eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

TRABAJO DE FIN DE GRADO- GRADO EN DERECHO

LOS DERECHOS FUNDAMENTALES DE INTIMIDAD, PROTECCIÓN DE DATOS Y SECRETO DE LAS COMUNICACIONES COMO LÍMITES AL PODER DE DIRECCIÓN DE LOS EMPRESARIOS

Trabajo realizado por Elene Garate Urcola

Dirigido por Koldo Mikel Santiago Redondo

Curso 2022-2023

ÍNDICE

I. Introducción

En el presente trabajo se abordan las cuestiones que supone el poder de control del empresario frente a los derechos fundamentales de los trabajadores. El Estatuto de los Trabajadores otorga al empresario una facultad para controlar el buen funcionamiento de la empresa. Esta facultad incluye la potestad para aplicar medidas de control que pueden utilizarse como prueba para imponer una sanción al trabajador por no estar cumpliendo debidamente su trabajo o haber cometido una infracción. No obstante, cualquier medida o medio de prueba no es válida dado que se deben respetar el contenido fundamental de los derechos de intimidad, protección de datos y secreto de las comunicaciones.

El objetivo de este trabajo se trata por lo tanto de ver cómo operan los elementos que componen el contenido esencial de estos derechos fundamentales y los que la jurisprudencia ha consolidado que hay que tener en cuenta para determinar la validez de la medida. Para ello nos basaremos en cuestiones como el principio de proporcionalidad o el deber de información. El conflicto entre poder de direccion y derechos fundamentales se trata de una problemática clásica en el derecho laboral sobre la cual los tribunales han ido cambiando de parecer en cuanto a los componentes que integran el principio de proporcionalidad y la importancia que se confiere al contenido esencial frente a este.

Podemos decir que el trabajo se divide en dos partes principales. En la primera parte analizaremos las definiciones del poder de dirección y de los derechos fundamentales de intimidad, protección de datos y secreto de las comunicaciones desde la perspectiva del derecho laboral. En la segunda parte nos centraremos en el estudio de varias sentencias que consideramos relevantes. Para ello hemos agrupado las sentencias según la clase de medida que se cuestiona en el caso, siendo cuatro las medidas que hemos tratado: la videovigilancia, el acceso a mensajería y correos electrónicos del trabajador, la grabación de sonidos y la geolocalización. De este modo, hemos ordenado el análisis de las sentencias desde más antiguas hasta más actuales.

Entre estas dos partes, se encuentra el apartado en el que expondremos la problemática concreta que vamos a tratar en la segunda parte. Estudiaremos en particular el principio de proporcionalidad y la problemática teórica constitucional que entraña su errónea aplicación por los tribunales. Estas reflexiones las incluiremos también en la segunda parte y en las conclusiones finales.

Para realizar este trabajo de investigación nos hemos basado principalmente en sentencias del Tribunal Constitucional español. No obstante también hemos hecho mención a sentencias del Tribunal Supremo y algunas de Tribunales Superiores de Justicia. Además también hemos examinado ciertas sentencias relevantes del Tribunal Europeo de Derechos Humanos (en adelante utilizaremos las abreviaturas de TC, TS, TSJ y TEDH). Todo ello lo hemos complementado mediante bibliografía, principalmente de revistas y manuales en las que se hace referencia a estas sentencias y a los conceptos que tratamos en el trabajo.

II. El control de dirección de los empresarios

Nuestro ordenamiento laboral atribuye al empresario una serie de facultades sobre la actividad de los trabajadores que se engloban en el concepto de "poder de dirección" que se desarrolla principalmente en el artículo 20 del ET[1], estableciendo en sus cuatro apartados las diferentes manifestaciones que puede revelar este concepto. Estas consisten en el poder de dirección en sentido estricto, en el ius variandi empresarial, en poder de vigilancia y control , en el poder disciplinario o de sanción.[2] y finalmente en el de control para realizar reconocimientos médicos a los trabajadores.

El poder de dirección ordinario o *stricto sensu* se define como el poder de dirección ordinario que tiene el empresario para tomar decisiones y dar órdenes para garantizar el normal funcionamiento de la empresa sin incidentes. Tiene su fundamento en el artículo 1.1 por el que se establece que se aplicará el ET al trabajador que quede dentro del ámbito de organización y dirección del empresario. El 20.1 ET añade que no tiene por que ser el empresario quien ejerza ese poder, la titularidad pertenece al empresario pero su ejercicio puede ser delegada a otro sujeto. Por último, en el 20.2 ET se especifica que el deber de obediencia deber cumplirse conforme las reglas de diligencia y la colaboración en las órdenes del empresario, al igual que debe hacerlo conforme a las reglas de buena fe, como se expone en el artículo 5a) del ET. En caso de no cumplir los trabajadores con sus obligaciones, entrará en juego el poder disciplinario del empresario.

---

[1] LAMPARERO ASQUERINO,JOSE Mª. (2012) "El derecho de resistencia frente al poder de dirección" Revista *Doctrinal Aranzadi Social.* Núm. 8.
[2] FABREGAT MONFORT, G. (2016). *Nuevas perspectivas del poder de dirección y control del empleador*. Editorial Bomarzo. Págs 17-19

El poder disciplinario o sancionador no se menciona expresamente en el artículo 20 ET, sin embargo, cumplir con las obligaciones impuestas es un deber del trabajador y si no se cumple con ello, el empresario podrá actuar aplicando sanciones conforme al artículo 58, 54 y 45 ET. La facultad disciplinaria es de uso directo, es decir, se le permite al empresario imponer sanciones con eficacia inmediata, sin tener que acudir a instancias judiciales[3], sin perjuicio de la posible revisión jurisdiccional a instancia del trabajador sancionado.

El poder de vigilancia y control se fija en el artículo 20.3ET, donde se dispone que el empresario puede adoptar las medidas de vigilancia y control que estime apropiadas para verificar que el trabajador está cumpliendo con sus obligaciones, pero siempre deberá guardar los límites de la dignidad y también los derechos fundamentales. El eje del trabajo se centra principalmente en esta potestad, dado que es la que permite al empresario imponer medidas que muchas veces terminan vulnerando derechos fundamentales como son la intimidad y protección de datos.

Otra de las manifestaciones del poder de dirección del empresario es el *ius variandi*, que es la facultad que éste tiene para alterar unilateralmente algunos aspectos de la prestación laboral contratada, con el fin de adaptarla a las necesidades organizativas de la empresa[4]. El empresario tiene la capacidad de modificar aspectos de la relación laboral, sin embargo, deberá tener en cuenta que para llevar a cabo ciertas modificaciones tendrá que atender a lo dispuesto en los artículos 39, 40, 41 ET y en la normativa laboral al respecto. En este trabajo no vamos a profundizar en el *ius variandi,* sino que como hemos mencionado, nos centraremos en el dirección en sentido estricto y el de vigilancia, analizando las problemáticas derivadas en cuanto a los derechos fundamentales como límite de esta facultad.

Por último cabe hacer mención al 20.4 ET, que regula la facultad del empresario para llevar a cabo reconocimientos durante una incapacidad temporal del trabajador. Se enmarca esta facultad dentro del poder de dirección ordinario puesto que el empresario tiene que verificar el normal funcionamiento de los medios productivos y por tanto también de sus trabajadores. No obstante, también profundizaremos en esta potestad al abarcar las problemáticas concretas.

Una vez definidas las diferentes manifestaciones del poder de dirección y de haber precisado en cual nos vamos a centrar, cabe relatar el origen de esta facultad y la razón de su

[3] STC 17/2000, de 31 de enero del 2000
[4]CONTRERAS NÚÑEZ-CORTÉS,P (2012) *Lecciones de contrato de trabajo*. Editorial Dykinson. Pág. 125

regulación. El Derecho del Trabajo nace fundamentalmente para limitar los poderes empresariales, no para apoyar la autonomía contractual, sino para regularla y limitarla[5]. Sin embargo,los derechos no dejan de ser disposiciones interpretables que dependen de la ideología y situación histórica y económica del momento, teniendo en cuenta que muchas de las sentencias analizadas en este trabajo y que han supuesto el seguimiento de una línea jurisprudencial surgen de un contexto de crisis económica. Es sin duda necesario regular el poder de dirección considerando que este es imprescindible para la buena marcha de la organización productiva [6]. No obstante, aprovechando la regulación, los tribunales están consintiendo medidas que quebrantan los derechos fundamentales de los trabajadores, como veremos en varios ejemplos.

El poder de dirección del empresario tiene su origen en el contrato de trabajo. Al igual que este también actúa como límite quedando la relación fijada contractualmente en una relación laboral, no pudiendo el empresario inmiscuirse en la vida privada del trabajador[7]. A modo de ejemplo podemos poner que el empresario tendrá la facultad de fijar los horarios pero estos no pueden sobrepasar lo fijado en el contrato. De todas maneras, este derecho a la privacidad del trabajador ya está reflejado constitucionalmente en dos variantes: como derecho a la intimidad (18.1 CE), como derecho al secreto de comunicaciones (art 18.3) y como derecho a la protección de datos (18.4 CE).Como derechos fundamentales, ambos se encuentran ubicados en la Sección 1.ª, Capítulo II del Título I de la CE. El Tribunal Constitucional ha afirmado en varias sentencias que el contrato de trabajo (y por tanto el poder de dirección basado en él) no legitima al empresario para vulnerar los derechos fundamentales de los trabajadores como ciudadanos, que no pierden su condición de tales por insertarse en el ámbito de una organización privada[8]. Por lo tanto, queda claro que el hecho de que estos derechos alcancen un rango constitucional de derecho fundamental les brinda una protección superior al resto de derechos laborales. Superior al propio poder de dirección, que queda regulado en la normativa expuesta del Estatuto de los Trabajadores.

