La sentencia en cuestión indica que *“la presencia de las cámaras en la mayor parte del centro de trabajo sugiere una finalidad protectora del patrimonio empresarial y la grabación de conductas que atenten contra esa finalidad como lo prueba que su instalación tuvo un detonante, las múltiples pérdidas últimamente sufridas, lo que convierte a todas las personas que se encuentren en el recinto en sujetos de sospecha”*¹⁸ De lo anterior se desprende, que el empleo de las cámaras viene siendo motivado por una situación de desconfianza generada en el centro de trabajo y, la empresa pretende solventar tal situación, de ahí que se procediera a la instalación de medidas de control que contaban con el precedente de una situación de sospecha en el centro de trabajo.

En esta misma línea, conviene citar el art. 22.1 LOPDGDD, el cual también se refiere al interés empresarial que puede justificar el uso de un sistema de videovigilancia. El mentado precepto establece que *“las personas físicas o jurídicas, públicas o privadas*

¹⁸ STS 630/2016, de 7 de julio de 2016, FJ 2.

podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de las instalaciones". Por lo tanto, el poder de dirección y control empresarial ha de circunscribirse siempre al cumplimiento de una finalidad concreta y legítima, la cual puede ser una finalidad protectora del patrimonio, o bien una finalidad de control de las obligaciones y deberes laborales del trabajador, de forma que, el empresario no puede proceder a la instalación de un sistema de videovigilancia con la finalidad de controlar aspectos ajenos a la relación laboral, ni para controlar aspectos propios de la vida privada y personal del trabajador.

Además, otra de las exigencias que se prevén para la incorporación de sistemas de videovigilancia en el centro de trabajo, es que la medida control que se incorpore tiene que estar sometida a una duración limitada en el tiempo, de forma que el control de la actividad laboral no puede prolongarse más de lo necesario, debiendo cesar una vez que se alcance la finalidad pretendida por la medida de control. Si bien puede ocurrir que las cámaras de videovigilancia sean colocadas ante un escenario de desconfianza y ante la existencia de irregularidades que motiven la implementación de un sistema de control en el lugar de trabajo, por lo que lo lógico es que tales medidas cesen una vez que las personas responsables sean identificadas. ¿Y qué duración es la adecuada en la implantación de medidas de videovigilancia? Sobre este parámetro no se ha establecido una duración temporal concreta, lo que sí que se ha establecido es que la duración de la medida de control ha de ser una duración temporal limitada o, lo que es lo mismo, la implantación de la medida de control no puede extenderse más allá del tiempo necesario para satisfacer la finalidad pretendida por la medida, así, por ejemplo, en la STEDH dictada por la Gran Sala de fecha 17 de octubre de 2019 relativa al asunto López Ribalda se pronuncia sobre la duración de la medida de control consistente en este caso en el establecimiento de videovigilancia encubierta. Concretamente, el TEDH, pese a que el empleador no había establecido con carácter previo una duración determinada, entendió que la duración no fue excesiva, dado que solo se enfocó a la zona de las cajas registradoras y, además, el control solamente se realizó durante un periodo de diez días.

Otro aspecto que hay que tener en cuenta para que la implementación de sistemas de videovigilancia sea válida, es el lugar de instalación de las cámaras de videovigilancia, ya que tal y como menciona la STS 96/2017, de 2 de febrero, las cámaras pueden estar

dirigidas a controlar la actividad de la caja registradora o pueden ser colocadas en espacios públicos o, mismamente, pueden estar orientadas a controlar la entrada del establecimiento. Cuestión distinta es que las cámaras se coloquen en lugares en los que se pueda provocar una lesión al derecho a la intimidad de los trabajadores. Al hilo de lo anterior, se ha de hacer una mención a la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de derechos digitales que en el art. 89 inadmite de forma terminante, la instalación de estos sistemas de control en lugares de descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y zonas análogas. En suma, a la hora de instalar sistemas de videovigilancia en el centro de trabajo se tendrá que atender de forma minuciosa a todos estos parámetros.

3.1. EL DEBER DE INFORMACIÓN PREVIA EN LA INSTALACIÓN DE SISTEMAS DE VIDEOVIGILANCIA

Cuando se procede a la instalación de sistemas de videovigilancia como medida de control en el seno de las relaciones laborales, es necesario que el empleador respete una serie de exigencias y que observe una serie de garantías, ya que no puede ejercer un control arbitrario, ni puede extralimitarse en sus funciones, puesto que la facultad de control que el empleador tiene reconocida en el art. 20.3 LET, no es una facultad omnímoda, sino que se encuentra sometida a ciertos límites. Uno de estos límites y a su vez una de las exigencias más importantes que han de observarse en la implementación de sistemas de videovigilancia empresarial, es el cumplimiento del deber información previa sobre la incorporación de este tipo de medidas en el entorno laboral.

Según parece, resulta razonable pensar que se ha de advertir al trabajador de la instalación de sistemas de videovigilancia, pero ¿es necesario informarle meramente acerca de su existencia?, ¿o también es necesario informarle de la finalidad que se persigue con su implementación? Al margen de estas precisiones, hay que matizar que no siempre será necesario emitir una comunicación sobre la instalación de medidas de videovigilancia, así, por ejemplo, parece lógico pensar que resulta innecesario emitir una comunicación formal informando de la instalación de cámaras de videovigilancia cuando estas hayan sido colocadas en un lugar visible, de forma que los trabajadores puedan deducir de forma notoria y evidente su instalación. Por otra parte, en determinados casos

advertir tanto a los representantes como a los trabajadores de la incorporación de un sistema de videovigilancia, puede resultar contraproducente, especialmente si existe una sospecha de que se están cometiendo irregularidades en el centro de trabajo, razón por la cual el empleador puede proceder a la instalación de un sistema de videovigilancia con el propósito de descubrir la comisión de conductas irregulares, siendo este el caso en el que si se advierte a los representantes de los trabajadores y a los trabajadores de la presencia de cámaras de videovigilancia en el centro de trabajo, se verá frustrada la finalidad pretendida con la medida de control. Esto nos lleva a mencionar la videovigilancia oculta o encubierta, esta es la videovigilancia que se lleva a cabo sin el consentimiento de los trabajadores afectados y, el empleador solamente podrá recurrir a esta medida en supuestos excepcionales, bien por razones de seguridad, o bien con la finalidad de descubrir actuaciones ilícitas de los trabajadores y, siempre y cuando, se den dos requisitos: en primer lugar, es necesario que se parta de un escenario en el que existan sospechas fundadas de que se están cometiendo irregularidades y, en segundo lugar, solamente se podrá acudir al control oculto, cuando no existan otros medios menos lesivos para los derechos de los trabajadores que igualmente cumplan con el interés empresarial pretendido.¹⁹ Así por ejemplo, todas estas cuestiones serán analizadas seguidamente a la luz de los diferentes pronunciamientos judiciales de interés sobre esta materia.

Si se acude a la casuística, podemos observar que el requisito exigido al empleador del cumplimiento del deber de información previa en la instalación de sistemas de videovigilancia no es una cuestión claramente delimitada y que el criterio seguido por la doctrina judicial ha ido evolucionando con el paso del tiempo. Si bien es cierto, inicialmente los tribunales adoptaron una postura muy flexible con respecto a los requisitos y limitaciones que debían respetarse en la instalación de sistemas de videovigilancia en el centro de trabajo. La causa principal de que los tribunales siguieran una interpretación más laxa la podemos situar en que tanto el Tribunal Constitucional como el Tribunal Supremo habían centrado la cuestión de la videovigilancia, atendiendo a las posibles vulneraciones que podían producirse en el derecho a la intimidad personal y a la propia imagen del art. 18.1 CE, prescindiendo del derecho a la protección de datos amparado constitucionalmente en el art. 18.4 CE. No obstante, la utilización de

¹⁹ MUNÍN SÁNCHEZ, L. M., “Las nuevas maneras de trabajar y los nuevos medios de prueba” en MELLA MÉNDEZ, L. y NÚÑEZ-CORTÉS CONTRERAS, P. *Nuevas tecnologías y nuevas maneras de trabajar: Estudios desde el Derecho Español y comparado*, Dykinson, Madrid, 2017, págs. 329-332.

dispositivos de videovigilancia en el centro de trabajo es una medida de control que entra dentro del ámbito del derecho a la protección de datos, es más, se trata de una medida de control apta para provocar una vulneración en el derecho a la protección de datos de carácter personal, puesto que las imágenes captadas por los dispositivos de videovigilancia son consideradas como un dato de carácter personal y los sistemas de videovigilancia son un medio idóneo para permitir o facilitar la identificación de la persona que es grabada por estos dispositivos. A lo anterior hay que agregar que se entiende como dato personal toda aquella información que identifique o permita la identificación de una persona. ¿Y qué mejor dato que aquel que es proporcionado por las imágenes captadas?, pues estas ofrecen una imagen visual y una representación física de la persona afectada²⁰. Por lo tanto, una vez que se plantea la posibilidad de que la videovigilancia en el centro de trabajo puede vulnerar el derecho a la protección de datos de carácter personal del trabajador, es entonces cuando podemos decir que el control empresarial basado en la videovigilancia experimenta un tratamiento jurídico notablemente distinto.²¹

Una vez expuesto lo anterior, resulta conveniente hacer una serie de precisiones y, para ello, es necesario analizar el deber informativo a la luz de la STC 29/2013, de 11 de febrero, ya que en esta sentencia no solo se incide en el deber informativo, sino que además se plantea la vulneración del derecho a la protección de datos de carácter personal y se deja de centrar la cuestión de la videovigilancia en el centro de trabajo en torno al derecho a la intimidad personal. En el presente caso se imponen diversas sanciones a un trabajador que prestaba sus funciones en la Universidad de Sevilla como Director de Servicio. Dichas sanciones, son impuestas por la comisión de infracciones muy graves, entre las que destacan las faltas reiteradas e injustificadas de puntualidad en la entrada de trabajo, así como el abuso de confianza y la transgresión de la buena fe contractual. El trabajador en cuestión incurrió en un abuso de confianza y en la transgresión de la buena fe contractual, porque en las hojas de control de entrada y de salida del lugar de trabajo registró una hora de entrada muy diferente a la hora efectiva. Hecho que se pudo comprobar por la instalación de cámaras de seguridad que evidenciaban que el trabajador estuvo en su puesto de trabajo en horarios muy diferentes a los que él fijó en las hojas de

²⁰ STC 29/2013, de 11 de febrero. FJ 5.

²¹ SERRANO GARCÍA, J. M., “La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia”, Bormazo, 2019, pág. 38.

control. La importancia de esta sentencia radica en que el tribunal estima que se ha producido una vulneración en el derecho a la protección de datos de carácter personal consagrado en el art. 18.4 CE, y no en el derecho a la intimidad personal del art. 18.1 CE. Concretamente, se concluye que hay un incumplimiento en el deber de información previsto en el entonces vigente art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal, ya que se procedió a la recogida de datos sin cumplir las exigencias del deber de información contenido en el mentado precepto legal.

En el presente caso, se pronuncian sobre la vulneración del contenido esencial del derecho a la protección de datos de carácter personal del art. 18.4 CE. Se considera como contenido esencial del derecho a la protección de datos, la capacidad que tiene el afectado de poder controlar en todo momento quién dispone de sus datos personales y con qué finalidad está disponiendo de los mismos. En el presente caso, entienden que se ha vulnerado el contenido esencial del derecho a la protección de datos del afectado, al haberse procedido a la utilización no consentida ni informada de las grabaciones, que además fueron utilizadas para un fin de control de la actividad laboral que era desconocido por el trabajador.

Finalmente, el TC entiende que, a pesar de la existencia de distintivos que anunciaban la existencia de cámaras de videovigilancia en el recinto universitario, se produjo una vulneración en el derecho a la protección de datos de carácter personal del afectado, ya que no se le proporcionó información previa, clara e inequívoca sobre la finalidad de la medida de control de la actividad laboral. Esta información debía de concretar cuáles eran las características y el alcance del tratamiento de datos realizado, esto es, durante cuánto tiempo y con qué finalidad iban a ser examinadas las imágenes captadas y, especialmente, se debía advertir al trabajador que dichas imágenes podían servir para la imposición de sanciones.²² En definitiva, podemos comprobar que, en la referida sentencia, el TC sigue una interpretación rígida sobre la exigencia del deber de información, no bastando con la mera colocación de un cartel o de un anuncio en el que se advierta de la presencia de un sistema de videovigilancia, sino que además se exige al empresario que facilite información previa sobre las características, alcance y finalidad de la medida de control.

²² STC 29/2013, de 11 de febrero. FFJJ 4, 5, 7 y 8.

En lo que respecta al derecho a la protección de datos de carácter personal y al contenido esencial de este derecho, ha de indicarse que el deber de información previa es contenido esencial del derecho a la protección de datos de carácter personal y, por ende, su vulneración comporta una vulneración del derecho a la protección de datos de carácter personal del art. 18.4 CE. Con lo cual, ha de precisarse que es necesario dar cumplimiento al deber de información que exige el contenido esencial del derecho a la protección de datos de carácter personal, por lo tanto, con carácter general debe proporcionarse al trabajador información previa sobre la implantación de sistemas de videovigilancia en el centro de trabajo. Además, esta garantía es exigida en diversos preceptos legales, tales como el art. 12 del Reglamento (UE) 2016/679, el art. 22 y el art. 89 LOPDGDD, ambos preceptos de la LOPDGDD han de entenderse conjuntamente, de hecho, así se establece en el propio art. 22.8 LOPDGDD, que impone que el tratamiento de la información obtenida a través de sistemas de videovigilancia ha de someterse a lo dispuesto en el art. 89 de la LOPDGDD.

Como podemos apreciar, el art. 22 LOPDGDD lleva por rúbrica “*tratamientos con fines de videovigilancia*”, mientras que el art. 89 de la LOPD se refiere al “*derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo*”, del cual, resulta conveniente destacar su primer apartado que habilita a los empleadores a tratar las imágenes captadas por medio de sistemas de videovigilancia para el ejercicio de la facultad de control prevista en el art. 20.3 LET, imponiendo a los empleadores la obligación de informar a los trabajadores, a los empleados públicos y, en su caso, a sus representantes. Además, el referido precepto impone que la información sobre la medida de control ha de ser proporcionada con carácter previo y de forma expresa, clara y concisa.

Por otra parte, el TS en la sentencia de 15 de enero de 2019 también se pronuncia acerca del deber de información previa. En este caso nos encontramos con que sí se había proporcionado información previa al trabajador sobre la instalación de cámaras de videovigilancia en el centro de trabajo, por lo que en este sentido no se plantea problema alguno. En particular, la controversia se centra en la ausencia de información al trabajador sobre el destino que se iba a dar a la grabación obtenida por medio de las cámaras de videovigilancia. En consecuencia, podemos apreciar que no basta con dar cumplimiento

al deber de información, sino que esa información ha de ser suficiente, es decir, se ha de justificar al trabajador la finalidad perseguida con la implantación de medidas de control, de tal modo que la sentencia objeto de análisis concluye que el deber de *“información al trabajador sobre la recogida de datos, su objeto y finalidad”* no concurre, ya que no se ha proporcionado información a la trabajadora de que el propósito de la instalación de los sistemas de videovigilancia era fiscalizar el cumplimiento de la prestación laboral y que dicha captación iba dirigida y podía utilizarse para la imposición de sanciones disciplinarias.

A modo de cierre, y en relación con el deber de información previa, cabe añadir que otro de los requisitos que han de exigirse en el tratamiento de datos de carácter personal y en la instalación de sistemas de videovigilancia, es la prestación del consentimiento por parte del afectado. Sin embargo, se entiende que, *“en el ámbito laboral el consentimiento del trabajador pasa, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial”*. Cuestión distinta es el supuesto en el cual el tratamiento de datos es utilizado para una finalidad distinta al cumplimiento del contrato, supuesto en el cual sí que será necesario que el afectado preste su consentimiento. Por el contrario, no será necesario que el afectado preste su consentimiento en determinados casos; principalmente cuando se trate de la recogida de datos que resulten necesarios para el mantenimiento y cumplimiento de la relación laboral, lo que indudablemente engloba las obligaciones derivadas del propio contrato de trabajo. No obstante, la dispensa de este deber de información en los supuestos señalados no comporta que el deber de información quede vacío de contenido, sino que el deber de información sigue existiendo, ya que, sin el deber de información, el trabajador no podrá hacer efectivos sus derechos y se verá indefenso, es más, si el trabajador no es conocedor de la finalidad de la medida, difícilmente podrá prestar su consentimiento a la misma.²³

3.2. La videovigilancia en el centro de trabajo al hilo de la STEDH en el caso López Ribalda

Dentro del uso de las herramientas tecnológicas en el ámbito laboral y, más concretamente, la instalación de cámaras de videovigilancia en el centro de trabajo,

²³ STS 363/2019, de 15 de enero de 2019 (rec. 341/2017), FFJJ 2 y 3.

resulta interesante hacer una mención a dos importantes sentencias del Tribunal Europeo de Derechos Humanos, entre las mismas la STEDH, de 9 de enero de 2018 (Caso López Ribalda y otros contra España) y, seguidamente, se hará una mención a la posterior STEDH, de 17 de octubre de 2019 dictada por la Gran Sala que supuso una rectificación de la anterior y que también se refiere al asunto López Ribalda.

Respecto a la primera sentencia del TEDH, de 9 de enero de 2018, en la misma, se aborda la cuestión de la videovigilancia efectuada en el centro de trabajo. En este asunto son demandantes cinco empleadas que trabajaban como cajeras para una empresa que contaba con una cadena de supermercados. Las demandantes fueron despedidas a causa de los siguientes hechos: el empleador tras comprobar el inventario percibe ciertas irregularidades de alcance relevante en la empresa, consecuentemente, inicia una investigación con el objetivo de solventar dicha situación. A tal fin, se procede a la instalación de dos tipos de cámaras. Por un lado, se instalaron cámaras visibles que fueron colocadas en las entradas y salidas del establecimiento y, por otro lado, se instalaron cámaras ocultas que fueron colocadas enfocando a las cajas registradoras. La empresa informó sobre la existencia de las cámaras visibles, pero no se informó a los trabajadores sobre la instalación de las cámaras ocultas. Tras visualizar el contenido de las cámaras, las demandantes fueron despedidas por motivos disciplinarios al ser descubiertas cometiendo diversos robos y ayudando a robar a sus compañeras de trabajo y a algunos clientes.

Las demandantes alegaron entre otras razones, que la vigilancia encubierta había supuesto una vulneración de su derecho a la intimidad personal, que las pruebas resultantes de la vigilancia encubierta habían sido obtenidas ilegalmente, asimismo, alegaron que el acuerdo transaccional que habían firmado tenía que ser declarado nulo, ya que concurría un vicio en el consentimiento, pues habían prestado su consentimiento bajo coacción.

El TEDH estimó algunas peticiones de las demandantes, concluyendo que la vigilancia encubierta suponía una intromisión en la vida privada de las demandantes, de acuerdo con el art 8.1 del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales. Dicho artículo, garantiza el derecho al respeto de la vida

privada de toda persona; derecho que no solo ha de proyectarse frente a las autoridades públicas, sino también en las relaciones personales.

El Tribunal examina si ha existido un equilibrio entre el derecho a la intimidad personal de las demandantes y el poder organizativo del empresario, concluyendo que no se ha garantizado el necesario equilibrio que ha de darse entre los bienes jurídicos en conflicto.

Por el contrario, los tribunales nacionales determinaron que la medida sí superaba un juicio de proporcionalidad, estimando que la medida de control era justificada, ya que se implementó tras mediar una sospecha fundada de que se estaban cometiendo robos en la empresa. Además, concluyeron que la medida era necesaria, proporcionada y adecuada con el fin legítimo perseguido.

En cambio, el TEDH entendió que el empresario podía haber garantizado sus intereses utilizando otros medios, en particular, si hubiera utilizado las mismas medidas, pero habiendo proporcionado a los trabajadores la información previa requerida, cumpliendo al mismo tiempo con la legislación vigente en el momento del acaecimiento de los hechos. Finalmente, el TEDH concluyó que no se respetó el deber de información que exigía la legislación vigente, la cual, establecía de forma clara y contundente que se debía informar a los trabajadores en caso de que existiera un medio de recogida y recopilación de datos, por ello, no se cumplieron los requisitos del art. 5 de la Ley de Protección de Datos Personales, que exigía que las demandantes tenían que ser informadas de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos datos de carácter personal y de quiénes iban ser destinatarios de la información recogida.²⁴

Una vez visto lo anterior, interesa hacer algunas reflexiones respecto a la singular decisión adoptada por el TEDH el 9 de enero de 2018, en la cual se acuerda indemnizar a las trabajadoras, pese a que algunas de ellas aceptaron haber cometido los robos. En concreto, la explicación a esta particular decisión la encontramos en que el TEDH sigue una interpretación bastante rigurosa del deber de información, entendiendo que para que

²⁴ STEDH (Sección 3ª), de 9 de enero de 2018, caso López Ribalda y otros contra España.

el deber de información se entienda superado, es necesario que las personas afectadas por el tratamiento de datos sean informadas de forma expresa, precisa e inequívoca, debiendo informar a las personas interesadas de la existencia del tratamiento de datos, de la finalidad de la recogida de estos y de las personas destinatarias de la información.

En esta línea y a efectos meramente aclaratorios, interesa traer a colación la doctrina constitucional acerca de la vigilancia encubierta, la cual resulta ser bastante dispar. Pues bien, tal y como apunta (López Cumbre, 2018),²⁵ la jurisprudencia constitucional se ha pronunciado acerca de la vigilancia encubierta en dos sentidos: por un lado, está la interpretación seguida en las SSTC 186/2000, de 10 de julio y 39/2016, de 3 de marzo, y, por otro lado, está la interpretación seguida en la STC 29/2013 de 11 de febrero.

En los dos primeros pronunciamientos del TC se defiende el recurso a la grabación encubierta, siempre y cuando se cumplan determinados requisitos, siendo necesaria la concurrencia de sospechas fundadas de que se están cometiendo irregularidades y también es necesario que la medida supere el principio de proporcionalidad.

Ahora bien, como es sabido, en el uso de videovigilancia como medida de control empresarial, se exige el cumplimiento de un deber de información, de forma que los trabajadores deben conocer si están siendo controlados a través de cámaras de videovigilancia. Sin embargo, se puede salvar esta supuesta omisión del deber de información dependiendo de las circunstancias del caso concreto. La explicación la encontramos de nuevo contenida en las SSTC 186/2000, de 10 de julio y 39/2016, de 3 de marzo, que siguen una interpretación del deber de información más flexible. Ambas sentencias, entienden que el requerimiento del consentimiento del trabajador para ser objeto de videovigilancia se entienda superado teniendo en cuenta dos datos:

En primer lugar, que los trabajadores podían conocer de la existencia de cámaras de videovigilancia en el establecimiento o, al menos, deducirlo a través del distintivo que anunciaba la existencia de videovigilancia en el establecimiento.

²⁵ LÓPEZ CUMBRE, L., "Grabaciones ocultas en la empresa y privacidad laboral de los trabajadores sorprendidos hurtando", Revista del Centro de Estudios de Consumo (CESCO), en <http://centrodeestudiosdeconsumo.com>, noviembre, 2018, 31 páginas.

