TRABAJO DE FIN DE GRADO DE DERECHO

Mecanismos de control empresarial y derechos del trabajador

ALUMNO: IRENE TRAVESEDO LASO

TUTOR: DOLORES CARRILLO MÁRQUEZ

DOBLE GRADO DE DERECHO Y RELACIONES INTERNACIONALES

CURSO 2024/2025

ABRIL 2025

ÍNDICE

1. INTRODUCCIÓN

1.1. Contextualización

La Ley trata de amoldarse a la realidad, yendo siempre un paso por detrás de esta. Esto es una característica fundamental de los sistemas normativos y regulatorios tanto nacionales como internacionales, desde el inicio de la Humanidad. Un ejemplo claro y actual de este fenómeno son las nuevas tecnologías. Su propio nombre indica algo fundamental del concepto, es “nuevo” y como tal, se antepone a todo lo demás, dejando a la Ley detrás, la cual trata de amoldarse lo más rápido y adecuadamente a estas realidades constantemente cambiantes.

Hoy en día cada persona tiene acceso a dispositivos a través de los cuales crean su propio mundo virtual, con datos personales que se les va alimentando, para hacer de ellos herramientas útiles a través de las cuales podemos desempeñar casi cualquier tarea. Dahl define el poder como “la capacidad de conseguir que un actor haga algo que por sí mismo no habría hecho” (Guzzini, 2015). Por su parte, Weber, califica este concepto de amorfo, pues a su juicio, cualquier cualidad humana puede dar esta oportunidad de la que habla Dahl de imponer la voluntad de uno. Así pues, Weber, diferencia entre el significado de poder (Macht), definiéndolo como “la probabilidad de imponer la propia voluntad, dentro de una relación social, aun contra toda resistencia y cualquiera que sea el fundamento de esa probabilidad” (Weber, 1977) y dominación (Herrschaft), la cual define como la capacidad de la "voluntad expresada" o "orden" de los actores dominantes de influir en la acción de los subordinados, hasta el punto de que estos lleguen a considerar la conformidad con esa orden como una decisión propia, transformando así la obediencia en un principio de su propia acción (Guzzini, 2015).

Esta estructura de dominación y ejercicio de influencias es la que conforman las nuevas grandes corporaciones, siendo en muchas ocasiones más destacables que muchos estados. Así pues, esta relación se convierte inevitablemente en un mercado, un negocio, en el cual el objetivo final es ejercer dicha influencia. Para conseguir esto, la materia prima necesaria, en nuestra era digital, son los datos. Estos nuevos modelos empresariales optimizan los datos obtenidos y comprados a otros, a través de algoritmos que permiten en última instancia, predecir comportamientos y tendencias humanas. Con esta

información, el mercado se alimenta de nuevas oportunidades de negocio futuras que los consumidores puede que no se hayan llegado siquiera a plantear todavía. Consecuentemente, aquel que posee la mayor cantidad de datos sistematizables, es el que será capaz de ejercer lo que Weber entiende como dominación.

Estos cambios radicales en los modelos de empresa y en las personas que los conforman han modificado consecuentemente el ámbito laboral. La tecnología se ha integrado en el lugar de trabajo, ofreciendo eficiencia, información y herramientas útiles para el desempeño de las labores individuales de todo empleado. Si bien, es verdad que las ventajas que ha traído el avance tecnológico son innegables, también ha supuesto la aparición de numerosos problemas que afectan a los derechos fundamentales de cada individuo, ya sea desde su condición de empresario o de trabajador, así como para los juristas encargados de solucionar dichas barreras.

Este sistema que se encuentra cada vez más asentado en nuestra sociedad, en el cual, los datos suponen la materia prima que concluye en beneficios para aquel que sepa tratarla, es relativamente nuevo, y por tanto, actualmente, la Ley trata de seguir el rastro a este avance, con numerosos éxitos y numerosas pérdidas. La tecnología como medio para la mayor obtención y optimización de estos datos se ha convertido en el medio idóneo de toda empresa, y no solo en una herramienta imprescindible, sino también en el propio fin de muchas.

Las nuevas tecnologías como smartphones, tabletas, y ordenadores, se han convertido en accesorios indispensables para el día a día, sin los cuales la gran mayoría de personas se encuentran perdidas. Un ejemplo ilustrativo de esto es la capacidad de pagar actualmente ya en casi cualquier establecimiento, a través de Google Pay instalado en el teléfono o la incapacidad de las nuevas generaciones de hacer nada sin una conexión a la red. Poco a poco estos dispositivos se están adueñando de nuestras vidas, y ocupando todas y cada una de las esferas tanto privadas como públicas.

En el ámbito laboral no solo supone la optimización del trabajo a la hora de realizar las obligaciones de los trabajadores, sino una facilitación y automatización de las tareas y responsabilidades de los empresarios. Esto se ha trasladado al disfrute de los derechos individuales de cada uno de estos colectivos. Como sabemos, la condición de trabajador

o empresario acarrea consigo una serie de derechos y deberes que son inherentes a dicha condición. Así pues, en ambos casos, la tecnología puede suponer un aliado o un enemigo, dependiendo de la perspectiva desde donde se mire y el papel otorgado a esta. Como establece José Luis Goñi, el uso de estas nuevas tecnologías vinculadas a la informática presentan una amenaza potencial para el trabajador en la medida en que registran los datos personales del trabajador, que pueden llegar a ser usados para deducir información con fines desconocidos o incluso discriminatorio (2017).

Ahora bien, es indiscutible, que actualmente, la tecnología se ha convertido en un nuevo ente sin el cual, estructuras sociales, políticas y económicas se vendrían abajo. Por ello, y haciendo referencia a lo expuesto *supra*, es necesario que la ley se adapte lo antes posible a esta realidad existente desde hace ya décadas, y que no parece disminuir su crecimiento sino todo lo contrario.

Por otro lado, si bien es verdad que, para el trabajador, se aprecian tanto efectos positivos como negativos en el uso de estas tecnologías y la participación de este mercado basado en la información, es también esencial analizar la injerencia de estos cambios en la figura del empresario. Uno de estos efectos claros, se aprecia en los métodos que el empresario tiene a su disposición para llevar a cabo sus obligaciones y ejercer sus poderes, especialmente el de control de la empresa y sus integrantes, y la injerencia que dicho poder tiene en la vida privada del empleado. La pandemia, trajo, entre otras muchas cosas, la normalización del teletrabajo. Con ello, la expectativa de disponibilidad de los trabajadores aumentó exponencialmente. La inexistencia de una barrera clara entre lo que es la vida privada y familiar de la vida laboral puede llegar a suponer, como se verá más adelante, una intromisión y vulneración de los derechos fundamentales del individuo. Tales han sido estas vulneraciones, que nuestro ordenamiento ha llegado tan lejos como a establecer la existencia de derechos digitales, que también serán objeto de análisis en este trabajo.

Así pues, es necesario para este trabajo hacer una distinción clara entre el concepto de trabajador y de empresario. El Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (de ahora en adelante ET), no contiene una definición como tal de trabajador, pero sí delimita claramente lo que se entiende por relación laboral, de lo cual se extrae después el concepto

de trabajador. El art 1.1 del ET determina que “esta ley será de 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”. De esta disposición se extrae, por tanto, que el trabajador, es aquella “persona física que, de manera personal, voluntaria, y retribuida presta servicios por cuenta ajena y dentro del ámbito de organización y dirección de un tercero, el empresario” (López, 2022). El empresario, por su parte, acorde a lo dispuesto por en el art 1.2 del ET serán “todas las personas, físicas o jurídicas, o comunidades de bienes que reciban la prestación de servicios de las personas referidas en el apartado anterior, así como de las personas contratadas para ser cedidas a empresas usuarias por empresas de trabajo temporal legalmente constituidas”.

1.2 Objetivo y preguntas

Analizar las implicaciones legales del uso sistemático de sistemas de video vigilancia y geolocalización por parte de las empresas en el ámbito laboral, es esencial para poder entender la evolución y el futuro de las relaciones laborales entre el empresario y los trabajadores. El uso de estos métodos impacta profundamente en los derechos fundamentales de los trabajadores y su conformidad con la normativa vigente.

Así pues, este trabajo pretende identificar y describir los cambios que ha habido en la jurisprudencia y la doctrina, para poder entender el camino que parece seguir la concepción de estos derechos y su protección. Por lo tanto, se pretende examinar cómo los métodos de vigilancia analizados afectan a la intimidad y a la protección de datos, y la manera en la que la normativa de protección de datos ha ido ganando más protagonismo en la resolución de estos conflictos.

Por último, tras haber hecho un estudio en profundidad de la jurisprudencia y normativa, y en vista de las conclusiones extraídas tras su análisis, se busca proponer ciertas recomendaciones para intentar garantizar el control equilibrado en el seno de las relaciones laborales.

Para la consecución de estos objetivos, se plantean diferentes preguntas entre ellas:

- Dentro del derecho de control y vigilancia del empresario, ¿qué limites puede encontrar el empresario?
- ¿Qué establece la normativa vigente nacional respecto al uso de nuevas tecnologías para el ejercicio del poder de vigilancia del empresario?
- ¿En qué medida, estos sistemas, pueden impactar a los derechos fundamentales del trabajador?

1.3 Metodología

En relación con la metodología que se ha usado para llevar a cabo este trabajo de investigación, cabe destacar el análisis de la normativa laboral pertinente, así como de la jurisprudencia existente relativa al ámbito estudiado. Por otro lado, se ha tenido en cuenta lo publicado por diferentes juristas en cuestión de doctrina jurídica.

Por otro lado, esta exposición se ha llevado a cabo desde una perspectiva cronológica con el objetivo de establecer un recorrido histórico sobre los cambios recientes de la percepción doctrinal y la normativa de los medios de control del empresario. Así mismo se ha buscado un enfoque descriptivo para poder plasmar una interpretación correcta de lo que forma parte de estos conceptos en el contexto actual laboral y social. Para esto, se ha analizado el fenómeno de manera documental a través de libros, manuales, revistas y artículos.

CAPÍTULO 1: Concepto de control empresarial

En este primer capítulo se va a hacer un estudio en profundidad de diversos conceptos, entre ellos, el concepto y características de los poderes del empresario. Como se determina en el art 1.1 del ET previamente citado, una de las notas características del contrato de trabajo es la dependencia. Esta relación dota de ciertas obligaciones al trabajador y de ciertos poderes al empresario. Entre ellos podemos distinguir tres grandes categorías, el poder de dirección, el poder de vigilancia y el poder disciplinario. Este trabajo se centrará en el poder de vigilancia y control del empresario, así como en el disciplinario, como expresión última del ejercicio del primero.

El objetivo fundamental del empresario es la organización de una actividad productiva para la obtención de un beneficio. A la hora de organizar dicha actividad, el empresario va a necesitar diferentes herramientas que le faciliten la puesta en práctica de su poder de vigilancia, para asegurarse que dicha actividad se está desarrollando conforme a los estándares establecidos por su propia política empresarial, por el contrato firmado con el trabajador y por la ley.

Para llevar a cabo el desarrollo de esta cuestión cabe hacer referencia como introducción al art. 20 del ET y al art. 38 de nuestra Carta Magna. La primera disposición establece, por una parte, la obligación del trabajador de realizar el trabajo convenido, mientras que, por su parte, otorga al empresario la capacidad para adoptar las "medias que estime oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales" (art 20.3 ET). Este otorgamiento de responsabilidades y obligaciones se basa en la libertad de empresa, derecho constitucionalmente garantizado a los españoles (art 38 CE).

Así pues, se reconoce un amplísimo poder de vigilancia y control simplemente limitado por la "dignidad humana del trabajador". Este límite ha sido duramente criticado por la jurisprudencia y la doctrina por la insuficiente claridad y concreción que supone. Parece pues, que el legislador pretende dar casi total libertad al empresario para ejercer sus derechos obviando los inherentes al trabajador que pueda vulnerar en el proceso. Así pues, la dignidad humana no solo es un derecho fundamental (art 10 CE) en sí, sino que es la

base de lo establecido en el Título I de la Constitución. Ahora bien, la generalidad de este concepto ha dado lugar a conflictos y desacuerdos.

Como determina Matorras, el poder de vigilancia del empresario implica el control sobre el cumplimiento de la jornada laboral, la dinámica de trabajo, y los resultados derivados del mismo [...] así como el establecimiento de sistemas de control sobre el uso que el trabajador hace de los medios, instrumentos y recursos puestos a su disposición para el cumplimiento de sus obligaciones laborales" (2022, pág. 221). La evolución tecnológica ha provocado la necesidad de revisitar estos conceptos para poder adaptarlos a la nueva realidad. Así pues, el art. 20 bis ET determina que "los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

Así pues, hoy en día más que nunca, es necesario un equilibrio entre el poder que el empresario puede ejercer para asegurar la satisfactoria consecución de sus objetivos y los derechos de aquellos encargados de obtener dichos objetivos, equilibrio que como se verá más adelante, cada vez está más en duda en nuestra normativa y jurisprudencia.

CAPÍTULO 2: Derechos del trabajador en relación con el poder de control del empresario

En este apartado se profundizará en los derechos del trabajador que se encuentran relacionados directamente con la facultad de control del empresario para más tarde poder hacer un análisis adecuado de los métodos empleados por el segundo y su correcta utilización para con el primero.

Si bien es verdad que la celebración de un contrato de trabajo supone la aceptación de las facultades del empresario en el marco de una relación de dependencia, no significa que, dentro de este contrato, los derechos fundamentales del trabajador queden mermados a la voluntad del empresario. Así pues, "ello ha sido una constante en nuestra doctrina constitucional, por la cual, se ha entendido que celebrar un contrato de trabajo no conlleva

para los trabajadores la privación de los derechos que la Constitución les confiere en su condición de ciudadanos" (Pascual, 2023, pág. 16).