Se ha afirmado en numerosa doctrina y jurisprudencia que hay cierta relación entre el poder de dirección y la libertad de empresa. La libertad de empresa queda reflejada en el artículo 38

[5] CATALÁ POQUET, R. (2022) “Poder de control empresarial a través de sistemas de videovigilancia: alcance y límites” *Revista Aranzadi Doctrinal.* Núm. 5.
[6] STC 186/2000, de 10 de julio.
[7] BURGOS FOVANÉ, J. (2015). “El poder de dirección del empleador vs. el acceso de los medios tecnológicos e informáticos dentro de la empresa”. *Revista Vía Iuris. Nº* 18. Págs 47-71
[8] STC 88/1985, 19 de Julio

de la CE, el cual constituye la libertad de empresa en el marco de la economía de mercado. La razón de la constitucionalización de este derecho proviene del establecimiento del modelo de economía de mercado en el Estado[9], formando este derecho parte del conjunto de disposiciones conocida como constitución económica. Sobre el alcance del contenido esencial de la libertad de empresa, ha dispuesto la jurisprudencia del Tribunal Constitucional que este "*no se corresponde con el derecho a acometer cualquier empresa, sino sólo con el de iniciar y sostener en libertad la actividad empresarial, cuyo ejercicio está disciplinado por normas de muy distinto orden*[10] ". Sin embargo, también ha manifestado el mismo que el contenido esencial de la libertad de empresa no solo se limita a la facultad para crear empresas, sino también a la facultad para establecer los propios objetivos de estas, al igual que para dirigir y planear su actividad en atención a sus recursos y a las condiciones del propio mercado.[11]

Esta afirmación sobre el contenido de la libertad de empresa nos recuerda a la definición del poder de dirección del empresario. Queda establecida por lo tanto una conexión entre ambos y un objetivo común que es garantizar la organización de la empresa. Esta conexión puede dar pie a que los tribunales lleguen a interpretar que el poder de dirección queda amparado constitucionalmente. Sin embargo, este análisis es erróneo, dado que no dejan de ser disposiciones y derechos separados de diferente rango y norma legal. Cabe tener presente además que el derecho de libertad de empresa (artículo 38 CE) está ubicado en la Sección 2.ª, Capítulo II del Título I de la CE, no en la sección primera. Es decir, el derecho de libertad de empresa no es un derecho fundamental. Esta afirmación realizada se entenderá en su plenitud cuando desarrollemos nuestro desacuerdo con la posición de los tribunales en algunos fallos de sentencias.

III. Los derechos fundamentales como límites al poder de dirección

[9] Ripollés Rastrollo, A.(2017) Sinopsis artículo 38 de la Constitución Española. https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=38&tipo=2
[10] STC 83/1984, 24 de Julio de 1984
[11] STC 225/1993, 8 de Julio de 1993

1. El derecho de intimidad

El derecho a la intimidad se configura en el artículo 18.1 CE, junto al honor, y a la imagen y tiene su correspondiente desarrollo en la breve Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. A su vez, en lo que se refiere al ámbito laboral vemos el derecho a la intimidad reflejado en el ET, concretamente en los artículos 4.2 e), 18 y en el reciente artículo 20 bis, que se incorporó al estatuto mediante la disposición final decimotercera de la ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Respecto a normativa internacional, encontramos el derecho de intimidad establecido en el artículo 12 de la declaración de derechos humanos de 1948, donde no se menciona el concepto de intimidad como tal pero se establece que "*nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia".* También le dedica el Convenio Europeo de Derechos Humanos (CEDH) el artículo 8, el cual al igual que el de la declaración de derechos humanos, se refiere en concreto al derecho al respeto a la vida privada y familiar.

El derecho de intimidad forma parte de un grupo de derechos fundamentales que se conocen como derechos fundamentales inespecíficos. Algunos de los que forman parte son precisamente los que vamos a tratar en este trabajo: el derecho a la intimidad , secreto de comunicaciones y protección de datos, (18.1, 3 y 4). No obstante, también caben otros como el de no discriminación (artículo 14 CE) o libertad de expresión e información (artículo 20 CE)... Se tratan de derechos fundamentales con rango constitucional pero que tienen también una dimensión en materia laboral por la repercusión y casuística que han cobrado a la hora de chocar con medidas impuestas con base en el poder de dirección del empresario. Son derechos que pertenecen al ciudadano y como indicábamos previamente, aunque no se incluyan en el contrato de trabajo, se aplican con plena eficacia por encima de este[12]. La casuística sobre la vulneración del derecho de intimidad en la relación de trabajo ha evolucionado a lo largo de los años debido al desarrollo de las tecnologías. Las nuevas tecnologías han supuesto una transformación para la concepción de los derechos de protección de datos y secreto de las comunicaciones. Al igual que ha traido consigo una creciente cantidad de jurisprudencia respecto a las medidas de poder empresarial que

[12] CRESPO RODRÍGUEZ, M J. (2018) "La necesaria observancia de los derechos fundamentales en las relaciones laborales como límite inexcusable del poder de dirección empresarial" *Revista IUSLabor*. Núm. 2. Pág 173-185

vulneran los derechos citados. Como pueden ser la videovigilancia de los trabajadores, grabación de sonidos, el uso de mensajes de los trabajadores como medio de prueba por los empresarios… Respecto a las casuísticas que se plantean en el trabajo, cabe decir que la mayoría de sentencias del Tribunal Constitucional citadas tienen cierta antigüedad, sin embargo son muy importantes para trazar la línea jurisprudencial que se usa actualmente en las salas de lo social de nuestro país.

La jurisprudencia constitucional ha establecido que el contenido esencial del derecho a la intimidad "*confiere a la persona 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*[13]*".* El origen del derecho a la intimidad personal deriva del derecho a la dignidad de la persona recogido por el artículo 10.1 CE, de tal forma que la conexión entre ambos supone que debe existir para el individuo un ámbito propio y reservado frente a la acción y el conocimiento de los demás, siguiendo las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana[14].

Queda constatado que el nacimiento de este derecho se debe a la necesidad humana de separar la vida privada de la pública. En el contexto de la relación laboral, su función se trata de garantizar al trabajador la separación de su propia vida privada de la laboral, excluyendo de terceros, de poderes públicos o particulares, y en concreto, del poder particular de dirección del empresario[15], que es el que estamos abordando. Otra de las razones por las que el derecho constitucional de intimidad es aplicable a la relación laboral[16] es debido a que en ella se generan relaciones interpersonales, vínculos o actuaciones que pueden considerarse que están dentro de la vida privada del individuo [17].

La existencia del derecho de intimidad en la jornada de trabajo es innegable. Sin embargo, no es tán fácil resolver esta lucha entre poder de dirección y vulneración de la intimidad, debido a que operan numerosos factores y casuística sobre ello. Elementos como los propios espacios físicos resultan complicados de delimitar. A modo de ejemplo, el lugar donde se instale una cámara (medida de videovigilancia) o se realice una grabación puede suponer la vulneración o no de derechos fundamentales en función de si ese lugar se considera público o

[13] STC 292/2000 de 30 de noviembre
[14] STC 57/1994, de 28 de febrero
[15] STC 159/2009, de 29 de junio
[16] SSTC 98/2000, de 10 de abril
[17] STC 12/2012, de 30 de enero

privado. Además de la esfera física, entra en juego también la digital[18], o la telefónica, en ese caso muchas veces intervienen a su vez el derecho de protección de datos o secreto de las comunicaciones, en medidas como las grabaciones hechas o mensajes privados descubiertos y usados como medios de prueba. Las circunstancias son inmensas, si bien, trataremos de abordarlas y desarrollarlas en el apartado de problemáticas de las medidas de dirección.

La llamada expectativa de privacidad o confidencialidad, ha contribuido, en general, a que se amplíe esta esfera de vida privada en el ámbito laboral del trabajador, debido en parte, a la tolerancia generalizada de los empleados del uso de medidas informáticas del empresario[19].Aunque desarrollaremos su origen y recorrido en las problemáticas respecto a las medidas del empresario, cabe adelantar que el argumento esencial de este concepto es que en determinadas condiciones y sin haber el empresario advertido de la medida impuesta ni las reglas de uso, se va considerar una presunción de intimidad a favor del trabajador y por lo tanto una vulneración del derecho de intimidad por parte del empresario. En caso de quedar demostrada la previa advertencia del empresario, no tendrá lugar esta expectativa ni por tanto vulneración[20] del derecho de intimidad, protección de datos o secreto de comunicaciones (dependiendo de cual estemos tratando). Por lo tanto, la dificultad de la determinación de si vulnera la medida el derecho de intimidad o no, yace en el deber de información del empresario y en el consentimiento del trabajador.

Por último consideramos importante que quede clara la autonomía del derecho de intimidad respecto al de protección de datos y secreto de comunicaciones, si bien lo detallaremos al desarrollar ambos. Puede darse por tanto el quebrantamiento del derecho a la intimidad a la vez que se desestima la vulneración de alguno de los otros dos derechos. Sin embargo, el derecho a la intimidad es la base conceptual, y usualmente la vulneración de alguno de los dos, supone la vulneración de la intimidad también.

[18]DEL CUVILLO ALVAREZ, A. (2020). "La delimitación del derecho a la intimidad de los trabajadores en los nuevos escenarios digitales". *Temas laborales: Revista andaluza de trabajo y bienestar social.* Nº 151. Págs. 275-292

[19] CARRIÓN DURO, S (2021) "El deber de información en el articulo 87 y 89 lop dgdd. La quiebra de la expectativa de privacidad vinculada al derecho a la intimidad y otros derechos fundamentales en liza en la relación laboral" *Revista de Derecho Laboral vLex.* Nº 2. Pág. 70-93

[20] STS 26 de septiembre de 2007

2. El derecho a la protección de datos

El derecho a la protección de datos queda regulado hoy en día por normativa tanto europea como nacional. En lo que a europea se refiere, se establece este derecho en el ya mencionado artículo 8.1 CEDH, así como en el 16.1 del TFUE. En 2016 se aprueba el reglamento (UE) 679/2016 del parlamento europeo y del consejo relativo a la protección de las personas físicas sobre el tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

A nivel nacional rige hoy Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)[21], que surge para estar acorde con lo dispuesto en la RGPD y por la cual se deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Muchas sentencias a las que nos vamos a referir en el trabajo hacen referencia a esta antigua ley ya derogada, ya que en el momento de dictaminarlas regía esa normativa. Sin embargo, nos centraremos fundamentalmente en los argumentos que componen la línea jurisprudencial que sigue siendo trascendental para definir el contenido de los derechos.