En segundo lugar, al anterior argumento, hay que añadir, la interpretación seguida en la STC 39/2016, de 3 de marzo, en función de la cual, se entiende que en el ámbito laboral, el consentimiento del afectado pasa como regla general a un segundo plano, porque se entiende que el consentimiento se encuentra implícito en la relación negocial, exigiéndose, además, para que este consentimiento se entienda superado, que el tratamiento de datos se efectúe estrictamente a fin de garantizar el mantenimiento y cumplimiento del contrato laboral firmado por ambas partes del mismo.

Por otra parte, el TC en la STC 29/2013, de 11 de febrero, sigue una interpretación mucho más restrictiva de la exigencia del deber de información entendiendo que, para que se entienda prestado el consentimiento del trabajador, no basta con la aportación de una información genérica, de tal forma que, no es suficiente con que se informe a las trabajadoras de la mera existencia de videovigilancia, sino que es preciso que se las aporte información sobre las características y la finalidad de la medida de control. Ahora bien, conviene diferenciar si el sistema de vigilancia tiene un carácter temporal o si tiene un carácter indefinido, dado que, en el primer supuesto se seguirá una interpretación más laxa del deber de información, es decir, la contenida en las SSTC 186/2000 y 39/2016, mientras que, si las cámaras son fijas, se tendrá que seguir una interpretación más rigurosa, esto es, la contenida en la STC 29/2013.

A continuación, haremos una breve exposición de la segunda STEDH del caso López Ribalda dictada por la Gran Sala, el 17 de octubre de 2019. Una sentencia que resultó bastante polémica, ya que no solo supone una rectificación de la anterior, sino que, además, con ella el Tribunal de Estrasburgo da un giro radical llegando a una conclusión completamente distinta. En esta segunda sentencia, las demandantes mantienen que la instalación de cámaras ocultas en el centro de trabajo produjo una afectación a su derecho a la vida privada contemplado en el art. 8 del CEDH, asimismo, las demandantes alegan que el hecho de ser objeto de control en el centro de trabajo supone la aplicación del art. 8 del CEDH al presente asunto.

En este sentido, el Gobierno manifiesta que las demandantes trabajaban en un espacio abierto al público, lo cual implica que el derecho a la vida privada de las trabajadoras se vea reducido.

Por otra parte, el Tribunal determina cuál ha de ser la interpretación que ha de darse al derecho a la vida privada según la jurisprudencia del TEDH, y, seguidamente, señala que la noción de vida privada ha de entenderse en un sentido amplio, lo que implica que se trata de una noción que no se presta a definiciones delimitadas, sino que su interpretación dependerá de las circunstancias existentes en cada caso. Asimismo, el Tribunal señala que el derecho a la vida privada no se limita al círculo íntimo del interesado, sino que también ha de garantizarse en la vida privada social, por lo tanto, el respeto a la vida privada también ha de estar presente y ha de garantizarse en las relaciones profesionales. En cuanto a las cámaras de videovigilancia que fueron colocadas enfocando a las cajas registradoras, estas solo captaron actividades dirigidas al cobro de los clientes, por lo que se trata de actividades que no se caracterizan por ser de carácter privado, por esta razón, la expectativa de intimidad de las demandantes se ve notablemente reducida. Dicho esto, vamos a centrarnos en la valoración que da el Tribunal a este asunto: en primer lugar, el art. 8 del CEDH impone al Estado no solo la obligación de abstenerse y de no producir injerencias en el derecho a la vida privada de las trabajadoras, sino que, además, se imponen al Estado una serie de obligaciones positivas que han de ir encaminadas a hacer efectivo el derecho a la vida privada de toda persona. Dichas obligaciones positivas son cumplidas y no han de ser cuestionadas en este asunto, dada la existencia en el momento de los hechos de un marco normativo en el derecho español que asegurara la protección de la vida privada de las trabajadoras; en segundo lugar, de la STEDH relativa al caso Barbulescu, dictada el 5 de septiembre de 2017, se extraen una serie de criterios a tener en consideración a la hora de valorar si se ha producido una afectación al derecho a la vida privada de las demandantes. Además, el TEDH señala que, aunque esos criterios vayan enfocados al control de la correspondencia y de las comunicaciones no profesionales de los trabajadores, igualmente pueden proyectarse al presente asunto.

En este asunto, lo primero que se comprobó acerca de las medidas de control es si las cámaras de seguridad respondían a una finalidad legítima y se concluyó que sí, ya que las cámaras fueron colocadas tras la existencia de una sospecha fundada de que se estaban cometiendo robos en el supermercado, igualmente tuvieron en cuenta el interés del empresario de garantizar el correcto funcionamiento de la empresa.

Lo siguiente que analizaron fue el alcance de la medida y su grado de intrusión, en este sentido, determinaron que el grado de intrusión no era muy intenso, ya que la medida estaba limitada no solo en cuanto al espacio al que iba dirigida, sino también en cuanto al personal vigilado, además, la duración de la medida fue la necesaria para identificar a los responsables y no se extendió más allá de lo estrictamente necesario.

Seguidamente, tuvieron en cuenta que las labores de las trabajadoras se desarrollaban en un espacio público, por lo que estas tenían un continuo contacto con los clientes, cuestión que resulta importante a efectos de determinar el grado de expectativa razonable de intimidad que tengan las interesadas, pues no es lo mismo que las cámaras de videovigilancia sean instaladas en vestuarios o en aseos, donde el grado de protección de la intimidad es mayor o incluso máximo, a que las cámaras sean instaladas en lugares abiertos al público o en espacios visibles.

Posteriormente, en lo que se refiere a la duración de la medida, se constató que la medida duró 10 días y cesó tan pronto como los responsables de las pérdidas fueron identificados.

Otro aspecto que fue analizado por el tribunal son las consecuencias de la medida de vigilancia, y se estimó que las consecuencias provocadas por la medida eran importantes, ya que los resultados de la grabación provocaron el despido de las trabajadoras.

También se analizó si existía otro medio menos intrusivo, respecto a lo que se determinó que no existía otro medio más moderado, ya que, de haberse informado a las trabajadoras de la instalación de la medida, se hubiera visto frustrada la finalidad pretendida por el empleador.

Igualmente, se analizó el ofrecimiento al trabajador de garantías adecuadas. En esta línea, se manifestó que sí existían garantías suficientes en el derecho interno que garantizaran los derechos de las personas cuyos datos personales estaban siendo recopilados y tratados.

Por último, se examinó el cumplimiento del deber de información acerca de la existencia y de la aplicación de medidas de seguridad. Sin embargo, dicha garantía no fue cumplida de forma íntegra en el presente asunto, ya que no se informó a las trabajadoras de la presencia de las cámaras ocultas. No obstante, la inobservancia de este deber de información que, además es un deber fundamental, no tiene por qué determinar un desequilibrio entre los intereses en juego, dado que no es el único criterio valorable, pero es importante matizar que su incumplimiento supone que ha de otorgarse más peso al resto de criterios a valorar, es decir, el resto de los criterios han de ser exigidos de forma mucho más estricta.

En base a todas estas consideraciones, el Tribunal termina concluyendo que la incidencia de la medida en la vida privada de las demandantes no es muy intensa, tomando en consideración la existencia de sospechas fundadas que legitiman el uso de la medida y también tiene en cuenta la ausencia de otra medida menos lesiva. Finalmente, hay que añadir el argumento del gobierno de que las demandantes disponían de otros medios para garantizar y hacer efectivos sus derechos, en particular, las demandantes podían haber denunciado a la Agencia de Protección de Datos del incumplimiento del deber de información recogido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal entonces vigente. En definitiva, el TEDH concluye que no hubo ninguna vulneración del art. 8 del CEDH, y, en consecuencia, sostuvo que los tribunales habían ponderado correctamente los intereses divergentes en el presente asunto.²⁶

Una vez vistas ambas sentencias, a modo de aclaración, se hará una comparación entre las mismas. Para empezar, podemos observar que en la primera STEDH relativa al caso López Ribalda, el TEDH se pronuncia sobre la prueba obtenida a través de la videovigilancia encubierta declarándola nula, ya que dichas cámaras de vigilancia fueron colocadas incumpliendo el deber de información previa, lo cual suponía una clara vulneración a su derecho a la intimidad, dejando el TEDH prácticamente vetada la posibilidad de recurrir a la videovigilancia encubierta.

²⁶ STEDH (Gran Sala), de 17 de octubre de 2019, caso López Ribalda y otros contra España.

A este respecto, es oportuno remarcar que el TEDH en esta primera sentencia determina que la medida no alcanzaba un equilibrio justo entre el derecho fundamental y el fin empresarial buscado, concretamente, la medida no cumplía el juicio de necesidad, habiéndose podido salvaguardar el interés empresarial a través de otros medios menos invasivos. Sin embargo, sobre este mismo punto (García Salas, 2018),²⁷ señala que hay que plantearse si realmente existen otros medios de fiscalización que susciten una menor intrusión y, que, al mismo tiempo, satisfagan de forma justa el fin legítimo perseguido por el empleador, puesto que para que la medida fuese menos intrusiva, es necesario cumplir el deber de información empresarial, lo cual evidentemente frustraría el propósito empresarial de identificar a los trabajadores responsables de las considerables pérdidas. Por ende, una vez examinadas todas estas circunstancias llegaríamos a la conclusión de que bien, no existe un medio de control menos intrusivo, o bien resulta sumamente complicado encontrar una medida de control que siendo más moderada garantice el deber de información empresarial, y que, al mismo tiempo, cumpla con el interés empresarial pretendido en el caso que está siendo objeto de análisis.

En cambio, en la segunda sentencia dictada por el TEDH también relativa al asunto López Ribalda, el TEDH cambia radicalmente el criterio seguido en la sentencia precedente. Esta segunda resolución presenta una importancia extraordinaria al pronunciarse sobre una cuestión que ha generado muchísima controversia, y que, al mismo tiempo, es considerada una cuestión fundamental en materia de videovigilancia y de protección de datos personales, concretamente se trata del deber de información empresarial, un derecho que tiene el afectado y que forma parte del contenido esencial del derecho a la protección de datos de carácter personal consagrado en el art. 10.4 CE. La Gran Sala en esta segunda resolución se pronuncia en un sentido opuesto sobre la grabación oculta al determinar que, en el caso de que concurren sospechas razonables de que se ha cometido un ilícito en el centro de trabajo queda justificada la grabación encubierta, no bastándonos para ello con una mera sospecha o suposición, ya que en este caso no estaría permitido grabar, sino que es necesario que las sospechas sean contundentes. Por lo tanto, partiendo de este escenario, hay que indicar que se puede producir una omisión del deber de información previa, en el caso de que existan sospechas

²⁷ 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*, núm. 2, 2018, parte jurisprudencia.

razonables de que se ha cometido una mala conducta, ya que si partimos de un clima de desconfianza en el que se sospecha no solo que un empleado ha cometido irregularidades, sino que además han sido varios los empleados responsables de las pérdidas, tratándose por si fuera poco de pérdidas económicas cuantiosas, lo más razonable es que el empresario no comunique a sus empleados que ha instalado cámaras ocultas en el lugar de trabajo, ya que si les advierte de ello, se verá frustrada su finalidad protectora del patrimonio y de garantizar el buen funcionamiento de la empresa, así como de identificar a las personas responsables de las pérdidas acaecidas, puesto que si dichas personas son advertidas, es lógico pensar que estas cesarán en su mala conducta a fin de evitar que se les descubra y, en consecuencia, se les imponga algún tipo de sanción como el despido disciplinario.²⁸

Además, al argumento anterior sobre las sospechas razonables, hay que añadir que, aunque no se hayan cumplido todas las imposiciones emanadas del deber de información, el cual no podemos olvidar que tiene naturaleza fundamental, sí que se aporta una información general sobre la implantación de las cámaras de seguridad al colocarse un distintivo informando sobre la existencia de las mismas, por lo tanto, aunque el personal no tenía una rotunda certeza de que se habían instalado las cámaras ocultas, sí que podría haber deducido su existencia, por lo que el deber de información es cumplido parcialmente. Además, el deber de información, aunque tenga naturaleza fundamental no es un derecho absoluto, pudiendo ceder ante otros bienes merecedores de tutela jurídica. Es por ello, que el TEDH acaba concluyendo que pese a que no se haya garantizado plenamente el deber de información, sí que se ha garantizado parcialmente, siendo además un criterio más a tener en cuenta, es decir, no se trata de un requisito nuclear a efectos de determinar la validez de la prueba, sino que existen muchos otros criterios adicionales que se han cumplido con todas las garantías, por lo que finalmente el TEDH acaba estimando de forma apodíctica que la medida de control adoptada por la empresa es plenamente válida.²⁹

²⁸ MONEREO PÉREZ, J. M., “Se justifica la grabación con cámaras ocultas en el centro de trabajo por la existencia debidamente acreditada de sospechas razonables de irregularidades graves”, *Revista de jurisprudencia laboral*, núm. 8, 2019, pág. 7.

²⁹ ZARAGOZA TEJADA, J. I., “La prueba obtenida por videocámaras de seguridad tras la STEDH del 17 de octubre de 2019. caso López Ribalda vs España”, *Revista Aranzadi Doctrinal*, núm. 2, 2020, parte jurisprudencia.

3.3. Legislación en materia de protección de datos de carácter personal. Los aspectos más relevantes en relación con el poder de vigilancia y control empresarial.

El incesante avance de las tecnologías de la información y de la comunicación y su evidente repercusión en el ámbito de las relaciones laborales, hace que sea necesaria la garantía de una adecuada protección a las personas trabajadoras en relación con el tratamiento de sus datos de carácter personal. A lo anterior hay que añadir que los dispositivos tecnológicos utilizados en el centro de trabajo posibilitan el almacenamiento de una cantidad ingente de información concerniente a las personas trabajadoras, información que normalmente es recogida en soportes informáticos de la entidad empresarial, de modo que los empleadores en el ejercicio de su facultad de dirección y control, manejan y recaban una importante cantidad de datos personales pertenecientes a los trabajadores, tales como datos relativos a la formación, a la salud, al salario, a su ubicación o a sus movimientos en el caso de que estén geolocalizados, datos familiares, aspectos relativos a su conducta o a su rendimiento en el trabajo, etc.

A todo ello hay que añadir que actualmente vivimos en un contexto de crisis sanitaria y de pandemia mundial lo que ha intensificado aún más el uso de los dispositivos tecnológicos en la vida cotidiana y en la vida laboral. Este escenario, a su vez, ha potenciado que muchas empresas tengan que acudir al teletrabajo para evitar el riesgo de contagio, siendo esta una modalidad de prestación laboral que ofrece infinidad de ventajas, pero que implica ciertos riesgos para el respeto del derecho a la intimidad personal y del derecho a la protección de datos de carácter personal, por lo que nos encontramos con que se produce un conflicto entre distintos bienes jurídicos, concretamente, se produce una colisión, por un lado, entre el derecho a la vida y a la integridad física frente al derecho a la intimidad y a la protección de datos personales por otro, siendo el derecho a la intimidad y el derecho a la protección de datos personales dos de los derechos fundamentales más susceptibles de sufrir algún tipo de afectación en el actual contexto de pandemia mundial. Así todo, tanto el derecho a la intimidad como el derecho a la protección de datos personales son derechos que no pueden quedar reducidos a la nada.

En este nuevo entorno de crisis sanitaria al que nos estamos refiriendo, cobra especial importancia la protección de un tipo de datos personales; son los datos caracterizados por ser especialmente sensibles. Concretamente, se trata de datos como las opiniones políticas, la creencia religiosa, la orientación sexual, la salud, etc. Dentro de este tipo de datos nos interesa a causa de la crisis sanitaria el tratamiento de los datos relativos a la salud, cuestión sobre la que surgen algunos interrogantes, tales como si el empresario puede adoptar medidas preventivas como tomar la temperatura de los empleados, preguntarles a los empleados si presentan algún tipo de síntoma característico del Covid-19 o si han tenido contacto con algún positivo. Este tipo de datos al que nos estamos refiriendo, los podemos calificar como datos sensibles y se caracterizan por ser datos que, como regla general, la empresa no puede solicitar, es decir, son datos cuyo tratamiento está prohibido, salvo que el interesado preste su consentimiento para ello, así lo establece el art. 9.2 del Reglamento (UE) 2016/679 que para referirse a este tipo de datos emplea la expresión “*categorías especiales de datos personales*”.³⁰

Todas estas circunstancias ponen de manifiesto la importancia que tiene el derecho a la protección de datos de carácter personal, un derecho que es reconocido en nuestra constitución en el art. 18.4 y que goza de la categoría de derecho fundamental. Dicho precepto establece que “*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*”. Inicialmente se consideraba que el derecho a la protección de datos de carácter personal estaba estrechamente ligado al derecho a la intimidad personal, pero más adelante el Tribunal Constitucional lo configura como un derecho autónomo y diferenciado del derecho a la intimidad personal, aunque si atendemos a la dicción literal del precepto podemos apreciar que es un derecho que presenta una cierta vinculación con el derecho a la intimidad personal, en la medida en que toda esa cantidad de datos de carácter personal, que es almacenada en soportes informáticos, afecta a la privacidad de las personas. En este sentido, es de interés la STC 290/2000, de 30 de noviembre en la que se especifica qué garantías otorga el derecho a la protección de datos personales, el cual atribuye a la persona un poder de control y disposición sobre sus datos personales, es decir, este derecho “*confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de datos personales integrado por*

³⁰ MUÑIZ AGUIRREURRETA, D., “Covid-19 Relaciones laborales y protección de datos”, *Aranzadi digital*, núm. 1, 2020, parte Estudios y comentarios.

*los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos”.*³¹

Como complemento de lo anterior, se ha de destacar la STC 292/2000, de 30 de noviembre que se encarga de definir el derecho a la protección de datos de carácter personal, y, al mismo tiempo, lo presenta de forma autónoma del derecho a la intimidad personal. En concreto, el TC precisa que la denominada libertad informática consiste en el derecho a controlar los datos concernientes a una persona que se encuentren almacenados en un programa informático y, añade, que es un derecho que comprende entre otras facultades, la oposición de la persona afectada a que determinados datos sean utilizados para una finalidad ilegítima, es decir para una finalidad distinta de aquella que justificó su obtención. Asimismo, el TC agrega que, pese a que el derecho a la intimidad y el derecho a la protección de datos están relacionados entre sí, dado que ambos *“comparten el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar”*, son en realidad derechos diferenciados e independientes, lo cual se hace patente en su distinta función, ya que el derecho a la intimidad personal tiene como función la de proteger frente a las injerencias que puedan realizarse en la vida íntima y familiar de la persona, mientras que el derecho a la protección de datos de carácter personal otorga a la persona titular del mismo un poder de disposición sobre sus datos personales, sobre su uso y destino, todo ello con la finalidad de evitar que dichos datos sean utilizados de forma ilícita y desleal. Esta es la peculiaridad del derecho a la protección de datos, que además goza de un objeto de protección mucho más amplio que el del derecho a la intimidad, ya que se protegen no solamente los datos íntimos de la persona, sino también todos aquellos datos que puedan afectar a la dignidad de la persona, al derecho al honor, la ideología, etc. Otra peculiaridad que tiene el derecho a la protección de datos es que atribuye a su titular un conjunto de facultades consistentes en la solicitud del previo consentimiento para poder recabar y utilizar los datos personales, el derecho a conocer y a estar informado sobre la finalidad y uso de esos datos y el derecho

³¹ STC 290/2000, de 30 de noviembre, FJ. 7.

a acceder, rectificar y cancelar esos datos, lo cual se traduce en un poder de control y disposición de los datos de carácter personal.³²

Por su parte, en la STS 766/2020, de 15 de septiembre, se señala que el derecho a la protección de datos confiere a su titular un poder de disposición y control sobre los datos personales que le conciernen, dicho poder de disposición al que ya hemos hecho alusión en líneas anteriores compone una parte del contenido del derecho a la protección de datos. En este sentido, es oportuno señalar que el derecho a la protección de datos como todo derecho fundamental, no es un derecho absoluto, de hecho, para que se pueda proceder a la recogida y ulterior tratamiento de los datos íntimos es necesario el requerimiento del consentimiento de la persona interesada, y esta facultad de la que dispone el titular del derecho a la protección de datos solo puede verse limitada cuando confluya con otros derechos y bienes constitucionalmente protegibles.³³ Respecto a lo anterior, cuando el TC se refiere a otros derechos y bienes merecedores de amparo constitucional, se está refiriendo entre otros a la libertad de empresa del art. 38 CE, por lo que si entran en conflicto ambos derechos, habrá que ponderar en función de las circunstancias del caso concreto, cuál de los dos tiene prevalencia sobre el otro.

En todo caso, dentro del ordenamiento jurídico español, es oportuno señalar la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Ley que es aprobada con el objetivo de adaptar nuestro ordenamiento jurídico al Reglamento (UE) 2016/679, de 27 de abril del 2016 (DOUE de 4 de mayo), relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y que reemplaza a otras dos leyes: la Ley Orgánica 5/1992 y la Ley Orgánica 15/1999, de 5 de diciembre, las cuales iban dirigidas a la concreción y desarrollo del derecho fundamental a la protección de datos personales del art. 18.4 CE.

En lo que respecta a nuestra actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, nos interesa hacer alusión a algunos aspectos de interés sobre la protección de datos personales enfocada al ámbito laboral. Para ello, hay que situarse en el título X de la citada ley, dentro del cual

³² STC 292/2000, de 30 de noviembre, FFJJ 5 y 6.

³³ STS 766/2020, de 15 de septiembre, FJ 2.

encontramos un conjunto de preceptos enfocados a la protección de datos dentro del ámbito laboral. En concreto, son los arts. 87 a 91 de la ley, en los cuales se recoge un elenco de derechos digitales. El primero de estos derechos, es decir, el derecho a la intimidad comienza siendo regulado en el art. 87 LOPDGDD, que establece que los trabajadores tendrán derecho a la protección de la intimidad personal en el uso de los dispositivos digitales puestos a su disposición por el empleador, lo cual no obsta que el empresario pueda acceder al contenido derivado del uso de los dispositivos digitales en el lugar de trabajo. En efecto, el empleador dispone de la facultad de controlar el uso de los dispositivos digitales utilizados por los trabajadores, dispositivos que son propiedad del empresario y puestos al servicio de los trabajadores como herramienta de trabajo. Ahora bien, para que el empresario pueda ejercitar el poder de control sobre los dispositivos digitales utilizados en el lugar de trabajo, es necesario que se cumplan una serie de exigencias: en primer lugar, que el empresario ejercite el poder de control con la exclusiva finalidad de controlar el cumplimiento de las obligaciones laborales, así como la finalidad de garantizar que esos medios de trabajo se encuentren íntegros y en buen estado, por lo que el empresario no podrá excederse de sus facultades reconocidas por la ley; en segundo lugar, se exige que el empresario establezca unos criterios de utilización de los dispositivos digitales y, además, en el supuesto en que se permita la utilización de los dispositivos digitales para fines particulares, el empleador deberá de precisar qué usos concretos permite y deberá de delimitar los periodos en los que tales usos están autorizados, todo ello a fin de preservar el derecho a la intimidad personal.³⁴ Dentro de los posibles usos que puede establecer el empleador, este puede permitir el uso libre de los dispositivos digitales, puede establecer periodos de uso para fines privados y periodos de uso para fines profesionales, puede prohibir el uso personal de los dispositivos digitales o, también, puede permitir el uso extralaboral de los dispositivos digitales, siempre y cuando se haga de forma moderada y razonable.