En consonancia con esto, el Tribunal Constitucional resume esta cuestión estableciendo un criterio que determina que "la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano" (STC 88/1985, de 19 de julio). Ahora bien, en ocasiones los derechos del primero y los deberes del segundo pueden llegar a chocar, ocasionando diferentes conflictos.

Para empezar, cabe hacer especial mención a la dignidad humana, pues constituye, como ya se explicó previamente, el único límite a la facultad de control del empresario en el seno de su organización empresarial. Así pues, el art 10 de la Constitución determina que "la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social". Igualmente, se establece en el apartado siguiente, que las normas relativas a los derechos fundamentales y las libertades reconocidas en la Constitución se deben interpretar conforme a la Declaración Universal de Derechos Humanos (de ahora en adelante DUDH) y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

Se establece que toda persona tiene derecho al trabajo en condiciones justas y libres de discriminación, a un salario igual por trabajo igual y a una remuneración que garantice su dignidad y la de su familia. Además, tiene derecho a la protección frente al desempleo y a la formación de sindicatos. Estos derechos deben ser acordes con la dignidad humana y el bienestar social (art 23 DUDH).

En conexión con este presupuesto básico que entraña la base para el reconocimiento de los derechos fundamentales, se encuentra el derecho a la no discriminación y a la igualdad. El artículo 14 CE dispone 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". En tanto en cuanto, el empresario ejerce unos deberes desde una posición de poder para con el trabajador, y que, para ello, cuenta con herramientas tecnológicas como cámaras de video vigilancia,

tarjetas magnéticas, dispositivos de geolocalización y las mismas herramientas de trabajo que proporciona a sus empleados como el correo o aplicaciones de mensajería rápida; este ejercicio de poder puede llevar a prácticas discriminatorias. Por ello, se han regulado dichos mecanismos de manera exhaustiva a través del 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. Este reglamento, deroga la Directiva 95/46/CE, también conocida como *Reglamento general de protección de datos.* Esta normativa internacional prevé la posibilidad de que se produzcan estas vulneraciones, y en consecuencia, otorga a los responsables del tratamiento de los datos obtenidos por esos medios, la obligación de adoptar medidas para paliar estos riesgos.

El grueso de la cuestión se encuentra en los conceptos de privacidad e intimidad y cómo la vigilancia y control, ejercido por parte del empresario sobre los trabajadores, puede incidir en estos conceptos. La STC de 30 de noviembre de 2000, 292/2000 establece que "la función del derecho fundamental a la intimidad del art 18.1 CE, es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad", es decir, dice el Tribunal Constitucional, que el derecho a la intimidada es "el poder de resguardar su vida privada de una publicidad no querida". En cambio, por su parte, el derecho fundamental a la protección de datos del art 18.4 CE "persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado", garantizando un poder de disposición sobre estos datos a los individuos.

La intimidad se encuentra recogida en el Título I, capítulo II, sección 1ª "de los derechos fundamentales y libertades públicas" de nuestro texto constitucional dentro de los derechos fundamentales en el artículo 18, que garantiza "el derecho al honor, a la intimidad personal y familiar y a la propia imagen". Como explica Federico de Montalvo Jääskeläinen, el derecho a la intimidad se interpreta por parte del Tribunal Constitucional como el derecho a la protección frente a terceros de determinadas esferas de la vida íntima (2020). Aplicando este concepto a la era digital en su esfera laboral, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos

digitales, dispone que “los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos puestos a su disposición por el empleador” (art. 87, LOPDPGDD).

En un inicio, la jurisprudencia, venía solucionando los conflictos relacionados con el ejercicio del poder de vigilancia y control del empresario, desde una perspectiva enfocada en el derecho a la intimidad del individuo. Aunque la distinción entre ambos ya se venía haciendo, fue con la STC 292/2000 de 30 de noviembre, cuando cambió esta aproximación, centrándose los tribunales en el derecho a la protección de datos y el derecho a la intimidad digital. Así pues, el mismo artículo 18 de la Constitución, en su apartado cuarto dispone 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”. Asimismo, el apartado 3 de este artículo, establece que “se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial”. Esta sistematización permite observar la relación intrínseca que existe entre el derecho a la intimidad, el derecho a la protección de datos y al secreto de las comunicaciones, como manera de asegurar el mantenimiento de esa intimidad. Actualmente, uno no puede existir sin el otro.

Estos derechos inherentes a la dignidad del ser humano se encuentran desarrollados en el Estatuto de los Trabajadores (de ahora en adelante ET), trasladándolos pues, al ámbito laboral. El art 4.2 reconoce al trabajador el derecho a la intimidad en el seno de su lugar de trabajo, estableciendo a la vez el vínculo entre este derecho y la dignidad que se ha explicado *supra*.

La necesaria adaptación al Reglamento 2016/679 del Parlamento Europeo y del Consejo de Protección de datos provoca que, en el año 2018, entre en vigor la Ley Orgánica 2/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. En ella se especifica y desarrolla la naturaleza y alcance del derecho a la protección de datos, derecho extensamente debatido y analizado actualmente. Este precepto se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención, configurándolo como un derecho de control y disposición de los datos personales y la decisión individual y personal de disponer de estos ante un tercero. Este derecho, también

permite al individuo conocer la identidad de aquel que posee los datos y revocarle la posesión.

Así pues, la LOPDGDD, tiene como finalidad última, el reconocimiento y protección del derecho a la protección de datos, pues busca configurar la facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos de los que se usaron para justificar su obtención. Para conseguir esta finalidad, la ley reconoce diferentes derechos en consonancia con los establecidos en la Constitución y en el Estatuto de los Trabajadores a los que denomina "derechos digitales". Además de desarrollar derechos como los de neutralidad, acceso o seguridad, hace hincapié en los reconocidos para la esfera laboral del individuo. El artículo 87, desarrolla el derecho a la intimidad y uso de dispositivos digitales en el ámbito de trabajo. Así pues, como ya se expuso *supra*, se dispone que "los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador".

Dentro de este uso de la tecnología proporcionada, el empresario podrá acceder a los contenidos de dichos dispositivos como método de control del cumplimiento de las obligaciones laborales del trabajador. Es en esta situación donde podemos observar la existencia de dos derechos en conflicto en tanto en cuanto el poder de control y vigilancia del empresario supone una característica inherente a su condición, y la intimidad, lo es de la condición de trabajador, y persona. Así pues, se encomienda al empresario, para proteger ambos derechos, la responsabilidad y deber de "especificar de modo preciso los usos autorizados [de dichos dispositivos] y el establecimiento de garantías para preservar la intimidad de los trabajadores". Como veremos más adelante, esta obligación será un factor determinante para la licitud de las medidas tomadas en consecuencia de esta vigilancia.

Por otro lado, el derecho a la intimidad frente al uso de dispositivos de vigilancia y de grabación de sonidos (art 89 LOPDGDD), así como ante la utilización de geolocalización en el ámbito laboral (art 90 LOPDGDD), determinan la licitud del tratamiento de datos obtenidos a través de estos métodos. En tanto en cuanto, el uso de estos dispositivos de manera ilícita provocará que, como consecuencia, los datos obtenidos no sean válidos, y por tanto tratables.

Por último, el art 91 de la LOPDGDD regula los derechos digitales en la negociación colectiva y el art 88 de la LOPDGDD, el derecho a la desconexión digital en el ámbito laboral, que busca garantizar el adecuado disfrute de los periodos de descanso, así como la intimidad personal y familiar.

Con el objetivo de asegurar la preservación de estos derechos, se van a tener en cuenta diferentes criterios a la hora de realizar un control sobre las herramientas puestas a disposición de los empleados. Por un lado, como determina Mestre, J.M y Marrero, C. (2025, 29 de enero) se debe verificar la política establecida por la empresa sobre el uso de las herramientas electrónicas. Esta política puede ser de prohibición o de autorización. Dependiendo de la que se establezca, las consecuencias ante la vigilancia del empresario pueden variar. En caso de ser un régimen de autorización, como se determina en el art 87 de la LOPD previamente analizado, se deberá actuar conforme a lo pactado, y a los protocolos establecidos, protegiendo siempre la intimidad de los trabajadores. Por último, para poder garantizar de una manera efectiva esta protección, se deberá comunicar tanto a los trabajadores como a la representación de estos de la posibilidad de llevar a cabo controles sobre el uso de dichas herramientas (Mestre, 2025, 29 de enero).

CAPÍTULO 3: Métodos de control del empresario: video vigilancia

En este apartado se profundiza en el uso cada vez más común de dispositivos de video vigilancia en el ámbito laboral, analizando este fenómeno desde una perspectiva normativa, jurisprudencial y doctrinal. Se estudiaré la convergencia de estos derechos en los diferentes métodos de vigilancia y control a los que el empresario puede recurrir, a la hora de ejercitar este poder esencial en su ámbito de actuación. Ante posibles vulneraciones de los derechos fundamentales afectados, se deberá buscar el cumplimiento del principio del equilibrio de derechos constitucionales, el cual, hace necesaria la superación del "juicio de proporcionalidad" (SSTC 14/2003, 89/2006 y 96/2012) de dicha medida de control (Jesús Enrique Pascual López, 2023, pág. 16), así como la información previa al trabajador de que va a ser sometido a ese control. Más adelante se verá la evolución jurisprudencial de estas exigencias.

La Agencia Española de Protección de Datos (de ahora en adelante, AEPD) desempeña un papel fundamental en la protección de datos personales y la salvaguarda del derecho de intimidad de los ciudadanos. Su función por excelencia es garantizar el cumplimiento de la normativa vigente como el RGPD y la LOPDGDD, a las que se hizo amplia referencia *supra*. En sus actividades de asesoramiento y supervisión controla la transparencia de las empresas, y los organismos públicos. En un informe publicado en el año 2021 sobre la protección de datos en las relaciones laborales, estableció que "la empresa no necesita el consentimiento de las personas trabajadoras para establecer los controles de acceso que estime convenientes, pero debe respetar los derechos fundamentales" (AEPD, 2021). Este criterio es fruto de una larga historia jurisprudencial que comenzó otorgando grandes garantías a la protección de la intimidad de los trabajadores y ha acabado dotando al empresario de una libertad casi total, sin siquiera ser un requisito necesario en esta práctica la información previa a los afectados.

3.1 La proporcionalidad como criterio de enjuiciamiento

Inicialmente, se destaca la importancia de equilibrar las facultades del empresario y las de los trabajadores, así pues, se establecen criterios claros de proporcionalidad y justificación que se verán reflejados años después en la normativa europea y legislación nacional, aunque poco a poco irán devaluándose, quedándose atrás como requisito secundario. En uno de los primeros casos emblemáticos y determinantes para la jurisprudencia sobre esta cuestión, el Tribunal Constitucional, (STC 186/2000 de 10 de julio), recibe recurso de amparo por el cual el recurrente, alega la vulneración de diversos derechos fundamentales.

En este caso, el demandante, cajero de "ENSIDESA", es grabado en su puesto de trabajo ante sospechas y rumores de llevar a cabo actividades irregulares en el seno de la empresa. La dirección, instala un circuito cerrado de televisión enfocando solamente a las tres cajas registradoras y al mostrador de paso de todas las mercancías en el radio de acción aproximado que alcanzaba el cajero. Al instalar dichos dispositivos se constata que el trabajador llevaba a cabo actividades ilícitas y contrarias a las obligaciones de su puesto quedándose con el dinero que obtenía de cambios de artículos de ropa, que no tenían que ser devueltos.

En el recurso, el trabajador alega la vulneración de derechos a la intimidad personal y a la propia imagen (art. 18.1 CE), el derecho a la tutela judicial efectiva (art.24.1 CE), y el derecho a la igualdad; por otro lado, alega la vulneración del derecho de acceso a los recursos (art 24.1) y, del derecho a utilizar los medios de prueba pertinentes para la defensa (art. 24.2 CE).

Las dos últimas pretensiones se desestiman rápidamente, ahora bien, cabe entrar en el análisis interpretativo que el Tribunal hace del resto de las cuestiones planteadas. Así pues, se reitera, como ya se ha mencionado previamente, la unión indudable existente entre el derecho a la intimidad personal (art. 18.1 CE), y la dignidad de la persona (art 10.1 CE), pues el primero se consagra como derecho fundamental "vinculado a la propia personalidad y que deriva sin ningún género de dudas" del segundo (FJ.5).

El demandante argumenta que la prueba documental propuesta por el demandado, consistente en ocho videos, vulnera su derecho a la intimidad (art 18.1 CE) y a la propia imagen, siendo, por tanto, nula. Así pues, al haberse utilizado pruebas nulas para fundar las decisiones de los órganos judiciales, se vulnera, el derecho a la tutela judicial efectiva del demandante (art 24.1 CE). Según el demandante, esto es así porque dichas cámaras no se limitaron a vigilar la actividad laboral del empleado, sino que captaron imágenes registrando actos de su propia intimidad. Además, fundamenta esta alegación en la falta de conocimiento de dicha medida de vigilancia por el Comité de Empresa y los trabajadores afectados por la medida. Por otro lado, se pone en duda la validez y autenticidad de las grabaciones argumentando que "se trata de pruebas fácilmente manipulables" que "no fueron grabadas con la presencia de fedatario público o judicial" (STC 186/2000 de 10 de julio).