Una de las primeras sentencias que exponen este derecho es la STC 254/1993 la cual nos aproxima al concepto que en aquel momento se denomina como derecho a la libertad informática y que hoy en día matizamos como derecho a la protección de datos. En ella se reconoce que el artículo 18.4 de la CE entraña un nuevo derecho diferente al de honor e intimidad, este se trata de un derecho que pretende operar frente agresiones a la dignidad y a la libertad de la persona cuando se hace un uso ilegítimo del tratamiento de datos, lo que la Constitución llama «la informática». La STC 94/1998, expone un suceso de vulneración del derecho de libertad sindical y de protección de datos por saber la empresa el la afiliación de un trabajador afiliado a un sindicato y haberle discriminatorio por ello. En ella se señala que el artículo 18.4 CE "*no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad».*"

[21] La anterior ley sobre protección de datos se conocía como " Ley Orgánica de Protección de Datos de Carácter Personal", sin embargo, podemos verla citada muchas veces bajo las siglas de LOPD (sin necesidad de hacer matiz en las siglas sobre el carácter personal de los datos). No obstante, sí que vemos en muchos textos que se hace referencia a la nueva ley con su nombre completo: LOPDGDD (Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales) aunque también podemos verla mencionada como LOPD. Por comodidad durante el trabajo nos referiremos a ella de esa manera,sin restar importancia a esa incorporación de derechos digitales. En caso de querer mencionar la antigua ley, nos referiremos a esta como la LOPD de 1999.

A su vez, debemos abordar en este trabajo la importante STC 292/2000 , de 30 de noviembre que fue clave para definir el contenido esencial del derecho fundamental de protección de datos. En ella se define concretamente que el contenido esencial consiste *"en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero."* Es decir, el derecho a la protección de datos se trata de la facultad de disposición y control que tiene la persona para disponer de sus datos y que no pasen a manos de un tercero sin su consentimiento ni se usen para un fin diferente al autorizado.

Podemos observar por lo tanto, cómo se va precisando en la sentencia la autonomía propia y las diferencias entre el derecho a la protección de datos y el de intimidad. Ambos comparten el objetivo común de la protección constitucional de la vida privada personal y familiar. Sin embargo, el derecho a la protección de datos engloba el ámbito de la privacidad que es más amplio[22] . Lo privado no siempre resulta íntimo, pero dependiendo de las circunstancias puede quedar amparado por el derecho de protección de datos y secreto de comunicaciones. Hay quien no apoya distinción teórica entre intimidad y privacidad, el profesor Daniel Toscani Gimenez opina que es una distinción artificial que termina perjudicando a los trabajadores, dando más margen de justificación al empresario y menoscabando los derechos fundamentales de los trabajadores[23], a mi parecer resulta una distinción correcta y permite concebir una vulneración en cuanto a datos que en un principio no se asemejan como íntimos.

A dónde queremos llegar es a las diferencias entre derecho a la intimidad y protección de datos. El primero se limita a proteger la llamada esfera de los bienes de la personalidad que pertenecen a la vida privada del individuo y si se vulnera, supondrá un menoscabo de la dignidad de la persona. Por otra parte, la privacidad de la protección de datos supone la protección de aquellos datos que sean relevantes "*para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales"*, esto es, incluso sin pertenecer estos aisladamente considerados al ámbito de intimidad pueden en determinadas circunstancias suponer una lesión al honor o resultar discriminatorios, como hemos visto en la STC 254/1993 referida a la afiliación de un trabajador a un sindicato. En

[22] UGINA MERCADER, JESÚS R(2019) *Protección de datos y garantía de los derechos digitales en las relaciones laborales.* Ediciones Francis Lefebvre. *https://online-elderecho-com.ehu.idm.oclc.org/seleccionProducto.do;jsessionid=DCF361A1EE34AAB6C42BCA174A271AC9.TC_ONLINE04?producto=DOCTR&javascriptInicial=presentarMarginalMemento(%27*%27,%27ES%27,%272013/900081%27)#%2FpresentarMemento.do%3Fnref%3D2013%2F900081%26producto%3DDOCTR%26marginal%3D%26rnd%3D0.40411201271504504*

[23] GIMÉNEZ TOSCANI, D (2015) "La vulneración del derecho a la intimidad por delatadores, detectives privados y medios tecnológicos"*Revista de derecho social.* Nº. 71. Pág. 55-78

definitiva, uno se refiere a la concreta disposición de datos y el otro a la prohibición de intromisión en la esfera privada.

Prosigue la STC 292/2000 delimitando los elementos característicos indicando que el poder de disposición de la protección de datos nada vale si" *el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin".* Además, estos datos deben usarse para el fin deseado y puede el ciudadano oponerse cuando se utilicen para fines distintos[24]. De este modo, fija la sentencia que los elementos particulares de la protección de datos son el consentimiento de la recogida de datos. La LOPDGDD concreta estas consideraciones en los artículos 6, 87,89 y 90 referidas a algunas de las problemáticas que trataremos.

3. El derecho al secreto de las comunicaciones

El secreto de comunicaciones se regula en el artículo 18.3 de la CE y queda claramente precisado señalando que "*se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial",* por lo tanto, no habrá que hacer un recorrido jurisprudencial para interpretar la constitución, como teníamos que hacer con el derecho a la protección de datos (debido a la evolución de las tecnologías y la escasa exactitud de libertad informática) sino que en este caso queda claro el derecho, aunque las nuevas tecnologías también hayan cambiado su concepto y necesitemos el criterio del TC para saber las comunicaciones que abarca. Al igual que el derecho a la intimidad y protección de datos, este se encuentra también establecido en el artículo 8 del CEDH. A diferencia del derecho de protección de datos, el de secreto de las comunicaciones no dispone de ley orgánica propia que lo desarrolle lo cual supone que es la jurisprudencia quien se va a encargar de acotar su contenido esencial y su ejercicio.

Cuando nos referimos al derecho del secreto de las comunicaciones debemos entender que este "*consagra la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas".* En este sentido, se precisa que puede resultar vulnerado tanto por la interceptación, como por la captación del proceso de comunicación o por el conocimiento del

[24] STC 94/1998, de 4 de mayo

acto ilícito de lo comunicado por llevar a cabo una apertura correspondencia ajena guardada de un correo electrónico o a través de un teléfono móvil[25].

Al igual que en el anterior epígrafe, detallábamos la independencia del derecho de protección al de intimidad, el derecho al secreto de comunicaciones también va a suponer una autonomía respecto a la intimidad. En la STC 170/2013 se desarrollan las diferencias entre ambas. Se expone en ella que el derecho del secreto de comunicaciones "*se predica de lo comunicado, sea cual sea su contenido"*[26] . Por lo tanto, su función, a diferencia de la del derecho a la intimidad, no trata como tal de proteger esa vida privada de los mensajes, sino que se ocupa de preservar la libertad en el proceso de comunicación y no por sí solo el mensaje contenido. De esta manera, el derecho del secreto de las comunicaciones se extiende tanto para la comunicación de mensajes pertenecientes a esta esfera privada, íntima o reservada del sujeto como para los que no pertenecen a esa dimensión. Ocurre parecido a lo que analizabamos sobre la protección de datos, no se trata del objeto del dato, sino más bien de la capacidad de protección de este.

El derecho al secreto de las comunicaciones se centra, por lo tanto, en la vía de comunicación que se lleva a cabo. Ahora bien, aclara la sentencia que el derecho al secreto de comunicaciones no envuelve todas las vías de comunicación, dado que entran en juego multitud de factores como que la comunicación sea abierta o cerrada o el medio de comunicación usado. De esta manera quedarán protegidos por el derecho al secreto de las comunicaciones los medios considerados de comunicación cerrada y quedarán sin amparo los medios considerados abiertos [27] pudiendo ser estos revisados de oficio y acceder el empresario a su contenido[28] y por lo tanto tampoco cabría alegar por los trabajadores una expectativa de privacidad.

Hay ciertos medios que la jurisprudencia ha establecido como comunicación cerrada y que por tanto quedan protegidos por este derecho.Uno de ellos es la correspondencia, como desarrollaremos en el apartado de ejemplos.También indica el propio 18.3 CE que se garantiza la protección en especial de las postales, telegráficas y telefónicas. Asimismo, la jurisprudencia ha consolidado que quedan amparados por el mismo derecho los mensajes de

[25] STC 241/2012 de 17 de diciembre
[26] STC 114/1984, de 29 de noviembre
[27] STC 241/2012, de 17 de diciembre
[28] STC 281/2006, de 9 de octubre

teléfono grabados en un contestador, archivados en el ordenador, mensajes impresos en papel, cartas abiertas y archivadas[29]. No obstante, los medios de comunicación se han multiplicado en los últimos años y hay cierta dificultad en determinar cuáles de los diversos medios de los que disponemos resultan protegidos por el derecho y cuáles no. Algunos otros medios que quedan fijados por la doctrina como abiertos y por tanto fuera de la garantía del derecho pueden ser las conversaciones por chat o programa de mensajería en un ordenador común[30], como examinaremos en su debido apartado. Solo gozan de amparo constitucional las comunicaciones indirectas realizadas por algún medio como los mencionados, no quedan protegidos los realizados por vía directa como la comunicación verbal o mediante gestos, aunque sí las escuchas telefónicas y grabaciones, como veremos también en su epígrafe correspondiente. Tampoco quedan amparados los medios de comunicación masiva como la radio o la televisión.[31]

No obstante, hemos indicado que los derechos fundamentales no son absolutos y que el poder de dirección puede imponer medidas que si resultan legítimas acorde al principio de proporcionalidad, no vulneran los derechos fundamentales. Es decir, que aunque en un principio los correos electrónicos queden amparados por el derecho al secreto de las comunicaciones, no significa que cada vez que el empresario acceda a los emails este lesionando tal derecho. Para que el juicio de proporcionalidad sea positivo para el empresario, será imprescindible la correcta configuración de elementos como el establecimiento de las reglas de uso por parte de la empresa y el deber de información de la normativa regulada. A su vez, la existencia de expectativa de privacidad del trabajador dependerá de la argumentación de estas dos cuestiones. En resumen, veremos que cada situación requiere un análisis preciso y la valoración de todos lo elementos en juego.

IV. El conflicto entre los derechos fundamentales de los trabajadores frente al poder de dirección del empresario y el origen del principio de proporcionalidad

[29] DEL CUVILLO ALVAREZ, A, op. cit.
[30] STC 241/2012 de 17 de diciembre
[31] REVORIO DÍAZ, F. JAVIER (2006) "El derecho fundamental al secreto de las comunicaciones" *Derecho PUCP: Revista de la Facultad de Derecho.* Nº. 59. Págs 159-175

Antes de sumergirnos en ejemplos concretos y materializar la abstracción de las definiciones de los derechos fundamentales expuestos, tenemos que hacer una referencia al conflicto de los derechos fundamentales frente al poder de dirección empresarial. Se trata de una parte fundamental del trabajo, por ende, también lo incluiremos ciertas consideraciones sobre este en el apartado de conclusiones, añadiendo opiniones propias, tras haber examinado la casuística.