Concretando aún más, en lo que respecta a los dispositivos digitales utilizados en el centro de trabajo, es importante matizar que el hecho de que estos dispositivos sean propiedad de la empresa es un dato sumamente relevante, dado que legitima al empresario para fijar unos criterios de utilización y a ejercitar las facultades de control sobre los

³⁴ GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A., “La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo”, *Revista Española de Derecho del Trabajo*, núm. 216, 2019, parte Estudios, 2019.

mismos que estime más oportunas. Además, si el empleador ha aportado unas instrucciones de uso concretas, imponiendo el uso exclusivamente profesional de los medios de trabajo, siendo este el caso, si se ejerce un control sobre los mismos, no se considerará vulnerado el derecho a la intimidad.³⁵ Esta es la razón por la que si nos fijamos existe una cierta discordancia entre el art. 20 bis del Estatuto de los Trabajadores y el art. 87 LOPDGDD. Ambos preceptos se refieren a la intimidad en el uso de dispositivos digitales. Sin embargo, como podemos apreciar, en el art. 20 bis LET, se reconoce a los trabajadores el derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición por el empleador. De hecho, si atendemos a la dicción literal del precepto, vemos que se utiliza el término “*tienen*”, lo cual parece indicar que con carácter general los trabajadores tienen reconocido el derecho a la intimidad en el uso de dispositivos digitales. En cambio, el art. 87 LOPDGDD dice que los trabajadores “*tendrán*” derecho a la protección de su intimidad, lo cual nos indica que el art. 87 LOPDGDD, no está reconociendo expresamente el derecho a la intimidad, sino que está garantizando su protección siempre y cuando se den las condiciones necesarias, ya que los trabajadores en el uso de dispositivos digitales puestos a su disposición por el empresario no tienen siempre derecho a la protección del derecho a la intimidad personal, especialmente en el caso de que el empresario haya prohibido el uso de los dispositivos para fines personales, supuesto en el cual no hay derecho a la intimidad.³⁶

Seguidamente, dentro del ámbito de los derechos digitales en el marco de las relaciones laborales, es de interés el art.88 LOPDGDD en el que se reconoce un derecho digital de incipiente regulación en nuestro ordenamiento jurídico: el derecho a la desconexión digital. De acuerdo con el art. 88 LOPDGDD los trabajadores y empleados públicos tienen derecho a la desconexión digital, derecho que es reconocido con el objetivo de garantizar fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto al tiempo de descanso, permisos y vacaciones, así como la intimidad personal y familiar de los empleados. Asimismo, la norma, en su segundo inciso, establece que las modalidades del ejercicio de este derecho han de ajustarse a la naturaleza y objeto de la relación laboral, potenciando la conciliación de la vida laboral y la vida personal y

³⁵ SERRANO GARCÍA, J. M., “La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia”, Bormazo, 2019, pág. 48.

³⁶ RIBAS, X., “Puntos destacados de la nueva Ley Orgánica 3/2018 de Protección de Datos”, *Aranzadi digital*, núm. 1, 2020, págs. 7 y 8.

familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

Por último, en el tercer inciso del art. 88 LOPDGDD, se establece que el empleador ha de elaborar una política interna dirigida a los trabajadores, incluidos los que ocupen puestos directivos, en la que definirá las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre el uso razonable de las herramientas tecnológicas que evite el riesgo de padecimiento de fatiga informática. Finalmente, el legislador hace una especial mención a la protección del derecho a la desconexión digital en un supuesto específico, que es en el caso de la realización total o parcial del trabajo a distancia o a domicilio, siempre y cuando, este vaya ligado al uso con fines laborales de las herramientas tecnológicas.

En suma, como se puede observar, el derecho a la desconexión digital está estrechamente vinculado con la conciliación de la vida laboral con la vida personal y familiar, siendo un derecho que presenta una mayor importancia en aquellos trabajos que son desempeñados a distancia o desde el domicilio, en cuyo caso, la propia empresa deberá de diseñar un protocolo de desconexión digital en el que se establezcan claramente cuáles son los periodos de trabajo y cuáles son los periodos destinados al descanso y a la vida familiar y personal.

En esta misma línea, no puede obviarse que las tecnologías de la información y de la comunicación desempeñan un papel clave en la nuestra sociedad o en la también llamada Sociedad de la información, gozando de una fuerte inserción en todos los ámbitos de nuestra vida. A nosotros nos interesa sobre todo el ámbito laboral, en el que las herramientas tecnológicas son utilizadas, entre otras utilidades, como instrumento eficaz para que el empresario pueda ejercer el poder de vigilancia y control que le es reconocido en el art. 20.3 LET. Dentro de estas facultades de control destaca el uso de videovigilancia como medida de control empresarial. Sobre esta cuestión hay que indicar que la Ley de Protección de Datos Personales se refiere a esta medida en su art. 89 con la rúbrica *“Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo”*. Concretamente, este precepto faculta a que el empresario pueda someter a tratamiento las imágenes obtenidas a través de cámaras o videocámaras para el ejercicio de las facultades de control reconocidas en el art 20.3 LET,

siempre que estas facultades se ejerzan dentro del marco legal previsto y respetando los límites previstos en la ley. Así todo, el precepto señala que los empresarios tienen el deber de aportar información previa, de forma expresa, clara y concisa, a los trabajadores y a sus representantes sobre la adopción de esta medida. Cuestión distinta es el supuesto de que se haya captado la comisión flagrante de un acto ilícito por parte de los trabajadores, ya que siendo este el caso, la interpretación del deber de información se flexibiliza, en la medida en que se considerará cumplido con la mera colocación de al menos un distintivo informativo en un lugar suficientemente visible, estableciendo en el mismo los siguientes extremos: la existencia del tratamiento, la identificación del responsable y la posibilidad de ejercitar los derechos establecidos en los arts. 15 a 22 RGPD.³⁷

Además, el art. 89.2 LOPDGDD se refiere a la vigilancia a través de sistemas de captación del sonido, estableciendo que no está permitida la instalación de sistemas de grabación del sonido, ni de videovigilancia en lugares destinados al descanso, esparcimiento, tales como vestuarios, aseos, comedores y lugares análogos, dado que se trata de espacios en los que la expectativa de privacidad de los trabajadores alcanza un grado máximo. Asimismo, el citado precepto en su apartado tercero establece que la utilización de sistemas de captación del sonido solamente estará permitida cuando existan riesgos relevantes para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y se hará respetando los principios de proporcionalidad, de intervención mínima y las garantías previstas en la LOPDGDD.

Por otra parte, para la supresión de todos estos datos obtenidos a través de sistemas de cámaras y de videocámaras, así como para la supresión de los sonidos conservados por sistemas de grabación, hay que hacer una especial alusión al art. 22.3 LOPDGDD, que establece que con carácter general dicha supresión se realizará en un plazo máximo de un mes desde su captación, salvo que dichos datos se utilicen para acreditar la comisión de un acto ilícito, en cuyo caso, los datos obtenidos deberán ser puestos a disposición de la autoridad competente. Asimismo, este mismo precepto habilita a que las personas físicas o jurídicas, públicas o privadas puedan llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones, estableciendo que solo podrán captarse

³⁷ SERRANO GARCÍA, J. M., “La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia”, Bormazo, 2019, págs. 35-37.

imágenes en la vía pública en la medida en que resulte imprescindible para la finalidad anteriormente mencionada.

En lo que respecta a la utilización de sistemas de geolocalización como mecanismo de control empresarial y su incidencia en el derecho a la intimidad, se trata de una facultad de control regulada en el art. 90 LOPDGDD. Dicho precepto, está habilitando a los empleadores para poder tratar los datos obtenidos a través de este sistema de control, siempre y cuando, el control vaya orientado exclusivamente a la verificación del cumplimiento de las obligaciones y deberes laborales. Asimismo, el precepto añade que los datos obtenidos a través de sistemas de geolocalización deberán ser suprimidos en los términos dispuestos en el art. 22.3 LOPDGDD, es decir, en un plazo de un mes. A continuación, el citado precepto, en su segundo inciso establece un mandato para los empresarios, concretamente, el cumplimiento de un deber de información previa. Dicha información deberá de facilitarse a los empleados y, en su caso, a sus representantes; información que además deberá de ser aportada de forma expresa, clara e inequívoca, comunicando a los empleados tanto sobre la existencia y las características de los dispositivos de control instalados como sobre el posible ejercicio de los derechos de acceso, rectificación y limitación del tratamiento y supresión.

Finalmente, resulta de interés hacer una mención al art. 91 LOPDGDD que hace un llamamiento a la negociación colectiva, encomendándole el papel de establecer unas garantías adicionales a los derechos y libertades relacionados con el derecho a la protección de datos, así como el establecimiento de unas cautelas destinadas a garantizar una correcta salvaguarda de los derechos digitales de los trabajadores.³⁸

4. VIGILANCIA MICROFÓNICA

Otra de las herramientas de control de las que dispone el empresario es la grabación del sonido en el centro de trabajo, control que puede hacer efectivo, bien a través de la instalación de micrófonos, bien por medio de la instalación de cámaras de

³⁸ LÓPEZ CUMBRE, L., “Protección de datos “laborales” (www.gomezacebo-pombo.com, diciembre de 2018).

videovigilancia con audio incorporado, o bien a través de la grabación de conversaciones telefónicas.

Si bien es cierto, la vigilancia auditiva es un mecanismo de control mucho más limitativo de la intimidad del trabajador que el control visual, lo cual se debe a que a través de una conversación entre dos o más personas pueden expresarse ideas, opiniones o pensamientos íntimos y, es precisamente por esta sencilla razón que el control auditivo constituye un medio mucho más invasivo que el control visual, por ende, esta concreta modalidad de control estará sometida a unos requisitos mucho más rigurosos y, además, será necesario tener en consideración una serie de cuestiones, para poder verificar si dicho medio de control puede suponer una vulneración del derecho a la intimidad personal del trabajador. Así todo, se ha de indicar que el derecho a la intimidad personal no es el único derecho que puede verse afectado con el uso de estos instrumentos de monitorización consistentes en la captación de sonido. Igualmente, pueden verse afectados otros derechos como el derecho al secreto de las comunicaciones del art. 18.3 CE o el derecho a la protección de datos del art. 18.4 CE. La razón por la cual este último derecho se ve afectado con el uso de mecanismos de control auditivo se debe a que la voz es considerada como un dato de carácter personal que permite la identificación de una persona, de hecho, el art. 3 LOPDGDD define el dato de carácter personal como “*cualquier información concerniente a personas físicas identificadas o identificables*”, en consecuencia, la voz es un dato que hace reconocible a una persona y, por lo tanto, se trata de un elemento que queda englobado en la definición prevista en dicho precepto.

En lo concerniente a la vigilancia microfónica y a la posible limitación que esta puede provocar en el derecho a la intimidad personal, han de analizarse una serie de factores, entre los mismos: la localización de los dispositivos de control, dado que no es lo mismo que los micrófonos sean colocados en espacios públicos y en lugares visibles a que sean colocados en las zonas de descanso, en los aseos o en los vestuarios, pues en este último caso, se trata de lugares en los que el trabajador tiene una mayor expectativa de privacidad. En este sentido, el art. 89.3 LOPDGDD establece que para que se admita la utilización de sistemas de captación del sonido han de respetarse tres requisitos: en primer lugar, es necesaria la concurrencia de riesgos relevantes para la seguridad de las instalaciones, de los bienes y de las personas derivados de la naturaleza de la actividad que se desarrolle en el centro de trabajo; en segundo lugar, se deberá respetar el principio

de proporcionalidad y el de intervención mínima y, en tercer lugar, se exige que el almacenamiento de los sonidos que sean captados a través de estos sistemas de seguridad, sea suprimida en el plazo máximo de un mes.

Por otra parte, ha de analizarse el propósito empresarial perseguido con la instalación de los dispositivos de captación del sonido. En efecto, la instalación de mecanismos de control audiovisual ha de estar justificada, y así será si la medida de control responde a una finalidad protectora de la seguridad de las instalaciones. De hecho, hay determinados lugares en los que se quiere ejercer un control adicional, dado que se trata de zonas en las que existe un mayor riesgo de que se produzcan atentados contra el patrimonio, el personal o los clientes de la empresa, como suele ocurrir, por ejemplo, en el caso de las entidades bancarias, aeropuertos o en museos.³⁹

Asimismo, se ha de analizar si la medida de control es apta para satisfacer el fin propuesto con su adopción, también ha de analizarse si no existe otro medio menos invasivo que de igual modo satisfaga el interés o finalidad que persiga el empresario, ya que, de ser así, será este último dispositivo el que deberá de ser instalado en el centro de trabajo. Igualmente, tales dispositivos de vigilancia no pueden ser colocados siempre en los mismos lugares, departamentos o de forma que siempre afecten a unas personas concretas, sino que han de ser colocados de forma aleatoria, ya que tales medidas no pueden resultar arbitrarias, ni pueden obedecer a fines discriminatorios. De hecho, según el art. 17.1 LET se entienden nulas las decisiones empresariales que den lugar en el empleo a situaciones de discriminación. En cualquier caso, nuestro Tribunal Constitucional viene exigiendo que las medidas de control implementadas por el empresario se sometan a un triple juicio de proporcionalidad, o lo que es lo mismo, ha de garantizarse un justo equilibrio entre los derechos fundamentales de los trabajadores afectados y el interés del empresario.

A continuación, será objeto de análisis una sentencia de nuestro Tribunal Constitucional, la STC 98/2000, de 10 de abril de 2000, en dicha sentencia el TC considera que se ha producido una intromisión en el derecho a la intimidad personal consagrado en el art 18.1 CE, intromisión que se produce tras la implementación en el

³⁹MONREAL BRINGSVAERD, E., THIBAUT ARANDA, X. y JURADO SEGOVIA, A., “Derecho del trabajo y nuevas tecnologías”, Tirant Lo Blanch, Valencia, 2020, pág. 240 y 418.

casino de un sistema de vigilancia microfónica en la empresa Casino de la Toja. En particular, son instalados varios micrófonos en diversas zonas del casino, concretamente en las instalaciones destinadas al juego de azar, así como en las dependencias de la caja y la zona en la que se halla ubicada la ruleta francesa.

Tras la instalación de la medida de seguridad no se solicitó ningún informe al Comité de empresa acerca de la misma, lo cual no se ajusta con lo dispuesto en el art. 64.4 d) LET. Dicha medida de control comienza a ser operativa con posterioridad a la comunicación al citado Comité, es por ello, que el presidente del Comité de Empresa interpone una demanda, la cual es estimada por el Juzgado de lo Social núm. 3 de Pontevedra, dicho Juzgado dicta una Sentencia, concluyendo que se ha producido una intromisión en el derecho a la intimidad personal del art. 18.1 CE, y consecuentemente, ordena a la empresa Casino de la Toja el cese inmediato en su conducta, así como el retorno a la situación anterior al momento en el cual se procede a la instalación del sistema de vigilancia microfónica.

Precisando aún más, el Juzgado de lo social concluye que la instalación de dispositivos de control auditivo se considera generalmente como ilícita, salvo algunas excepciones, y, además, el Juzgado de lo social añade que la vigilancia microfónica se constituye como un medio de control mucho más invasivo, dado que el control auditivo permite grabar y almacenar conversaciones entre los trabajadores o con los clientes, en las que estos pueden expresar ideas o pensamientos propios de la esfera privada de la persona, es por esta razón, que el Juzgado de lo social considera que se ha producido una vulneración al derecho a la intimidad personal y, además, entiende que la medida no está suficientemente justificada, ya que con el mero control efectuado por los circuitos cerrados de televisión, ya se satisface la finalidad pretendida por el empresario y, por lo tanto, la incorporación de una medida de control auditivo no solo resulta intrusiva e innecesaria, sino que además produce una limitación completa de la intimidad personal.

Tras la sentencia dictada por el Juzgado de lo Social, es interpuesto por el Casino de la Toja un recurso de suplicación ante la sala de lo social del Tribunal Superior de Justicia de Galicia. Dicho Tribunal llega a una conclusión opuesta a la del Juzgado de lo social y entiende que la instalación de aparatos de control microfónico no conculca el derecho a la intimidad personal y, para ello, se basa en diversas razones; entre las mismas,

el Tribunal Superior de Justicia de Galicia entiende que el centro de trabajo no es un lugar en el que se ejerza el derecho a la intimidad personal de los trabajadores, sino que el derecho a la intimidad personal es un derecho propio de la esfera privada de la persona y, en consecuencia, las conversaciones mantenidas por los trabajadores en el centro de trabajo no quedan amparadas por el derecho a la intimidad personal del art. 18.1 CE.

Asimismo, el Tribunal Superior de Justicia entiende que desde el punto de vista de la finalidad de la medida no se plantea ningún problema, pues la medida contribuye a añadir un mayor control y seguridad a la actividad de juego ofrecida por el Casino. Además, añade que los micrófonos son perfectamente visibles y son colocados en zonas concretas, es por ello, que la medida no puede reputarse como arbitraria, ni es susceptible de provocar vulneración alguna al derecho a la intimidad personal consagrado en el art 18.1 CE.

Contra la anterior Sentencia dictada por la Sala de lo Social del Tribunal Superior de Justicia de Galicia, se interpone recurso de amparo, entendiendo que el sistema de control microfónico ha producido una vulneración al derecho a la intimidad personal regulado en el art. 18.1 CE, asimismo, se cuestiona la legitimidad de la finalidad de la medida, ya que la función de seguridad y control ya quedaba cubierta por el circuito cerrado de televisión y, por lo tanto, el sistema de control auditivo no queda suficientemente justificado, ni puede ampararse en la potestad de vigilancia y control reconocida al empresario en la Ley del Estatuto de los Trabajadores.

Asimismo, serán objeto de análisis las observaciones ofrecidas por el Tribunal Constitucional respecto al fondo del asunto, concretamente, entraremos a determinar si se ha suscitado o no una vulneración al derecho a la intimidad personal. El derecho a la intimidad personal es entendido como una derivación del derecho a la dignidad de la persona del art. 10 CE, que cumple la función de salvaguardar un espacio privado y reservado del individuo frente a las eventuales injerencias que puedan producirse y se concibe como un espacio cuya protección es necesaria para garantizar un mínimo de calidad de vida humana según las pautas de nuestra cultura.

A este respecto, conviene matizar, que desde la óptica de las limitaciones que inciden en la dignidad de la persona, la colocación en cualquier lugar de aparatos de

escucha o de cualquier otro medio análogo que sea apto para grabar o reproducir la vida íntima de las personas, se percibe como una intromisión ilegítima al derecho a la dignidad e intimidad personal, de acuerdo con lo dispuesto en el art. 7 de la Ley Orgánica 1/1982, de 5 de mayo de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen en conexión con el art. 2 de la citada Ley.⁴⁰

El TC mantiene una postura contraria a la de la sentencia recurrida, ya que sostiene que el derecho a la intimidad personal no solamente puede ser ejercido en la esfera privada de la persona, sino que también ha de proyectarse al centro de trabajo, lugar en el cual pueden suscitarse intromisiones ilegítimas al derecho a la intimidad personal de los trabajadores. En consonancia con lo anterior, se ha de aclarar que el derecho a la intimidad personal no es un derecho absoluto, y en ocasiones puede ceder ante otros intereses constitucionalmente relevantes. Por lo tanto, a la hora de verificar si realmente se ha producido una vulneración al derecho a la intimidad personal han de ser objeto de análisis una serie de elementos: se ha de considerar el lugar en el que se coloque la medida, la cual ha de ser instalada en zonas concretas del Casino y, de ninguna manera, puede ser colocada de forma arbitraria e indiscriminada, asimismo, se ha de atender a si la medida de control ha sido emplazada en zonas visibles o si, por el contrario, se trata de una medida de control velada.

Igualmente, ha de ser examinada la finalidad pretendida al implementar la medida de control auditivo, ya que, pese a que el interés empresarial es un interés constitucionalmente relevante y merecedor de tutela y protección, esto no quiere decir que para lograr satisfacer dicho interés empresarial pueda provocarse cualquier sacrificio a los derechos fundamentales. Ha de garantizarse un equilibrio entre los dos bienes jurídicos que aparecen contrapuestos en el contrato de trabajo, ya que ambos son merecedores de protección constitucional, aunque pueden producirse limitaciones en alguno de estos derechos con vistas a garantizar el otro. Sin embargo, no puede ser admitida cualquier tipo de modulación, sino que dicha modulación ha de ser la estrictamente necesaria, y, además, dicha modulación no será admisible cuando existan otras medidas de control menos intensas, se trata ni más ni menos, de la aplicación del principio de proporcionalidad como canon de constitucionalidad.

⁴⁰ STC 98/2000, de 10 de abril, FFJJ 5,6,7 y 9.

En síntesis, sobre las base de las ideas expuestas, el Tribunal Constitucional infiere como conclusión, que la instalación de aparatos microfónicos es una medida ilegítima e invasiva, ya que su instalación no puede reputarse como estrictamente necesaria, pues el control y la seguridad ya quedaban cubiertos con la colocación del circuito cerrado de televisión, y aunque ciertamente, la medida otorgaba un plus de seguridad y resultaba útil para la empresa, ya que lograba controlar transacciones económicas importantes que eran efectuadas en las zonas de control. No obstante, no basta con que tales medidas resulten provechosas y convenientes para la empresa, sino que han de ser suficientemente justificadas y fundarse en razones de estricta necesidad. En definitiva, no basta con la concurrencia de un interés empresarial relevante, sino que dicho interés empresarial ha de conjugarse con el principio de proporcionalidad y, por ende, ha de garantizarse un necesario equilibrio entre ambos bienes jurídicos, sin que tengan lugar intromisiones ilegítimas.

Dentro del marco de la vigilancia auditiva de cara a las eventuales incidencias que puedan suscitarse en el derecho a la intimidad personal del art. 18.1 CE y, especialmente en el derecho al secreto de las comunicaciones reconocido en el art 18.3 CE, es necesario distinguir entre la grabación de una conversación de “otros” y la grabación de una conversación “con otros”. A dicha diferenciación hace alusión la STS 678/2014, de 20 de noviembre de 2014 (rec. 3402/2012). En la referida sentencia se analiza si la grabación de un conversación efectuada por una trabajadora a través de un teléfono portátil ha provocado una vulneración al derecho a la intimidad personal del empleador, llegando el Tribunal a la conclusión de que no se ha provocado conculcación alguna y, para ello se basa en las siguientes razones: en primer lugar, que la grabación de la conversación tiene lugar en la vía pública, concretamente en la entrada al lugar de trabajo; en segundo lugar, en dicha conversación que es mantenida por la trabajadora y su jefe, no se hace referencia a ningún aspecto íntimo, ni referente a la vida privada o personal del demandante, asimismo, ha de tenerse en cuenta la finalidad de la grabación. En particular, la demandada con la grabación de la conversación pretendía protegerse de los ataques y ofensas del empleador, dado que ya había sido objeto vejaciones y afrentas por parte de este. Es por ello, que el propósito de la grabación no es inmiscuirse en la vida privada del empleador, ni difundir la conversación, sino simplemente protegerse frente a posibles agravios y proponer la grabación como prueba en el proceso judicial.