Para contestar a todas las cuestiones planteadas, el Tribunal Constitucional establece que, "la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad" (FJ, 6º). En el juicio sobre la existencia de dicha proporcionalidad, el Tribunal se basa en lo dispuesto en diversa jurisprudencia (STC 66/1955, de 8 de mayo. FJ 5; STC 55/1996, de 28 de marzo, FJ 6; STC 207/1996, de 16 de diciembre., FJ 4 e), y STC 37/1998, de 17 de febrero., FJ 8, entre otras). Así pues, será necesario constatar si se cumplen los tres requisitos o condiciones siguientes (FJ, 6º):

a) Juicio de idoneidad: si tal medida es susceptible de conseguir el objetivo propuesto.
b) Juicio de necesidad: si tal medida es necesaria, pues no existe ninguna otra más moderada para la consecución de tal propósito con igual eficacia.
c) Juicio de proporcionalidad en sentido estricto: si tal medida es equilibrada al derivarse de ella más beneficios para el interés general que perjuicios para el resto de los bienes o valores en conflicto.

Según Fernández Avilés y Rodríguez-Rico Roldán la existencia de este juicio de proporcionalidad en el ámbito laboral es un indicativo claro de la forma en la que, la doctrina constitucional no otorga el mismo peso a los intereses de los trabajadores y a los de la empresa. En consecuencia, "el equilibrio entre los derechos fundamentales del trabajador y el poder de dirección del empresario no se encuentra en un punto medio entre ambos, ya que no poseen la misma relevancia constitucional" (2016, pág. 55 y 56).

En el caso que nos concierne el Tribunal Constitucional establece que la medida adoptada por el empresario es idónea, pues es susceptible de obtener el objetivo establecido, en este caso, verificar si el trabajador cometía las irregularidades sospechadas. Además, es necesaria, al servir de prueba lícita de las irregularidades cometidas. Y, por último, las se estiman equilibradas las medidas, al limitarse la grabación a la zona de la caja, el movimiento de las manos de los empleados y durante un tiempo limitado para comprobar que no se trataba de un simple hecho aislado (FJ. 7º). Así pues, al cumplirse todos los requisitos del juicio de proporcionalidad se puede afirmar que la medida adoptada por el empresario en este caso está justificada, y por ello, no implica una vulneración del derecho de intimidad del trabajador.

Al no considerarse nulas las grabaciones pues no puede afirmarse que dicha prueba hubiese sido ilícitamente obtenida, carece de fundamento la pretensión relacionada con la vulneración del derecho de tutela judicial efectiva, quedando completamente desestimada por el Tribunal (FJ, 8º).

Sin entrar a valorar si el empresario informó debida y diligentemente al trabajador sobre las medidas adoptadas, los tribunales aceptan la validez del control establecido por la empresa basándose únicamente en el cumplimiento o no del test de proporcionalidad. El

uso de este test es necesario por existir un conflicto de derechos que no se puede resolver de otra manera. En palabras de López de la Fuente, este juicio de proporcionalidad analizado en la STC 186/2000, entre otras, se convierte en el "canon de enjuiciamiento" de los tribunales (2020).

Si bien el uso de este test no desaparece, irá evolucionando con el tiempo pues, se irá dejando en un segundo plano, por detrás de la obligación del empresario de informar al trabajador de manera previa y expresa, así como justificada[1]. Por otro lado, se puede ver como en este caso se hace únicamente referencia al derecho a la intimidad, omitiendo posibles vulneraciones del derecho a la protección de datos, precisión que será esencial para el enjuiciamiento de casos futuros.

3.2 Diferencia entre derecho de intimidad y derecho de protección de datos

A propósito del análisis jurisprudencial de la videovigilancia como medida de control dentro del ámbito de los poderes del empresario, cabe estudiar la STC 292/2000 de 30 de noviembre, pues clarifica la interpretación y alcance de ciertas disposiciones de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Cabe recordar que esta ley fue derogada por la LOPDGDD de 2018, pero, es esencial para un estudio exhaustivo de la materia.

El Defensor del Pueblo interpone recurso de inconstitucionalidad contra ciertos incisos de los arts. 21.1, 24.1 y 24.2 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (en adelante, LOPD) por vulnerar los arts. 18. 18.1, 18.4 y 53.1 CE. Ante el riesgo que suponen las nuevas tecnologías para la divulgación de los datos personales del individuo son necesarias determinadas garantías que aseguren al ciudadano la capacidad para controlar el flujo de dicha información. Atendiendo a la regulación que se impugna en este recurso, se aprecia como el consentimiento por parte del trabajador para el tratamiento de sus datos, es desde el principio un concepto o requisito regulado de una forma cuestionable. Se encuentran contradicciones en la ley que otorgan diferentes grados de importancia a esta característica que a mi juicio es esencial.

[1] Asunto Copland vs Reino Unido del Tribunal Europeo de Derechos Humanos (en adelante TEDH)

El inciso del art. 21.1[2] que se impugna es el siguiente: "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso". Este artículo hace referencia a la comunicación de los datos de carácter personal obtenidos entre distintas Administraciones Públicas. Según esta disposición, está prohibido el intercambio de dichos datos en el caso de que las competencias de las Administraciones Publicas sean de diferentes materias. A esta prohibición la ley impone dos excepciones, el inciso objeto de estudio por el Defensor del Pueblo, y los fines históricos, estadísticos o científicos que pueda tener del tratamiento posterior de dichos datos.

Alega el Defensor del Pueblo que, este inciso prevé una excepción al art 11 LOPD [3], según el cual, será necesario el consentimiento del interesado a menos que dicha cesión

---

[2] El art. 21.1 se la LOPD establece lo siguiente: "Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo **cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o** cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos."

[3] El artículo 11 de la LOPD regula la comunicación de los datos personales obtenidos en los siguientes términos: "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.
3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

esté regulada por Ley. Así pues, argumenta que el inciso del art. 21.1 es inconstitucional al permitir la cesión de datos para fines diferentes para los que habían sido recabados, sin consentimiento del interesado y basándose en una norma de rango inferior a la ley, pues permite que una disposición reglamentaria imponga un límite a un derecho fundamental, vulnerando la reserva de ley recogida en el art 53 de la CE.

Por otro lado, el art 24.1 y 2[4], determina el Defensor del Pueblo, no respetan el contenido esencial del art. 18.4 CE pues no permiten garantizar el honor y la intimidad de los ciudadanos, estableciendo límites a estos derechos sin la necesaria cobertura constitucional. Así pues, tanto la frase "impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas y o administrativas" como el apartado 2 del art. 24 en su totalidad, a su juicio deben ser declarados inconstitucionales. Estas disposiciones se amparan en el interés público para dar casi total libertad a la privación del derecho de rectificación y cancelación del afectado, regulado en el art 15 de la misma ley.

El recurso es estimado, y el Tribunal declara inconstitucional el inciso del art 21.1 LOPD, pues esta ley no fija por sí misma como queda establecido en el art 53 CE, los límites al derecho a permitir la cesión de datos entre Administraciones Publicas cuando los fines sean diferentes a los que motivaron su recogida. Solo se ha limitado a identificar la norma que puede regularlo, y por tanto, pudiendo ser esta de naturaleza reglamentaria, siendo

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores".

[4] 1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

desde luego contrario a la Constitución (FJ 14º). De esta manera, el Tribunal resalta la necesidad de que las posibles limitaciones del derecho a la intimidad estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas, estando expresadas con precisión todas y cada una de las limitaciones. Así pues, "la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. No es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales" (FJ 16º). Además, los motivos de limitación, determina el Tribunal Constitucional, se establecen con tal grado de indeterminación que "deja excesivo campo de maniobra a la discrecionalidad administrativa, incompatible con las exigencias de la reserva legal en cuanto constituye una cesión del poder normativo que defrauda la reserva de ley" (FJ 18º). Declara, por tanto, los incisos del art 24.1 y 24.2 inconstitucionales.

Teniendo en cuenta la argumentación del Defensor del pueblo como base de la resolución de este asunto, el tribunal constitucional establece un precedente que será esencial para la resolución de asuntos sobre la misma materia en el futuro. Desde un principio acepta la impugnación de inconstitucionalidad que desarrolla el recurrente, pero haciendo una diferenciación clara entre el derecho a la intimidad y el derecho a la protección de datos, estableciendo el precedente que se usará desde ese momento en adelante para enjuiciar aquellos casos que nos atañen.

De esta manera, establece el Tribunal, "la función del derecho a la intimidad es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad" (FJ 6º). Así pues, el derecho a la intimidad permite resguardar determinados datos e información del conocimiento ajeno no deseado. Sin embargo, el derecho a la protección de datos persigue garantizar a la persona dueña de dichos datos, el poder de control y disposición sobre estos, en cuanto a su uso y destino, esto se garantiza evitando el "tráfico ilícito y uso lesivo para la dignidad y derecho del afectado" (FJ 6º).

Por tanto, a diferencia de la finalidad del derecho de intimidad de resguardar determinados datos e información del conocimiento ajeno, el derecho a la protección de datos garantiza a los individuos el poder de disposición y control sobre dichos datos. Mientras el primero supone un derecho de naturaleza negativa, el segundo es un derecho de naturaleza positiva. Además, el objeto de este derecho, como determina el Tribunal Constitucional es más amplio que los datos íntimos de la persona, porque alcanza a cualquier tipo de dato personal sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, sino los datos de carácter personal (Fj 6º). Este derecho atribuye al sujeto el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (STC 73/1982, FJ 5; STC 110/1984, FJ 3; STS 89/1987, FJ 3; STS 231/1988, FJ 3; STS 197/1991, FJ 3, y en general las SSTC 134/1999, 144/1999 y 115/2000).

Así pues, el Tribunal Constitucional establece la necesidad de establecer claramente y de manera justificada por ley, cualquier excepción o límite a los derechos fundamentales de intimidad y autodeterminación informática, declarando, por tanto, inconstitucionales las disposiciones que permitan la cesión de datos personales sin las garantías adecuadas. Con esta diferenciación en mente los tribunales se aproximarán a este tipo de conflictos de derechos desde la perspectiva de la protección de los datos personales de los afectados, dejando de lado alegaciones basadas única y exclusivamente en el derecho fundamental a la intimidad y vida privada que se venía haciendo hasta el momento. Esta nueva perspectiva se verá en funcionamiento en la sentencia analizada en el siguiente apartado.

3.3 Obligación de informar al trabajador de la existencia de dispositivos de vídeo vigilancia y su finalidad

En este apartado se analizará la STC 29/2013 de 11 de febrero, por la importancia que supuso en su momento al cambiar radicalmente la jurisprudencia relativa a los dispositivos de vigilancia como medida de control del empresario.

Lo esencial de esta sentencia es que la diferenciación que el tribunal ya había hecho entre el derecho a la intimidad y el derecho a la protección de datos se materializa como el criterio a la hora de enjuiciar estos casos. Así pues, como ya se mencionó *supra* a partir

de ese momento, el debate sobre la videovigilancia en el ámbito laboral se aproximará desde la perspectiva de la autodeterminación informativa y el derecho a la protección de datos.

El Tribunal Constitucional, estando vigente todavía la LOPD, establece la necesidad de cumplir un requisito fundamental a la hora de hacer uso de dispositivos de videovigilancia, la información. Esta debe ser "previa, clara, expresa, precisa e inequívoca para los trabajadores, expresando su finalidad del control, dejando claro si en su caso, se pretenden usar dichas grabaciones para la imposición de sanciones disciplinarias" (Alonso, 2023). Por tanto, se declara la ilicitud del uso de grabaciones instaladas con la finalidad de garantizar la seguridad de los bienes y las personas, para una finalidad distinta, en este caso, el control de la actividad del trabajador.

El TC establece una conexión directa entre el derecho a ser informado y el derecho a la intimidad y a la limitación de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos. Este derecho se vería vulnerado, según lo dispuesto por el TC si se incumple el deber de informar al trabajador, lo cual provocaría que no fuera necesario llevar a cabo el test de proporcionalidad para ponderar la constitucionalidad de la medida, pues la medida sería inmediata e indudablemente, ilícita (Caballeros, 2024, pág. 25-26). Si por el contrario se estima no vulnerado este derecho, se procedería a realizar dicho test. Así pues, se puede observar, como determina Goñi Sein, que en esta sentencia se valora por primera vez la prueba de la video vigilancia desde la perspectiva de la protección de datos (2017, pág. 15). Como se ha dicho previamente, el criterio utilizado hasta entonces, analizado a través de la STC 186/2000 de 10 de julio, era el del test de proporcionalidad, que analizaba la medida establecida en términos de idoneidad, necesidad y estricta proporcionalidad. En este caso, el fator fundamental que determinará la licitud de las medidas de vigilancia del empresario será la existencia o no de información previa, por ser una medida que implica el tratamiento de datos personales, siendo pues, aplicable la normativa relativa a la protección de los datos personales, en ese momento la LOPD.

Los hechos que traen causa a esta conclusión se suceden dentro del ámbito de la Universidad de Sevilla. El recurrente, profesor y director de departamento de la institución, se convierte en sujeto de sospecha por incumplimiento de jornada laboral.

Ante dicha sospecha el director de recursos humanos encarga a los jefes de seguridad usar cualesquiera sean los medios necesarios, incluidos las cámaras de vigilancia, para constatar si efectivamente, dicha vulneración se estaba cometiendo durante los meses de enero y febrero de 2006. Como resultado de esta tarea se determina que el trabajador entraba a su puesto de trabajo con retrasos de entre media y varias horas, aunque en su registro figuraba como puntual. Por otro lado, a finales de febrero, el trabajador pidió licencia por asuntos particulares, ausentándose de su puesto de trabajo, cuando dicha licencia había sido denegada.

La apertura de expediente disciplinario y la suspensión de empleo y sueldo del trabajador concluyen en la presentación de demanda por el trabajador, considerando que el expediente disciplinario era nulo pues estaba basado en pruebas ilegalmente obtenidas, mediante el uso de vídeos pese a no existir autorización expresa para tal control laboral. Contra esta alegación las Universidad de Sevilla prueba que cuenta con autorización expresa de la Agencia Española de Protección de Datos para controlar el acceso del personal de la comunidad universitaria, así como para hacer uso de dichos soportes informáticos.