Hemos visto que las definiciones de estos tres derechos tienen su origen en las sentencias del TC expuestas. Veremos que el Tribunal Supremo también precisará las definiciones, mencionando muchas veces estas mismas sentencias. Es por eso que para analizar cómo operan los derechos fundamentales frente a las medidas del empresario nos centraremos en las sentencias más emblemáticas del TC, pero también mencionaremos muchas otras importantes del TS. A continuación examinaremos el recorrido jurisprudencial del TC respecto al derecho de intimidad.

El TC es un órgano sometido a la Constitución, que se trata de una ley muy proclive a ser interpretada en función del contexto social e histórico. Hasta aproximadamente mitades de los años 90, este tribunal seguía una tesis contractualista,[32] en la que se primaba lo establecido en el contrato de trabajo incluso sobre los propios derechos fundamentales (Con excepción de la STC 88/1985 que determina justamente lo contrario). En consecuencia, se restringe mucho en esta época el derecho a la imagen y a la intimidad , reduciendo la posibilidad de espacios donde podía concurrir una vulneración de la intimidad, estableciendo incluso que no cabe este derecho en el lugar de trabajo, salvo en espacios privados como aseos[33].

La STC 99/1994 de 11 de Abril de 1994 (caso del deshuesador de jamón) supuso un punto de inflexión en este aspecto debido a que fue una de las primeras sentencias en aplicar el principio de necesidad en materia de medidas del poder del empresario, que posteriormente constituirá lo que conocemos como principio de proporcionalidad[34]. La sentencia hace hincapié en que el empresario no se puede basar en el contrato ni en el poder de dirección

[32] SEIN GOÑI, J. LUIS (2014) *Los derechos fundamentales inespecíficos en la relación laboral individual ¿necesidad de una reformulación?* XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Pamplona
[33] Jiménez, A. F. D. (2021). "El Derecho a la Intimidad y a la Protección de Datos Personales en el Ámbito Laboral." *Revista Internacional Consinter De Direito*. Nº 7(13). Págs 357–385
[34]SEIN GOÑI, J. LUIS, op. cit.

para restringir un derecho fundamental, sino que esta medida habrá de ser valorada según "*los intereses en presencia mediante una adecuada ponderación de las circunstancias concurrentes."* De este modo, a partir de esta sentencia queda instaurada la postura de que los derechos fundamentales pueden quedar restringidos por las medidas de dirección del empresario, tan solo en concordancia con la debida proporcionalidad. Posteriores sentencias, algunas ya citadas en este trabajo, han confirmado la instauración del principio de proporcionalidad con afirmaciones como que los derechos fundamentales no son absolutos, "*tampoco el de intimidad, pudiendo ceder ante intereses constitucionalmente relevantes, y con la condición de que el límite fijado sea para lograr un fin constitucionalmente avalado y proporcionado*[35]"

Algunas sentencias posteriores como son las SSTC 186/2000 292/2000, 98/2000 serán de gran importancia puesto que como hemos mencionado durante el trabajo, además de delimitar el contenido esencial del derecho a la intimidad y protección de datos, destacan la debida aplicación del principio de proporcionalidad. En este sentido, indican las sentencias que es el tribunal quien se va a encargar de ponderar en qué circunstancias puede considerarse legítima la medida del empresario y quien va a aplicar el principio, "*atendiendo siempre al respeto de los derechos fundamentales del trabajador, teniendo siempre presente el principio de proporcionalidad.*[36]*"*

El principio de proporcionalidad lleva una treintena de años aplicándose de forma mecanizada, por entonces, cuando se consagró como método ideal para resolver esta clase de conflictos, no se había aprobado la LOPD de 13 de diciembre de 1999 hoy en día derogada. Incluso, actualmente, disponemos de otra LOPD de 5 de diciembre 2018 y 30 años después seguimos utilizando el mismo principio para ponderar las medidas del empresario, aunque veremos que la forma de aplicarlo si ha cambiado. Sin duda podemos decir que el principio de proporcionalidad se ha convertido en el dogma de los tribunales, incorporando otros criterios, como el deber de información del empresario, o el supuesto sospecha razonable (a favor del empresario) para ponderar las medidas de los empresarios que pueden afectar a los derechos fundamentales de los trabajadores. Relacionados con los dos anteriores está el criterio de expectativa de privacidad [37]. El cual, en vez de centrarse en valorar la medida del

[35] STC 57/1994, de 28 de febrero
[36] STC 98/2000, 10 de Abril
[37] SEIN GOÑI, J. LUIS, op. cit.

empresario, valora la expectativa del trabajador analizando el posible conocimiento que podía tener sobre las reglas de uso y la precisión de las reglas de uso establecidas, si lo están.

En la STC 186/2000 se precisan los tres requisitos del juicio de proporcionalidad que hay que cumplir para que la medida no se considere restrictiva. El primero de ellos es que la medida sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad), por ota otra parte, también habrá que tener en cuenta que no puede existir una medida más moderada que la utilizada(juicio de necesidad), y, finalmente, hay que determinar que la misma sea equilibrada *"por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto*[38]*".* Sin embargo, como hemos señalado antes, no se trata de la única medida a tener en cuenta para determinar la licitud de la medida impuesta por el empresario, además de que aunque estos 3 componentes son siempre los que hay que tener en cuenta, se dará más importancia a uno u otro dependiendo del derecho en juego y de la medida impuesta por el empresario.

Por último, cabe hablar del voto particular del magistrado Fernando Valdés Da-Re en la STC 39/2016. Este voto particular versa sobre la aplicación del principio de proporcionalidad y la consecuente decadencia que está suponiendo para los derechos fundamentales de los trabajadores, en concreto para el de intimidad y protección de datos.

En este voto particular Valdés hace un profundo análisis de teoría constitucional en el que cuestiona el sistema de ponderación en sí mismo y pone en evidencia sus fallas. El magistrado critica la relación que se está fijando entre poder de dirección y la libertad de empresa, al igual que la colisión ficticia que se está llevando a cabo entre esta y los derechos fundamentales. Señala que el poder de dirección de los empresarios está regulado en el Estatuto de los Trabajadores (en concreto y en consonancia con la materia que estamos tratando, en el artículo 20.3) y por lo tanto, no es un parámetro de constitucionalidad que pueda limitar los derechos fundamentales. Debido a que *"los poderes o facultades del empresario no son expresiones directas ni indefendibles de los artículos 33 y 38 CE"* y por lo tanto no pueden ponerse al nivel ni restringir derechos fundamentales como son el de intimidad, protección de datos y secreto de las comunicaciones. Puntualiza que son los derechos fundamentales los que delimitan el ejercicio del poder de dirección y no a la

[38] STC 186/2000, 10 de Julio

inversa. Es decir, el problema tiene su raíz en que los tribunales están aplicando el principio de proporcionalidad para cualquier conflicto de intereses, y lo cierto es que cualquier conflicto de intereses no supone un conflicto de derechos fundamentales. A modo de opinión, cabe afirmar que que estoy de acuerdo con el magistrado respecto a la confusión que manifiestan los tribunales en algunas sentencias, como por ejemplo la propia STC 99/1994 mencionada, la cual sostiene que *"en todos los casos de colisión de derechos fundamentales o bienes constitucionalmente protegidos, los intereses en presencia, mediante una adecuada ponderación de las circunstancias concurrentes."* Valdés indica que artículo 38 no es un derecho fundamental y por lo tanto, no se puede hablar de colisión. En definitiva, reprocha que el principio de proporcionalidad está suponiendo una disipación del contenido esencial, que se avala con la dialéctica de la razón empresarial.

El artículo 53.1 CE establece la necesidad de respetar el contenido esencial de los derechos expuesto en el capítulo segundo de la carta magna. El TC ha determinado que constituye el contenido esencial aquella parte del contenido de un derecho sin la cual éste pierde su particularidad. Es decir, se trata de lo necesario para que el derecho sea recognoscible como pertinente al tipo descrito, entendiendo que sin esas características el derecho quedaría desnaturalizado[39]. De esta manera, aclara el tribunal que se produce una vulneración del contenido esencial "*cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección[40]."*

Mediante sentencias relevantes del TC hemos desarrollado cuál es el contenido esencial de los derechos de intimidad, protección de datos y secreto de las comunicaciones. Sin embargo, el contenido esencial del derecho puede variar en función del "*momento histórico de que en cada caso se trata y a las condiciones inherentes en las sociedades democráticas, cuando se trate de derechos constitucionales[41]"*. No obstante, no es nuestra intención limitarnos a decir que ha cambiado el contenido esencial, eso se trataría de una falsedad, dado que la jurisprudencia actual sigue refiriéndose a esas sentencias relevantes que configuraron los contenidos de tales derechos.

---

[39] STC 11/1981, 8 de Abril
[40] Ripollés Rastrollo, A.(2017)Sinopsis del artículo 53 CE https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=53&tipo=2
[41] STC 11/1981, 8 de Abril

A lo que nos queremos referir es a que el magistrado plantea con este voto particular varios debates esenciales. El primero de ellos es el teórico conflicto de derechos constitucionales entre el poder de dirección, avalado por el artículo 38 CE y los derechos fundamentales. Derechos que son de diferente rango, gozando los segundos de especial protección y que por lo tanto, a la hora de plantearse la utilización del principio de proporcionalidad se debe recordar y tener siempre en cuenta el contenido esencial. En mi opinión, a nivel teórico resulta una crítica muy importante, puesto que a pesar de cambiar la jurisprudencia con el paso del tiempo y a pesar del crecimiento de la irrupción de la nuevas tecnologías frente a los derechos laborales, se trata de una premisa ajena a la evolución del tiempo que siempre hay que tener presente. Por lo tanto, no se trata de una crítica destructiva que manifiesta la necesidad de acabar con el sistema de proporcionalidad, (debido a su profundo arraigo en la doctrina sería imposible) sino una reflexión constructiva para intentar reconducir la razón esencial para la que se planteó. No obstante, desarrollaremos este planteamiento en las conclusiones.

Una vez expuesta la necesidad de considerar el contenido esencial como referencia para la aplicación del principio de proporcionalidad, Valdés indica en este caso concreto el hecho de tener el empresario una sospecha razonable de comisión flagrante no puede usarse como criterio en el juicio de proporcionalidad dado que vulnera el deber de información que forma parte del contenido esencial de derecho a la protección de datos [42].