Si bien es cierto, se ha de tener en cuenta el hecho de que la grabación de la conversación no era consentida, ni conocida por el empleador. Sin embargo, esta circunstancia no es suficiente para estimar que se ha suscitado una afectación al derecho a la intimidad personal del art. 18.1 CE, dado que también hay que valorar otros elementos como, por ejemplo, el contenido de la conversación, el cual no hace referencia a ningún aspecto privado del empleador, sino que en la conversación mantenida meramente se hace referencia a temas laborales. En todo caso, la medida se considerará ilícita por el mal uso posterior que se haga de la misma, esto es en caso de que la grabación sea difundida a terceros.

Por otra parte, si analizamos la licitud o no de la medida desde la perspectiva del derecho al secreto de las comunicaciones, que encuentra cobertura legal en el art. 18.3 CE, se ha de concluir que no se ha provocado vulneración alguna, ya que el derecho al secreto de las comunicaciones trata de proteger el carácter secreto de la conversación, pero solo frente a las intromisiones de terceros ajenos a la comunicación, y no frente a los propios interlocutores y a aquellos a los que la conversación les atañe.⁴¹

4.1. LA VIGILANCIA TELEFÓNICA

Una de las manifestaciones concretas de la vigilancia auditiva efectuada por el empresario, es la intervención de las llamadas efectuadas por el propio trabajador en la empresa. La interceptación de las llamadas telefónicas efectuadas en el centro de trabajo consiste en la captación de las conversaciones mantenidas por los trabajadores, así como las conversaciones entre trabajadores y clientes, siendo una medida de control que normalmente interfiere con el derecho al secreto de las comunicaciones del art. 18.3 CE. Si bien es cierto, las escuchas telefónicas también pueden atentar contra otros derechos fundamentales, como el derecho a la intimidad personal del art. 18.1 CE. Esta tipología de control que se basa en la captación del sonido presenta una incidencia mayor en estos derechos fundamentales, porque tiene por objeto captar conversaciones y, normalmente, de estas conversaciones se extraen pensamientos, opiniones y sentimientos que no se

⁴¹ STS 678/2014, de 20 de noviembre de 2014 (rec. 3402/2012), FFJJ 1, 2 y 3.

refieren tanto a la espera profesional, sino al ámbito privado de la persona⁴². Esto no quiere decir que el empresario no puede hacer efectiva esta modalidad de control, pues efectivamente está legitimado para ejercer este tipo de control, de hecho, hay numerosas sentencias que aprueban la implementación de mecanismos de control auditivo y, además, el empleador puede adoptar las medidas que estime más oportunas, siempre y cuando, respete un límite principal: la dignidad del trabajador que se vea afectado por la medida. Con ello, lo que se quiere decir realmente, es que el empleador podrá implementar este sistema de control, siempre y cuando, la naturaleza de la prestación laboral y las circunstancias del caso lo justifiquen, y siempre que se respeten los límites legales para que la medida pueda reputarse como válida.

Es evidente, que el empresario puede establecer con carácter previo las reglas y restricciones de uso del teléfono en el centro de trabajo, sobre todo si dicho teléfono es un medio de producción para la propia empresa. De hecho, esta sería la situación idónea, es decir, el supuesto en el cual el empresario inicialmente ha establecido un conjunto de reglas y condiciones que rigen en la utilización del teléfono de la empresa, de tal manera que el empresario puede verse legitimado para sancionar a aquel trabajador que haga caso omiso del protocolo de uso del teléfono de la empresa y lo utilice de forma irregular y abusiva. También es posible que el empresario prohíba el uso de los medios de trabajo para fines particulares, ya que, si el empresario pone a disposición del trabajador un teléfono, normalmente será con la finalidad de que el trabajador lo utilice como herramienta de trabajo y, en consecuencia, el uso del teléfono ha de quedar limitado al desempeño de la actividad laboral.

Por otra parte, existe el escenario en el cual el empleador no haya establecido un conjunto de instrucciones en el uso del teléfono como herramienta de trabajo, en este caso, el empleador adopta una actitud más permisiva y, es por ello, que estará más limitado a la hora de sancionar al trabajador, ya que este tendrá una cierta expectativa de privacidad. Sin embargo, que no se haya establecido con carácter previo un protocolo de utilización del teléfono en el trabajo, no quiere decir que el empleador se encuentre despojado de la facultad disciplinaria de la que es titular, de hecho, que no se hayan establecido un conjunto de reglas previas en la utilización del teléfono no quiere decir

⁴² THIBAUT ARANDA, J., "Control Multimedia de la Actividad Laboral", Tirant Lo Blanch, Valencia, 2006, pág. 3.

que el trabajador pueda utilizarlo de forma abusiva e irregular sin sufrir ninguna consecuencia por ello, ya que no podemos olvidar que uno de los deberes básicos del trabajador es el deber de buena fe. En este sentido, uno de los supuestos que se recogen como causa de incumplimiento del contrato de trabajo y como causa de despido disciplinario en el art. 54.2 ET, es la transgresión de la buena fe, así como el abuso de confianza en el desempeño de la actividad laboral por parte del trabajador.⁴³

Si bien es cierto, esta tipología de control no solo está destinada a controlar a los trabajadores que se sirven del teléfono como herramienta de trabajo, verificando así, si cumplen con sus obligaciones y deberes laborales, sino que también puede ser utilizada para fiscalizar la calidad de los servicios de atención al cliente, es decir, el empleador puede controlar las conversaciones mantenidas con los clientes con la finalidad de verificar que el trabajador cumpla con unos estándares determinados en el desempeño de la actividad laboral. Así, por ejemplo, en la STS de 5 de diciembre de 2003, se hace referencia a la cuestión de las escuchas telefónicas. En concreto, se interpone una demanda solicitando que se declare la ilegalidad de la vigilancia telefónica practicada por la empresa sobre las llamadas efectuadas por los asesores que se encargaban realizar labores de telemarketing, para ello, los asesores se servían de un teléfono denominado plataforma 2004. La mentada plataforma estaba destinada exclusivamente al uso profesional.

La primera precisión que ha de reseñarse, es que tales medidas de control pueden ser implementadas en la empresa, pero de su colocación se deriva un conflicto de intereses que necesariamente han de ser compatibilizados, específicamente se trata del derecho a la libertad de empresa y a la dirección de la actividad laboral que ostenta el empresario y de los derechos fundamentales del trabajador, en este caso el derecho a la intimidad de los trabajadores con cobertura legal en el art. 18.1 CE y en el art. 4.2 ET. Como ya se ha indicado en líneas anteriores se pueden producir recortes en ambos bienes jurídicos, pero para que de tales afectaciones no originen resultados inconstitucionales es necesario que las medidas de control empresarial superen un triple juicio de proporcionalidad.

⁴³ THIBAUT ARANDA, J., “Control Multimedia de la Actividad Laboral”, Tirant Lo Blanch, Valencia, 2006, págs. 12-13.

La medida de control finalmente es calificada como proporcionada, dado que la fiscalización es implementada con la estricta finalidad de controlar la correcta realización de las funciones de telemarketing, que eran desempeñadas por los asesores de cara a lograr la fidelidad de los clientes, así como de la captación de otros nuevos. Por otra parte, el control tenía por objeto controlar aleatoriamente el contenido de las conversaciones mantenidas entre trabajadores y clientes con la finalidad de calificar la calidad del servicio prestado por los asesores. Dicho control exclusivamente iba destinado a las llamadas entrantes, de las cuales solo eran interceptadas aproximadamente un 0.5 % y, además, los asesores eran conocedores de que las llamadas podían ser interceptadas, por lo que la medida no resultaba abusiva.

En base a lo anteriormente expuesto, el TS llega a la conclusión lógica de que la medida no solo se ajusta a la legislación vigente, sino que, además, la medida resulta ponderada al superar un triple juicio de proporcionalidad, ya que únicamente tiene como finalidad controlar la calidad del servicio prestado por los asesores, además, se trata de una medida necesaria al no existir otra herramienta de control menos intrusiva y es una medida idónea y ponderada, pues de ella se extraen más beneficios que desventajas, ya que sirve para mejorar el servicio prestado por los asesores y las limitaciones producidas en el derecho a la intimidad de los trabajadores son mínimas, dado que solo eran controladas las llamadas entrantes y el teléfono estaba exclusivamente destinado al uso profesional, pues para fines particulares disponían de un teléfono distinto.⁴⁴

4.2. La regulación del uso del teléfono móvil en la negociación colectiva

Una de las principales aplicaciones que trae consigo la implantación de los dispositivos tecnológicos en las empresas, es el uso del teléfono móvil como herramienta de trabajo. El teléfono móvil es un dispositivo fundamental para los trabajadores. Lo habitual es que este dispositivo tecnológico sea propiedad del empleador, que suele ceder su uso a los empleados para facilitar el ejercicio de la prestación laboral, ya que se trata de una herramienta que resulta muy beneficiosa, pues facilita los negocios, permite realizar cursos y actividades formativas, permite la comunicación con los clientes, enviar y recibir emails, etc.

⁴⁴ STS, de 5 de diciembre de 2003 (rec. 52/2003), FJ 3.

El problema está en saber diferenciar entre el uso personal y profesional del teléfono móvil y en conocer cuáles son las reglas de uso de los dispositivos tecnológicos, puesto que el uso inadecuado de estas herramientas puede ser considerado como una falta grave en la empresa. Ahora bien, para que los trabajadores puedan utilizar adecuadamente los medios de trabajo es necesario que el empleador les haya facilitado de forma previa unas reglas e instrucciones de uso. A esta cuestión se refiere el art. 87 LOPDGDD, en cuyo apartado tercero impone a los empleadores el deber de establecer unos criterios de utilización de los dispositivos digitales y, por otra parte, es de interés el art. 91 LOPDGDD que hace un llamamiento a la negociación colectiva para que esta pueda establecer mayores garantías en la salvaguarda de los derechos digitales y de los derechos y libertades relacionados con el tratamiento de datos personales, por lo que de este precepto, se extrae que los convenios colectivos desempeñan un papel fundamental en esta materia, estableciendo entre otras previsiones qué usos están autorizados y cuáles no, así como el tiempo de uso que debe ser dedicado a fines particulares y el tiempo que ha de estar destinado a fines profesionales.

Algunos ejemplos de Convenios colectivos en los que se han incluido previsiones relativas a la salvaguarda del derecho a la intimidad en el uso de dispositivos digitales son: el Convenio colectivo estatal de estaciones de servicio (C.C. 99001995011981), suscrito el 19 de diciembre de 2019, en el cual se considera como falta grave el uso del teléfono móvil (aun siendo propiedad del trabajador) para fines personales durante el tiempo efectivo de trabajo, así como el uso reiterado o el perjuicio generado por el mismo en el proceso productivo, además también es considerada como falta grave el uso no autorizado y con carácter personal de las herramientas de la empresa, ya sea dentro o fuera de la jornada laboral, teniendo a estos efectos consideración de herramientas de la empresa todos los equipos informáticos, mientras que se considera como falta leve el uso del teléfono de la empresa para asuntos particulares sin autorización, salvo que el uso del mismo se deba a motivos de urgencia o imperiosa necesidad;

Otro ejemplo de Convenio colectivo de aplicación en esta materia es el III Convenio colectivo estatal de la industria, la tecnología y los servicios del sector del metal (C.C. 99003435011900), que fue suscrito con fecha 5 de noviembre de 2019. En el mismo, se recogen previsiones relativas al uso de dispositivos digitales y al derecho a la

intimidad, reconociendo el derecho a la intimidad de las personas trabajadoras en el uso de dispositivos digitales puestos a su disposición por el empresario. Asimismo, en el convenio se reconoce al empresario la facultad de acceder al contenido derivado del uso de los medios digitales a los efectos de verificar el cumplimiento de las obligaciones laborales y estatutarias y garantizar la integridad de los dispositivos;

Asimismo, el II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU. (C.C. 90100303012015) regula el uso de los dispositivos digitales prohibiendo con carácter general el uso de los dispositivos digitales para fines particulares, salvo que dicho uso esté justificado conforme a parámetros de razonabilidad como son la atención de necesidades domésticas, familiares, cuestiones de necesidad o urgencia, usos esporádicos para acceder a información no prohibida por Telefónica y análogos, siempre que tal uso no interfiera en el normal cumplimiento de las obligaciones laborales y se lleve a cabo durante el tiempo indispensable. Además, el convenio establece que el uso de estos dispositivos digitales no puede atentar contra la confidencialidad de la información de Telefónica, su reputación, ni poner en riesgo la seguridad de la información, o de los dispositivos y medios digitales que hayan sido facilitados a los trabajadores. Por otra parte, se reconoce en el mismo la facultad de controlar el uso de estas herramientas puestas a disposición de los trabajadores para controlar el desempeño de la actividad laboral, siempre y cuando dicho control se efectúe respetando los términos del Convenio Colectivo y respetando en todo caso los derechos fundamentales de las personas trabajadoras, debiendo adoptarse unas medidas de control que sean proporcionadas con el riesgo existente.

5. CONTROL DEL USO DE MEDIOS INFORMÁTICOS Y DEL ACCESO A INTERNET EN EL CENTRO TRABAJO

En la era digital el recurso a internet en el centro de trabajo se ha convertido en una realidad recurrente. El uso de internet y del ordenador como herramienta de trabajo, por un lado, aporta múltiples beneficios en el ámbito laboral, ya que facilita y agiliza el trabajo y, además, su uso en determinadas modalidades de empleo, como por ejemplo, el teletrabajo, resulta imprescindible para que el trabajador pueda cumplir con las funciones

que le han sido asignadas, es más, hoy en día es habitual que los trabajadores realicen sus funciones en una oficina en la que dispongan de un ordenador con acceso a internet. Por otro lado, el libre acceso a internet por parte del trabajador puede comportar desventajas, pues los trabajadores pueden utilizar esta herramienta de trabajo para fines personales y para acceder a redes sociales. Este tipo de acciones, pueden parecer inocuas, ya que en ocasiones el trabajador necesita desconectar de la sobrecarga de tareas que tiene que atender diariamente, sin embargo, que el trabajador dedique su tiempo a atender sus redes sociales puede provocar un perjuicio al empresario, ya que este tipo de acciones suelen provocar una disminución de la productividad y eficiencia del trabajador, y, en consecuencia, el empresario puede sufrir pérdidas económicas.

Es por ello, que en todo centro de trabajo es indispensable que el empleador establezca con carácter previo una serie de instrucciones y condiciones de uso del ordenador que han de ser puestas a disposición del trabajador. Asimismo, también puede resultar necesario un control del uso de estos dispositivos digitales en la empresa, de hecho, el empleador está capacitado para controlar la debida ejecución de la prestación laboral, dicha facultad de control es reconocida en el art 20.3 LET y habilita al empleador a adoptar las medidas de control que estime más oportunas, entre tales facultades se encuentran las facultades de vigilancia y control de la utilización de los medios informáticos que el trabajador utilice en su puesto de trabajo. Ahora bien, la potestad de control que ostenta el empresario no es una potestad ilimitada, y, además, hay que reseñar que el uso del ordenador por parte del trabajador para fines personales puede estar permitido, bien porque se parta de un escenario de permisibilidad en la empresa, o bien, porque el uso del ordenador para fines personales se produce de forma puntual y sin hacer mella en la productividad del trabajador. En todo caso, si el empleador tolera que el trabajador utilice los dispositivos digitales para fines privados, entonces, deberá de concretar cuáles son los usos concretos a los que el trabajador está autorizado y, además, en aras a preservar el derecho a la intimidad personal, deberá de establecer unas garantías, tales como la determinación de los periodos en los cuales el trabajador puede utilizar los dispositivos digitales para fines personales.⁴⁵

⁴⁵ Art. 87.3 LOPDGDD.

Si bien es cierto, el uso de internet como herramienta de trabajo ofrece al trabajador un sinnúmero de posibilidades de entretenimiento a través de la navegación por internet, de tal forma que, el trabajador puede utilizar esta herramienta para consultar sus redes sociales, para chatear y comunicarse con otras personas o para visitar páginas webs. Si el trabajador deja de utilizar de forma racional los medios digitales, dejando desatendidas las tareas que le han sido encomendadas, entonces es lógico que el empresario pueda hacer uso de su potestad disciplinaria e imponer al trabajador determinadas sanciones, tales como el despido disciplinario previsto en el art 54.2 ET, que prevé distintas causas de despido, de las cuales nos interesan: la indisciplina y desobediencia, la transgresión de la buena fe o el abuso de confianza por parte del trabajador en el desempeño de la actividad laboral, así como la disminución continuada y voluntaria del rendimiento.⁴⁶

Asimismo, como ya se ha indicado en líneas anteriores, el empleador con el fin de controlar el correcto desenvolvimiento de la prestación laboral, así como el cumplimiento de las obligaciones laborales por parte del trabajador, puede hacer uso de su potestad de control reconocida en el art. 20.3 LET, siempre y cuando, respete determinadas limitaciones impuestas al poder de control empresarial, tales como el respeto de la dignidad del trabajador, el respeto al derecho a la intimidad personal, etc. De hecho, en el art. 87 LOPDGDD se reconoce a los trabajadores el derecho a la protección de su intimidad en el uso de medios digitales en el trabajo, al mismo tiempo, en este mismo precepto se reconoce al empleador la posibilidad de acceder a los contenidos derivados del uso de medios digitales puestos a disposición del trabajador. Sin embargo, el empleador solo puede revisar el contenido derivado del uso de estos medios digitales con la sola finalidad de controlar el cumplimiento de las obligaciones laborales, estableciendo con carácter previo un conjunto de reglas y criterios de utilización de los medios digitales garantizando en todo caso una mínima protección del derecho a la intimidad.

Ahora bien, el empresario al implementar medidas de control del ordenador y del acceso a internet ha de respetar un juicio de proporcionalidad. Así, por ejemplo, en la STSJ de la Comunidad Valencia núm. 3390/2018 de 19 de noviembre, se concluye que

⁴⁶ PAZOS PÉREZ, A., “La utilización de internet en el ámbito laboral y el control empresarial en MELLA MÉNDEZ, L. y NÚÑEZ-CORTÉS CONTRERAS, P., *Nuevas Tecnologías y Nuevas Maneras de Trabajar. Estudios desde el derecho español y comparado*, Dykinson, Madrid, 2017, págs. 197-214.

la medida de control implementada por el empleador no es proporcional, concretamente se instala un programa espía con el fin de monitorizar y controlar el uso que hacen los trabajadores los medios informáticos. Esta medida de control provoca una vulneración al derecho a la intimidad personal, dado que no supera el triple juicio de idoneidad, necesidad y proporcionalidad, ya que entre otras razones la medida no es proporcional con el fin pretendido por el empleador, que es la defensa y protección del patrimonio empresarial, pues dicho fin puede ser igualmente garantizado con el uso de otras medidas de control, que presenten un carácter menos invasivo de la privacidad del trabajador. Asimismo, la empresa demandada al instalar el programa espía no cumplió con las garantías y condiciones previamente estipuladas en el protocolo de uso de medios informáticos que había sido firmado por ambas partes. En el mentado protocolo se establecían entre otras previsiones el derecho a revisar el uso del ordenador y, dicha revisión, debía efectuarse en presencia del trabajador afectado y de su representante. Sin embargo, el empleador no cumplió con esta previsión, ya que el programa espía que instaló para la monitorización del acceso a internet y del uso del correo y los sistemas informáticos, era un programa que resultaba inadvertido para sus usuarios.⁴⁷ De lo anteriormente expuesto se infiere que, para poder efectuar un control de la prestación laboral a través de medios informáticos, es necesario que el empresario tenga una finalidad específica y legítima, debiéndose ceñir a la misma estrictamente y, además, debe plantearse la posibilidad de utilizar otras medidas de control que susciten una intrusión menor en la esfera privada de los trabajadores.

5.1. USO DEL CORREO ELECTRÓNICO EN EL ÁMBITO LABORAL

Como se ha ido indicando en líneas anteriores, una de las modalidades de control existentes en el ámbito laboral, es el control de los medios informáticos puestos a disposición del trabajador, dichos medios informáticos son herramientas de trabajo que suelen ser propiedad del empleador y, por lo tanto, ha de ser el empresario quien establezca las condiciones de uso de estas herramientas de trabajo. La utilización de los medios digitales como medios de producción permite facilitar el ejercicio de la prestación laboral. Uno de estos medios de producción más utilizados en el ámbito laboral es el ordenador y el acceso a internet y, por consiguiente, el correo electrónico: una

⁴⁷ STSJ de Comunidad Valenciana (Sección 1ª) núm. 3390/2018, de 19 de noviembre, FJ 2.

herramienta que permite a sus usuarios enviar y recibir mensajes, dichos mensajes pueden consistir tanto en mensajes de texto, como archivos y documentos adjuntos.

La particularidad de este medio de comunicación reside en que los sistemas de correo electrónico permiten almacenar información, es decir, son sistemas de comunicación que utilizan un servidor de correo intermediario que se encarga de almacenar los mensajes de forma temporal antes de que estos sean enviados a sus receptores. Es por ello, que la supervisión y control de este medio de comunicación puede producir una afectación más intensa en algunos de los derechos fundamentales del trabajador, concretamente, pueden resultar conculcados el derecho a la intimidad personal, el derecho al secreto de las comunicaciones, así como la libertad de expresión⁴⁸.

En lo que respecta al derecho a la intimidad personal y el uso del correo electrónico, el TC ha considerado que *“el uso del correo electrónico por los trabajadores en el ámbito laboral queda dentro del ámbito de protección del derecho a la intimidad”* a lo que ha añadido que *“el cúmulo de información que se almacena por su titular en un ordenador personal -entre otros datos sobre su vida privada y profesional- forma parte del ámbito de la intimidad constitucionalmente protegido; también que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado el derecho a la intimidad personal, en la medida en que estos correos escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado”*⁴⁹. Además, hay que señalar que el derecho a la intimidad personal que se haya constitucionalmente protegido en el art 18.1 CE, es uno de los derechos que más inciden el poder de dirección y control que ostenta el empresario y, es por esta razón, que ha adquirido un fuerte reconocimiento en la jurisprudencia constitucional a diferencia de lo que ocurre con el derecho al secreto de las comunicaciones que no goza de una normativa específica que se encargue de desarrollarlo, ni tan poco ha sido tan examinado por el TC.

Como ya hemos señalado anteriormente, dentro del control ejercido por el empleador sobre los medios informáticos tienen especial importancia el derecho a la

⁴⁸ ROIG BATALLA, A., GALA DURÁN, C., MARTINEZ FONS, D. y MUÑOZ LORENTE, J., “El uso laboral y sindical del correo electrónico e Internet en la empresa, aspectos constitucionales, penales y laborales”, Tirant Lo Blanch, Valencia, 2007 pág. 63.