A juicio del recurrente, el contenido del derecho a la protección de datos fue vulnerado con la utilización no consentida ni previamente informada de las grabaciones para un fin, desconocido por el afectado, de control de su actividad laboral.

El tribunal comienza resolviendo las dudas sobre la procedencia de incluir los datos obtenidos en forma de imagen dentro de una grabación, en los datos personales del individuo a los que se les debe garantizar una especial protección. El art 3.1 de la LOPD define los datos personales como “cualquier información concerniente a personas físicas identificadas o identificables”. En tanto en cuanto las grabaciones obtenidas por las cámaras de videovigilancia constituyen la reproducción de ciertos datos incluidos en el alcance del art 18.1 de la CE, por ser suficientes para identificar o permitir identificar a la persona, permitiendo su representación física y obedeciendo a una información fotográfica sobre su identidad, se estiman incluidos en el alcance de esta norma.

Haciendo expresa referencia a la STC 292/2000 de 30 de noviembre ya analizada, el TC pone en práctica la diferenciación entre el derecho a la intimidad y el derecho a la

protección de datos. Así pues, parece establecer la existencia de dos derechos a la intimidad, uno genérico (art. 18.1) y otro más específico (art. 18.4), el cual requiere un ámbito más amplio de protección y que se encuentra intrínsecamente ligado a la facultad inherente del individuo de disposición de sus datos personales. Para poder ejercer ese derecho de disposición, reconocido en la STC 292/2000 de 30 de noviembre, es indispensable la salvaguarda del derecho de información del que es sujeto el individuo. Por ello, "ese derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento" (STC 29/2013, de 11 de febrero).

No se acepta, por tanto, una información genérica si no que, el tratamiento de los datos de carácter personal como las grabaciones de videovigilancia en las que se identifique al individuo, podrán ser tratados, si se hubiese informado previamente a la obtención de dichos datos, de manera clara y explicita al empleado, de la finalidad "supervisora laboral" (FJ 8º) de la captación de dichas imágenes. Por esto, en el caso analizado, dice el TC, se "vulneró el art 18.4 de la CE" (FJ 8º).

Se puede apreciar, el cambio de criterio en la jurisprudencia a la hora de dilucidar si una medida llevada a cabo por el empresario con el fin de ejercer su poder de vigilancia es licita o no. Por un lado, el criterio del test de proporcionalidad que fundamenta el caso de "ENSIDESA" (STC 186/2000) queda en un segundo plano, pues si no existe información previa, explícita, clara y precisa a los trabajadores, la medida queda calificada como inconstitucional directamente, siendo nulas las consecuencias que hubieran acarreado para el trabajador. A partir de esta sentencia, aunque el consentimiento del trabajador no sea necesario, se debe informar a aquél de la existencia de videovigilancia y de los fines que se persiguen con esta (Caballeros, 2024, pág. 24-25), en defecto de dicha información se incurriría en la vulneración del art 18.4 de la CE.

En este caso, el Tribunal hace hincapié en la distinción entre derecho el derecho a la intimidad y el derecho a la protección de datos, que se pone de manifiesto en la STC 292/2000 de 30 de noviembre. Reproduciendo las palabras de Inmaculada Jiménez-Castellanos Ballesteros, la STC 29/2013 puede resumirse en que "la omisión del deber de información previa al trabajador supone una lesión del contenido esencial del derecho

fundamental a la protección de datos que puede restringir el ejercicio de las facultades que lo conforman" (Castellanos, 2017, pág. 153).

3.4 Inicio de la devaluación de los derechos fundamentales en riesgo

Partiendo de los criterios establecidos por el TC anteriormente, hay que hacer especial referencia a la STC 39/2016 de 3 de marzo. En junio de 2012, la demandante, trabajadora de BERSKA BSK España, S.A., es despedida por trasgresión de la buena fe contractual. Las cámaras de videovigilancia habían captado imágenes de la demandante, apropiándose de dinero y realizando operaciones de devolución falsas. La cámara fue instalada sin comunicación previa a los trabajadores a raíz de las sospechas sobre la concurrencia de estas actividades irregulares, ahora bien, se colocó un distintivo informativo en el escaparate.

La demandante de amparo interpuso demanda contra BERSKA BSK ESPAÑA, S.A. solicitando la nulidad del despido por atentar contra su honor, intimidad y dignidad. Alegó que, si bien tenía conocimiento de la existencia de las cámaras, no se le había informado con carácter previo, explicito, claro e inequívoco de la instalación de dichos dispositivos y por tanto tampoco de su finalidad de control, disciplinaria y sancionadora. Así pues, argumenta que el criterio establecido en la STC 29/2013 de 11 de febrero, se incumple, y, por tanto, la empresa incurre en una vulneración clara del derecho a la protección de datos personales del art 18.4 de la CE.

La empresa, por el contrario, se fundamenta en la jurisprudencia establecida por el mismo tribunal en su STC 186/2000, determinando que la medida, cumple los requisitos de test de proporcionalidad. Así pues, alega que el establecimiento de las cámaras de videovigilancia sin informar previamente al trabajador era idóneo, necesario y estrictamente proporcional para los objetivos que pretendía conseguir, prevenir hurtos y vigilar la zona de las cajas.

En el antecedente de hecho primero, se determina que, con la resolución de este caso, el TC busca aclarar su doctrina relacionada con la videovigilancia en el ámbito laboral, y el alcance de la información que se debe facilitar a los trabajadores sobre la finalidad de estas medidas, si es suficiente la información general o, si, por el contrario, la información proporcionada tiene que ser de carácter específico. En efecto, esta sentencia aclara la

posición del Tribunal en cuanto a estas cuestiones, pero a la vez inicia un proceso de devaluación de los derechos fundamentales del individuo, pues se decantan por concluir, como veremos, que un simple distintivo es suficiente para dar por cumplido el deber de información, no siendo necesario tampoco el consentimiento por parte de los afectados.

En este caso se puede observar como la fuerza de un distintivo de la Agencia Española de Protección de Datos (de ahora en adelante AEPD), es mayor que la del mismo conocimiento del afectado. Se basa el Tribunal, en la Instrucción 1/2006, de 8 de noviembre, de la AEPD sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. La Instrucción establece los requisitos que deben cumplir dichos distintivos para ser prueba válida y suficiente del conocimiento de los trabajadores acerca de las medidas llevadas a cabo. Según el art 3 la empresa deberá "colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados" y "tener a disposición de los/las interesados impresos en los que se detalle la información prevista en el art. 5.1 de la Ley Orgánica 15/1999" (art. 3 Instrucción 1/2006, de 8 de noviembre de la AEPD). Debe contener una referencia a la LOPD, a la finalidad del tratamiento de los datos obtenidos, la "zona vigilada" y la identificación del responsable ante quien se pueden ejercitar los derechos reconocidos por la LOPD (Goñi, 2016, pág 288). Se determina pues, que el art. 18.4 CE no ha sido vulnerado en este caso pues, la trabajadora podía conocer de la existencia de las cámaras y su finalidad.

Ahora bien, en este caso no estamos ante una medida general y ordinaria puesta en marcha por la empresa en uso de su poder de vigilancia sino de una medida ad hoc, individualizada hacia el puesto de trabajo concreto de la demandante para confirmar las sospechas de un incumplimiento grave, habiéndose instalado un distintivo informativo. Así pues, se podría decir que la simple existencia de una sospecha faculta al empresario para limitar los derechos fundamentales del trabajador ejerciendo esta facultad de control.

Aunque en su argumentación jurídica establece que "el consentimiento del afectado es, por tanto, el elemento definidor del sistema de protección de datos de carácter personal", en la realidad la conclusión del fallo de esta sentencia es todo lo contrario, pues devalúa dicho consentimiento, convirtiéndolo en mero conocimiento, para dejarlo en un segundo plano, por detrás de la voluntad y capacidad de control del empresario. Como explica

Francisco Andrés Valle Muñoz, se cambia la tendencia jurisprudencial para determinar que la grabación de imágenes mediante cámaras situadas en un lugar visible (en este caso frente a una de las cajas registradoras) y con un dispositivo informativo (un cartel de la AEPD) de la empresa de vigilancia contratada, no vulneraría el derecho de protección de datos de carácter personal si existen sospechas de la comisión de actos ilícitos por parte de los trabajadores (2021, pág. 38).

Ante este cambio de criterio radical, José Luis Goñi expresa su apoyo hacia Xiol Ríos, magistrado autor de uno de los votos particulares de la sentencia, opinando que tiene que haber un interés legítimo y además una estricta observancia del principio de proporcionalidad en estos casos. Y que "ese interés legítimo no puede justificarse en «la mera utilidad o conveniencia para la empresa» como tiene declarado el TC en las SSTC 98/2000 y 186/2000" (Goñi, 2016, pág. 289). Critica vehementemente que sea el criterio de un órgano administrativo, la AEPD, el que se tenga en cuenta en una interpretación legislativa a la hora de dilucidar el alcance de ciertos derechos fundamentales como es el de protección de datos personales (art. 18 CE), sin siquiera adaptar ese criterio al ámbito que nos ocupa, el ámbito laboral. De la misma manera que Goñi, Xiol Rios en su voto particular de la sentencia, determina que no se puede afirmar que el deber de información se cumpla a través de este simple aviso al público, ya que "dinamita" (2.f) el derecho fundamental a la protección de datos. El aviso al público pasa por encima la previsión del art 5 de la LOPD que prevé la obligación de informar a "todos los interesados". Esta falta de información lesiona el derecho del art. 18.4 CE puesto que, afecta a su contenido esencial, al hacerlo ineficaz, carente de todo su sentido práctico e irreconocible (2.e).

No parece aceptable pues, que el mismo requisito que se usa para obtener grabaciones de videovigilancia sobre colectivos desconocidos, se pueda aplicar igualmente y sin ningún matiz, a un grupo específico o a determinados individuos, dentro de una relación de subordinación. No parece razonable pues, que la información pueda ser recogida en un mero indicativo y no dentro de las exigencias establecidas en el art 5 de la LOPD, para el resto de las medidas de control. Lo que se consigue con esta sentencia es un retroceso claro en los criterios que se había establecido en 2013. Además, parece perderse una oportunidad excelente para establecer claramente qué requisitos habría que seguir o en qué casos sería posible instalar cámaras ocultas ante sospechas de comisión de algún ilícito por algún empleado en el seno del lugar de trabajo.

El hecho de que el Tribunal deduzca que no es necesario el consentimiento del trabajador para el tratamiento de las imágenes obtenidas, se fundamenta en que "se trata de una medida dirigida a controlar el cumplimiento de la relación laboral (art 20.3 ET)" (Jiménez-Castellanos, 2017, pág. 144) Así pues, se trata de lo que la doctrina ha denominado "un control de irregularidad, no de regularidad laboral" (Sepúlveda, 2016, pág. 222) estando la medida orientada a constatar ciertas irregularidades basadas en sospechas o indicios.

Se puede ver como la jurisprudencia constitucional ha evolucionado desde una tesis más protectora y garantista de los derechos fundamentales de los trabajadores a una posición que los desestima buscando la consecución de los objetivos empresariales. Se pasa de la necesaria comunicación expresa y clara de las medidas y sus fines a un simple conocimiento genérico. Ahora bien, cabe destacar, como dice Ferrando García, que en ningún caso se admitiría el "test de honestidad" o la provocación al trabajador a incurrir en una irregularidad para grabar el incumplimiento, siendo esta actuación de mala fe (2016, pág. 47).

3.5 Jurisprudencia del Tribunal Europeo de Derechos Humanos: Asuntos López Ribalda I y II contra España, Asunto Barbulescu contra Rumanía

El recorrido jurisprudencial que se ha venido haciendo no estaría completo si no se tuviera en cuenta la doctrina y criterios internacionales. El caso López Ribalda y otros contra España, desarrollado en el Tribunal Europeo de Derechos Humanos, llega a ciertas conclusiones que solucionan algunas de las dudas surgidas con la STC 39/2016 de 3 de marzo.

Ante sospechas de hurto y una serie de pérdidas continuadas, en uno de sus establecimientos, la empresa (Mercadona), decide instalar unas cámaras de videovigilancia ocultas y sin informar previamente a los afectados. Establece la exposición de hechos de la sentencia que "se informó al personal del supermercado de la instalación de las cámaras visibles [pero no] fueron informados de las cámaras ocultas" además "la empresa había notificado a la AEPD su intención de instalar cámaras [ante lo que se señaló] las obligaciones de proporcionar información en virtud de la legislación sobre protección de datos personales". Así pues, se procedió a instalar un cartel distintivo

en la tienda “que indicaba la presencia de cámaras [...] pero no su ubicación ni el contenido preciso” (TEDH, 2019).

A través de estas grabaciones se confirmaron las sospechas sobre cinco trabajadoras que habían estado llevando a cabo las actividades descritas. Fueron despedidas y tres de ellas llegaron a un acuerdo transaccional con la empresa, en los términos siguientes: si las empleadas no interponían demanda ante los tribunales laborales contra la empresa, la empresa no interpondría demanda contra las trabajadoras ante los tribunales penales. Pese a ello, todas ejercitan acción por despido nulo al entender que se ha vulnerado su derecho s la intimidad.

Tanto en primera como en segunda instancia, las pretensiones de las demandantes son desestimadas y se determina, que no ha habido violación de derechos de privacidad, y las pruebas, al haber sido obtenidas de manera ilícita, no serían nulas. En cuanto a las tres demandantes que habían firmado el acuerdo con la empresa comprometiéndose a no demandar, se determina que dicho acuerdo, no fue firmado bajo coacción, como alegaban las demandantes. Así pues, los TSJ de Cataluña consideran procedentes los despidos y el Tribunal Constitucional no admite el recurso de amparo.