Por otra parte, argumenta que no se está respetando la cláusula social que se establece en el artículo 33.2 CE. La función social (la clase trabajadora) queda reducida a los intereses del empresario que con el apoyo de los artículos 33 y 38 adquieren un rango de constitucionalidad. A su vez, hay que recordar los principios forjados por el artículo 1.1 de la CE, que reflejan, en palabras del magistrado, el nuevo modelo de relaciones laborales que garantiza a los trabajadores una cobertura de sus derechos fundamentales. Los valores están decayendo y se están fortaleciendo otros como los que reflejan las cláusulas de constitución económica que protegen los intereses del empresario. Valdés también realiza consideraciones

[42] No obstante, esta sentencia es de 2016 y veremos que en la aprobación del art 89 de la LOPD en 2018 sí que se incluye una referencia a la excepción del deber de información con carteles. Y por lo tanto sí que podría decirse que constituye un elemento para la proporcionalidad. Sobre ello profundiza el voto particular de la STC 119/2022. Sin embargo, nuestro objetivo en este apartado es centrarnos en la teoría de fondo que nos está exponiendo el magistrado.

sobre el caso que examinaremos en el apartado de videovigilancia, ya que se trata de la medida analizada en la sentencia.

El segundo conflicto que consideramos destacable es la necesidad de delimitar el contenido esencial del propio artículo 38 en lo que a poder de dirección del empresario respecta. El ya mencionado artículo 53 CE establece que hay que respetar el contenido esencial de los derechos que se indican en el capítulo segundo de la CE. Lo cierto es que artículo 38 es el último derecho que se dispone en el capítulo. Asimismo, hemos expuesto la opinión de Valdés respecto al rango de constitucionalidad de este derecho frente a los derechos fundamentales que se tratan en el trabajo. Al igual que en el primer apartado del trabajo, hemos expuesto la definición de la libertad de empresa y poder de dirección. Como última mención a este artículo, queremos manifestar la necesidad de desarrollar este contenido de la libertad de empresa en lo referente al poder de dirección para que no haya un constante choque entre este y los derechos fundamentales. Nos encontramos por lo tanto con un problema no solo de contenido esencial de derechos fundamentales (intimidad, secreto y protección de datos) sino también con un problema de contenido de libertad de empresa del artículo 38 CE.

Todas estas cuestiones relativas al principio de proporcionalidad van a ser clave para determinar la validez de la actuación del empresario. Cuestiones como son el deber de información y la expectativa de privacidad se han incorporado al juicio de proporcionalidad. En la siguiente parte del trabajo trataremos de ejemplificar cómo opera el principio de proporcionalidad y el deber de información en sentencias clásicas algunas ya comentadas y en sentencias más recientes.

V. Problemáticas

Decíamos al hablar del poder de dirección del empresario que este podía adoptar las medidas para vigilar y controlar el cumplimiento de los trabajadores. No obstante, la problemática del poder de dirección y los derechos fundamentales no abarca sólo la aplicación de una medida, como puede ser la instalación de un sistema de videovigilancia o un sistema de geolocalización. Sino que se discute también la validez de un medio de prueba obtenido bajo

el pretexto de control de dirección, como puede ser un correo electrónico o mensaje al que ha accedido el empresario sin conocimiento del trabajador, estando en juego en este caso la vulneración del derecho al secreto de las comunicaciones.

Las cuestiones que vamos a examinar son la videovigilancia, el acceso al correo electrónico de los trabajadores, la grabación de sonidos en el trabajo y la geolocalización de los trabajadores. En ellas veremos cómo operan los derechos de intimidad, secreto de comunicaciones y protección de datos.A pesar de organizar las sentencias dependiendo de la medida que se trate en el caso, cabe decir que todas ellas están relacionadas entre sí ya que el objeto de todas ellas es la discusión de si se lleva a cabo la vulneración de estos tres derechos, el deber de información y el principio de proporcionalidad.

1. La videovigilancia

El control de los trabajadores mediante videovigilancia queda confirmado hoy en día por el artículo 89 LOPD y el 20 bis del ET. La instalación de cámaras como medio de control y de prueba es una de las cuestiones más polémicas que opera en materia laboral respecto al derecho fundamental de intimidad y sobre todo en relación con el derecho de protección de datos. Este derecho está viviendo un desarrollo acelerado en todos los aspectos, a medida que se van incrementando las posibles medidas tecnológicas de control, la jurisprudencia y legislación tratan de adaptarse a la nueva era del derecho a la protección de datos.

Los sistemas de videovigilancia captan la imagen de los trabajadores, es por eso que se considera que puede, si no se establece la medida de manera correcta con los criterios que analizaremos, vulnerar el derecho a la protección de datos. El artículo 4.1 RGPD establece la definición de dato personal que se entiende como "t*oda información sobre una persona física identificada o identificable («el interesado»)"* En este sentido, procede el mismo artículo a explicar lo que se considera persona física identificable: "*toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador"*, y sigue la definición insertando ejemplos[43]. En el artículo 4.14 RGPD se especifica que *se consideran*

[43] Prosigue el art 4.1 RGPD indicando que: *como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*

datos biométricos aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Por lo tanto, la definición de dato personal abarca la imagen de una persona y por consiguiente, queda la imagen dentro de la cobertura del derecho a la protección de datos configurado por el artículo 18.4 CE [44].

De esta manera, cabe diferenciar el derecho a la propia imagen que se establece en el artículo 18.1 CE y el derecho a la protección de datos que abarca en el caso de las medidas de videovigilancia, la imagen grabada del trabajador y que está amparada por el artículo 18.4 CE. El primero de ellos puede estar vinculado con el derecho a la intimidad en lo que a la vida privada y familiar se refiere, sin embargo, el objetivo del derecho de imagen es proteger los atributos más característicos y definitorios de la propia persona, que son una posesión irreductible e inherente a ella[45]. Se define el derecho a la propia imagen como el "*derecho a controlar la captación, difusión y, en su caso, explotación de los rasgos físicos que hacen reconocible a una persona como sujeto individualizado"*[46]. Mientras que, como hemos explicado anteriormente, el propósito del derecho a la protección de datos es asegurar que las personas tengan control sobre su información personal, sin importar de qué tipo sea. Esto incluye el control sobre cómo se utilizan y a dónde se dirigen, con el fin de prevenir la circulación ilegal o el uso dañino de dicha información, lo cual podría vulnerar la dignidad y los derechos de aquellos que se ven afectados.[47] De esta manera, es el derecho de protección de datos el que queda involucrado respecto a las medidas de vigilancia, por lo tanto haremos hincapié en él, no en el derecho a la propia imagen. Por otra parte, mencionaremos el de intimidad, aunque sin embargo, es un derecho que se ha ido empleando cada vez menos en videovigilancia dado que ha ido consolidando la autonomía de éste respecto a la intimidad y que el uso las imágenes sin consentimiento supone en concreto una vulneración de la protección de datos.

---

[44] STC 119/ 2022 de 29 de septiembre
[45] ALCALÁ NOGUEIRA, H (2007) "El derecho a la propia imagen como derecho fundamental implícito: Fundamentación y caracterización" *Ius et Praxis*. Vol. 13, Nº. 2. Págs. 245-285
[46] Diccionario panhispánico del español jurídico. https://dpej.rae.es/lema/derecho-a-la-propia-imagen
[47] Preámbulo. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE núm. 294, de 6 de diciembre de 2018)

El contenido esencial del derecho a la protección de datos lo componen el deber de información del empresario y el consentimiento del trabajador. Como hemos analizado en su correspondiente apartado, este contenido se estableció en las sentencias clásicas y no ha cambiado desde entonces. Sin embargo, veremos que sí que ha cambiado a lo largo del tiempo la relación del principio de proporcionalidad respecto al deber de información, habiendo un debilitamiento de este y poniendo en manifiesto la problemática respecto a la vulneración del contenido esencial.

1.1 Las SSTC 29/2013 y 39/2016

La STC 29/2013 de 11 de Febrero de 2013 se trata de una sentencia clave en la que se establecen definitivamente estos dos pilares del derecho a la protección de datos. No solo para los casos de videovigilancia, sino para todas las medidas de control. En la sentencia se presenta el recurso de amparo de un trabajador en relación a los artículos 18.1 y 18.4 por haberle impuesto sanciones debido a unas pruebas captadas con cámaras. Se relata que el centro tenía sospechas de que un miembro del personal no estaba cumpliendo con su horario de trabajo y de esta manera, para confirmar las sospechas, decidieron utilizar las cámaras de videovigilancia que estaban instaladas en el exterior del edificio. Una vez que se confirmó que el empleado no estaba cumpliendo con sus obligaciones laborales, la universidad decidió tomar medidas disciplinarias. Se estima en esta resolución la vulneración del derecho de protección de datos de la recurrente, por no ejercer el centro un adecuado deber de información.

La STC 29/2013 fue pionera en establecer el planteamiento de que no es suficiente con la colocación de distintivos o carteles informativos aunque estos sean visibles para todos, sino que el empresario tenía que proceder a informar a los trabajadores. Esta información, debía de ser "*previa y expresa, precisa, clara e inequívoca a los trabajadores con la finalidad de controlar la actividad laboral a la que esa captación podía ser dirigida".* La descripción coincide con la que indica en el artículo 89.1 de la actual LOPD, que sin embargo, contiene también otro precepto controvertido en relación al deber de información que analizaremos a posteriori. Prosigue la sentencia indicando que esta información debe especificar las características y alcance del procesamiento de datos, estableciendo en qué situaciones las grabaciones pueden ser revisadas, la duración y los objetivos para los que se van a utilizar.

Además, precisa que el empresario debe concretar que las grabaciones pueden utilizarse para aplicar sanciones disciplinarias en caso de que se incumpliera el contrato laboral.

Por lo tanto,a modo de resumen, concluimos que la sentencia incorpora dos elementos esenciales y novedosos a la doctrina del TC respecto al deber de información del empresario. El primero de ellos es que, a diferencia de lo que se indicaba en la STC 186/2000, el deber de información a los trabajadores afectados no es una cuestión de legalidad ordinaria. Al contrario, se trata de una materia que adquiere alcance constitucional, dado que el deber de información forma parte del contenido esencial del derecho a la protección de datos. Por otra parte, la sentencia destaca que incluso cuando hay sospechas de incumplimiento de las obligaciones laborales y se haya establecido por el empresario que la grabación tendrá como objetivo obtener pruebas concretas de tales incumplimientos, el poder dirección empresarial no justifica la omisión de este deber[48].