⁴⁹ STC 173/2011, de 7 de noviembre, FFJJ 3 y 5.

intimidad personal y el derecho al secreto de las comunicaciones del trabajador. Sin embargo, en la navegación por internet adquiere un mayor protagonismo el derecho a la intimidad personal, mientras que cuando nos referimos al correo electrónico como herramienta de trabajo, es el derecho al secreto de las comunicaciones el que mayor incidencia presenta y el que mayor grado de limitación suscita al conciliarse con el poder de control empresarial sin negar con ello la incidencia del derecho a la intimidad personal en esta área.⁵⁰

Asimismo, respecto a los equipos informáticos y al correo electrónico utilizados como herramientas de trabajo y puestos a disposición del trabajador, se ha de distinguir entre un uso laboral y un uso extralaboral de los referidos medios, lo cual puede traer consigo multitud de problemas. En particular, los problemas se plantean cuando el empresario no fija unas reglas de utilización de tales medios o cuando no establece una prohibición expresa del uso particular del ordenador y del correo electrónico, ya que en el caso de que el empleador haya establecido una prohibición clara y absoluta del uso extralaboral de estos medios, entonces dicho uso no tendrá cabida, y no solo eso, sino que además, el trabajador no podrá alegar que el control ejercido por el empleador produce una afectación en su derecho a la intimidad personal y al secreto de las comunicaciones, dado que en ese caso no existe expectativa de privacidad. En definitiva, el empleador dispone de un poder fiscalizador de los medios digitales, el cual encuentra su fundamento legal en el art 20.3 LET. Dicha facultad fiscalizadora podrá modularse, siendo más o menos intensa en función de cómo hayan sido diseñadas las instrucciones y reglas de uso de los medios tecnológicos puestos a disposición del trabajador, aun cuando a partir de esos dispositivos tecnológicos, se hayan atribuido al trabajador espacios individualizados o personalizados, tales como cuentas personales de correo electrónico, es decir, tales espacios pueden ser igualmente objeto de control en función de las circunstancias y de las reglas y condiciones de uso previamente elaboradas por la empresa. Se trata, por tanto, de evitar que la empresa se vea privada de la posibilidad de ejercer sus poderes de dirección y control de la actividad empresarial, así como de evitar que esta se vea expuesta o inmersa en la situación de tener que asumir cualquier tipo de uso, incluso usos

⁵⁰ ROIG BATALLA, A, GALA DURÁN, C., MARTÍNEZ FONTS, D. y MUÑOZ LLORENTE, J., “El uso laboral y sindical del correo electrónico e Internet en la empresa, aspectos constitucionales, penales y laborales”, Tirant Lo Blanch, Valencia, 2007, págs. 64-66.

inadecuados que no deberían de ser tolerados en las herramientas tecnológicas que son de su propiedad y puestas a disposición de las personas trabajadoras.⁵¹

En este sentido, resulta relevante la STS 119/2018, de 8 de febrero de 2018, caso en el cual el TS se pronuncia sobre el control empresarial efectuado en los medios tecnológicos de la empresa. Control que se efectúa por un hallazgo casual que aportó a la empresa indicios de que uno de los empleados estaba cometiendo irregularidades al aceptar transferencias de entidades proveedoras de la empresa; hecho que estaba expresamente prohibido en el Código de Conducta de la empresa y que determinó el control posterior efectuado sobre el ordenador de la persona trabajadora.

La empresa tenía diseñada una política de uso de los medios informáticos y cada vez que uno de los empleados accedía al ordenador y, en consecuencia, al sistema informático de la empresa, debía de aceptar de forma previa al acceso una política de uso en la que se aportaban las directrices de uso de los medios digitales, mediando una prohibición expresa de uso de las herramientas de trabajo para fines extralaborales. Es por ello, que tras el hallazgo casual de dos resguardos o facturas en las que constaba las transferencias efectuadas a favor de la persona trabajadora, se inicia un control sobre el contenido de ciertos correos del actor, control que no fue genérico e indiscriminado, sino que se ciñó a lo estrictamente necesario, utilizando para ello palabras clave que permitieran encontrar información relevante para la investigación, a lo que hay que añadir que el control no se aplicó a ninguna cuenta privada del actor.

Además, la existencia de un hallazgo casual excluye la aplicación de la doctrina del “fruto del árbol envenenado”, en función de la cual el juez tiene vedada la posibilidad de valorar no solo las pruebas obtenidas vulnerando derechos fundamentales, sino también las pruebas que emanen de aquellas. Asimismo, la clara y previa prohibición de utilización de los medios digitales de la empresa para fines personales, excluye de manera contundente la posible expectativa de privacidad, de manera que *“si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque al no existir una situación de tolerancia del uso personal,*

⁵¹ STC 241/2012, de 17 de diciembre, FJ 5.

tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo”⁵² En definitiva, la Sala concluye en base a todas estas consideraciones, que la medida de control es válida, ya que no existe ninguna expectativa razonable de privacidad y, además, la misma supera el triple juicio de proporcionalidad, así como los requisitos exigidos por la jurisprudencia constitucional.⁵³

Dejando a un lado lo anterior, la problemática que se plantea en el uso de los medios informáticos para fines ajenos a la actividad laboral, surge cuando no existe ningún tipo de prohibición, ni tampoco se ha establecido un protocolo de uso de los medios informáticos de comunicación, pues si nos encontramos en esta concreta coyuntura, se crea una expectativa razonable de privacidad y, por lo tanto, el trabajador se verá amparado y podrá exigir la protección a su derecho a la intimidad personal; protección que podrá exigir no solo cuando el uso particular del ordenador sea esporádico, sino también cuando dicha herramienta de trabajo se utilice con fines particulares de forma poco moderada y, es precisamente aquí donde surge el problema, ya que el destino personal de tales medios no solo supone un gasto de tiempo y una reducción de la productividad en el trabajador, sino que además genera un coste adicional para la empresa, ya que el uso particular del ordenador puede provocar un daño en los equipos informáticos de la empresa o incluso puede provocar que estos se vean infectados por un virus informático⁵⁴. Además, hay que señalar que existe “*un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores*”, y como ya se ha señalado anteriormente, en un clima de tolerancia del uso personal del ordenador y del correo, se crea una expectativa de privacidad en esos usos, sin embargo dicha expectativa no obstruye el eventual control que pueda ejercer el empresario para poder controlar el correcto uso de los medios de producción facilitados por la empresa, así como el correcto desenvolvimiento de la prestación laboral. Si bien es cierto, el art. 4.2 e) LET reconoce a todo trabajador como derecho básico un derecho al respeto de su intimidad y a la consideración debida de su dignidad, pero el derecho a la intimidad no es un derecho absoluto y en ocasiones este derecho tendrá que ceder para poder compatibilizarse con el

⁵² STS, de 6 de octubre de 2011 (rec. 4053/2010), FJ 4.

⁵³ STS 119/2018, de 8 de febrero de 2018 FFJJ 4 y 5.

⁵⁴ MELLA MÉNDEZ, L. y NÚÑEZ-CORTÉS CONTRERAS, P., “Nuevas tecnologías y nuevas maneras de trabajar: Estudios desde el derecho español y comparado”, Dykinson, 2017.

poder de control del empresario. Además, el trabajador no puede exigir un respeto al derecho a la intimidad que le es reconocido, si utiliza los equipos informáticos y los medios de comunicación contraviniendo las instrucciones e indicaciones de uso establecidas por la empresa y actuando al margen de los controles previstos, *“por ello, lo que debe de hacer la empresa con arreglo a las exigencias de la buena fe es establecer previamente las reglas de uso de esos medios – con aplicación de las prohibiciones absolutas o parciales- e informar a los trabajadores de que va a existir un control”*⁵⁵

Dentro el ámbito del control de los medios informáticos y del correo electrónico en el centro de trabajo, es importante hacer alusión a dos importantes STEDH. Se trata de la STEDH de 12 de enero de 2016 y la STEDH de 5 de septiembre de 2017 relativas al caso Barbulescu contra Rumania. Ambas sentencias, se pronuncian sobre una posible vulneración al derecho a la vida privada garantizado en el art. 8 CEDH a causa de la adopción de una medida de control del correo electrónico utilizado en el ámbito laboral. La primera sentencia es dictada por la Sección 3ª del TEDH, en particular, el asunto versa sobre un trabajador que venía prestando sus servicios como ingeniero de ventas para la empresa demandada. El trabajador a petición de la empresa procedió a crear una cuenta de Yahoo Messenger, a través de la cual se encargaba de asesorar a sus clientes. En el año 2007, la empresa emite un comunicado advirtiendo a sus trabajadores de que las comunicaciones solo podían ser utilizadas para fines laborales. En ese mismo año, se comunica al trabajador que sus comunicaciones habían sido objeto de control. Concretamente, habían sido objeto de control las comunicaciones realizadas entre el 5 y 13 de julio. Tras la adopción de la medida, la empresa descubre que el trabajador había estado utilizando el citado medio de comunicación para fines personales, contraviniendo así las instrucciones establecidas por la empresa, en consecuencia, la empresa decide imponer al trabajador una sanción de despido.

En esta sentencia, el TEDH llega a la conclusión de que no se ha producido vulneración alguna en el derecho a la vida privada y a la correspondencia garantizado en el art. 8 CEDH y, para ello, se apoya en diversas razones, entre las mismas que el trabajador había declarado al empleador que había utilizado las comunicaciones exclusivamente para fines profesionales, por lo que en base a esta declaración, el

⁵⁵ STS 6128/2007, de 26 de septiembre de 2007, FJ 4.

empleador accedió a las comunicaciones amparándose en la existencia de un fin legítimo, pues tenía la expectativa razonable de que dichas comunicaciones solamente contenían información laboral. Asimismo, el tribunal entiende que es razonable que el empleador quiera controlar las herramientas de trabajo con el objetivo de verificar que los trabajadores estén cumpliendo con sus obligaciones y deberes laborales. Finalmente, el tribunal observa que la medida de control solamente fue utilizada para acceder a las comunicaciones de Yahoo Messenger y que no se utilizó para acceder a ningún otro documento ni información, por lo que, en este sentido, concluye que la medida es limitada y proporcionada, y que no produce ninguna vulneración al respeto a la vida privada y a la correspondencia del trabajador.⁵⁶

Por otra parte, en la segunda sentencia también relativa al asunto *Barbulescu* contra Rumania dictada por la Gran Sala, el TEDH llega a la conclusión opuesta, entendiendo que ha sido vulnerado el derecho al respeto de la vida privada y de la correspondencia del trabajador, de conformidad con lo dispuesto en el art. 8 CEDH. Para ello, el Tribunal adopta una posición más garantista en la medida en que establece mayores limitaciones al poder de control del empresario sobre los medios de comunicación utilizados en el ámbito laboral, entendiendo que no basta con una prohibición expresa del uso para fines personales del correo para que el empresario pueda proceder al control de las comunicaciones, concretamente, el Tribunal establece que han de tenerse en cuenta una serie pautas que funcionan como complemento del principio de proporcionalidad, y que han de ser tenidas en consideración para poder aplicar la medida. A este conjunto de elementos se les ha denominado “*Test Barbulescu*”, en concreto, los tribunales han comprobar que se cumplan los siguientes requisitos:

En primer lugar, tienen que verificar si se ha facilitado información al empleado sobre la posibilidad de que en la empresa se adopten medidas de control de las comunicaciones, así como sobre su posible aplicación.

En segundo lugar, ha de tenerse en cuenta la extensión de la medida, así como su grado de intrusión en la vida privada.

⁵⁶ STEDH de 12 de enero de 2016, caso *Barbulescu* contra Rumania.

En tercer lugar, los tribunales han de comprobar si el empleador ha aportado argumentos suficientes para justificar la legitimidad de la medida.

En cuarto lugar, los tribunales han de valorar si es posible adoptar otra medida más moderada, asimismo, se ha de valorar si el empresario puede alcanzar su objetivo adoptando una medida de carácter parcial, es decir, una medida que no tenga un acceso pleno y directo.

En quinto lugar, se ha de observar cuáles son las consecuencias de la medida para el trabajador afectado.

Finalmente, se ha de comprobar si se ofrecieron al trabajador afectado por la medida de control las garantías oportunas, en particular, si se le notificó sobre la posibilidad de adopción de la medida de control de forma previa a su aplicación.⁵⁷

Dejando a un lado lo anterior, respecto a las medidas de control empresarial sobre el uso de medios informáticos, concretamente sobre el uso del ordenador y del correo electrónico, es una cuestión debatida la aplicación analógica del art. 18 LET, dicho precepto recoge una serie de garantías que han de aplicarse al registro de los efectos personales y de las taquillas del trabajador. En este precepto, a fin de ejecutar un registro de los efectos personales y de las taquillas del trabajador, se exigen dos condiciones: en primer lugar, el registro ha de desarrollarse con la estricta finalidad de preservar el patrimonio empresarial y, en segundo lugar, el registro ha de llevarse a cabo en el centro de trabajo y dentro del horario laboral. Asimismo, el registro de las taquillas y de los efectos personales del trabajador ha de llevarse a cabo en presencia de un representante legal de los trabajadores y, en su ausencia, deberá efectuarse en presencia de otro trabajador siempre que ello fuese posible.

A este respecto, lo primero que hay que señalar es que no existe una opinión unánime sobre esta cuestión, de tal manera que hay autores que entienden, que pese a que un ordenador facilitado por la empresa puede contener información y datos relativos a la vida privada de la persona, el ordenador no es en sentido estricto un efecto personal,

⁵⁷ STEDH, de 5 septiembre de 2017, caso Barbulescu contra Rumania.

puesto que es una herramienta de trabajo que es propiedad del empleador y no del trabajador y, en consecuencia, no le son aplicables las garantías previstas en el art. 18 LET. Además, estos autores niegan la posibilidad de que el ordenador como herramienta de trabajo sea utilizado para fines personales, puesto que es un instrumento de trabajo y, por lo tanto, es puesto a disposición del trabajador exclusivamente para el ejercicio de la prestación laboral. Si bien es cierto, la taquilla también se trata de un bien que es propiedad de la empresa, pero se cede su uso personal al trabajador y, además, dicho uso es cedido al margen de la ejecución de la prestación laboral a diferencia del ordenador que se cede como herramienta de trabajo y para el desempeño de la prestación laboral, es por ello, que resulta razonable la modalidad de control de ambos bienes se lleve a cabo con arreglo a regímenes legales diferentes.

En este sentido, se ha pronunciado el TS que manifiesta que *“la utilización del ordenador en la empresa -aunque está personalizada- queda dentro del ámbito de poder de vigilancia del empresario y por ello el ejercicio de las correspondientes facultades de control se ampara en el art. 20 LET y no tiene las limitaciones que corresponden a la función de “policía privada” que consiente el art. 18 LET”*⁵⁸ Ello supone que para que la actuación de control sobre los dispositivos informáticos sea considerada lícita, no es necesario que dicha actuación se ejecute en presencia de terceros, tal y como impone el art 18 LET para el registro de los efectos personales y de las taquillas. Sin embargo, pese a la anterior postura, hay autores que defienden la aplicación de este mismo precepto y para ello, estos autores entienden que el ordenador ha de ser considerado un efecto personal, en la medida en que puede contener y almacenar datos relativos a la esfera privada de la persona.

Precisando aún más, podemos distinguir entre dos tipos de control que pueden efectuarse en el ámbito laboral, el primero de ellos es un control ordinario sobre los medios de producción, el cual se lleva a cabo a la luz del art. 20. LET. Dicho precepto habilita al empresario a adoptar las medidas de control que estime más oportunas para verificar el correcto desenvolvimiento de la prestación laboral, ahora bien, dicha potestad de control está supeditada al respeto de la dignidad humana. Es precisamente en este tipo de control ordinario en el que debemos encajar el acto de control de los equipos

⁵⁸ STS 594/2018, de 8 de febrero de 2018, FJ 4.

informáticos, y la razón principal, es que los equipos informáticos puestos a disposición del trabajador son propiedad de la empresa y no son efectos personales.

La segunda modalidad de control se enmarca en un poder de control empresarial que podemos calificar como extraordinario, ya que se trata de un régimen excepcional, con sus consiguientes garantías, cuyo régimen legal se haya previsto en el art. 18 LET y hace referencia a la inviolabilidad de la persona del trabajador. Atendiendo a la rúbrica del art. 18 LET, podemos observar que este poder de control no se ejercita desde la normalidad laboral, ya que en este caso no hablamos de un control de las herramientas de trabajo que han sido puestas a disposición del trabajador para el exclusivo ejercicio de la prestación laboral, sino que ahora se trata de un control que precisa mayores cautelas, puesto que se trata de controlar las taquillas y los efectos personales del trabajador. Además, a diferencia de la anterior modalidad de control empresarial amparada en el art 20.3 LET, esta facultad excepcional de control, tiene una finalidad distinta que es la protección del patrimonio empresarial, por lo que para su adopción, será necesaria la concurrencia de indicios previos de incumplimiento del trabajador y, es por ello, que ha de entenderse como un poder excepcional que queda al margen de la normalidad laboral, contractual y en consecuencia no puede ampararse en el art 20.3 LET.

6. LA GEOLOCALIZACIÓN EN EL ÁMBITO LABORAL Y EL DERECHO A LA DESCONEXIÓN DIGITAL

Las modalidades de supervisión de la prestación laboral son prácticamente ilimitadas gracias a los continuos avances tecnológicos y a su implementación en el ámbito de las relaciones laborales. De hecho, la sofisticación y el constante avance de la tecnología es cada vez mayor, de tal forma que el empresario puede servirse de las herramientas tecnológicas logrando efectuar un control de la actividad laboral no solamente dentro del centro de trabajo, sino también fuera del mismo. Ciertamente, efectuar un control de la actividad laboral fuera del centro de trabajo puede parecer complicado, y al mismo tiempo, el trabajador al no estar bajo la mirada del empleador y no sentirse continuamente vigilado por encontrarse fuera del centro de trabajo, es posible que pueda relajarse y adoptar una postura mucho más confiada, de tal modo que puede

terminar adoptando conductas irregulares bajo la falsa creencia de no estar siendo vigilado.

Precisamente, para poder efectuar un mejor seguimiento de la actividad laboral, el empleador puede hacer uso de los sistemas de geolocalización, evitando así comportamientos inadecuados por parte del empleado. Estos sistemas de geolocalización son muy variados, los más característicos son el GPS o sistema de posicionamiento global y el GMS, que es el sistema global para las comunicaciones móviles. Todas estas herramientas permiten acceder a una gran cantidad de datos resultando ser de gran utilidad para las empresas dedicadas al sector del transporte, al reparto de mercancías e incluso para las empresas dedicadas al comercio electrónico, tal y como veremos más adelante. Todo ello se debe a que los sistemas de geolocalización permiten que el empresario pueda conocer la ubicación real del trabajador, realizando así un mejor seguimiento de la prestación laboral, puesto que permiten conocer una serie de datos, tales como el itinerario del conductor, las paradas que realiza, los kilómetros que recorre, la cantidad de combustible que gasta, etc.

Así por ejemplo, una de las empresas que se ha beneficiado de este tipo de medidas de control, es la conocida empresa Amazon, una compañía estadounidense dedicada al comercio electrónico, que incorpora como medida de control empresarial una pulsera que han de colocarse los empleados; a esta ocurrencia también se la conoce como “wearable” es decir, tecnología “llevable” o “vestible”, consistente en un conjunto de aparatos y dispositivos electrónicos que son incorporados en nuestra vestimenta, en pulseras, zapatillas, todo ello a fin de controlar nuestra localización, nuestra actividad, nuestra salud, etc. Amazon, con el diseño de esta medida tan sofisticada que además vibra en el caso de que la actividad cese, lo que pretende es rastrear los movimientos de sus trabajadores para verificar si efectivamente están cumpliendo con sus obligaciones y deberes laborales y mejorar así su producción.⁵⁹ El problema que plantea el diseño de este tipo de medidas de control cada vez más perfeccionadas, es que los trabajadores están siendo sometidos a un control excesivo por parte del empleador, de manera que cada vez son más difusos los contornos entre la vida privada y la vida laboral, convirtiéndolos en

⁵⁹ RODRIGO, B., “Una pulsera de Amazon controla empleados ‘vagos’. ¿Puede usarla tu jefe en España?”. *El Confidencial*, 8 de febrero de 2018 (Disponible en https://www.elconfidencial.com/tecnologia/2018-02-08/pulsera-amazon-rastrear-ubicacion-empleados_1516056/).

trabajadores transparentes que se hayan continuamente expuestos a la atenta mirada del empleador, y no solo eso, sino que además el uso de estos dispositivos que vibran cada vez que el trabajo es desatendido y que controlan si el trabajador hace algo mal, hacen ver a los trabajadores como máquinas, en la medida en que estos se encuentran expuestos a una carga de trabajo desmesurada.

No obstante, el uso de pulseras como dispositivo de control no es lo habitual. De hecho, dentro del uso de la geolocalización, lo más usual es que el empleador utilice el propio vehículo de empresa e instale el dispositivo de geolocalización o GPS en el mismo. Sin embargo, existen otras posibilidades, ya que estos mecanismos de control pueden estar incorporados en otras herramientas de trabajo facilitadas al empleado por la empresa, como pueden ser los dispositivos móviles, los ordenadores o las tabletas, asimismo, puede darse la situación en la que sea el empresario el que solicite al trabajador que aporte un teléfono móvil de su propiedad y encargarle la implantación de un sistema de geolocalización. Así sucede en el caso enjuiciado en la SAN núm. 13/2019, de 6 de febrero de 2019, en el que una empresa decide imponer a los trabajadores en su contrato de trabajo una cláusula contractual en virtud de la cual los trabajadores se obligan a aportar un Smartphone con capacidad suficiente para poder instalar una aplicación diseñada por la empresa. No obstante, sobre esta cuestión se ha de indicar que el empresario ha de instalar los dispositivos de control de la actividad laboral en las herramientas de trabajo que sean propiedad de la empresa, de forma que los trabajadores no se vean obligados a facilitar sus efectos personales como instrumentos de control.⁶⁰ Asimismo, en esta sentencia se determinó que la medida de control empleada por el empleador era excesiva y se resolvió la cuestión aplicando el conocido principio de proporcionalidad, en función del cual, para que la medida de control empresarial sea calificada como válida y legítima, es necesario que supere las tres exigencias siguientes: en primer lugar, es necesario que la medida sea idónea o lo que es lo mismo, que la medida resulte apta para cumplir el objetivo perseguido por el empleador; en segundo lugar, se ha de comprobar si la medida es necesaria, es decir, se ha de analizar si no existe otra medida menos intrusiva e igualmente válida para cumplir el objetivo propuesto; finalmente, se ha de analizar si la medida es proporcional en sentido estricto, esto es que la medida resulte ponderada por derivarse de ella más beneficios que perjuicios.

⁶⁰ REYES HERREROS, J. y ALCAIDE, L., “Geolocalización de trabajadores”, *Actualidad Jurídica Uría Menéndez*, núm. 52, 2019, pág. 74.

Una vez visto el funcionamiento del principio de proporcionalidad, se ha de concretar que, en la citada sentencia, la Audiencia Nacional termina concluyendo que la medida de control no es válida, y, para ello, principalmente se centra en la segunda exigencia del citado principio de proporcionalidad, declarando finalmente que la medida es desproporcionada, ya que el empleador podía haber utilizado otra medida más moderada e igualmente apta para cumplir el propósito propuesto, así por ejemplo, el empleador podía haber optado por instalar el sistema de geolocalización en un medio propiedad de la empresa, como lo son por ejemplo las motocicletas en las que eran transportados los pedidos, lo cual supondría una menor intrusión al derecho a la intimidad personal del trabajador afectado, en el sentido de que la intromisión en el derecho a la intimidad es mayor cuando el sistema de geolocalización es instalado en un teléfono móvil, ya que el trabajador al llevar siempre consigo el teléfono móvil está siendo objeto de un control constante, y más aún, cuando el objeto de control es un teléfono móvil particular, en la medida en que el trabajador puede seguir haciendo uso del mismo fuera de la jornada laboral y, por lo tanto, puede seguir siendo objeto de control durante ese lapso de tiempo si no se le advierte de que ha de desactivarlo, mientras que, si la implantación de la medida de control se realiza en el vehículo propiedad de la empresa, el trabajador solamente es controlado mientras se encuentre dentro del vehículo y esté haciendo uso del mismo, por lo que en este último supuesto la injerencia en el derecho a la intimidad personal es menor y, por lo tanto, la medida es mucho más moderada e igualmente eficaz para cumplir con la finalidad propuesta.⁶¹

Ahora bien, esta concreta facultad de control que estamos analizando y que permite al empresario conocer la localización del trabajador, como toda gran potestad ha de estar sometida al cumplimiento de unas garantías y limitaciones para que finalmente la medida sea considerada legítima. En primer lugar, y como ya se ha indicado en líneas anteriores, lo más razonable es que el empleador instale estos mecanismos de control en los propios medios de producción y en las herramientas de trabajo que sean propiedad de la empresa, de forma que el trabajador no se vea obligado a tener que aportar sus efectos personales para que puedan ser utilizados como instrumento de control.