El TEDH determina a grandes rasgos que se ha vulnerado el derecho al respeto de la vida privada de las trabajadoras, garantizado por el artículo 8 del Convenio[5], y que los tribunales nacionales habían incumplido su obligación de garantizar la protección efectiva de ese derecho. En virtud del artículo 6 del Convenio[6], las demandantes alegan que la

[5] Art 8 del Convenio Europeo de Derechos Humanos:
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[6] Art. 6 del Convenio Europeo de Derechos Humanos:
1. Toda persona tiene derecho a que su causa sea oída equitativa, públicamente y dentro de un plazo razonable, por un Tribunal independiente e imparcial, establecido por la Ley, que decidirá los litigios sobre sus derechos y obligaciones de carácter civil o sobre el fundamento de cualquier acusación en materia penal dirigida contra ella. La sentencia debe ser pronunciada públicamente, pero el acceso a la Sala de Audiencia puede ser prohibido a la prensa y al público durante la totalidad o parte del proceso en interés de la

prueba obtenida mediante la videovigilancia era inadmisible. Por último, las dos demandantes que en su momento habían firmado el acuerdo con la empresa, alegan la nulidad del acuerdo por haberse firmado bajo coacción. El TEDH estima la primera pretensión.

Así pues, la clave de su razonamiento radica en que la normativa nacional española, que regula las cámaras de videovigilancia, exige que se informe mediante un letrero de la existencia de la videovigilancia, criterio amparado por la jurisprudencia nacional constitucional (STC 39/2016) y por ello, crea una expectativa razonable de privacidad para los trabajadores, que, al no informar sobre el uso de dichas medidas, se incumple (Alfaro, 2018). La existencia de una regulación clara sobre el derecho de cada uno de los sujetos a ser informado de la existencia de las medidas, la finalidad que persiguen y la posibilidad de establecer videovigilancia encubierta, hace que los recurrentes tengan una expectativa razonable de privacidad. Consecuentemente, según la Sala Tercera del TEDH, al instalar las cámaras y usar sus grabaciones con objetivos disciplinarios y sancionadores vulnera esa expectativa de privacidad y por tanto el art 8 del CEDH.

Dicha decisión es recurrida y pasa a conocer del asunto la Gran Sala del TEDH. En esta instancia, se determina que "la expectativa razonable de una persona respecto a su

---

moralidad, del orden público o de la seguridad nacional en una sociedad democrática, cuando los intereses de los menores o la protección de la vida privada de las partes en el proceso así lo exijan o en la medida considerada necesaria por el Tribunal, cuando en circunstancias especiales la publicidad pudiera ser perjudicial para los intereses de la justicia.

2. Toda persona acusada de una infracción se presume inocente hasta que su culpabilidad haya sido legalmente declarada.

3. Todo acusado tiene, como mínimo, los siguientes derechos:
a) a ser informado, en el más breve plazo, en una lengua que comprenda y detalladamente, de la naturaleza y de la causa de la acusación formulada contra él;
b) a disponer del tiempo y de las facilidades necesarias para la preparación de su defensa;
c) a defenderse por sí mismo o a ser asistido por un defensor de su elección y, si no tiene medios para pagarlo, poder ser asistido gratuitamente por un Abogado de oficio, cuando los intereses de la justicia lo exijan;
d) a interrogar o hacer interrogar a los testigos que declaren contra él y a obtener la citación y el interrogatorio de los testigos que declaren en su favor en las mismas condiciones que los testigos que lo hagan en su contra;
e) a ser asistido gratuitamente de un intérprete, si no comprende o no habla la lengua empleada en la Audiencia.

intimidad es un factor revelador, pero no necesariamente concluyente" (STEDH (Sección 3ª). Asunto López Ribalda y otros v. España, 9 de enero de 2018, ap. 57). Se puede observar cómo desde un inicio ya comienza a alejarse del criterio establecido por la Sala Tercera del TEDH. Así mismo dice que si bien en la mayoría de los casos el derecho a controlar el uso de los datos obtenidos implica la posibilidad de que un individuo se niegue a publicar su imagen, también abarca el derecho del individuo a oponerse a la grabación, conservación y reproducción de la imagen por parte de otra persona.

El tribunal, basándose en el Caso Barbulescu, numera los requisitos que se deben cumplir con el fin de garantizar la proporcionalidad de las medidas de videovigilancia en el ámbito laboral y por tanto la estricta observancia y cumplimiento del art. 8 CEDH (STEDH (Gran Sala). Caso Barbulescu vs. Rumanía 5 de septiembre de 2017, ap. 121):

a) Notificación al trabajador de la puesta en marcha de dichas medidas
b) Tenerse en cuenta el nivel de privacidad en la zona vigilada, y las limitaciones de tiempo y espacio, así como el número de personas que tienen acceso a los resultados.
c) Las razones de la imposición de dichas medidas tienen que ser justificadas
d) Si hubiera sido posible establecer un sistema de vigilancia basado en métodos y medidas menos intrusivas
e) Las consecuencias que estas medidas supondrán para el empleado.
f) Si se han proporcionado al empleado los medios adecuados para la aceptación de dichas medidas.

El Tribunal concluye que las autoridades españolas no vulneraron su obligación positiva de garantizar el respeto al art 8 CEDH, no existiendo ninguna violación de esta disposición. Además, determina, de la misma manera que la STC 29/2013 de 11 de febrero, que es necesario distinguir aquellas grabaciones hechas en lugares públicos, en los cuales la expectativa de privacidad es prácticamente inexistente, y lugares privados como vestuarios, baños e incluso despachos, donde la expectativa de privacidad del trabajador será elevada. En este caso, nos encontramos en la primera situación en la que la expectativa razonable de privacidad debe ser muy leve.

Además, el Tribunal, considera que la intrusión en la vida privada de las demandantes no alcanzó un alto grado de gravedad, pues se hizo durante un tiempo muy limitado (10 días) y pocas personas tuvieron acceso a la visualización de los vídeos (TEDH, 2019). Por otro lado, estima la medida necesaria, dadas las circunstancias para la consecución de su finalidad, descubrir a los responsables de los robos, pero también obtener pruebas para utilizarlas en los procedimientos disciplinarios contra ellos. Vemos que estos requisitos se asemejan al test de proporcionalidad del ordenamiento español en el cual se pondera la idoneidad, necesidad y estricta proporcionalidad.

Considera que el requisito de transparencia y el consiguiente derecho a la información son de carácter fundamental, sin embargo, y criterio que cabe destacar por su divergencia al nacional, "el suministro de información a la persona objeto de la vigilancia y su alcance constituye sólo uno de los criterios que deben tenerse en cuenta para evaluar la proporcionalidad de una medida de este tipo en un caso determinado". Al cumplirse el test de proporcionalidad del ordenamiento jurídico español, muy similar al establecido por la jurisprudencia internacional de este Tribunal, se estima que las medidas eran idóneas, necesarias y estrictamente proporcionadas. Así pues, se establece que “la existencia de una sospecha razonable de que se ha cometido una falta grave y la magnitud de las pérdidas identificadas en el presente caso pueden parecer una justificación de peso” contestando así a las dudas que se planteaban con la STC 39/2016.

Por lo tanto, el deber de información a los trabajadores queda en un segundo plano, en el caso en el que existan sospechas razonables de la comisión de algún ilícito por parte de estos. De esta manera la causa de la instalación de dispositivos de videovigilancia puede servir de justificación suficiente para llevar a cabo estas acciones de manera unilateral y no informada.

Ante el criterio establecido por el TEDH, cabe incluir las opiniones de catedráticos y expertos en la materia, así como las tesis doctrinales relevantes para estos asuntos, pues los cambios de criterio que ha sufrido el enjuiciamiento de estos casos en tan poco tiempo, es realmente extraordinario. Así pues, primero cabe hacer una breve explicación sobre la expectativa de privacidad razonable, lo que es y qué consecuencias tiene.

Hay que recordar que este test no supone una prueba o factor determinante a la hora de dilucidar la conclusión de estos casos, como ya se ha visto en el Asunto López Ribalda y otros vs. España, y como se aprecia en la argumentación jurídica del Asunto Barbulescu vs Rumanía, caso que se analizará posteriormente pues si bien, los antecedentes de hecho difieren, la argumentación que hace el TEDH será jurisprudencia muy relevante en cualquier caso relativo a los medios de control del empresario.

Por un lado, se plantean dudas en cuanto a la razonabilidad de la expectativa. ¿Razonable para quién? La gran mayoría de la doctrina parece estar de acuerdo con que esta razonabilidad debe estar enmarcada dentro del ámbito y alcance de una sociedad democrática, y en tanto en cuanto este es un principio aplicado por el TEDH, dentro del marco de aquellos estados que hubieran ratificado la CEDH (Álvarez, 2022). El pertenecer todos a un mismo marco normativo da por hecho que se comparten ciertas tradiciones políticas, ideas y perspectivas jurídicas y culturales, teniendo que ser pues, razonable para los estándares de una sociedad democrática. También cabe tener en cuenta que, este test permite meramente razonar si el art. 8 CEDH es aplicable al procedimiento y, aun así, tampoco parece ser imprescindible, pues el Tribunal de Estrasburgo no lo utiliza en todos los procedimientos en los que entra en juego el derecho a la vida privada (Álvarez, 2022). De todas formas, se puede observar como el propio Tribunal se echa para atrás con López Ribalda II y determina que no se dio esa vulneración de derechos de las trabajadoras, pues se habían cumplido con el deber de información previa regulado en la normativa nacional. Así, a pesar de la ausencia de información previa, el tribunal entiende que la existencia de sospechas razonables de que se ha cometido una infracción grave y la constatación de la magnitud de las pérdidas en la empresa, constituyen una justificación suficiente (López, 2020, ap 3.4.3.2., párrafo 2).

Como ya se adelantó supra, en relación a la jurisprudencia que debemos tener en cuenta al analizar esta cuestión, el Asunto Barbulescu contra Rumanía, es esencial para poder entender el criterio del TEDH. Este caso establece determinados requisitos que la empresa debe cumplir a la hora de establecer medidas de control que puedan entrar en conflicto con los derechos fundamentales de los trabajadores afectados.

La empresa donde trabaja Barbulescu, le otorga el consentimiento para que el demandante abra una cuenta de Yahoo messenger con el propósito de resolver preguntas a los clientes

de una manera más rápida y eficiente, y desarrollando pues, sus funciones como encargado de ventas, de forma más satisfactoria y directa para los clientes. Se explica en los antecedentes de hecho que el trabajador comienza a usar esta herramienta para fines personales, “los mensajes se referían a asuntos personales y algunos eran de naturaleza íntima” (STEDH (Gran Sala). Caso Barbulescu vs. Rumanía 5 de septiembre de 2017, ap. 21), incumpliendo una prohibición expresa de la empresa, motivo por el cual es despedido. El demandante impugna su despido, pretensión que es desestimada por el tribunal competente tanto en primera como en segunda estancia. Ante el TEDH el demandante alega que su despido se llevó a cabo violando su derecho a la vida privada y al secreto de la correspondencia, amparándose en el art. 8 del CEDH.

La sentencia detalla los requisitos que se deben cumplir por parte del empresario, la información a través de notificación, el grado de intromisión y alcance de supervisión, la existencia de razones legítimas, si existía la posibilidad de usar medidas menos intrusivas, las consecuencias del control establecido y si en todo momento de proporcionaron las garantías adecuadas a los trabajadores para proteger sus derechos.

Basándose en estos requisitos, el TEDH concluye que no se respetaron los derechos fundamentales del trabajador, pues no existió una protección por parte del estado del derecho a la vida privada y el secreto de las comunicaciones del demandante. No consiguieron una ponderación justa de los intereses en juego por lo que se aprecia una violación del art. 8 del CEDH.

Como se puede observar la inobservancia de la protección de la intimidad, protección de datos y vida privada del individuo en el seno laboral, no es solamente propio de nuestra jurisprudencia y tribunales, sino que esta tendencia existe incluso, internacionalmente.

3.6 Concepto de flagrancia

La STC 119/2022 de 29 de septiembre de 2022, es un ejemplo clave que pone de manifiesto la jurisprudencia actual respectiva a la videovigilancia en el lugar de trabajo. En este caso, la empresa Saltoki Araba, S.A. despidió a un trabajador "una transgresión de la buena fe contractual”. Los hechos causa del despido consistieron en la entrega de ciertos productos de la empresa a un tercer a cambio de una cantidad desconocida en metálico, sin entrega de ningún recibo. Ante estas conductas y teniendo las imágenes de

este intercambio en grabadas por las cámaras de videovigilancia, la empresa decide despedir al empleado, que consecuentemente demanda a la empresa por despido nulo, al considerar este, que las pruebas se obtuvieron vulnerando sus derechos fundamentales. El Juzgado de lo Social lo declara procedente haciendo referencia a la jurisprudencia analizada *supra* (STC 292/2000 y STC 29/2013), argumenta que "dichas cámaras de videovigilancia estaban expuestas dentro del local a plena vista de todos, con advertencia de su existencia a través del cartel informativo colocado en el exterior del local" y por tanto estima la pertinencia de las medidas. Más tarde el TSJ del País Vasco, revoca esta decisión declarándolo improcedente, haciendo, en este caso, referencia al asunto Barbulescu y López Ribalda. La empresa recurre en casación para la unificación de doctrina, pero el Tribunal Supremo inadmite el recurso, interponiendo la empresa recurso de amparo ante el Tribunal Constitucional alegando vulneración de du derecho a la tutela judicial efectiva.