Estas dos afirmaciones se ven contradichas por la ya mencionada STC 39/2016 que sienta un precedente sobre el derecho de información. En este caso, en la tienda donde trabajaba la demandante se instaló una cámara de videovigilancia sin que se notificara explícitamente a los empleados (aunque sí que se colocó un distintivo informativo en un lugar visible del establecimiento). A partir de las imágenes captadas por la cámara, se pudo verificar que la demandante en cuestión había sustraído dinero en efectivo de la tienda y por ello fue despedida. En esta sentencia se desestima la vulneración del artículo 18.1 y 18.4. Lo significativo del pronunciamiento es que se descarta la vulneración del derecho a la protección de datos debido a que la empresa ha cumplido en este caso con el deber de información colocando un distintivo informativo. La STC 29/2013, nos mostraba que no es suficiente con colocar un distintivo, sino que hay que informar a los trabajadores de que esas imágenes pueden ser objeto de sanción. En este supuesto parece ser que esa advertencia expresa no es necesaria, al igual que tampoco lo es el consentimiento de los datos por parte del del trabajador, ya que se considera implícito en la relación contractual, siempre y cuando el tratamiento de datos sea necesario para cumplir con el contrato que las partes han acordado. Por contra, si se utilizan los datos del trabajador para una finalidad diferente a lo establecido en el contrato, sí que será necesario el consentimiento del empleado.

[48] DAL-RÉ VALDÉS, F (2017) “Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa” *Revista de derecho social.* Nº 79 . Págs. 15-35

Estas afirmaciones, como ya exponíamos en el apartado del principio de proporcionalidad, suponen retroceso en materia de protección de datos. El consentimiento y el deber de información son los dos pilares fundamentales de este derecho fundamental. En este sentido, expone Valdés en su voto particular que este retroceso del deber de información supone un retorno hacia la aplicación de la tesis contractualista por el TC, en el que se primaba el contrato de trabajo por encima de los derechos fundamentales. Además indica el magistrado el hecho de que a pesar de que quedaba constatado que la medida vulneraba un artículo de la antigua LOPD sobre el deber de información, el tribunal decide aplicar el principio de proporcionalidad, lo que sin duda se trata de un *despropósito jurídico-constitucional*. Respecto al deber de información con las medidas de vigilancia, el profesor Daniel Toscani opina que es vital informar sobre la posibilidad de emprender sanciones a través de las medidas, ya que el trabajador puede llegar a pensar que esas medidas no tienen como finalidad el control de los empleados y por tanto acogerse al argumento de expectativa de privacidad [49].

En definitiva la STC 39/2016 supuso el fin de la era de exigencia informativa impuesta por la STC 29/2013, dando paso a una etapa de flexibilidad informativa, que es la que predomina en la actualidad[50]. En este sentido, el caso Lopez Ribalda integrará el deber de información dentro del principio de proporcionalidad, considerándolo un elemento más, lo cual supondrá también una debilitación del deber de información (lo analizaremos más adelante).

1.2 La STEDH López Ribalda II

En el caso Lopez Ribalda un supermercado instala cámaras de videovigilancia para controlar que no se produzcan robos tras detectar desajustes en el inventario. Para ello decide colocar cámaras en un lugar visible de la entrada, sobre las cuales se informa a los trabajadores y también coloca cámaras ocultas enfocando a las cajas registradoras sobre las cuales no se les avisa, las cámaras captaron a algunas trabajadoras apropiándose de los productos, tras enseñarles las grabaciones ella reconocen los hechos y son despedidas procedentemente.

[49] TOSCANI GIMENEZ, D. (2017) "Las facultades de la empresa de videovigilancia de sus trabajadores. Comentario a la STC 39/2016, de 3 de marzo" *Revista Boliviana de Derecho* Nº. 23 . Págs. 366-373
[50] HENRÍQUEZ TILLERÍA, S (2019) "Protección de datos, videovigilancia laboral y doctrina de la sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información." *IUSLabor*. Nº 3. Págs 55-80

Las trabajadoras recurrieron a los juzgados. El juzgado de instancia y el TSJ Cataluña ratificaron la validez de los despidos. De esta manera, deciden presentar un recurso al TEDH alegando una violación del art 8 y 6 CEDH. El 9 de enero de 2018 la cámara se pronuncia sobre el caso en la conocida como sentencia Lopez Ribalda I , en la cual estima la demanda de las trabajadoras. No obstante, el caso no acaba aquí, dado que el estado español recurre a la sentencia. El TEDH estima la demanda y emite el 17 de octubre de 2019 la sentencia Lopez Ribalda II que adopta una postura diferente a la anterior y que es en la que nos vamos a centrar en este trabajo.

La cámara de Estrasburgo razona que cada estado debe reflejar la protección de la vida privada del artículo 8 CEDH y por eso en este caso la normativa a aplicar es la LOPD 1999 dado que es la que es la que estaba vigente en el momento que acontecieron los hechos. Considera que los tribunales españoles aplicaron de forma correcta el principio de proporcionalidad siguiendo el modelo del caso Barbulescu, que expondremos posteriormente.

Por lo tanto, la cámara aplica el principio de proporcionalidad y llega a la conclusión de que la medida fue un fin necesario dado el interés legítimo de la empresa para comprobar la solución de los desajustes en el inventario y verificar los robos. En cuanto al deber de información, el TEDH afirma que se trata de un importante criterio a tener en cuenta para valorar la ponderación de la medida, pero que no es el único, debiendo valorarse junto a los demás criterios. En definitiva, integra el deber de información como un elemento más en este juicio. Esta consideración del tribunal supone que un elemento del contenido esencial del derecho a la protección de datos que debería quedar especialmente protegido, queda limitado a ser un factor más a analizar cómo es la idoneidad, necesidad y proporcionalidad. En este sentido podemos decir que el argumento coincide con la sentencia STC 39/2016.

Respecto a la sospecha razonable, la cámara rectifica lo defendido en la sentencia Lopez Ribalda I donde se indicaba que la sospecha razonable no era criterio suficiente para la instalación de cámaras ocultas. Por el contrario, la sentencia López Ribalda II indica que la mínima sospecha no es argumento suficiente para el incumplimiento del deber de información, pero que en este caso particular no se trata de una mínima sospecha, sino de una

justificación seria debida a las graves irregularidades y la cantidad de los robos constatados[51]. De esta manera, establece como criterios de gravedad el hecho de que las sospechas atenten al buen funcionamiento y al clima general de desconfianza de la empresa[52]. A mi parecer, estas consideraciones suponen la creación de una peligrosa zona gris: la determinación de cuándo se da o no se da una grave y razonable sospecha y qué criterios debemos tener en cuenta para delimitar la naturaleza de la sospecha. En este sentido, la STC 39/2016 argumenta que las sospechas eran previas y fundadas. Como conclusión cabe decir que la STC 39/2016 y la López Ribalda II integran el concepto de sospecha razonable en el juicio de proporcionalidad, como un elemento más, en la misma posición que el deber de información, lo que perjudica sin lugar a dudas al derecho fundamental de protección de datos del trabajador.

La LOPD actual se basa en la STC 29/2013 para configurar el artículo 89 sobre el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos. En el artículo se indica que el deber de información del empresario sobre la medida impuesta debe ser ser previo, expreso, claro y conciso y que además de avisar a los trabajadores, se debe informar de las medidas a los representantes de estos. Estos criterios respecto al deber de información se aplica para toda clase de medidas de control a los trabajadores.

Sin embargo, la ley tampoco ha ignorado los giros jurisprudenciales consolidados por las STC 39/2016. De manera que se establece la excepción del deber de información que establece en el párrafo siguiente en el supuesto de que el empleador haya captado la comisión flagrante de un acto ilícito. En ese caso bastará con haber tenido instalado el dispositivo informativo o pegatina que se detalla en el artículo 22.4 de la misma ley. Ahora bien, aunque la captación de comisión flagrante de un delito y el concepto de sospecha razonable no sean lo mismo, parece ser que la jurisprudencia los usa de forma complementaria, como veremos a continuación en la STC 119/2022. Otras veces, se menciona que la se ha captado el acto de comisión flagrante mediante un hallazgo casual, concepto que también analizaremos más adelante.

[51] BALAGUER LÓPEZ, M y MORAGUES RAMOS, F (2020) "Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad" *Lex social: revista de los derechos sociales*. Vol. 10, Nº. 2 . Págs. 506-540
[52] *Íbid*

En definitiva, esta disposición del artículo 89 LOPD abre una peligrosa puerta dado que confirma la validez de la aplicación del argumento de sospecha razonable, el cual se trata de un razonamiento poco analizado y queda por ver en qué situaciones cabe hacer uso de él. Sin duda alguna, supone un aspecto positivo para el empresario y negativo para el trabajador, ya que facilita el uso del control mediante videovigilancia y también la validez de la prueba obtenida por esta.

1.3 La STC 119/2022 del 29 de septiembre de 2022

En la reciente STC 119/2022 del 29 de septiembre de 2022 se analizan algunos de estos aspectos comentados en López Ribalda y la STC 39/2016. La sentencia relata el caso de una empresa que tenía colocada una cámara (sobre la cual se informaba mediante un cartel colocado en el exterior) que usa como prueba al quedar filmado claramente cómo un trabajador se lleva un producto de la empresa sin dejar registrada la factura, cometiendo una apropiación indebida. El TSJ del País Vasco y el TS determinaron que la prueba obtenida era ilegal, por lo tanto la empresa presentó un recurso de amparo al TC alegando que se había vulnerado el artículo 24.2 CE (derecho a la prueba).

Respecto a los derechos de intimidad y protección de datos, el tribunal describe que el deber de información forma parte del contenido esencial del derecho a la protección de datos. Sin embargo, el ya mencionado artículo 89.1 LOPD establece una disposición que permite eximir a los empresarios del deber de información. El Tribunal interpreta esta disposición de la manera que hemos indicado antes, estableciendo que *"la utilización de las imágenes captadas para verificar o acreditar la comisión flagrante de un acto ilícito no exigirá el previo deber de información"*. Podemos observar en esta afirmación la conexión que se hace entre la sospecha y la captación de la comisión flagrante, de modo que se podrán imponer las medidas si hay sospecha y así poder verificar la infracción. A mi parecer, esta disposición resulta francamente nociva para la garantía del derecho a la protección de datos. Esto se debe a que los tribunales pueden acogerse a la aplicación de esta dispensa para validar su prueba, sin tener que apoyarse en el resto de criterios que configuran el propio principio de proporcionalidad que ni siquiera se menciona en el apartado que analiza la vulneración derecho a la protección de datos. Por ende, parece que la excepción del artículo exime al tribunal de aplicar todos los medios de valoración que lleva consolidando la jurisprudencia

durante 30 años. La argumentación de los fundamentos de derecho resultan tán polémicas que son 5 magistrados que se atienen a un extenso voto particular que expondremos más adelante.