⁶¹ SAN núm. 13/2019, de 6 de febrero de 2019, FFJJ 5 y 6.

En segundo lugar, otra de las limitaciones al uso de la geolocalización como herramienta de control se extrae del art. 90.1 LOPDGDD, del cual se deduce que esta concreta modalidad de control empresarial se engloba dentro de la facultad ordinaria de vigilancia y control que ostenta el empresario y que se encuentra regulada en el art. 20.3 ET, por lo tanto, de ello se desprende que otra de las garantías que han de cumplirse y, que a su vez funciona como límite aplicable a esta modalidad de control, es la misma limitación que se prevé para el poder de vigilancia y control del empresario, esto es, el respeto a la dignidad del trabajador en el ejercicio de la prestación laboral y, además, al suponer esta medida de control una limitación en los derechos fundamentales del trabajador también será necesario que se haga una ponderación de los bienes jurídicos concurrentes, lo cual se efectuará verificando si se ha respetado el juicio de proporcionalidad.

En tercer lugar, otra de las garantías que se exigen al empleador en el uso de sistemas de geolocalización es el cumplimiento del deber de información, en función del cual, los empleadores con carácter previo deberán informar de forma expresa, clara e inequívoca a los trabajadores y, en su caso, a los representantes tanto sobre la implementación como sobre las características de estos mecanismos tecnológicos de control.⁶² En este sentido, es importante indicar lo que la doctrina judicial ha venido entendiendo respecto al incumplimiento del deber de información previa, la cual ha venido apreciando que la omisión en el cumplimiento del deber de información empresarial sobre la implantación de un sistema de control a través de la geolocalización, determina, en todo caso, que la medida sea considerada nula por ser contraria a los derechos a la intimidad personal y a la protección de datos de carácter personal de la persona afectada.⁶³

Asimismo, para que la medida de control a través de dispositivos de geolocalización sea calificada como válida y legítima es necesario que tal mecanismo de control responda a una concreta finalidad, que normalmente será el cumplimiento de un

⁶² SERRANO GARCÍA, J. M., “Límites de la ley de protección de datos al poder de dirección del empresario”, Bormazo, 2019, pág. 45.

⁶³ LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., “Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral”, en AA.VV. MONREAL BRINGSVAERD, E., THIBAUT ARANDA, X, y JURADO SEGOVIA, A. “Derecho del trabajo y nuevas tecnologías”, Tirant Lo Blanch, Valencia, 2020, págs. 419 y ss.

interés empresarial. En particular, el uso de estos mecanismos de control ha de estar enfocado a la fiscalización del cumplimiento por parte del trabajador de las obligaciones y deberes laborales dimanantes del contrato de trabajo, por lo que ha de responder a criterios puramente profesionales y nunca a motivos caprichosos y arbitrarios.

En relación con lo anterior, para poder asegurar que la medida responde a criterios estrictamente profesionales, será necesario que la implantación de la medida se produzca exclusivamente durante la jornada laboral y no fuera de la misma, cuestión sobre la que se pronuncia la STSJ de Madrid (Sala de lo Social, Sección 5ª), núm. 739/2014 de 29 de septiembre, que determina la ilicitud de la prueba practicada por la empresa demandada al suponer una vulneración al derecho a la intimidad personal del art. 18.1 CE. Concretamente, la prueba consistía en un seguimiento de la actividad de la demandante a través de la incorporación de un sistema de geolocalización en el vehículo de la empresa que había sido cedido a la trabajadora para fines estrictamente laborales y, además, tenía que estar en todo momento bajo su custodia y cuidado. En concreto, el control efectuado comportaba la posibilidad de conocer en todo momento, incluso fuera de la jornada laboral el lugar en el que se encontraba la demandante, mediante un sistema de geolocalización que permite un continuo y permanente seguimiento del vehículo durante su uso, no solo el posicionamiento de este por razones de seguridad, sino también el lugar exacto en donde se hallaba el trabajador.⁶⁴

En esta misma línea, se pronuncia la STSJ de Castilla- La Mancha núm. 715/2014 de 10 de junio. En este supuesto, la empresa pone a disposición del actor un teléfono móvil en el que se había instalado un dispositivo GPS a fin de realizar un mejor seguimiento de la actividad del trabajador. El problema radica en que el seguimiento de la actividad del trabajador se efectuaba tanto durante las horas de trabajo, como fuera de las mismas y, todo ello, sin conocimiento del afectado por la medida, por lo que finalmente se determina que el control de la actividad del trabajador en todo momento e incluso fuera de la jornada laboral y sin conocimiento de este, constituye una clara intromisión en el derecho a la intimidad personal.⁶⁵ Además, con respecto a lo anteriormente expuesto, en virtud del art. 20.3 LET el ejercicio de las facultades de control empresariales ha de estar constreñido a la verificación del cumplimiento de las

⁶⁴ STSJ de Madrid (Sección 5ª) núm. 739/2014, de 29 de septiembre, FJ 4.

⁶⁵ STSJ de Castilla- La Mancha núm. 715/2014, de 10 de junio FFJJ 3 y 4.

obligaciones laborales, por lo que parece razonable que el uso de mecanismos de control a través de dispositivos de geolocalización ha de limitarse únicamente a controlar la actuación del trabajador durante las horas de trabajo, puesto que es precisamente ese el intervalo de tiempo en el que el trabajador efectúa sus obligaciones y deberes laborales, de forma que un control que se efectúa fuera de la jornada laboral, no solo es excesivo y carente de sentido, sino que además supone una clara intromisión en el derecho reconocido en el art. 18.1 CE.

Así, por el contrario, la STS núm. 766/2020, de 15 de septiembre, se pronuncia en sentido opuesto, considerando válida la medida de control consistente en un sistema de geolocalización, pese a que dicha medida se extiende fuera de la jornada laboral. En particular, el TS se pronuncia declarando procedente el despido que es interpuesto contra una trabajadora que estaba siendo objeto de control a través de un sistema de geolocalización incorporado en el vehículo de empresa. La empresa antes de proceder a la adopción de la medida de control cumple con el deber de información previa, facilitándole a la trabajadora un documento en el que se indicaban las instrucciones de uso del vehículo de la empresa y en el que se la informaba de que dicho vehículo tenía incorporado un sistema de localización por GPS. Dentro de la información que le es aportada a la trabajadora, se impone la obligación de utilización del vehículo para fines exclusivamente laborales y, en consecuencia, dicho vehículo debía ser utilizado por la trabajadora solamente dentro de la jornada laboral, debiendo asumir la persona trabajadora la responsabilidad por el estado de este.

Pese a la obligación de uso del vehículo para fines estrictamente profesionales, la persona trabajadora contraviene las instrucciones facilitadas por la empresa, utilizando el vehículo durante un periodo en el que se encontraba de baja médica, de forma intensa y continuada para fines ajenos a la actividad laboral, fuera de la jornada laboral y excediendo la velocidad máxima permitida. En concreto, el TS se plantea si se ha suscitado una intromisión en el derecho a la intimidad personal y el derecho a la protección de datos de la actora, llegándose a la conclusión de que no se ha producido vulneración alguna en sendos derechos. Respecto al derecho a la intimidad de la actora, el TS determina que la trabajadora no tenía ninguna expectativa de intimidad, dado que se la había prohibido previamente el uso del vehículo para fines particulares, así como su uso fuera de la jornada laboral. Además, el uso personal de los medios de trabajo,

existiendo una prohibición expresa al respecto, se considera ilícito y no se puede exigir al empresario que tolere dicha situación y que se abstenga de controlar los posibles usos inadecuados del vehículo empresarial. Tampoco se plantea intromisión alguna en el derecho a la protección de datos, puesto que los datos que son aportados mediante la medida de localización del vehículo no reflejan ningún dato íntimo de la trabajadora, sino que meramente reflejan datos de movimiento del vehículo fuera de los periodos permitidos, afectando únicamente a la ubicación y movimientos del vehículo.

También es de sumo interés uno de los puntos controvertidos que se plantean en este supuesto. Concretamente, el TS se pronuncia sobre si la medida de control se excede de la finalidad pretendida por el empleador, que es garantizar la seguridad del vehículo y la coordinación del trabajo. Verificar si se ha producido dicho exceso es importante a efectos de considerar que se ha producido una intromisión en la esfera personal de la trabajadora. A este respecto, hay que indicar que la empresa es responsable de garantizar la seguridad del vehículo, así como de la responsabilidad civil ante un quebranto de la misma, se trata, por tanto, de obligaciones propias de la empresa como titular del vehículo, no pudiéndose pretender que la empresa no utilice los datos del GPS fuera de la jornada laboral y, menos aún, ante una prohibición expresa de uso del vehículo durante este intervalo de tiempo, ya que esto supondría ubicar a la empresa ante un situación de riesgo y de oscuridad por el mal uso que haga la trabajadora del vehículo del que la empresa es titular.⁶⁶

Por otra parte, otra de las limitaciones que inciden en el uso de dispositivos GPS como medida de control de la actividad laboral, la podemos extraer de los arts. 4, 20.3 y 20 bis de la Ley del Estatuto de los Trabajadores, de los cuales, se desprende que los derechos fundamentales también se configuran como un límite a las facultades de control de las que dispone el empresario, debiendo de matizarse que, fundamentalmente, los derechos del trabajador que pueden ser conculcados con la utilización de dispositivos de geolocalización en el ámbito laboral, son el derecho a la intimidad personal del art.18.1 CE y el derecho a la protección de datos de carácter personal reconocido en el art. 18.4 CE. A este respecto, conviene hacer algunas precisiones; por una parte, el uso de estos mecanismos de control afecta a una vertiente específica del derecho a la intimidad: “*el*

⁶⁶ STS 766/2020, de 15 de septiembre, FFJJ 1 y 2.

*derecho a que los demás no sepan dónde está en cada momento y cuáles son sus movimientos; o dicho, en otros términos, el derecho a no estar localizado de manera continua por medios electrónicos colocados en sus bienes”.*⁶⁷

Además del derecho a la protección de datos, con la utilización de dispositivos de geolocalización se puede afectar al derecho a la intimidad, puesto que estos mecanismos de control permiten tener acceso a datos relativos a la esfera privada de la persona, pues permiten conocer los lugares que frecuenta una persona, sus hábitos, las personas con las que se relaciona, etc.⁶⁸ Por otra parte, respecto al derecho a la protección de datos de carácter personal y a su posible vulneración, se ha considerado que la localización de una persona es un dato de carácter personal, así se prevé en el art. 4.1 del Reglamento 679/2016 del Parlamento Europeo y del Consejo de 27 de abril de 2016.⁶⁹

Por último y a modo de cierre, interesa hablar de otra de las utilidades que ofrecen los dispositivos de geolocalización. Como podemos ver en líneas anteriores, lo más frecuente es que el empresario se sirva de la geolocalización para controlar la localización del trabajador, y así, comprobar si efectivamente está cumpliendo con sus obligaciones laborales. Sin embargo, los sistemas de geolocalización pueden ofrecer una utilidad adicional pudiendo ser utilizados como sistema de control horario. Ahora bien, esta herramienta de control de la jornada laboral solamente es válida si la jornada laboral se lleva a cabo entre la conexión y la desconexión del dispositivo de geolocalización.

En este sentido, se pronuncia el TS en un auto dictado el 16 de julio de 2019. En el asunto enjuiciado, la empresa utiliza como sistema de registro de la jornada laboral el dispositivo GPS instalado en el vehículo de la empresa, computándose como tiempo de trabajo el tiempo que transcurre entre la activación y desactivación del dispositivo GPS. Sin embargo, se acaba determinando que el dispositivo de control no se ajusta a la legalidad vigente, porque, por un lado, no resulta garantista al ser susceptible de sufrir alteraciones por parte de la empresa, y, por otro lado, este dispositivo de fichaje no se ajustaba a la jornada laboral efectivamente realizada por los empleados, ya que solamente computaba una parte de esta, concretamente la que era desarrollada en el vehículo,

⁶⁷ STSJ País Vasco, de 10 de mayo de 2011 (rec. 644/2011), FJ 5 C.

⁶⁸ REYES HERREROS, J. y ALCAIDE, L., “Geolocalización de trabajadores”, *Actualidad Jurídica Uribe Menéndez*, pág. 73.

⁶⁹ SAN 13/2019, de 6 de febrero de 2019, FJ 6.

mientras que la parte de la jornada laboral que era desarrollada fuera del vehículo quedaba fuera del cómputo. Por lo tanto, existía una parte de la jornada laboral que no era registrada por el GPS y durante la cual los trabajadores desarrollaban otras tareas que tenían lugar fuera del vehículo, tales como la revisión del extintor, consultas de seguros y otros trámites administrativos. A lo anterior, hay que añadir que la empresa no corregía diariamente la jornada laboral de cada uno de los trabajadores, por lo que este mecanismo de registro de la jornada laboral no resulta un medio lícito, dado que únicamente computa el tiempo de trabajo desarrollado en el vehículo, quedando excluida una parte de la jornada en la que los trabajadores se encargaban de acudir a las oficinas de la empresa y de realizar diversas gestiones, también consideradas como tiempo de trabajo efectivo y que tenían lugar antes de que los trabajadores accedieran al vehículo de la empresa y tras abandonar el mismo.⁷⁰

6.1. EL TELETRABAJO

Ciertamente los avances tecnológicos traen consigo multitud de ventajas en el ámbito de las relaciones laborales mejorando la productividad y eficiencia del trabajador y permitiendo al empresario efectuar un mejor control de la actividad laboral. De igual manera, la incorporación de la tecnología en el ámbito laboral conlleva que la actividad laboral pueda desarrollarse no solo en cualquier momento, sino también en cualquier lugar e incluso fuera del centro de trabajo. Esta posibilidad que tiene el empleador nos lleva a hablar de tres modalidades de prestación laboral muy particulares: el trabajo a distancia, el trabajo a domicilio y el teletrabajo. En este sentido, es importante matizar que, aunque son conceptos que presentan características comunes, en realidad son conceptos diferentes.

Lo primero que ha de añadirse es que el trabajo a distancia es una categoría en la que se integra como subespecie el teletrabajo, de hecho, el trabajo a distancia es una modalidad de prestación laboral, cuya realización se produce fuera de las instalaciones de la empresa, mientras que el teletrabajo se realiza fuera del centro de trabajo, pero implica la prestación de los servicios laborales con el uso de las TICs.

⁷⁰ LÓPEZ CUMBRE, L., “GPS como sistema de control de jornada: sólo si la prestación laboral se desarrolla entre la conexión y la desconexión” (www.gomezacebo-pombo.com, septiembre de 2019).

Con respecto al teletrabajo, el Acuerdo Marco Europeo sobre teletrabajo firmado en el año 2002, define el teletrabajo como una forma de organización o de realización del trabajo utilizando las tecnologías de la información, en el marco de un contrato o de una relación laboral en la que un trabajo que también habría podido ejecutarse en los locales de la empresa, se ejecuta habitualmente fuera de ellos.

Por otra parte, el trabajo a distancia es aquel que se desarrolla fuera de los establecimientos y centros habituales de la empresa, pudiendo desarrollarse en el propio domicilio del trabajador (trabajo a domicilio) o en otro lugar libremente designado por este y que no sea el domicilio del trabajador (trabajo a distancia). Por su parte, el texto refundido del Estatuto de los Trabajadores de 1980 definía en su art. 13 el trabajo a domicilio, como aquel en el que la prestación de la actividad laboral es realizada en el domicilio del trabajador o en un lugar libremente elegido por este y sin vigilancia del empresario. En el año 2012, se introduce una modificación en el art. 13 que sustituye en su redacción el trabajo a domicilio por el trabajo a distancia, considerando que el trabajo a distancia es aquella prestación laboral que es realizada de manera preponderante en el domicilio del trabajador o en un lugar libremente elegido por este de modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa. El propósito de esta reforma que sustituyó el trabajo a domicilio por el trabajo a distancia era precisamente, según la exposición de motivos, dar acogida al teletrabajo, esto es el trabajo a distancia basado en el uso intensivo de las nuevas tecnologías.

De la nueva regulación en la que se suprime la referencia expresa a la ausencia de vigilancia del empleador, se puede deducir que la vigilancia por parte del empleador está presente en las tres modalidades, solo que esta vigilancia será más o menos intensa en función de la forma de organización de la actividad laboral en la que nos situemos, de modo que, si hablamos del teletrabajo, la vigilancia será mucho más intensa e invasiva gracias a los propios medios telemáticos que hacen posible un mayor control de la actividad laboral, que en el trabajo a distancia o a domicilio en los que la ausencia de tales medios técnicos hace que el control sea menos intenso.⁷¹

⁷¹ LÓPEZ CUMBRE, L., “Teletrabajo, trabajo a distancia y trabajo a domicilio” (www.ga-p.com, junio de 2020).

Dentro del ámbito de la digitalización y los derechos laborales nos interesa mucho más ahondar en la figura del teletrabajo consistente en un nuevo modelo de prestación laboral que supone una ruptura con el modelo tradicional de trabajo, además, es una forma de prestación laboral que actualmente se encuentra muy a la orden del día, no solo debido a la irrupción de las TICs en el ámbito laboral, sino también, debido a la crisis generada por el COVID-19, que ha impulsado el recurso al teletrabajo de manera importante, de forma que esta forma tan particular de organización de la actividad laboral ha dejado de ser una alternativa para resultar ser una medida imprescindible a fin de asegurar el distanciamiento físico y evitar así la propagación del coronavirus.⁷² De hecho, según los datos proporcionados por el INE durante el estado de alarma decretado en España el 14 de marzo de 2020, cerca de un 48,8 % de los establecimientos hicieron uso de esta concreta modalidad de prestación laboral.

Cabe señalar que el teletrabajo es una modalidad de prestación laboral que ofrece ventajas e inconvenientes para ambas partes del contrato de trabajo. Desde la óptica del empresario, el recurso al teletrabajo supone una notable reducción de los gastos en infraestructura, también supone una reducción de la siniestralidad laboral, así como una mejora de la productividad de los empleados, logrando a través del teletrabajo una mejor gestión del tiempo dedicado a la prestación de los servicios laborales. Por otro lado, desde el punto de vista del trabajador, el recurso al teletrabajo supone grandes ventajas, como son la reducción del tiempo empleado en el desplazamiento, el ahorro en los gastos asociados al desplazamiento, tales como el combustible, los gastos empleados en el vehículo, en el caso de que se trate de un vehículo propio y los gastos destinados al mantenimiento de este. Además, el teletrabajo también otorga mayor flexibilidad horaria y una mejor conciliación de la vida laboral y personal del trabajador, aunque al mismo tiempo, el recurso al teletrabajo también puede complicar la conciliación de la vida profesional con la vida personal del trabajador, ya que en ocasiones los trabajadores no disponen de un espacio adecuado y habilitado para desempeñar la actividad laboral y no tienen otra alternativa que realizar la prestación laboral desde el salón o desde un espacio común transitado por sus familiares.⁷³

⁷² LÓPEZ CUMBRE, L., “Efectos laborales del coronavirus (II): antes inviable, ahora imprescindible; el teletrabajo como medida de “distanciamiento físico” (www.ga-p.com, marzo de 2020).

⁷³ SALA FRANCO, T., TODOLÍ SIGNES, A. y MARTÍN-POZUELO LÓPEZ, A. “El teletrabajo”, Tirant Lo Blanch, Valencia, 2020, págs. 27-34.

En esta misma línea, si acudimos al art. 34.8 LET podemos ver que se reconoce a la persona trabajadora el derecho a solicitar las adaptaciones de la duración y distribución de la jornada, en la ordenación del tiempo de trabajo y en la forma de prestación, incluida la prestación de su trabajo a distancia, para hacer efectivo su derecho a la conciliación de la vida familiar y laboral. Seguidamente, el precepto añade que dichas adaptaciones han de ser razonables y proporcionadas en relación con las necesidades de la persona trabajadora y las necesidades organizativas de la empresa. Asimismo, se prevé la posibilidad de solicitar la adaptación de la jornada en los términos mencionados anteriormente para el supuesto en el cual la persona trabajadora tenga hijos, siempre y cuando estos sean menores de doce años.

Si bien es cierto, si tenemos en cuenta que la nueva Ley del Teletrabajo reconoce la voluntariedad como una de las notas caracterizadoras del teletrabajo, entonces podemos pensar que dicha voluntariedad predicable del teletrabajo no resulta compatible con el derecho reconocido a la persona trabajadora en el art 34.8 LET. Sin embargo, la nueva ley es previsoras en este sentido y en el art. 5 de la misma proclama la voluntariedad del teletrabajo para ambas partes y, al mismo tiempo, establece que todo ello ha de ser entendido sin perjuicio del derecho al trabajo a distancia que puedan reconocer la legislación o la negociación colectiva.⁷⁴

En lo que respecta al teletrabajo, el principal problema con el que nos encontramos es que hasta la reciente promulgación del Real Decreto-Ley 28/2020, de 22 de septiembre, de trabajo a distancia, disponíamos de un marco normativo insuficiente. Concretamente, el marco legal existente hasta la actual regulación del teletrabajo era el siguiente: contábamos con la Ley 3/2012, de 6 de julio, de medidas urgentes que en la reforma del mercado laboral se encarga de modificar la regulación tradicional del trabajo a domicilio a fin de dar acogida al trabajo a distancia basado en el uso intensivo de nuevas tecnologías, de forma que se optó por incluir el teletrabajo como una subespecie de trabajo a distancia, el cual se encuentra regulado en el art. 13 LET que lleva por rúbrica “*trabajo a distancia*”. Según este precepto, se entiende que el trabajo a distancia es una actividad laboral que se realiza de forma preponderante, bien en el domicilio del trabajador, o bien en cualquier

⁷⁴ LÓPEZ CUMBRE, L., “Teletrabajo ocasional” (www.ga-p.com, agosto de 2020).

otro lugar que haya sido designado por este. Sin embargo, esta definición legal del art. 13 LET resultaba insuficiente y no se acomodaba a las particularidades del teletrabajo.

Asimismo, a nivel comunitario tenemos el Acuerdo Marco Europeo sobre Teletrabajo de 16 de febrero de 2002 y, a nivel internacional hay un Convenio de la OIT, que es el Convenio núm. 177 sobre trabajo a domicilio, el cual actualmente no se encuentra ratificado por España, por lo que no será de obligado cumplimiento hasta que sea ratificado.