El Tribunal concluye que no existió vulneración alguna, tanto del derecho a la intimidad como el derecho a la protección de datos. Determina que "la empresa había colocado el correspondiente distintivo en lugar visible, ajustado a las previsiones legales en materia de protección de datos" y que "las cámaras se utilizaron para comprobar un hecho concreto, que resultó flagrante, y sobre la base de una sospecha indiciaria concreta" (FJº 6º), y por tanto, descarta la vulneración del derecho a la protección de datos. En cuanto al derecho a la intimidad, el Tribunal lleva a a cabo el test de proporcionalidad, el cual estima superado, descartando que hubiera habido una lesión contra este derecho.

En este caso, el hecho de que el empresario no hubiera informado correctamente durante años pudiendo y debiendo hacerlo es completamente irrelevante. Así pues, en el seno de esta empresa ya se había despedido a un trabajador en el año 2014 tras las pruebas obtenidas por las mismas cámaras que contaban con el mismo distintivo que el que se trata de defender en el caso que nos ocupa. El tribunal determina que el hecho de que el trabajador conociera del despido producido en 2014 y los medios que se usaron para realizarlo no exime de responsabilidad a la empresa (FJ 6b).

Cabe tener en cuenta para la explicación de este concepto, jurisprudencia reciente del Tribunal Supremo, así pues, la STS 23/2025 de 14 de enero de 2025, trata el despido de una trabajadora de Stradivarius en País Vasco, tras constatarse ciertas "operaciones

anómalas" constitutivas de fraude interno. En este caso se concluye que "las cámaras de video vigilancia son visibles y los empleados conocen su instalación, habiendo sido informados los representantes de los trabajadores" (FJ 3º) y que la medida instalada adecuadamente verifica la comisión de un ilícito ante la sospecha flagrante del empresario, por lo tanto, siendo lícito el despido (FJ 3º). La conducta irregular fue captada en el momento de su ejecución, por tanto, el Tribunal determina que la grabación de esta conducta por las cámaras de videovigilancia

En ambas sentencias se usa el concepto de flagrancia como un mecanismo que da pie a la excepción de cumplir el deber de informar al trabajador. Como determina Miguel Ángel Cabellos, la flagrancia "deja de ser algo que es percibido a través de los sentidos mientras que ocurre, para ser cualquier cosa que quede grabada, a la que se tiene acceso en cualquier momento" (año, pág 37). "Todo es flagrante, aunque nadie lo haya visto" (Cabellos, año, pág 37), y cualquier sospecha dará la capacidad al empresario de ignorar el deber establecido por la ley para reemplazarlo con un simple distintivo en aluna pared, anulando cualquier garantía de los derechos de los trabajadores. Por su parte, y con razón, el magistrado de la Sala Social del Tribunal Superior de Justicia del País Vasco Florentino Eguaras, lamenta, a raíz de esta sentencia que "se ha omitido el reajuste que requiere el desequilibrio que existe entre empresa y trabajador" (2022), perspectiva pesimista, pero al mismo tiempo, realista del camino que sigue la protección de ciertos derechos en el ámbito laboral.

4. MÉTODOS DE CONTROL DEL EMPRESARIO: Geolocalización

En este apartado se hará un análisis en profundidad sobre el uso de dispositivos tecnológicos por parte de la empresa, con la finalidad de conocer en todo momento la localización de sus trabajadores, ya sea, mediante GPS (Global Positioning Systems) instalados en los vehículos, teléfonos o tabletas proporcionadas por el empresario. Se analizará esta cuestión atendiendo tanto al criterio jurisprudencial de los tribunales como al criterio riguroso de la AEPD, teniendo en cuenta que, como dice Fernández Orrico, constituye uno «de los dispositivos digitales menos regulados en el ámbito jurídico laboral» (2021, p. 331). Pese a su escasez regulatoria la realidad es que el uso empresarial

de estos dispositivos ha aumentado progresivamente en contextos en los que el trabajador debe ausentarse del lugar típico de trabajo para realizar sus funciones, convirtiéndose en un elemento esencial de estas labores. Así pues, se ha llegado a considerar que la manipulación consciente de estos aparatos de localización supondría una trasgresión de las obligaciones contractuales de carácter grave y por tanto un motivo legítimo de despido disciplinario (STSJ– de Canarias de 11 de mayo de 2015, rec. 834/2014 y STSJ de Murcia de 29 de marzo de 2022 (rec. 1084/2021), entre otras).

El artículo 90 de la LOPDPD[7] regula la relación entre el derecho a la intimidad y el uso de sistemas de geolocalización en el ámbito laboral. Se establecen limites, la puesta en práctica de esta facultad conforme a la ley, y la información de carácter previa, clara, e inequívoca hacia los trabajadores, sobre la existencia y características de estos dispositivos, así como sobre el ejercicio de sus derechos de acceso, rectificación, limitación del tratamiento y supresión.

Es cierto que el uso de dispositivos de geolocalización facilita la gestión del trabajo de una forma más eficaz, en empresas cuyo objeto es trasladarse de un sitio a otro para cumplir sus objetivos, esto es, repartidores, comerciantes, conductores, vigilantes de seguridad... Ahora bien, con la instalación de estos dispositivos nace el mismo conflicto analizado *supra*, entre el derecho del empresario a establecer las medidas que estime oportunas (art. 20.3 ET), amparado por su libertad de empresa (arts. 33 y 38 de la CE), y el derecho a la intimidad (art. 18.1 CE) y a la protección de datos personales (art. 18.4 de la CE) del trabajador. Dice Fernández Orrico, "que la vigilancia y control que la empresa efectúa sobre el trabajador [con el uso de estas medidas], debe focalizarse en si con tales dispositivos de geolocalización puede comprobar que ha cumplido con su actividad

[7] Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

laboral sin ir más allá, existiendo el peligro de sobrepasar ese límite, si se controla la conducta del trabajador" (2021, ap. 2, párrafo 3).

Cabe detenerse en el análisis de los datos obtenidos a través de dispositivos GPS y su naturaleza. Como se dijo previamente serán datos personales "cualquier información concerniente a personas físicas identificadas o identificables" (art 3.1 de la LOPD). Los datos que se pueden llegar a extraer si esta medida es implementada son de diversa índole, por un lado, saber en todo momento, la posición geográfica del sujeto, conocer los recorridos que efectúa, así como las paradas si existiesen. De la sistematización de estos datos se pueden llegar a extraer hábitos, el lugar de residencia, preferencias y gustos. Así pues, los peligros de la geolocalización no vienen tanto por los datos concretos que de manera individual muestran la posición de una persona, sino, como explica Polo Roca, "por la suma de estos datos que pueden mostrar una tendencia que permita predecir esos movimientos y comportamientos y, en consecuencia, lleven a conocer aspectos muy concretos de la esfera de la intimidad" (2020, pág. 152). Por tanto, la localización se puede calificar como dato personal del individuo y que por tanto se encuentra regulado por la LOPDGDD. La recogida, tratamiento o uso de estos datos, cuando se ponen a disposición del empresario por el mero hecho de la existencia de un vínculo laboral, puede llegar a vulnerar el derecho que el individuo tiene a la protección de sus datos, que en estos casos se puede definir como "el derecho a que los demás no sepan dónde está en cada momento y cuáles son sus movimientos o el derecho a no estar localizado de manera continua" (STEDH, 2010).

4.1 Información previa como requisito necesario

Si bien la jurisprudencia más reciente, hace hincapié en la necesidad de proporcionar informacion previa, explicita, clara y precisa al trabajador, cuando se pretende instalar medidas de control a través de dispositivos GPS y de las funciones que se pretenden llevar a cabo, esto no siempre fue así. Debido a la escasez normativa, este criterio ha sido construido a lo largo de una larga historia jurisprudencial y doctrinaria, por lo que en un principio este requisito era extremadamente flexible, hasta el punto de quedar casi

anulado. Esto ocurría en aquellos casos en los que se cumplía el juicio de proporcionalidad y no existía ninguna otra medida menos restrictiva[8].

La STSJ de Castilla-La Mancha 370/2015, de 31 de marzo, establece la necesidad, como se establecía en un principio con relación a la videovigilancia, de proporcionar la suficiente información a los trabajadores, cuando una medida de control y vigilancia como la instalación de dispositivos GPS, se vaya a llevar a cabo. También será imperativo informar de la finalidad que se busca con dicha recaudación y tratamiento de datos.

En este caso se establece que si bien, el hecho de que exista un acuerdo descrito por ambas partes es recomendable, no es necesario que se dé un "consentimiento específico por parte del trabajador" (FJ. 4º). Por ello, los datos obtenidos del sistema GPS del vehículo podían utilizarse por la empresa para la comprobación del cumplimiento de los deberes laborales del interesado (FJ 4º).

El TSJ hace una diferenciación temporal esencial para determinar la validez de los datos obtenidos. Así pues, en este caso concreto, los datos que se obtienen se han creado durante la jornada laboral del trabajador, lo cual faculta al empresario a obtenerlos, tratarlos y usarlos, al haber informado previamente al trabajador. Ahora bien, en el caso de que el vehículo en el cual se hubiera instalado el dispositivo GPS fuera puesto a disposición del trabajador de forma permanente, aquellos datos ajenos a la jornada laboral no serían válidos. Este es el mismo criterio utilizado por el TSJ de Andalucía-Granada 1608/2015, de 15 de julio que declara la procedencia del despido de una delegada comercial, argumentando que "los datos GPS generados por el vehículo durante la jornada laboral, que demuestran que los reportes de visitas que se dicen efectuadas no son ciertos, no siendo preciso el *consentimiento* previo del trabajador para implantar el GPS en el coche de empresa" (Miquel Angel Purcalla, 2017).

En 2015, la empresa Manuel Orejas S.A., hace llegar a todos los trabajadores un documento denominado "Clausula confidencial y competencia desleal" por el cual se les informa de que se les va a entregar unas tablets para el buen desarrollo de sus funciones.

[8] La STSJ de Cataluña de 5 de marzo de 2012 (rec. 5194/2011) es un ejemplo claro de esta situación. Así pues, se estima la validez y licitud de un dispositivo GPS instalado en el vehículo puesto a disposición del trabajador por la empresa (TESSAG IBÉRICA, S. A). Ahora bien, la única información que se le proporcionó al trabajador fue una advertencia sobre la posibilidad que sopesaba la empresa de adoptar medidas de vigilancia y control del cumplimiento de sus obligaciones.

Estas tablets serán utilizadas como si fueran teléfonos móviles exclusivamente en el ámbito laboral mediante los cuales se supervisará el servicio de venta a distancia. Además, se incorpora una plataforma que hace posible la gestión de los clientes, un módulo GPS para controlar las visitas de los trabajadores sin permitir la geolocalizacion de manera ininterrumpida, creando simplemente marcas cartográficas. Así mismo, el documento incluye una cláusula que detalla las consecuencias de su incumplimiento, entre ellas, el despido disciplinario.

A finales del mismo año, se avisa al demandante de que la empresa cuenta con información que confirman la comisión de dos faltas graves. La primera "incumplimiento reiterado y sistemático de sus funciones" y la segunda "el cobro de dietas cuando comía en su domicilio". Dicho aviso buscaba que no se volvieran a repetir estas conductas, pero a pesar de la buena fe de la empresa, el demandante reincidió de manera notable, ante lo cual se presentó carta de despido.

La Sentencia del Juzgado de lo social núm. 1 de Oviedo de 11 de mayo de dos mil diecisiete desestimó la demanda formulada por el actor declarando la procedencia del despido acordado por la empresa demandada y, frente a dicha resolución, el demandante interpone recurso de suplicación. En este caso, no se cuestiona la idoneidad ni la proporcionalidad del medio de prueba.

Dice Ignasi Beltrán que el derecho a la intimidad no es el único que puede verse vulnerado, criterio que vimos en la diversa jurisprudencia relativa a la videovigilancia, "pues, si se prevé un control de estos instrumentos informáticos es probable que también se esté procediendo a una recogida sistemática y exhaustiva de datos memorizados sobre aspectos del comportamiento del trabajador. Y, por consiguiente, el derecho a la libertad informática puede verse afectado" (Beltrán de Heredia, 2017). Habla este autor del principio de autodeterminación que debe cumplirse, según el cual el empresario tiene derecho a obviar el consentimiento de los trabajadores, no así la información que les debe procurar, relativa a las medidas tomadas, la información que se pretende obtener y la finalidad del tratamiento de dichos datos, cumpliendo así con lo previsto en la LOPD. Así pues, "siempre que los datos hayan sido obtenidos de un modo lícito, una vez creado el fichero, el sistema de garantías debe prevalecer" (Beltrán de Heredia, 2017).

4.2 Ámbito temporal en el que la instalación de GPS es válida

La STSJ de Asturias de 27 de diciembre de 2017, (rec. 2241/2017) establecerá un requisito fundamental a la hora de imponer este tipo de medidas de control en el ámbito laboral, haciendo una distinción de exigencias según el momento en el que se encuentren en funcionamiento. Este requisito ya se veía en sentencias anteriores como la TSJ de Andalucía-Granada 1608/2015, de 15 de julio y la STSJ de Castilla-La Mancha 370/2015, de 31 de marzo.