Por otra parte, antes de presentar recurso al TC, el Tribunal Supremo declaró sobre el caso que se había vulnerado el derecho a la protección de datos porque se había informado a los trabajadores que las cámaras se utilizarían con el fin de garantizar una seguridad y no se les había informado que se podían usar con fines disciplinarios. En este sentido, el Tribunal Supremo se ha pronunciado en varias sentencias indicando que "*el empresario no necesita el consentimiento del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral"*[53]. En este sentido considera el TS que la instalación de videovigilancia para seguridad incluye, además de la seguridad del centro de trabajo, la vigilancia de actos ilícitos de los empleados y de terceros. A la vez que excluye los tipos de control que no tengan que ver con la seguridad como pueden ser la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc...[54]" De esta manera se pronuncia también el TC en la sentencia que estamos analizando señalando que "*no tendría sentido que la instalación de un sistema de seguridad en la empresa pudiera ser útil para verificar la comisión de infracciones por parte de terceros y, sin embargo, no pudiera utilizarse para la detección y sanción de conductas ilícitas cometidas en el seno de la propia empresa. Si cualquier persona es consciente de que el sistema de videovigilancia puede utilizarse en su contra, cualquier trabajador ha de ser consciente de lo mismo."* Por lo tanto, se considera que no se ha vulnerado el derecho a la protección de datos.

En relación a la vulneración del derecho de intimidad, el tribunal expone que la medida cumple el principio de proporcionalidad. Me parece interesante destacar que el tribunal considera válida la medida dado que cualquier otra "*habría advertido al trabajador, haciendo entonces inútil la actuación de la empresa."* Este planteamiento carece de motivación probatoria alguna, suponiendo que una mera especulación del tribunal se convierte en una de las razones principales para ponderar la medida como necesaria. A mi parecer, se están considerando como argumentos para el principio de proporcionalidad suposiciones sin base alguna dejando claro que, como ya manifestó Fernando Valdés, el principio de

[53]STS 96/2017 (Sala de lo Social), de 2 de febrero de 2017 (recurso 554/2016)
[54] STS 77/2017 (Sala de lo Social), de 31 de enero de 2017 (recurso 3331/2015)

proporcionalidad muchas veces queda avalado por mera retórica que acaba favoreciendo al empleador[55]. En mi opinión, el tribunal está basando la excepción del deber de información en el planteamiento de que si el trabajador hubiese sabido de la medida, hubiese buscado otras formas de cometer el ilícito. Es decir, el tribunal está suponiendo que si hubiese sabido el trabajador que había cámaras instaladas en ese lugar, quizás habría dejado la bolsa en otro sitio y por ello era necesario colocar las cámaras en ese lugar y no informar a los trabajadores sobre ella. A mi parecer, se tratan de conjeturas que pueden resultar erróneas. Lo cierto es que a un trabajador que está informado de la grabación de las cámaras enfocando la caja registradora, quizás no se le hubiese ocurrido cometer el ilícito, dado que sabe que se le grabaría cometiendo la infracción.

Son cinco los magistrados que no están de acuerdo con algunas reflexiones llevadas a cabo en la sentencia y que se atienen al voto particular. En relación al deber de información del derecho a la protección de datos, los magistrados exponen un recorrido jurisprudencial en materia de videovigilancia muy parecido al que hemos hecho nosotros y llegan a la conclusión de que en efecto, esta excepción de sospecha razonable parece estar afincándose ahora no solo a nivel de doctrina, sino también a nivel legislativo. Sin embargo, el problema recae en que sentencia sitúa en este caso el deber de información (la regla general) y la captación de comisión flagrante (la excepción) en el mismo nivel, cuando esto no es así, puesto que se aplica como regla general el párrafo primero del art 89 LOPD y como excepción, el segundo párrafo. De manera que se tienen que llevar a cabo la explicación de las razones por las que se ha omitido el deber específico de información a los trabajadores y/o sus representantes. En el caso de la sentencia no se expresan estas explicaciones y por lo tanto no se debería conceder la excepción ni determinar la validez de la medida.

En este sentido se afirma que si se aplica este artículo sin necesidad de motivar nada más, cualquier mínima sospecha de ilícito podría justificar la instalación de un sistema de videovigilancia, y por tanto, si las sospechas resultan razonables, se pueden usar las grabaciones probatorias. En todo caso, deduzco yo, que el empresario siempre sale favorecido con esta excepción. Esto se debe a que en caso de que las sospechas fueran erróneas y se haya filmado a los trabajadores, al no usarse las grabaciones como medio de prueba (porque no se habrían realizado sanciones hacia ellos) los trabajadores quedan al

[55] STC 39/2016, Voto particular de Fernando Valdés

margen de ser informados. Sus derechos podrían haber sido vulnerados pero ellos nunca lo sabrían a no ser que descubran ellos mismos las cámaras instaladas.

Concluye el voto particular indicando que no se puede considerar que en este caso la captación de la comisión flagrante se haya llevado a cabo mediante un hallazgo casual. En mi opinión, los tribunales confunden tres conceptos a los que hacen referencia de la misma manera: la captación de la comisión del acto ilícito, la sospecha razonable y el hallazgo casual. Ha quedado claro por lo anteriormente expuesto que la sospechas razonables (teniendo en cuenta las directrices establecidas en Lopez Ribalda II para considerar qué es razonable) es un elemento que valida la instalación de cámaras. En ese sentido, no entiendo porque muchas argumentaciones de sentencias (como es la del caso) se empeñan en decir que la captación fue un hallazgo casual, cuando se ha indicado precisamente que se tenían sospechas y que en base de ellas se aplica la medida. A mi parecer, se debería de considerar que las sospechas descartan el hallazgo casual. Con esta consideración, no queremos decir que es relevante la distinción de conceptos para la determinación de la licitud o no de la medida, sino que simplemente tratamos de remarcar la necesidad de que los tribunales se pronuncien y diferencien ambos términos.

2. El acceso a los correos electrónicos y mensajería

La revisión de los correos electrónicos y mensajes como prueba de despido, es junto a la medida de videovigilancia, una de las cuestiones más desarrolladas y controvertidas en relación a la vulneración de los derechos fundamentales de los trabajadores mencionados. Se trata de una problemática muy amplia que aborda numerosas cuestiones en relación a los derechos fundamentales de intimidad y secreto de comunicaciones. En concreto engloba cuestiones como la utilización de algún correo del trabajador como medio de prueba, el uso del correo personal en el trabajo, la necesidad del empresario de establecer las reglas de uso del correo en las empresas y la expectativa de privacidad.

2.1 Las STCS 241/2012 y 170/2013

En la STC 241/2012 se presenta un caso de posible vulneración de derecho a la intimidad y secreto a las comunicaciones. Las trabajadoras de una empresa instalan un programa de mensajería en un ordenador de uso común. Los mensajes transmitidos quedan archivados en un fichero del ordenador al que se accede sin clave de acceso. Respecto al derecho de intimidad declara el Tribunal que no se ha vulnerado tal derecho. Lo cierto es que el tribunal apenas fundamenta su decisión, limitándose a decir que el hecho de estar instalado ellas mismas el programa en un ordenador común excluye de toda privacidad a las trabajadoras. Esta postura será criticada por el magistrado Valdés en su voto particular. Una cuestión que no se menciona en la sentencia y que me parece relevante es la naturaleza del contenido de los propios mensajes. Definitivamente, los mensajes eran personales, y se deberían de considerar dentro de la vida privada las interacciones sociales que realizan los trabajadores en el entorno laboral[56]. Veremos en la proxima sentencia a analizar, la STC 170/2013, que los mensajes no eran personales sino de naturaleza laboral. La distinción del contenido supone de una gran relevancia, sin embargo para el tribunal no parece importante, ya que la nula expectativa de privacidad parece eximir de todo tipo de razonamiento y principio de proporcionalidad.

En cuanto a la vulneración del derecho al secreto de comunicaciones, el Tribunal indica que hay 2 circunstancias que hay que tener en cuenta, 1) el ordenador era de uso común para todos los trabajadores de la empresa; y 2) la empresa había prohibido expresamente a los trabajadores instalar programas en el ordenador. En este sentido, expresa el tribunal que al ser el ordenador de uso común y por lo tanto la comunicación utilizada se considera abierta y no queda amparada por el secreto de las comunicaciones. Ya hemos expuesto la distinción entre comunicación abierta y cerrada a la hora de definir el derecho al secreto de las comunicaciones. En este sentido cabe recordar que las relaciones entre los trabajadores en horario laboral también forman parte de su vida privada y por lo tanto también opera el secreto de las comunicaciones en el trabajo. No obstante en este caso no se ha interceptado ni infringido nada porque no había nada que proteger. Además, en opinión del tribunal el hecho de que estuviese prohibido instalar programas supone todavía menos expectativa de privacidad. El tribunal se basa en pronunciamientos anteriores establecimiento de reglas de uso extingue la expectativa de privacidad, dado que "a*l no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el*

[56] STC 12/2012, de 30 de enero

uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo"[57] .

El magistrado Fernando Valdés formula un voto particular en el que pone en manifiesto varias cuestiones importantes sobre los dos derechos fundamentales. En él, expone al igual que en el voto particular de la STC 39/2016, la necesidad de proteger el contenido esencial de derechos fundamentales, al igual que critica que se está forjando doctrina alrededor de cómo establecen los empresarios las reglas de uso y que en función de ello, se limita el ejercicio del 18.1 y 18.3, lo que supone que el contrato de trabajo pueda restringir los derechos fundamentales. Sin embargo, ha quedado manifiesto en varias sentencias que el contrato de trabajo no puede implicar la lesión de derechos fundamentales[58], sin perjuicio de que pueda ser regulado por ley. Añade el magistrado su discrepancia sobre la desestimación de la vulneración del 18.3, por dos razones.
La primera, es que el hecho de haber establecido en las normas de uso prohibiciones, supone la imposición de sanción al trabajador, pero no da derecho al empresario a violar el secreto a las comunicaciones. En efecto, comparto esta opinión, dado que el hecho de que hubiese o no expectativa de privacidad no quita la interceptación de una comunicación privada. La segunda cuestión que critica Valdés es el hecho de que se considerase una comunicación abierta por el mero hecho de que el ordenador fuese de uso común. De esta manera, ilustra su opinión con el ejemplo físico de abrir las cartas depositadas en el casillero de otra persona aunque el buzón fuese común. El magistrado no hace ninguna consideración de la calificación del tribunal como hallazgo casual el haber encontrado los mensajes, sin embargo critica que tiene cierta dificultad encontrar los mensajes archivados por casualidad. De esta manera, manifiesta el Tribunal que hubo una voluntad intrusiva por parte de la empresa que no respetaba el principio de proporcionalidad que ni se menciona en los fundamentos jurídicos y que sabemos que es necesario aplicar.