En cuanto al ámbito nacional, disponemos del art. 13 LET, así como el Real Decreto-Ley 15/2020, de 21 de abril, de medidas urgentes complementarias para apoyar la economía y el empleo, que establece como forma de trabajo con carácter prioritario el trabajo a distancia, así como todos aquellos convenios colectivos que regulen esta modalidad de prestación laboral.⁷⁵

Recientemente, a causa de la situación de crisis sanitaria en la que estamos inmersos, se ha producido una intensificación del recurso al teletrabajo como forma de organización de la prestación laboral, por lo que muchas empresas se han visto envueltas en la necesidad de tener que adaptarse de forma inmediata a las nuevas circunstancias y han tenido que incorporar esta nueva modalidad de trabajo como medida de prevención frente al riesgo de contagio. Todo ello, ha hecho patente la necesidad de aprobación una nueva ley que se encargue de desarrollar esta forma de prestación laboral, dado que hasta el momento solamente disponíamos de una regulación genérica y deficiente contenida en el art. 13 LET, por lo que era necesario subsanar las insuficiencias normativas para poder aportar una mayor seguridad jurídica y satisfacer así las diferentes necesidades tanto de las personas trabajadoras como de las empresas que incorporaran esta modalidad de trabajo. Esta nueva ley, que se encarga de regular con mayor exhaustividad el teletrabajo ya ha sido publicada en el BOE el 23 de septiembre de 2020, concretamente, se trata del Real Decreto-Ley 28/2020, de 22 de septiembre, de trabajo a distancia que ha entrado en vigor a los 20 días de su publicación en el BOE, es decir, el 13 de octubre de 2020. Sobre este nuevo RDL 28/2020 del trabajo a distancia han de remarcarse una serie de aspectos:

⁷⁵ TRUJILLO PONS, F., “Camino a una nueva ley sobre el trabajo a distancia (teletrabajo) y derecho a la desconexión digital en el trabajo”, *Revista Aranzadi Doctrinal*, núm. 8/2020.

En su primer artículo, la nueva ley delimita cuál es su ámbito de aplicación, siendo aplicable a las relaciones laborales por cuenta ajena en las que concurran las condiciones previstas en el art. 1.1 LET, que se desarrollen a distancia y con carácter regular. En este sentido, la ley añade un aspecto clave a la hora de calificar la modalidad de prestación laboral como teletrabajo. Para ello, la ley establece que es necesario que el trabajo a distancia se preste con carácter regular y se entiende por trabajo a distancia regular, cuando en un periodo de referencia de tres meses, este es prestado al menos durante un treinta por ciento de la jornada o el porcentaje proporcional equivalente en función de la duración del contrato de trabajo. Por lo tanto, no se considera como trabajo a distancia si el trabajador trabaja menos del treinta por ciento de la jornada.

Asimismo, la nueva ley en su art. 2 establece las definiciones de trabajo a distancia, de teletrabajo y de trabajo presencial. Según la presente ley, el trabajo a distancia es una modalidad de organización del trabajo que se presta en el domicilio de la persona trabajadora o en cualquier lugar que haya sido escogido por esta, bien durante toda la jornada laboral, o bien durante parte de la jornada. Con respecto a esta definición de trabajo a distancia se ha de destacar un aspecto clave: su carácter regular, así como la necesaria flexibilidad en su uso.

Seguidamente, la ley define el teletrabajo como aquel trabajo a distancia que se lleva a cabo mediante un uso exclusivo o preminente de medios informáticos, telemáticos y de comunicación, y, finalmente, se encarga de definir el trabajo presencial como aquel trabajo que es desarrollado en el centro de trabajo o en un lugar que haya sido determinado por la empresa.

Otro de los aspectos de interés que presenta la nueva ley de trabajo a distancia se encuentra contenido en su art. 5 en el que se regula el acuerdo de trabajo a distancia. Con respecto a esto, lo primero que ha de indicarse es que el trabajo a distancia es de carácter voluntario. Ha de ser fruto de la voluntad de las partes contratantes, no pudiéndose imponer a través de la figura de la modificación sustancial de las condiciones de trabajo regulada en el art. 41 LET.

Asimismo, el trabajo a distancia requiere que su adopción se lleve a cabo a través de un acuerdo por escrito, que deberá de recoger un contenido mínimo y, además, este

acuerdo, ha de ser firmado por el empresario y el trabajador, no pudiendo el empleador alegar como causa de despido la negativa del trabajador a prestar sus servicios a distancia, puesto que se trata de una modalidad de prestación laboral de carácter voluntario. Asimismo, hay que indicar que la decisión de trabajar en remoto es reversible tanto para la empresa como para el trabajador, de tal manera que se podrá solicitar de forma unilateral la vuelta al trabajo presencial. Respecto al momento de celebración del acuerdo que prevea la prestación de servicios a distancia, este podrá ser incorporado en el contrato de trabajo inicial o podrá incorporarse en un momento posterior al mismo, siempre y cuando se cumpla la condición de que este contrato sea celebrado antes de que se dé comienzo a esta particular forma de prestación laboral.

Hemos hablado del carácter voluntario del teletrabajo, que además lo es para ambas partes del contrato, ello supone que cabe la posibilidad de que la persona trabajadora se niegue a prestar sus servicios en remoto, pues bien, la negativa a prestar los servicios en remoto, la negativa a la reversibilidad al trabajo presencial o la falta de adaptación por parte del trabajador a esta modalidad de prestación laboral no pueden suponer la extinción del contrato de trabajo, ni tampoco su modificación, estando vetada la posibilidad de recurrir al despido objetivo del teletrabajador por su falta de adaptación al trabajo en remoto, no pudiendo ser alegada esta circunstancia como causa justificativa del despido objetivo.⁷⁶

Respecto al contenido mínimo del acuerdo de trabajo a distancia, se han de incluir los siguientes extremos: el inventario de los medios, equipos y herramientas que exige el desarrollo del trabajo a distancia concertado, incluyendo los consumibles y los elementos muebles, así como la vida útil o el periodo máximo para la renovación de estos; la enumeración de los gastos que pudiera tener la persona trabajadora por el hecho de prestar servicios a distancia; así como la forma de cuantificación de la compensación que obligatoriamente debe abonar la empresa y el momento y la forma para realizar la misma, que se corresponderá, en caso de que exista, con la previsión contenida en el convenio o acuerdo colectivo aplicable. También ha de contener el horario de trabajo de la persona trabajadora, así como las reglas de disponibilidad, el porcentaje y distribución entre trabajo presencial y trabajo a distancia en su caso.

⁷⁶ LÓPEZ CUMBRE, L., “Claves de la nueva ley del teletrabajo” (www.ga-p.com, octubre de 2020).

Asimismo, se ha de hacer constar en el acuerdo de trabajo a distancia el centro de trabajo en el que se encuentra adscrita la persona trabajadora y donde desarrollará la parte de la jornada que se corresponda con el trabajo en modalidad presencial, ha de incluirse el lugar elegido por la persona trabajadora para la realización del trabajo a distancia, la duración de los plazos de preaviso para el ejercicio de las situaciones de reversibilidad en caso de que se decida su imposición, los mecanismos empresariales para el control de la actividad laboral, el procedimiento a seguir en el caso de que surjan dificultades técnicas que impidan el normal desenvolvimiento del trabajo a distancia. Finalmente, han de incluirse en el acuerdo las instrucciones dictadas por la empresa con previa información a los representantes legales sobre la materia de protección de datos de carácter personal y la duración del acuerdo del trabajo a distancia.

Respecto a los derechos de los trabajadores en remoto, conviene indicar como punto de partida, que se establece un equiparamiento entre los derechos del trabajador a distancia y del trabajador que desempeña sus servicios de forma presencial, de forma que esta modificación de la organización no puede suponer ningún menoscabo en los derechos de los trabajadores a distancia respecto a los trabajadores ordinarios en determinadas condiciones, tales como su retribución, estabilidad en el empleo, tiempo de trabajo, formación y promoción profesional

Entrando en detalle, los derechos de las personas que prestan sus servicios a distancia son regulados en los arts. 9 y ss. En particular, los trabajadores a distancia tienen derecho a recibir formación, derecho a la promoción profesional al igual que los trabajadores de forma presencial, derecho a la dotación y mantenimiento por parte de la empresa de medios, equipos y herramientas adecuadas para el ejercicio de la actividad laboral, derecho al abono y a la compensación de los gastos derivados del desarrollo del trabajo a distancia, tienen derecho a un horario flexible en los términos establecidos en el acuerdo de trabajo a distancia, además, los trabajadores a distancia tienen derecho a un sistema de registro horario adecuado, el cual debe de reflejar fielmente el tiempo en que la persona trabajadora realiza el trabajo en remoto y también tienen derecho a la prevención de riesgos laborales, derecho a la evaluación y planificación de la actividad preventiva.

Por otra parte, en la Sección 5ª se regulan los derechos relacionados con la utilización de dispositivos digitales, concretamente, se regula en el art. 17 el derecho a la intimidad y a la protección de datos, estableciéndose que el uso de medios telemáticos y el control de la prestación laboral a través de dispositivos automáticos ha de garantizar necesariamente el derecho a la intimidad y a la protección de datos, debiendo de respetarse en la utilización de estos medios los principios de: idoneidad, necesidad y proporcionalidad. Además, este mismo artículo añade que la empresa no puede exigir la instalación de programas o aplicaciones en los dispositivos particulares, ni tampoco puede exigir que el trabajador utilice estos dispositivos para el desarrollo del trabajo a distancia.

A continuación, dentro de los derechos relacionados con el uso de medios digitales, en el art. 18 se regula el derecho a la desconexión digital, estableciéndose que las personas que trabajen en remoto, en particular, a través de la modalidad del teletrabajo, tienen derecho a la desconexión digital fuera de su horario de trabajo en los términos establecidos en el art. 88 de la Ley Orgánica 3/2018, de 5 de diciembre. Además, la empresa deberá de elaborar una política interna en la que se incorporarán las modalidades del ejercicio del derecho a la desconexión digital y, además, se deberá de formar y sensibilizar al personal para que haga un uso razonable de los dispositivos tecnológicos a fin de evitar el riesgo de sufrir fatiga informática. A este respecto, hay que destacar el papel de los convenios o acuerdos colectivos de trabajo como instrumentos eficaces para establecer los medios y medidas adecuadas para poder garantizar un ejercicio efectivo del derecho a la desconexión digital.

En la Sección 6ª, concretamente, en el art. 19 de la ley, se regulan los derechos colectivos de las personas que trabajan a distancia. Dicho artículo establece que en lo concerniente a la negociación colectiva los trabajadores a distancia tienen derecho a ejercitar sus derechos de naturaleza colectiva en las mismas condiciones que el resto de las personas trabajadoras del centro al que están adscritas. Seguidamente, en lo relativo a las facultades de organización, dirección y control empresarial en el trabajo a distancia, el art. 20 dispone que las personas trabajadoras en el desarrollo del trabajo a distancia deben cumplir las instrucciones que hayan sido fijadas por la empresa en el marco de la legislación sobre protección de datos, previa participación de la representación legal de las personas trabajadoras.

Asimismo, en el art. 21 se establece que la empresa ha de aportar a los trabajadores instrucciones de uso y de conservación de los equipos informáticos, los cuales deberán de ser cumplidas por las personas trabajadoras dentro de los términos, que, en su caso, establezcan la negociación colectiva. En lo relativo a las facultades de control empresarial, el art. 22 faculta al empresario a adoptar las medidas de vigilancia y control que estime más oportunas con el objeto de verificar el cumplimiento por parte de la persona trabajadora de la prestación laboral, especialmente en la utilización de los medios digitales, debiendo de preservarse en todo caso, el debido respeto al derecho a la dignidad personal del trabajador.⁷⁷

6.2. El derecho a la desconexión digital

La omnipresencia de las TICs en la sociedad es un hecho. Hoy en día estas herramientas tecnológicas se han convertido en una parte esencial de nuestra vida, hasta tal punto que ha cambiado nuestra forma de relacionarnos y de trabajar. Con respecto al uso de las tecnologías en el seno de las relaciones laborales nos encontramos con una contrariedad, ya que las herramientas tecnológicas en el ámbito laboral presentan una doble cara: pueden ser un enemigo o un aliado. Si lo analizamos desde la óptica del trabajador, por un lado, el uso de la tecnología en el seno de las relaciones laborales comporta importantes ventajas, dado que se trata de una herramienta eficaz para mejorar la productividad y eficiencia del trabajador y, además, estas herramientas permiten que el trabajador tenga una mayor autonomía para poder gestionar su horario laboral, permitiendo a su vez una mejor conciliación entre la vida laboral y personal, lo cual, al mismo tiempo, ayuda a reducir los niveles de estrés a los que están sometidos los trabajadores.

Por otro lado, el uso intensivo de las herramientas tecnológicas en el ámbito laboral lleva aparejada una infinidad de inconvenientes y genera riesgos para la salud de los trabajadores. Una de las afecciones laborales más comunes y que está asociada a aquellos trabajos en los que utiliza el ordenador como herramienta de trabajo, es la fatiga ocular. La fatiga ocular es uno de los principales riesgos vinculados al uso del ordenador

⁷⁷ MARTÍNEZ-BOTELLO, P., “El trabajo a distancia, nuevo régimen jurídico, *Revista Aranzadi Doctrinal*, núm. 9/2020 parte Legislación.

y esta puede surgir tras la lectura o escritura en la pantalla del ordenador durante largos periodos de tiempo o ante la realización de tareas frente al ordenador en las que es necesario que el empleado se mantenga plenamente concentrado en su trabajo, ya que en estos casos el trabajador tiende a reducir el número de parpadeos que realiza, lo cual favorece el sufrimiento de sequedad ocular y, en consecuencia, el padecimiento de fatiga visual. Es por ello, que resulta necesario que el trabajador realice pausas periódicas de descanso, lo cual ayudará a reducir significativamente el sufrimiento de fatiga ocular. En este sentido, el art. 88 LOPDGDD establece que es al propio empresario al que le corresponde la labor de elaborar una política interna dirigida a los trabajadores en la que se establezcan unas instrucciones y reglas para que se haga un uso razonable de las herramientas tecnológicas, todo ello a fin de evitar el sufrimiento de fatiga informática y en aras de preservar el llamado derecho a la desconexión digital.

La incorporación de las tecnologías al ámbito laboral trae consigo la exigencia de que el trabajador esté virtualmente presente. Sin embargo, el problema surge cuando el trabajador tiene que estar constantemente conectado, de tal forma que se amplía su jornada laboral, haciendo un uso inadecuado de las TICs, por ejemplo, cuando realiza su trabajo en momentos inusuales, ya sea durante el fin de semana, por la noche, etc.⁷⁸

Es este nuevo contexto de hiperconectividad digital, lo que nos lleva a hablar del auge cada vez mayor del derecho a la desconexión digital, sobre el cual, hay que indicar que, pese a que se trate de un derecho que no reúne la categoría jurídica de derecho fundamental, aun así, ocupa un lugar destacable en el marco del derecho a la intimidad personal en el uso de dispositivos digitales. Este derecho es regulado en el art. 88 LOPDGDD bajo la rúbrica de *“Derecho a la desconexión digital en el ámbito laboral”*. En este precepto legal se reconoce a los trabajadores el derecho a la desconexión digital, el cual se entiende como el derecho que tienen los trabajadores de que fuera del periodo de trabajo se garantice su derecho al descanso, vacaciones, permisos, así como el respeto al derecho a la intimidad personal y familiar.

Como podemos observar, es de vital importancia que se garantice el derecho al descanso del trabajador, puesto que el hecho de que el trabajador descanse adecuadamente

⁷⁸ SERRANO ARGÜESO, M., “Digitalización, tiempo de trabajo y salud laboral”, *IUSlabor*, núm. 2, 2019, págs. 30-53

y, de que tenga derecho a vacaciones, conlleva importantes beneficios tanto para la salud del trabajador como para la calidad del trabajo prestado, por lo que ambas partes del contrato de trabajo salen beneficiadas. Además, como es sabido, todo trabajo lleva aparejado un esfuerzo físico o mental, por lo que es esencial recuperarse del trabajo realizado a fin de evitar el padecimiento de estrés laboral. Al mismo tiempo, la posibilidad de que el trabajador disfrute de un tiempo de descanso ayuda a mejorar su estado anímico, lo cual a su vez favorece a la productividad y eficiencia en el trabajo.

Asimismo, la necesidad de garantizar correctamente el derecho a la desconexión digital de los trabajadores se pone de manifiesto en el hecho de que los trabajadores cada vez encuentran mayores dificultades para poder desconectar de su trabajo y este problema se hace aún más palpable para aquellos trabajadores que prestan sus servicios a través del uso de las TICs o para aquellos que desarrollan la actividad laboral a través de la forma de organización laboral conocida como teletrabajo. Una de las razones por las que cada vez resulta más complejo desconectar del trabajo, es el sentimiento de culpabilidad que experimenta el empleado cuando se encuentra fuera de la jornada laboral y se encuentra a la espera de que llegue algún mensaje sobre algún asunto laboral. En estos casos, los trabajadores sienten la necesidad de tener que responder a dichos mensajes inmediatamente, bien por temor a que por algún descuido u olvido se queden desatendidos, bien para adelantar trabajo, o bien por la creencia de que al realizar las tareas lo antes posible serán valorados más positivamente, aun pudiéndolo hacer en un momento posterior. A lo anterior, hay que añadir que, en nuestra sociedad existe la creencia de que aquel trabajador que se encuentra digitalmente disponible de forma continuada es reconocido como un trabajador mucho más responsable y, al mismo tiempo, es tenido en una mejor estima que aquel que no se encuentra virtualmente disponible de forma constante. A este comportamiento se le conoce como “*presentismo laboral*” y consiste en el comportamiento del trabajador de dedicar más tiempo al trabajo, aun cuando suponga rebasar la jornada laboral, todo ello con la intención de que se note su presencia en el trabajo. Básicamente consiste en estar en el puesto de trabajo, pero sin estar realmente, puesto que no se reúnen las condiciones mentales mínimas para poder realizar eficientemente el trabajo, ya que como hemos señalado anteriormente, dedicar demasiadas horas al trabajo puede provocar fatiga mental y falta de motivación, lo cual evidentemente repercutirá negativamente en el rendimiento y en la eficiencia del trabajador, y es que, por contradictorio que parezca no necesariamente ha de existir una

correlación entre el tiempo dedicado a las tareas laborales y la calidad del trabajo prestado.⁷⁹ En definitiva, los trabajadores tienen derecho a que se garantice su derecho a la desconexión digital, lo cual beneficiará a ambas partes del contrato: al empleado y al empleador, ya que el trabajador podrá desarrollar su trabajo en mejores facultades mentales y, además, esto tendrá un efecto positivo para uno de los factores determinantes del crecimiento económico de la empresa: la productividad.

Por otra parte, hay que señalar que la garantía del derecho a la desconexión digital es un deber atribuible al empresario, en este sentido, se pronuncia el art. 19 LET, el cual establece que uno de los principales deberes que tiene el empresario es garantizar una correcta protección al trabajador en materia de seguridad y de salud, por lo tanto, el empresario es el que tiene la obligación de evitar que los trabajadores sufran una sobrecarga digital, haciendo efectivo el derecho a la desconexión digital. Este derecho no impide al empresario enviar mensajes al trabajador fuera de la jornada laboral para tratar cualquier asunto de contenido laboral, sin embargo, sí que faculta al trabajador para decidir ignorar dichos mensajes y no atenderlos hasta que comience la jornada laboral, sin tener por ello que atenerse a ningún tipo de sanción laboral. ¿Y cómo puede el empresario garantizar el derecho a la desconexión digital de los trabajadores? Este derecho puede ser garantizado, bien a través de la elaboración de políticas internas en las que se fijen unas instrucciones de uso de los dispositivos tecnológicos, siendo el diseño de estas políticas internas de obligado cumplimiento para las empresas, asimismo, el empresario deberá garantizar que los empleados reciban una adecuada sensibilización y formación para que puedan hacer un uso razonable de los dispositivos digitales.

Por último, hay que señalar que la negociación colectiva también adquiere un papel destacable como medio eficaz para garantizar el derecho a la desconexión digital de los trabajadores. No obstante, pese a que el derecho a la desconexión digital se configura como un derecho cada vez más necesario para los trabajadores, son pocos los convenios colectivos que lo reconocen y, además, aún existen empresas que no han diseñado un protocolo de actuación para poder garantizar un uso razonable de las

⁷⁹ PÉREZ CAMPOS, A. I., “La desconexión digital en España ¿un nuevo derecho laboral?”, *Anuario jurídico y económico*, núm. 52, 2019, págs. 101-124.

herramientas tecnológicas, y, en definitiva, para poder garantizar una efectiva desconexión digital de los trabajadores.⁸⁰

6.3 Regulación del derecho a la desconexión digital

Partiendo del uso cada vez mayor de los dispositivos digitales en nuestra vida cotidiana, de la crisis sanitaria en la que estamos inmersos a causa del COVID-19 y, sobre todo, teniendo en cuenta que el teletrabajo se ha convertido en una modalidad de prestación laboral en auge, especialmente para aquellas empresas que pueden adaptarse a esta forma de organización de la actividad laboral que al parecer ha llegado para quedarse. Todas estas circunstancias hacen que sea más necesaria que nunca una regulación más exhaustiva del derecho a la desconexión digital y, más aún, teniendo en cuenta que se trata de un derecho especialmente aplicable a los trabajadores que prestan sus servicios, bien a través del teletrabajo y, por lo tanto, a través del uso de las TICs.

En lo que respecta a la regulación del derecho a la desconexión digital, lo primero que hay que matizar es que el derecho a la desconexión digital ya es mínimamente garantizado con las normas laborales existentes que, aunque no regulan expresamente el derecho a la desconexión digital, si regulan otros derechos estrechamente vinculados con este. Con ello, me refiero a que ya se garantiza la protección del derecho a la desconexión digital con el reconocimiento de otros derechos laborales; los acuñados según PALOMEQUE como “*derechos laborales específicos*”⁸¹, tales como el derecho al descanso reconocido en los arts. 34 y ss. LET y en el art. 40.2 CE y, con el mismo, el derecho a una jornada laboral limitada y el derecho a unas vacaciones periódicas retribuidas. Es por ello, que algunos autores defienden la idea de que con el cumplimiento efectivo del derecho al descanso, así como el derecho a una jornada laboral limitada y a unas vacaciones, ya se está garantizando el derecho a la desconexión digital de los trabajadores, o lo que es lo mismo, la garantía de que fuera de la jornada laboral los trabajadores tengan derecho al descanso, lo cual se traduce en que los trabajadores se

⁸⁰ TRUJILLO PONS, F., “La desconexión digital en el ámbito laboral”, Tirant lo Blanch, Valencia, 2020, págs. 17 y 18.

⁸¹ PALOMEQUE LÓPEZ, M. C. y ALVAREZ DE LA ROSA, M., “Derecho del Trabajo”, Editorial Universitaria Ramon Areces, 2019, págs. 97-106.

hayan facultados a ignorar los mensajes procedentes del trabajo y a no enviar correos electrónicos fuera de la jornada laboral.