Zener Comunicaciones S.A., empresa de colocación de Telecable a domicilio, emite diversas comunicaciones a sus trabajadores sobre la futura puesta en marcha de medidas de control amparadas por el art 20.3 ET. En una de las comunicaciones se detalla las funciones principales de los dispositivos de geolocalización que se van a instalar en algunos vehículos. La finalidad de dichos dispositivos dice la demandada será la "localización en tiempo real, visualización de trayectos con posición segundo -a segundo, visualización de tramos conducidos con exceso de velocidad, detección de vehículo más cercano a un punto / calle, cuentakilómetros basado .en GPS y creación de alertas, datos que a su vez permitirán elaborar informes de distancia por día o por periodos, ralentí, recorridos, (reconstrucción de recorridos duración, kilometraje, recorridos efectuados fuera de horario), exceso de velocidad, localización, detalle de actividad (número de paradas, duración de la parada, retrasos). El dispositivo permitirá también configurar alertas, entre otras, de hora de arranque y aparcamiento del vehículo, hora de aparcamiento" exceso de velocidad, paradas no autorizadas, duración excesiva de las paradas, puntos de paso y paradas, entre otras." (STSJ de Asturias de 27 de diciembre de 2017). Esta medida se comunicó a Comisiones Obreras (de ahora en adelante, CCOO), a los trabajadores y se inscribió en el fichero de la AEPD. Ahora bien, dichas medidas se mantuvieron activas fuera del horario laboral motivo por el cual, CCOO presenta demanda.

El Tribunal concluye que, aunque la medida de geolocalización es licita mientras esté activa durante la jornada laboral, habiéndose cumplido los deberes de información hacia los trabajadores y habiendo cumplido el test de proporcionalidad, no es admisible fuera de la jornada laboral. Expone claramente el Tribunal que "cuando finaliza la jornada laboral o acaba el tiempo de trabajo, dichas facultades empresariales desaparecen y el

contrato de trabajo deja de constituir el vínculo entre las partes que ampara el poder de la demandada para imponer las medidas implantadas de captación y tratamiento de datos" (FJ 5º). A partir de ese momento el consentimiento de los trabajadores sería requisito necesario para mantener en funcionamiento las medidas de control y vigilancia. Así pues, con esta sentencia se establece un precedente sobre la ilicitud del ejercicio de su poder de vigilancia y control del empresario, fuera de las horas de trabajo del empleado, pues esto vulnera flagrantemente su derecho a intimidad de la vida personal y familiar (art. 18.1 CE).

Así pues, como se puede observar por la conclusión a la que llega el Tribunal, y como expone Fernández Orrico, "en principio, al finalizar la jornada laboral el empresario, debe desconectar el dispositivo de geolocalización instalado en el vehículo u otro dispositivo destinado al control de la actividad laboral del trabajador" (2021, ap. 5, párrafo 4).

4.3 Uso del vehículo geolocalizado fuera de la jornada laboral y contrariando la prohibición de uso establecida por el empresario

Ahora bien, qué sucede si el trabajador hace uso del vehículo proporcionado por la empresa fuera de su jornada laboral, cuando el uso del vehículo solo se permite con finalidad laboral dentro de la jornada. En este caso se llegan a plantear dudas, pues los dispositivos GPS como venimos diciendo, no pueden estar activados en momentos no correspondientes a la jornada laboral para los cuales el trabajador no ha dado su consentimiento expreso (STSJ de Castilla-La Mancha 370/2015, de 31 de marzo, STSJ de Andalucía-Granada 1608/2015, de 15 de julio, entre otras). El Tribunal Supremo da respuesta a esta cuestión en 2017 cuando recibe recurso de casación para la unificación de doctrina.

Tiendas Conexión S.L.U. despide a una trabajadora por indisciplina o desobediencia en el trabajo, transgresión de la buena fe contractual y abuso de la confianza, al constatar a través de los dispositivos GPS de su vehículo de trabajo, se hacía uso personal de él. Así mismo comprueba la empresa, que, durante una baja por ansiedad grave, el uso del vehículo de trabajo continuó, estando la trabajadora fuera de la jornada laboral, disfrutando una baja por incapacidad temporal de 25 días. Ante el despido, la trabajadora interpone demanda, la cual es desestimada. Más tarde, en recurso, el TSJ de Andalucía

revoca la anterior sentencia y declara nulo el despido. Tiendas Conexión S.L.U. formaliza recurso de casación para la unificación de doctrina.

Una vez más como se viene observando, el Tribunal aproxima este asunto desde la vulneración del derecho a la protección de datos personales (art 18.4 CE) por el carácter autónomo que confiere al individuo de disponer de dichos datos. En este caso, el Tribunal se aleja del criterio anterior de la STSJ de Asturias de 27 de diciembre de 2017, para determinar que existe una diferencia clara. En este caso, la trabajadora era plenamente consciente de la prohibición de usar el vehículo fuera de la jornada laboral y con finalidades distintas, así como el hecho de que el vehículo era localizable por el dispositivo GPS que se instaló previa información a los trabajadores. Determina pues el Tribunal Supremo que "había conocimiento previo y no se aprecia invasión de la esfera privada de la trabajadora, al afectar exclusivamente a la ubicación y movimiento del vehículo del que, eso sí, ella era responsable y debía utilizar con arreglo a lo pactado" (FJ 2º). Por tanto, se estima procedente el despido de la trabajadora, en tanto en cuanto el uso del vehículo se efectuó fuera de la jornada laboral pese a la prohibición clara y expresa por parte del empresario, sentando un importante precedente para los conflictos futuros.

4.4 Geolocalización mediante aplicaciones en el teléfono móvil personal: caso "Proyecto Tracker"

Cabe destacar un asunto que llega hasta el Tribunal Supremo que desestima el recurso de casación interpuesto contra la sentencia de la Audiencia Nacional, relacionado con la instalación de dispositivos de geolocalización por parte Telepizza SAU. En esta ocasión CCOO y UGT interponen demanda contra la empresa, por haber establecido lo que se conoce como "Proyecto Tracker", el cual impone "la obligación para el trabajador con categoría de repartidor de aportar a la actividad empresarial de un teléfono móvil con conexión a internet de su propiedad, y la aplicación informática de la empresa que permite la geolocalización del dispositivo y del trabajador durante su jornada laboral" (STS 63/2021 de 8 febrero de 2021). Subsidiariamente se pidió que en caso de que la empresa precisara de un dispositivo móvil para ejercer esta función de control, proporcionase los teléfonos a los trabajadores.

En la comunicación efectuada a los trabajadores se especifica que "la negativa reiterada o imposibilidad sobrevenida de aportación de esta herramienta por parte del trabajador, o de la aplicación informática antes mencionada, será causa suficiente para la extinción del contrato de trabajo al amparo de lo previsto en el artículo 49.1.b) del ET" (STS 63/2021 de 8 febrero de 2021). Así pues, se informa a los trabajadores de los medios que se van a usar, la forma de utilización y la responsabilidad del empleado, así como el régimen disciplinario aparejado a esta medida y las medidas compensatorias por los gastos que genere.

Las preocupaciones declaradas por UGT y CCOO llevan a la celebración de diversas reuniones del comité intercentros con la empresa, al no llegar a ningún acuerdo se interpone demanda, tras la cual se estiman todas las pretensiones. El Tribunal de primera instancia argumenta que la información que se dio a los trabajadores no fue suficiente en el momento previo a instalar la medida, que la obligación de aportar su propio teléfono móvil "quiebra la ajenidad en los medios, al hacer responsable al trabajador de cualquier impedimento en la activación del sistema" (FJ 1º), y por último, que dicha medida no cumple los requisitos de proporcionalidad. Ante esto, la empresa interpone recurso de amparo.

Se plantea si la medida es conforme a derecho y si la información proporcionada a los trabajadores era suficiente, alegando la empresa el cumplimiento estricto de ambos requisitos. Por un lado, dice la Sala que existen otros instrumentos adecuados para cubrir la finalidad que persigue la empresa y que no resultan ser invasivos de aquellos derechos constitucionalmente protegidos. Por otro lado, el TS determina que, aunque se entendiera que la información relevante se conoce al ponerse en funcionamiento la medida, parece ser que antes de que se diera la información pertinente a los trabajadores, la medida ya se había puesto en funcionamiento. Por lo tanto, determina que "el derecho que otorga el art 64 del ET a la representación legal de los trabajadores fue ignorado por la demandada que procedió a implantar el sistema sin poner a disposición de dicha representación la información realmente necesaria para un exacto conocimiento del alcance del mismo" (FJ 1º).

Así mismo, se establece, citando la STS de 25/09/2020, rcud 4746/2019, que la ajenidad seguiría existiendo en este caso, si la obtención de los dispositivos móviles no fuera un

elemento esencial para la configuración del contrato. Ahora bien, en tanto en cuanto, la obtención de dichos dispositivos, su cuidado y la manera de usarlo, suponen causas de extinción del contrato y con ello, de la relación laboral, se puede afirmar que dichos dispositivos son esenciales para esta relación. Por tanto, al configurarse como elemento esencial, esa ajenidad, se desvanece.

Así pues, el Tribunal Supremo concluye que esta medida vulnera los derechos fundamentales de intimidad y protección de datos del trabajador al no contar este con la información adecuada, necesaria y suficiente antes de la implementación de las medidas, y por no cumplir el test de proporcionalidad pues no se puede afirmar que el mandato imperativo por parte del empresario de aportar un dispositivo esencial para el desarrollo del trabajo sea válido. No cumple el juicio de idoneidad, de necesidad ni de proporcionalidad estricta. Por último, el Tribunal establece que dichas cláusulas que imponen al trabajador la obtención del dispositivo móvil y las responsabilidades para con el dispositivo, son abusivas y en ningún caso, ajustadas a la realidad.

4.5 STEDH de 13 de diciembre de 2022, Asunto Florindo de Almeida Vasconcelos Gramaxo vs Portugal

De la misma manera en que se hizo en el apartado anterior relativo a la videovigilancia como medida de control del empresario, en este apartado se analizará el uso de dispositivos GPS por parte del empresario desde una perspectiva jurídico internacional. Para ello cabe adentrarse en la Sentencia del Tribunal Europeo de Derechos Humanos de 13 de diciembre de 2022, (rec. 26968/2016), por la importancia que tiene para la cuestión objeto de estudio. Este es el primer pronunciamiento de este Tribunal en un caso en el que se valora la colisión entre los derechos fundamentales de intimidad de un individuo y el control de la empresa a través de dispositivos de geolocalización.

Con esta resolución, el TEDH estima la decisión de los tribunales portugueses que declararon justificado el despido de un trabajador, tras comprobar los datos de los GPS del vehículo que la empresa había puesto a su disposición para uso laboral. Estamos ante una empresa farmacéutica que, para facilitar la consecución de los objetivos de venta del trabajador, le proporciona un vehículo, el cual podrá usar con fines privados fuera de la

jornada laboral, siempre que reembolse el gasto derivado de dicho uso a la empresa. Los empleados afectados por la medida adoptada fueron "informados de la instalación del dispositivo de geolocalización y de los motivos de la medida, destinada principalmente a controlar las distancias recorridas por los empleados en el ejercicio de sus actividades, así como de las consecuencias en caso de discrepancia entre los datos del GPS y los introducidos en el CRM" (STEDH, Asunto Florindo de Almeida Vasconcelos Gramaxo v. Portugal, de 13 de diciembre de 2022, legal summary) aplicación usada por la empresa para recopilar los datos de las jornadas.

A través del tratamiento de estos datos, se constató que el empleado había aumentado los recorridos durante su jornada para de alguna manera compensar los recorridos que hacía fuera de su jornada y disminuir así la cantidad a reembolsar. Además, se pudo comprobar que, en más de una ocasión, el trabajador había acortado su jornada de ocho horas diarias. En primera instancia se declara el despido procedente. En segunda instancia, el Tribunal confirma la sentencia anterior, pero teniendo en cuenta solamente los datos relativos a las distancias recorridas, estimando inválidos los datos de seguimiento de su actividad profesional (TEDH, Asunto Florindo de Almeida Vasconcelos Gramaxo v. Portugal, de 13 de diciembre de 2022, legal summary). Los tribunales nacionales estiman la medida en base a su consideración de que la información proporcionada era suficiente y la firma del trabajador de un documento que constataba su conocimiento acerca de la instalación, uso, finalidades y posibles consecuencias del uso de las medidas. Ahora bien, el tribunal de segunda instancia desestima uno de los motivos de despido, argumentando que "los dispositivos de geolocalización no podían utilizarse para controlar el rendimiento de los empleados o el cumplimiento de su horario de trabajo", argumento que el TEDH, posteriormente, tendrá en cuenta.

Esta consideración esencial, redujo el ámbito de intrusión del empresario en la esfera de privacidad y protección de datos del empleado, limitándose a lo estrictamente necesario para cumplir con el objetivo de las medidas, controlar los gastos de la empresa.

El TEDH, analiza esta resolución emitida por el Tribunal de Apelación y estima que el Estado no se extralimitó, cumpliendo su obligación de proteger los derechos del demandante, derechos que se respetaron en todo momento. Desestima pues, las pretensiones del demandante, dando la razón al Estado, y por consiguiente a la empresa.

Ahora bien, si algo se puede extraer de esta resolución como enuncia Eduardo Rojo, es que el TEDH "parece decantarse hacia una interpretación y aplicación del art. 8 del Convenio que concede más importancia a la valoración de los medios de prueba obtenidos en sede judicial nacional y a su apreciación por los tribunales nacionales, y que deja en un segundo plano, aunque no descartado evidentemente, el acudir a la valoración de si esa apreciación, y su impacto sobre el respeto al derecho a la vida privada de la persona trabajadora, es contraria a derecho por ser irrazonable" (2023).

Por tanto, se concluye que "la autorización del uso mixto del vehículo –laboral y personal– no impide el control del mismo" (Rico, 2024, pág. 141), pudiendo de esta manera tratarse los datos referentes a los kilómetros recorridos fuera del tiempo de trabajo.