A mi juicio, este incipiente derecho a la desconexión digital se configura como un derecho esencial para los trabajadores, puesto que se trata de un derecho que guarda relación con el uso de las TICs en el ámbito laboral y con el teletrabajo. Para poder garantizar una adecuada protección del derecho a la desconexión digital hay que partir de la necesidad de garantizar un uso razonable de las TICs en el entorno laboral y, para ello, es crucial que el empresario aporte unas directrices a los trabajadores en las cuales establezca cuáles son los periodos que han de ser dedicados al trabajo efectivo y los tiempos de descanso. Por otra parte, sin una normativa que ofrezca seguridad jurídica a los trabajadores, estos no sabrían usar de forma razonable estas herramientas, puesto que los trabajadores experimentan sentimientos de culpabilidad al no realizar sus tareas, a lo cual hay que añadir que muchas veces resulta complicado desapegarse de las herramientas tecnológicas y desconectar realmente del trabajo, puesto que la tecnología es un producto especialmente adictivo. Pero no solo este es el problema, sino que, además, se trata de un instrumento que posibilita que el trabajador esté constantemente conectado, siendo una herramienta propicia para empeorar la situación de aquellos trabajadores que sufren adicción al trabajo y que sienten la necesidad de trabajar en exceso y de rellenar su tiempo libre con la realización de tareas laborales, causando un detrimento de la salud mental y empeorando las relaciones familiares y personales.

En definitiva, este es el planteamiento del que partimos, por lo que se hace evidente la necesidad de una regulación más específica del derecho a la desconexión digital, la cual tiene lugar por primera vez en el año 2018 con la Ley Orgánica de Protección de Datos y garantía de Derechos Digitales 3/2018, por lo que se trata de un derecho naciente en nuestro ordenamiento jurídico. En lo que respecta al cuadro normativo encargado de regular expresamente el derecho a la desconexión digital, en concreto, disponemos de la siguiente regulación:

En primer lugar, el art. 20 bis LET hace referencia al derecho a la intimidad y al derecho a la desconexión digital. Este precepto es introducido en el año 2018 por la LOPDGDD y contempla el derecho a la desconexión digital como un derecho vinculado al derecho a la intimidad, indicando que el derecho a la desconexión digital ha de

complementarse con los artículos de la ley de protección de datos personales y garantía de los derechos digitales;

En segundo lugar, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, dedica el Título X a garantizar y reconocer un elenco de derechos digitales, de los cuales ocupa un lugar destacable el derecho a la desconexión digital. Este derecho se encuentra regulado en el art. 88 LOPDGDD, precepto en el que se reconoce a los trabajadores y empleados públicos el citado derecho, todo ello, a fin de garantizar fuera de la jornada laboral el respeto de un tiempo de descanso, permisos y vacaciones, así como el respeto de la intimidad personal y familiar del trabajador. Asimismo, el mentado precepto añade que las modalidades de ejercicio del derecho a la desconexión digital han de atenerse a la naturaleza y objeto de la relación laboral, potenciando el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo dispuesto en la negociación colectiva o, en su defecto, a lo que hayan acordado la empresa y los representantes de los trabajadores. En otras palabras, esta disposición normativa en su apartado segundo recoge un límite al derecho a la desconexión digital, en concreto, establece que el derecho está supeditado a la actividad laboral que se realice, por lo que ha de adaptarse a la naturaleza de la actividad que desarrolle el trabajador, ya que cada trabajo tiene sus peculiaridades y, por lo tanto, cada trabajo requerirá del establecimiento de unas limitaciones y de la satisfacción de unas necesidades distintas. Así, por ejemplo, un trabajador de oficina requiere del establecimiento de unas limitaciones distintas de las que se pueden establecer a un camarero o a un dependiente de comercio. Lo que se quiere decir con ello, es que no se pueden establecer las mismas reglas y limitaciones para todas las modalidades de prestación laboral, sino que cada una tiene sus particularidades y, por lo tanto, cada actividad laboral precisará de unas limitaciones concretas u otras, o de mayores o menores limitaciones, y el instrumento idóneo para determinar dichas limitaciones es sobre todo la negociación colectiva y, en su defecto, a través de lo convenido entre la empresa y los representantes de los trabajadores.⁸²

⁸² FERNÁNDEZ ORRICO, J., “Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la ley orgánica 3/2018, de 5 de diciembre”, *Revista Española de Derecho del Trabajo*, núm. 222/2019, parte Editorial. 2019

Por otra parte, este mismo precepto en su apartado tercero establece una obligación fundamental para todas las empresas, exigiéndolas la elaboración de una política interna dirigida a los trabajadores a fin de garantizar adecuadamente el derecho a la desconexión digital, asimismo, establece que han de desarrollarse acciones de formación y de sensibilización del personal laboral, de tal modo que sepan hacer un uso razonable de las herramientas tecnológicas.

Finalmente, dentro de la legislación encargada de regular el derecho a la desconexión digital, ha de hacerse una especial mención a un Real Decreto-Ley de muy reciente promulgación, concretamente del Real decreto-Ley 28/2020, de 22 de septiembre, de trabajo a distancia. La citada ley dedica el capítulo tercero a regular los derechos de las personas trabajadoras en remoto, de entre los cuales, se ocupa de regular el derecho a la desconexión digital en el art. 18 de la ley, reconociendo a los trabajadores a distancia el derecho a la desconexión digital fuera de la jornada laboral, el cual ha de entenderse en los términos establecidos en el art. 88 LOPDGDD.

Además, el mentado precepto concibe el derecho a la desconexión digital como un deber empresarial, que el empresario ha de observar, limitando el uso de las herramientas tecnológicas durante los periodos de descanso, velando por el respeto de la duración de la jornada máxima, así como otros límites y cautelas que se establezcan en materia de jornada laboral, tanto en la normativa legal como convencional que resulte aplicable.

Por otra parte, el artículo impone a la empresa la elaboración de una política interna dirigida a las personas trabajadoras en la que han de concretarse las modalidades de ejercicio del derecho a la desconexión digital y las acciones de formación y de sensibilización al personal para que estos puedan hacer un uso razonable de las herramientas tecnológicas a fin de evitar el riesgo de padecimiento de fatiga informática, añadiendo que ha de preservarse el ejercicio del derecho a desconectar digitalmente del trabajo en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio de la persona trabajadora ligado a la realización de la actividad laboral mediante herramientas tecnológicas.

Finalmente, el citado precepto dedica el último párrafo a exponer cuál es el papel de los convenios colectivos en esta materia, estableciendo que los acuerdos o convenios colectivos podrán establecer los medios y medidas adecuadas para procurar una efectiva garantía del derecho a la desconexión digital en el trabajo.

Así por ejemplo el VIII Convenio colectivo de Iberdrola Grupo (C.C. 90012013011998), suscrito el 16 de diciembre de 2020, dedica su disposición final octava al derecho a la desconexión digital, estableciendo una serie de medidas a fin de garantizar el derecho a la desconexión digital, entre las que destacan las siguientes: que se trata de evitar, salvo en situaciones justificadas, las prolongaciones de jornada y la realización de horas extraordinarias; también, se trata de impulsar una cultura enfocada en los resultados y en la mejora de la productividad, eliminando la cultura del presentismo; se trata de fomentar una ordenación racional del tiempo de trabajo y su aplicación flexible, así como el uso de las tecnologías y herramientas de planificación; se trata de promover el uso racional y eficiente del e-mail y el teléfono corporativo, no solicitando respuesta fuera de los horarios de trabajo, ni durante los tiempos de descanso, permisos, licencias o vacaciones, salvo caso de fuerza mayor o circunstancias excepcionales.

Otro ejemplo de convenio colectivo que contempla el derecho a la desconexión digital es el Convenio colectivo estatal de centros y servicios veterinarios (C.C. 99100235012020), suscrito el 16 de enero de 2020, que dedica su art. 95 al derecho a la desconexión digital formalizándolo como un derecho y no como una obligación, lo cual significa según los términos del presente convenio que aquellas personas trabajadoras que quieran realizar comunicaciones fuera de su jornada laboral podrán hacerlo con total libertad. Por otra parte, establece que las personas tienen derecho a no responder a ninguna comunicación, fuere cual fuere el medio digital utilizado, una vez finalizada su jornada laboral, salvo que concurran circunstancias excepcionales señaladas en el convenio o de fuerza mayor. Además, se señala que el ejercicio del derecho a la desconexión digital no repercutirá negativamente en el desarrollo profesional de las personas trabajadoras. Asimismo, el presente convenio trata de potenciar la conciliación de la vida profesional y de la vida personal, tratando de garantizar que las reuniones de trabajo a nivel interno y con los clientes, así como la formación obligatoria, se realicen teniendo en cuenta el tiempo aproximado de duración, y, preferiblemente, no deben

extenderse hasta más tarde de la finalización de la jornada ordinaria de trabajo, a fin de que no se vea afectado el tiempo de descanso de las personas trabajadoras.

Finalmente, mencionar el II Convenio colectivo de grupo Vodafone España (C.C. 90102473012016), suscrito el 11 de diciembre de 2020, que también se pronuncia sobre el derecho a la desconexión digital, contemplándolo como un derecho y no como una obligación y definiendo cuál es su protocolo de actuación a fin de garantizar el derecho a la desconexión digital. Dicho protocolo de actuación está dirigido a potenciar la adopción de una serie de medidas, entre las cuales se puede mencionar que la reuniones de trabajo serán realizadas con carácter general dentro del horario laboral, esto es, entre la primera hora de entrada y entre la primera hora de salida del horario de trabajo, contemplando, además, la posibilidad de poder enviar comunicaciones fuera del horario de trabajo, debiendo asumir el solicitante de las mismas, la posibilidad de no obtener respuesta hasta el día hábil siguiente al tener las personas trabajadoras el derecho a no responder fuera del horario laboral.

7. CONCLUSIONES

El principal objetivo de este trabajo es elaborar un análisis sobre la incidencia que tienen las TICs utilizadas como herramienta de control de la actividad laboral en los derechos de los trabajadores, de lo cual se pueden extraer las siguientes premisas:

1. En este trabajo, se ha efectuado un estudio de las diferentes manifestaciones de control que ostenta el empresario y que puede ejercer gracias a la inserción de las TICs en el entorno laboral, llegando a la conclusión de que el empresario dispone de una infinidad de mecanismos de control, de los cuales, se han analizado los siguientes: la videovigilancia, los sistemas de captación del sonido, la vigilancia microfónica, la vigilancia telefónica, la vigilancia a través de las propias herramientas de trabajo, como el ordenador, las tabletas, el teléfono móvil, el vehículo de empresa, así como el uso del correo electrónico. Por último, se ha elaborado un análisis acerca del seguimiento de la actividad laboral a través de dispositivos de geolocalización.
2. Se ha analizado la legislación y, sobre todo, los diferentes pronunciamientos judiciales existentes en materia de digitalización y de derechos laborales con el fin de identificar cuáles son las principales limitaciones y garantías que han de observarse en el uso de las TICs como medio de supervisión de la actividad laboral.
3. Respecto al poder de dirección y control empresarial reconocido en el art. 20.3 LET, podemos decir que no es un poder ilimitado, puesto que su ejercicio debe estar condicionado al cumplimiento de una serie de garantías y limitaciones.
4. De estas garantías y limitaciones, la ley recoge como límite general el respeto de la dignidad humana. De esta limitación general se derivan otras limitaciones, de las cuales sobresale el respeto a los derechos y libertades fundamentales, cuya titularidad corresponde a todo ciudadano y, en consecuencia, son derechos que asisten a todo trabajador.

5. Respecto a los derechos fundamentales que pueden resultar vulnerados con el uso de las TICs, se ha de hacer una especial mención al derecho a la intimidad personal, el derecho a la protección de datos de carácter personal y al derecho al secreto de las comunicaciones.
6. Según la doctrina constitucional, el principio de proporcionalidad funciona como un elemento clave en la determinación de la legalidad de toda medida de control restrictiva de derechos fundamentales, de forma que toda medida de control de la actividad laboral, para ser considerada válida, ha de superar una triple prueba de idoneidad, necesidad y proporcionalidad en sentido estricto.
7. Toda medida de supervisión de la actividad laboral ha de estar justificada en un interés legítimo. Normalmente, dicho interés legítimo o finalidad consiste en la protección del patrimonio empresarial o en el control de la prestación laboral sin poder ser controlados otros ámbitos de la vida del trabajador pertenecientes a su vida privada.
8. El lugar de instalación de la medida de control también se configura como límite al poder de dirección y control empresarial. El empleador no puede escoger cualquier lugar para la implantación de la medida de control, no estando permitida la instalación de sistemas de grabación de sonidos ni de videovigilancia en zonas en las que el trabajador tiene una alta expectativa de privacidad. Así ocurre en determinados espacios, tales como los aseos, vestuarios, comedores, zonas de descanso o esparcimiento y análogos.
9. En la adopción de medidas de control de la actividad laboral, se exige el cumplimiento al deber de información previa. El empleador debe informar con carácter previo, de forma expresa, clara y concisa, a los trabajadores, empleados públicos y, en su caso, a los representantes de los trabajadores sobre la implantación de medidas de control, así como sobre las características y finalidad de las medidas.
10. En el caso de que concurren sospechas fundadas de que se están cometiendo irregularidades graves en el centro de trabajo, la exigencia del deber de

información se flexibiliza y se entiende superado con la colocación de un distintivo anunciando la existencia de la medida de control.

11. Con respecto a vigilancia a través de la captación del sonido, se puede observar que es un medio de control mucho más invasivo que las cámaras de videovigilancia, ya que este permite captar conversaciones en las que con frecuencia son expresadas pensamientos íntimos, ideas u opiniones que nada tienen que ver con la actividad laboral, por lo que, en estos casos, se deberá de analizar minuciosamente que el empleador no se excede en el control y que estas medidas realmente contribuyen a satisfacer la finalidad empresarial de protección del patrimonio o de supervisión del correcto desempeño de la actividad laboral.
12. La principal solución con la que cuenta el empleador para garantizar el respeto de los derechos fundamentales y, evitar, en la medida de lo posible, que se generen intromisiones en la privacidad de los empleados, es el diseño de una política interna dirigida a los trabajadores a fin de garantizar un uso razonable de los medios digitales. Además, deberá de emitir unas instrucciones de uso de los medios digitales, indicando qué usos están autorizados y cuáles se consideran ilícitos y si permite el uso de los medios digitales para fines personales o si el uso de estas herramientas ha de ir destinado exclusivamente a fines profesionales.
13. El control de la ubicación física del trabajador es una medida plenamente válida siempre que su instalación obedezca a la exclusiva finalidad de verificar el cumplimiento de la actividad laboral, y como regla general, es una medida que únicamente puede ser utilizada dentro de la jornada laboral y no fuera de la misma.
14. También se ha analizado en detalle la existencia de tres modalidades de prestación laboral muy particulares: el trabajo a distancia, trabajo a domicilio y el teletrabajo. Destacando entre las mismas el teletrabajo, el cual es definido por la ley como aquel trabajo a distancia que se lleva a cabo mediante un uso exclusivo o preminente de medios informáticos, telemáticos y de comunicación.
15. En lo concerniente al trabajo a distancia y al teletrabajo (cuyo uso ha sido acentuado debido a la crisis sanitaria generada por el Covid-19), resulta

conveniente destacar la reciente aprobación del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, del cual se han puesto de manifiesto los aspectos más esenciales del mismo.

16. Finalmente, sin olvidar la infinidad de ventajas que ofrecen las TICs en el seno de las relaciones laborales, se ha de señalar que el uso desmedido de estas puede ocasionar problemas de diversa índole en la persona del trabajador, tales como el tecnoestrés, la fatiga visual y la hiperconexión, la cual a su vez genera agotamiento y falta de rendimiento en el trabajador. Es por ello, que ha de garantizarse el derecho a la desconexión digital de los trabajadores mediante la limitación del uso de los medios digitales durante los periodos de descanso, así como a través del respeto de la duración máxima de la jornada laboral.

8. BIBLIOGRAFÍA

- ARAGÓN GÓMEZ, C., “El deber de buena fe contractual” en CRUZ VILLALÓN, J., GARCÍA-PERROTE ESCARTÍN, I, GOERLICH PESET, J. M., MERCADER UGUINA, J. R., *Comentarios al estatuto de los trabajadores*, Aranzadi, 2016.
- CHARRO BAENA, P. y ESPINOZA ESCOBAR, J. H., “Cuestiones actuales del derecho del trabajo” *Un estudio desde las dos orillas*, Dykinson, 2014.
- FERNÁNDEZ ORRICO, J., “Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la ley orgánica 3/2018, de 5 de diciembre”, *Revista Española de Derecho del Trabajo*, núm. 222/2019, parte Editorial. 2019.
- FERRER SERRANO, R. L., “Guía de protección de datos de los trabajadores”, Tirant Lo Blanch, Valencia, 2019.
- GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A., “La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo”, *Revista Española de Derecho del Trabajo*, núm. 216/2019, parte Estudios, 2019.
- GARCÍA NINET, J. y VICENTE PACHÉS, F., “El control empresarial en el ámbito laboral”, Ciss, 2005, pág. 21.
- 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*, núm. 2/2018, parte jurisprudencia.

- LLAMOSAS TRAPAGA, A., “Relaciones laborales y nuevas tecnologías de la información y de comunicación” *Una relación fructífera no exenta de dificultades*, Dykinson, 2015.

- LÓPEZ BALAGUER, M. y RAMOS MORAGUES, F., “Derecho a la intimidad y a la protección de datos y licitud de la prueba en el proceso laboral”, en AA.VV. MONREAL BRINGSVAERD, E., THIBAUT ARANDA, X, y JURADO SEGOVIA, A. “*Derecho del trabajo y nuevas tecnologías*”, Tirant lo Blanch, Valencia, 2020, págs. 419 y ss.

- LÓPEZ CUMBRE, L., "Grabaciones ocultas en la empresa y privacidad laboral de los trabajadores sorprendidos hurtando", *Revista del Centro de Estudios de Consumo (CESCO)*, en <http://centrodeestudiosdeconsumo.com>, noviembre, 2018, 31 páginas.

- LÓPEZ CUMBRE, L., “Protección de datos “laborales” (www.gomezacebo-pombo.com, diciembre de 2018).

- LÓPEZ CUMBRE, L., “GPS como sistema de control de jornada: sólo si la prestación laboral se desarrolla entre la conexión y la desconexión” (www.ga-p.com, marzo de 2020).

- LÓPEZ CUMBRE, L., “Efectos laborales del coronavirus (II): antes inviable, ahora imprescindible; el teletrabajo como medida de “distanciamiento físico” (www.ga-p.com, marzo de 2020).

- LÓPEZ CUMBRE, L., “Teletrabajo, trabajo a distancia y trabajo a domicilio” (www.ga-p.com, junio de 2020).

- LÓPEZ CUMBRE, L., “Teletrabajo ocasional” (www.ga-p.com, agosto de 2020).

- LÓPEZ CUMBRE, L., “Claves de la nueva ley del teletrabajo” (www.ga-p.com, octubre de 2020).

- MARTÍNEZ-BOTELLO, P., “El trabajo a distancia, nuevo régimen jurídico”, *Revista Aranzadi Doctrinal* núm. 9/2020 parte Legislación.
- MERCADER UGUINA, J. R., “Lecciones de Derecho del Trabajo”, Tirant Lo Blanch, 2019.
- MONEREO PÉREZ, J. L., “Se justifica la grabación con cámaras ocultas en el centro de trabajo por la existencia debidamente acreditada de sospechas razonables de irregularidades graves”, *Revista de Jurisprudencia Laboral*, núm. 8/2019.
- MONREAL BRINGSVAERD, E., THIBAUT ARANDA, X. y JURADO SEGOVIA, A., “Derecho del trabajo y nuevas tecnologías”, Tirant Lo Blanch, Valencia, 2020, pág. 240.
- MUNÍN SÁNCHEZ, L. M., “Las nuevas maneras de trabajar y los nuevos medios de prueba” en MELLA MÉNDEZ, L. y NÚÑEZ-CORTÉS CONTRERAS, P. *Nuevas tecnologías y nuevas maneras de trabajar: Estudios desde el Derecho Español y comparado*, Dykinson, Madrid, 2017. Págs. 329-332.
- PALOMEQUE LÓPEZ, M. C. y ÁLVAREZ DE LA ROSA, M., “Derecho del trabajo”, Editorial Universitaria Ramón Areces, 2019, págs. 97-113 y 591.
- PAZOS PÉREZ, A., “La utilización de internet en el ámbito laboral y el control empresarial en MELLA MÉNDEZ, L. y NÚÑEZ-CORTÉS CONTRERAS, P., *Nuevas Tecnologías y Nuevas Maneras de Trabajar. Estudios desde el derecho español y comparado*, Dykinson, Madrid, 2017, págs. 197-214.
- PÉREZ CAMPOS, A. I., “La desconexión digital en España ¿un nuevo derecho laboral”, *Anuario jurídico y económico*, núm. 52, 2019, págs. 101-124.
- REYES HERREROS, J.; ALCAIDE, L., “Geolocalización de trabajadores”, *Actualidad Jurídica Uría Menéndez*, núm. 52, 2019, pág. 74.

- RIBAS, X., “Puntos destacados de la nueva Ley Orgánica 3/2018 de Protección de Datos” *Aranzadi digital*, núm. 1/2020, págs. 7 y 8.
- RODRIGO, B., “Una pulsera de Amazon controla empleados ‘vagos’. ¿Puede usarla tu jefe en España?”, *El Confidencial*. 8 de febrero de 2018 (Disponible en https://www.elconfidencial.com/tecnologia/2018-02-08/pulsera-amazon-rastrear-ubicacion-empleados_1516056/).
- RODRIGUEZ ESCANCIANO, S., “Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores”, Tirant lo Blanch, 2015.
- ROIG BATALLA, A; GALA DURÁN, C., MARTÍNEZ FONTS, D. y MUÑOZ LLORENTE, J., “El uso laboral y sindical del correo electrónico e Internet en la empresa, aspectos constitucionales, penales y laborales”, Tirant Lo Blanch, Valencia, 2007, págs. 63-66.
- SALA FRANCO, T., TODOLÍ SIGNES, A. y MARTÍN-POZUELO LÓPEZ, A. “El teletrabajo”, Tirant Lo Blanch, Valencia, 2020, págs. 27-34.
- SERRANO ARGÜESO, M., “Digitalización, tiempo de trabajo y salud laboral”, *IUSlabor*, núm. 2, 2019, págs. 30-53.
- SERRANO GARCÍA, J. M., “La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia” *Límites de la ley de protección de datos al poder de dirección del empresario*, Editorial Bormazo, Albacete, 2019, págs. 35-48.
- THIBAUT ARANDA, J., “Control Multimedia de la Actividad Laboral”, Tirant Lo Blanch, Valencia, 2006, págs. 3-13.
- TRUJILLO PONS, F., “Camino a una nueva ley sobre el trabajo a distancia (teletrabajo) y derecho a la desconexión digital en el trabajo”, *Revista Aranzadi Doctrinal* núm. 8/2020, págs. 17 y 18.

- ZARAGOZA TEJADA, J. I., “La prueba obtenida por videocámaras de seguridad tras la STEDH del 17 de octubre de 2019. Caso López Ribalda vs España”, *Revista Aranzadi Doctrinal*, núm. 2/2020, parte jurisprudencia.

Agradecimientos: A la profesora Lourdes López Cumbre por haberme guiado con tanta dedicación en la elaboración de este trabajo y a mis padres por estar siempre ahí, acompañándome y dedicándome todo su esfuerzo y apoyo.