4.6 Criterio de la AEPD

La Agencia Española de Protección de Datos, hace una interpretación muy acertada de lo que significa la instalación de dispositivos de geolocalización en el seno del trabajo. Por un lado, determina en su guía "Protección de datos y relaciones laborales" como ya ha hecho la jurisprudencia, que el hecho de almacenar los datos referentes a la localización del trabajador puede derivar en la extracción de datos inherentes a su vida privada como pueden ser sus tendencias al volante, los lugares frecuentados e incluso sus rutinas, por lo que la geolocalización aplicada a la herramienta de trabajo, en estos casos, el vehículo o los dispositivos móviles, se traduce en una vigilancia a la persona del trabajador. Esto, como determina la AEPD hace necesario que se cumplan ciertos presupuestos:

- Deberá realizarse una evaluación del impacto antes de implantar tecnologías de este tipo, así como el cumplimiento de los principios de proporcionalidad y subsidiariedad
- Los datos recogidos deben ser tratados con un fin específico
- Las personas trabajadoras que utilicen herramientas de geolocalización deben ser plenamente informados sobre el seguimiento llevado a cabo y la finalidad de su utilización por parte del empleador.

- No es lícito imponer a la persona trabajadora la obligación de proporcionar medios personales para facilitar la geolocalización (por ejemplo, teléfono móvil), (STS 63/2021 de 8 febrero de 2021).

La AEPD maneja un criterio riguroso mediante el cual se permite la instalación de estos mecanismos solo en aquellos casos en los que exista una finalidad específica, excluyendo el fin único de controlo del trabajo de un empleado, cuando existan otros medios menos dañinos. Además, se deberá informar al afectado de las medidas y la finalidad que se busca con ellas, obligando también al empresario a instalar algún dispositivo que permita desactivar la geolocalización fuera de las horas de trabajo (Goñi, 2017, pág. 16).

5. CONCLUSIONES

BIBLIOGRAFÍA

Fuentes normativas

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. Boletín Oficial del Estado, *255*, de 24 de octubre de 2015. https://www.boe.es/eli/es/rdlg/2015/10/23/2/con

Constitución Española. Boletín Oficial del Estado, *311*, de 29 de diciembre de 1978. https://www.boe.es/eli/es/c/1978/12/27/(1)/con

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). EUR-LEX. http://data.europa.eu/eli/reg/2016/679/oj

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, *294*, de 6 de diciembre de 2018. https://www.boe.es/eli/es/lo/2018/12/05/3/con

Convenio Europeo de Derechos Humanos https://www.echr.coe.int/european-convention-on-human-rights

Jurisprudencia

STC 88/1985, de 19 de julio.

STC 186/2000 de 10 de julio

STC de 30 de noviembre de 2000, 292/2000

STC 29/2013 de 11 de febrero

STC 39/2016 de 3 de marzo

Tribunal Europeo de Derechos Humanos. (2019). López Ribalda y otros contra España (Sentencia No. 1874/13 y 8567/13).

Tribunal Europeo de Derechos Humanos. (2017) Barbulescu contra Rumanía

STC 119/2022 de 29 de septiembre de 2022

STS 23/2025 de 14 de enero de 2025,

Tribunal Superior de Justicia de Castilla-La Mancha, Sala de lo Social, Sentencia 370/2015 de 31 Mar. 2015, Rec. 19/2015

STSJ Asturias 3 de octubre 2017 (rec. 1908/2017)

STSJ de Asturias de 27 de diciembre de 2017, (rec. 2241/2017)

STS, 163/2021 de 8 de febrero de 2021, Rec. 84/2019

Tribunal Supremo, Sala Cuarta, de lo Social, Sentencia 766/2020 de 15 Sep. 2020, Rec. 528/2018

STSJ de Cataluña de 5 de marzo de 2012 (rec. 5194/2011)

Florindo de Almeida Vasconcelos Gramaxo v. Portugal

Otros

AFLabor & Colaboración de Miquel Àngel Purcalla Bonilla. (2017, julio 21). *Control empresarial y geolocalización*. https://aflabor.wordpress.com/2017/07/21/control-empresarial-y-geolocalizacion-colaboracion-de-miquel-angel-purcalla-bonilla/

Agencia Española de Protección de Datos (2021). La protección de datos en las relaciones laborales. Recuperado de: https://www.aepd.es/preguntas-frecuentes/8-videovigilancia/FAQ-0805-se-puede-instalar-camaras-con-la-finalidad-de-control-empresarial

Alfaro, J. (2018). La sentencia López Ribalda del Tribunal Europeo de Derechos Humanos. Almacén el Derecho. Recuperado de: https://almacendederecho.org/la-sentencia-lopez-ribalda-del-tribunal-europeo-derechos-humanos

Alonso, M. (2023). Licitud de la prueba de videovigilancia en supuestos de despido. Redacción Aranzadi. (https://soluciones-aranzadilaley-es.eu1.proxy.openathens.net/Content/Documento.aspx?params=H4sIAAAAAAAEADVOzWrDMAx-mvoSKHFGaXPwJekGG2yMNoxdFVtNTV3bk-2sfvu5DRNISOL7-0lIecBbFMehr5p21Zyamj9VCivO7_OEIyE5FrJ1Nl_FQAlZhDEIvtrKXemWgYwJzN5Jwe-7nnGAUeyYI4XUZVGz6CKYAxYSC2f3-wGzniBqZzugRVIrJZ6_61K85e12w2akUADiS09oI7KAQPL8CROKt0Q6eEoKrdSwhuBvzNhLCXB8gBbFhdClGIvKi7bqHcKFSVPee4jYg0Gr_u3Be5MPzpSIj9u7UOTStVi_2h7IpYBG1H94knT7LwEAAA==WKE)

Álvarez, A. (2022). El derecho a la vida privada en la doctrina del Tribunal Europeo de Derechos Humanos: un largo camino por recorrer. Revista Aranzadi Unión Europea. (5), pp. . recuperado de: https://soluciones-aranzadilaley-es.eu1.proxy.openathens.net/Content/Documento.aspx?params=H4sIAAAAAAAEAE1OTU_DMAz9NeSChJKutOyQS9fLLhMahbubWl1ElnT5KCu_HqcFiUjPsf2e7XdL6JcO71EaN-H3o9c9mAFYWKyzy1V2PiGL0AcpOH-olSAUhJzvCPtcVISa8JIbWbQqhVhjDpkUzzlk6X7NCsFAxQSmdUoWOdczdtDLijk_oG8WyVl0EcwZgyx3LFzc1wlmPULUzjbgN3N6GGTbcXolr-qyZDP6QAL5oUe0EVlA8OryCiPKo9VKuycI050Z-0mX31byd1N4tzpPg_nf3uabFCMt7aPdOKYM_S1EPIBBO_zZgWkyy9kZ8rzWkwt0Jl3JytEewLsU0Ej-A7lwp4R4AQAAWKE

Avilés, J.A.F & Roldán V.R.R. (2016) “Nuevas tecnologías y control empresarial de la actividad laboral es España”, Revista Labour & Law Issues, Vol. 2, nº 1. pp. 46-74.

Beltrán de Heredia Ruiz, I. (2017, noviembre 23). Control empresarial mediante GPS y despido: ¿y la libertad informática?. *Una mirada crítica a las relaciones laborales*. Recuperado de https://ignasibeltran.com/2017/11/23/control-empresarial-mediante-gps-y-despido-y-la-libertad-informatica/

Caballeros, M.A. (2024). El derecho a la protección de datos personales ante la videovigilancia en el ámbito laboral: la progresiva devaluación en la jurisprudencia constitucional de la obligación de informar al trabajado. *Revista Vasca de Administración Pública, 47*(128), p. 17-44. **doi:** 10.47623/ivap-rvap.128.2024.1.01

Eguaras, F. (2022). Videovigilancia: Sentencia del Tribunal Constitucional de 29 de septiembre de 2022, número 119/2022. *Jurisdicción Social Revista de la Comisión de lo Social de Juezas y Jueces para la Democracia* 239. Recuperado de: https://www.juecesdemocracia.es/2022/12/29/revista-jurisdiccion-social-239-diciembre-2022/?cn-reloaded=1

Fernández, F.J. (2021). Criterios sobre uso de dispositivos tecnológicos en el ámbito laboral. Capítulo VI. La geolocalización como medio de control empresarial a distancia de la actividad laboral de los trabajadores. *Tirant lo blancholine.* https://www-tirantonline-com.eu1.proxy.openathens.net/tol/documento/show/8451667?general=medidas+de+control+del+empresario+geolocalizaci%C3%B3n&index=4&navigate_url=%2Fbase%2Ftol%2Fdoctrina%2Fsearches%2Fnavigate%3Ftoken_id%3D67c03d0b02267e00101f5f90&next_index=5&num_found=7&pais=esp&prev_index=3&search_type=doctrina&search_url=%2Fbase%2Ftol%2Fdoctrina%2Fsearches%3Findex%3D4%26token_id%3D67c03d0b02267e00101f5f90&token_id=67c03d0b02267e00101f5f90&controller=documents&action=show&appname=tol&legacy=true&librodoctrina=17933

Ferrando, M.F. (2016). Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías. *Revista De Trabajo Y Seguridad Social. CEF*, (399), 37–68. https://doi.org/10.51302/rtss.2016.2126

Goñi, J. L. (2017). Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016. *Revista de derecho social, (78)* pp. 15-42, recuperado de: https://vlex.es/vid/nuevas-tecnologias-digitales-poderes-701526261

Goñi, J. L. (2016). Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo: Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de

información previa. Reseñas de Jurisprudencia: Ars Iuris Salmanticensi *(4)*, pp. 288-291. Recuperado de: https://academica-e.unavarra.es/handle/2454/41000

Guzzini, S. (2015). El poder en Max Weber. *Relaciones Internacionales*, (30), 97–115. https://doi.org/10.15366/relacionesinternacionales2015.30.005

Hernández, M. (2017). Sistemas de control de gestión y de medición del desempeño: conceptos básicos como marco para la investigación. *Ciencia y Sociedad, 42*, (1), pp. 111-124. DOI: https://doi.org/10.22206/cys.2017.v42i1.pp115-128

Jääskeläinen, F. M. (2020). Los derechos y libertades públicas (II). Álvarez, M. I (Coord). (2020). Lecciones de derecho constitucional. (Ed. 7). pp. 401-441. Tirant lo blanch,

Jiménez-Castellanos, I. (2017). Videovigilancia laboral y derecho fundamental a la protección de datos. Temas laborales: Revista andaluza del trabajo y bienestar social. *136,* pp. 126-156. Recuperado de: https://hdl.handle.net/11441/149537

López, G. (2020). La Revolución Tecnológica y su Impacto en las Relaciones de Trabajo y en los Derechos de los Trabajadores. Capítulo III Poderes de control del empresario y nuevas tecnologías. Tirant lo blanch. Recuperado de: https://www-tirantonline-com.eu1.proxy.openathens.net/tol/documento/show/8131116?general=La+Revoluci%C3%B3n+Tecnol%C3%B3gica+y+su+Impacto+en+las+Relaciones+de+Trabajo+y+en+los+Derechos+de+los+Trabajadores&index=2&navigate_url=%2Fbase%2Ftol%2Fdoctrina%2Fsearches%2Fnavigate%3Ftoken_id%3D67bb52fcc54816000fd5e521&next_index=3&num_found=6&pais=esp&prev_index=1&search_type=doctrina&search_url=%2Fbase%2Ftol%2Fdoctrina%2Fsearches%3Findex%3D2%26token_id%3D67bb52fcc54816000fd5e521&token_id=67bb52fcc54816000fd5e521&controller=documents&action=show&appname=tol&legacy=true&librodoctrina=17303

López, M. J (Coord.). (2022). Lecciones de contrato de trabajo. Capítulo Cuarto: Poderes empresariales. (Ed: 3). Thomson Reuters (Legal).

Mestre, J.M y Marrero, C. (2025, 29 de enero). Protección de datos: Tendencia Actual en la UE y casos recientes [miércoles jurídico]. Sagardoy Abogados. Madrid, España.

Pascual, J.E. (2023). Análisis Jurisprudencial del control empresarial a través de las TIC y su incidencia en los derechos fundamentales de los trabajadores (seguir citando)

Polo Roca, A. (2020). Geolocalización, motores de búsqueda y cookies: tres grandes retos para la protección de datos. Revista Jurídica de Castilla y León, 52, 141-184.

Rodríguez-Rico Roldán, V. (2024). Derecho a la protección de datos personales y control laboral a través de dispositivos de geolocalización. *Revista de Trabajo y Seguridad Social. CEF*, 479, 115-142. https://doi.org/10.51302/rtss.2024.20107

Rojo, E (2023). La importancia de la jurisprudencia del Tribunal Europeo de Derechos Humanos en el ámbito laboral y de protección social (III). Arts. 8 y 6 del Convenio Europeo de Derechos Humanos. ¿Cuáles son los límites del control por geolocalización del vehículo de trabajo? Notas a la sentencia de 13 de diciembre de 2022. caso Alfonso Florindo de Almeida Vasconcelos Gramaxo contra Portugal (con tres votos radicalmente discrepantes). *Eduardo Rojo Torrecilla.* Recuperado de: http://www.eduardorojotorrecilla.es/2023/01/la-importancia-de-la-jurisprudencia-del_5.html

Sepúlveda, M. (2016). Poder de control empresarial mediante cámaras de videovigilancia y derecho de los trabajadores a la protección de datos personales: Sentencia del Tribunal Constitucional (Pleno), 39/2016, de 3 de marzo. *Temas laborales. (133)*, pp. 219-235.

Valle, F. (2021). Las cámaras de videovigilancia en la empresa como medio de prueba en el proceso laboral. *Iuslabor*, (3), 31-59. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=7222064

Weber, M. (1977). Economía y Sociedad. México: F. C. E BUSCAR RESUMEN DE LIBRO PARA CITAR, ESTO NO ME LO HE LEIDO