En la sentencia STC 170/2013 del 7 de octubre se aborda la vulneración del artículo 18.1 y 18.3 desde un supuesto en el que la empresa hace uso del correo electrónico de una trabajadora como medio de prueba para corroborar la conducta improcedente de la recurrente. En el caso que se expone, la actora había enviado unos correos electrónicos con información confidencial a la empresa competente que perjudicaban a la empresa demandada. Los

[57] STS (Sala de lo Social), de 6 de octubre de 2011(recurso 4053/2010)
[58] STC 19/1985, de 5 de marzo

mensajes se enviaron mediante el correo profesional (de la empresa) de la trabajadora a través de un dispositivo propiedad de la empresa (ordenador). Estos dos factores tienen su importancia a la hora de valorar la actuación de la empresa. Los supuestos pueden ser varios:

- Mensaje desde correo profesional a través de dispositivo de la empresa (como ocurre en el caso)
- Mensaje desde un correo personal a través de dispositivo de la empresa
- Mensaje desde correo personal a través de dispositivo personal en horario de trabajo. Este supuesto no lo examinaremos ya que resultaría una evidente vulneración del derecho de intimidad y secreto de comunicaciones.

En la sentencia anterior abordábamos un caso sobre mensajería, sin embargo en este los mensajes intercambiados son correos electrónicos. Recordamos que los correos electrónicos pueden ser medios vulnerados y por lo tanto quedan amparados por tal derecho[59]. La jurisprudencia ha indicado que de antemano, los correos electrónicos quedan protegidos por el secreto de las comunicaciones, no obstante,"*es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentale*s"[60] La empresa tiene una facultad fiscalizadora sobre los correos electrónicos otorgados a los trabajadores, no obstante, deberá cumplir con el principio de proporcionalidad. En este caso se dictamina que se ha cumplido con tales requisitos.

Una cuestión relevante que destaca el tribunal es la importancia de establecer unas reglas de uso debido a que la intensidad con la que se va a valorar las medidas del empresario dependen de la configuración de la normativa e instrucciones de las herramientas informáticas[61]. Por consiguiente, cabe determinar una relación entre la expectativa de privacidad y las reglas de uso. La expectativa de privacidad se define como Un criterio a que sirve para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas y que pueda la persona encontrarse al resguardo de la observación o del escrutinio ajeno[62]. De manera que no puede considerarse que haya

[59] STEDH de 3 de abril de 2007, caso *Copland v. Reino Unido.*
[60] STC 241/2012, de 17 de diciembre
[61] STC 241/2012, de 17 de diciembre
[62] STC 12/2012, de 30 de Enero

una expectativa razonable cuando se participa de forma consciente en actividades que claramente pueden ser objeto de examen.

En el caso expuesto se contaba con la regulación establecida en el convenio colectivo. Es por ello que aunque la empresa no tuviese reguladas sus propias normas de uso, el convenio colectivo si que podía contener disposiciones que hay que tener en cuenta[63]. El convenio aplicable disponía que sólo estaba permitido al trabajador el uso del correo profesional para cuestiones sobre el trabajo, indicándose una prohibición expresa del uso extralaboral con la sola excepción de comunicarse entre trabajadores. En mi opinión, la mera regulación de las reglas de uso por el convenio colectivo sin que éstas queden reflejadas ni informadas en la normativa de la empresa, entraña un grave problema de desinformación para los trabajadores (veremos que la sentencia barbulescu II supone un cambio al respecto). Además, supone un punto a favor para la empresa en lo que a argumentación se refiere porque muchos trabajadores no suelen estar informados ni conocen el convenio.

Se utiliza este mismo argumento para desestimar descartar la vulneración del derecho al secreto de las comunicaciones pero también para desestimar la vulneración del derecho de intimidad, debido a que la configuración de reglas de uso extingue la expectativa de privacidad. En este sentido, hace una reflexión parecida a la sentencia a la STC 241/2012, indicando que la nula expectativa de privacidad supone que el empresario, cumpliendo con el principio de proporcionalidad, puede acceder a los correos que le servirán como medio de prueba. En esta sentencia se hace más referencia al cumplimiento del principio de proporcionalidad que en la anterior. Se mencionan en este aspecto ideas interesantes como la sospecha y la necesidad de la medida. Sobre esta última indica el Tribunal que era necesario el acceso para obtener un medio de prueba válido contra el trabajador. La medida se considera proporcional puesto que el contenido de los correos a los que se accede trataban ta solo sobre información de la empresa y no sobre aspectos específicos de la vida personal y familiar. En mi opinión, se trata de un argumento considerable para la discusión sobre la vulneración de la intimidad, de manera que los mensajes de índole personal deberían de quedar más protegidas.

[63] STC 29/2013, de 11 de febrero

2.2 La STEDH Barbulescu II

La STEDH Barbulescu II es, junto a la STEDH Lopez Ribalda II, una de las sentencias del Tribunal Europeo de Derechos Humanos más mencionadas en los casos de medidas de empresario frente a los derechos fundamentales. La doctrina que fija respecto al principio de proporcionalidad se ha utilizado como referencia y argumento para todo tipo de conflictos.

El caso Barbulescu consta de dos sentencias, la primera se publica el 12 de enero de 2016 y en ella desestima la vulneración del artículo 8 del CEDH, dando la razón a la empresa. No obstante, el trabajador demandante formula una petición de reenvío a esa sala. La STEDH Barbulescu II se emite el 5 de septiembre de 2017 y deja sin validez la primera, estimando la vulneración de tal artículo. Siendo por lo tanto es en la que nos vamos a centrar. La segunda sentencia rectifica la decisión tomada anteriormente y declara que el Estado rumano ha vulnerado el art. 8 del CEDH. Los hechos consisten en el despido de un trabajador por usar el el programa de mensajería y los recursos de la empresa con fines personales. A la hora del despido la empresa le enseña al trabajador un documento donde aparecen mensajes intercambiados con su novia y hermano, cuando quedaba prohibido usar los recursos de la empresa (y por tanto el programa de mensajería en el que trabajaba) para fines personales.

La sentencia tiene en cuenta dos elementos para fijar el debate y exponer varias cuestiones siguiendo el principio de proporcionalidad. De esta manera indica el Tribunal que las reglas de uso establecidas por el empresario no pueden reducir a la nada el ejercicio de la vida privada social en el lugar de trabajo, sin embargo, se debe tener en cuenta el interés legítimo de la empresa para asegurar su buen funcionamiento[64] .

Una de las cuestiones destacables de esta sentencia y que supone un cambio de doctrina respecto a las sentencias mencionadas es lo dispuesto sobre las reglas de uso del empresario. La sentencia, al igual que se venía determinando por nuestros tribunales, dispone que sí que se puede destruir la expectativa de privacidad con el establecimiento de las reglas de uso. Sin embargo, el mero establecimiento general de las reglas no es suficiente, sino que la empresa debe advertir a los trabajadores tanto de las prohibiciones, como de la posibilidad de control o

[64] BONETE DESDENTADO, A y DAROCA DESDENTADO, E (2018) "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador." *Revista de información laboral.* Nº. 1, Págs. 19-39

supervisión y acceso de las comunicaciones. Y debe hacerlo de forma previa, clara y expresa. Esta sentencia servirá también de modelo para regular el deber de información a los trabajadores en materia de videovigilancia y para la incorporación del artículo 89 en la LOPD en 2018. Veíamos en la STC 170/2013 que con haber establecido normativa en el convenio colectivo era suficiente, sin embargo, en la sentencia Barbulescu II se establece que además de haber reglas de uso, es necesario que se informe al trabajador sobre ellas. El TEDH opina que no se cumplió este requisito. La empresa sí advirtió al trabajador de la prohibición de usar internet con fines personales, sin embargo no cumplió con los requisitos de que sea una advertencia previa, expresa y clara[65].

Además del deber de información (mencionado por la sentencia como principio de transparencia), se analizan de esta manera los criterios de idoneidad (justificación para la aplicación de la medida) , necesidad (si la medida podría haber sido menos intrusiva) proporcionalidad(en este aspecto se analiza la relación causa- efecto de la medida y el equilibrio entre el fin alcanzado y los derechos fundamentales)[66].

Podemos ver por lo tanto, que esta sentencia supuso un avance para la protección de derechos fundamentales que habían mermado las SSTC 29/2013 ya que remarcó la necesidad del deber de información de las reglas de uso. No obstante, en mi opinión, siguen habiendo cuestiones en las que no se profundiza como puede ser la naturaleza del contenido de los mensajes y su relevancia con el derecho de intimidad. En este caso los mensajes eran claramente personales y no tenían repercusión ni eran perjudiciales para la empresa, como sí ocurría en las sentencias 29/2013 y 241/2012. En la primera se trataban de correos sobre información confidencial para la competencia y en el segundo caso es más controvertido dado que también se trataban de mensajes personales pero que versaban sobre los trabajadores de la empresa. No obstante, los mensajes intercambiados en el caso Barbulescu se tratan de mensajes personales cuyo contenido no afectaba a la empresa. Es por ello considera el tribunal que la empresa no justificó suficiente como para cumplir el requisito de necesidad y proporcionalidad de la medida.

---

[65] *Ibid*

[66] ORMAECHEA TERRADILLOS, M. E. (2017) "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español" *Revista de derecho social.* Nº 80. Págs. 139-162

La STEDH enumera todos los principios que se debe de tener en cuenta en el momento de valorar la medida. De esta manera, ¿Podemos decir que está poniendo al mismo nivel el principio de deber de información y el resto de principios? Hay que tener en cuenta que la sentencia critica la decisión de tribunales rumanos y no españoles, por lo tanto no podemos hablar de teoría constitucional española ni vulneración del contenido esencial. Cuestiones que sí se tratan en la ya analizada STEDH Lopez Ribalda II (que critica la decisión de los tribunales españoles) y que por tanto tendremos más en cuenta para fijar nuestra opinión sobre la evolución del principio de proporcionalidad. En este sentido, expone la profesora Edurne Terradillos que se deben tener en cuenta los principios del test barbulescu, pero considerando que si no se cumple el contenido esencial del derecho al secreto de las comunicaciones, no cabe proceder al examen del resto de principios del juicio de proporcionalidad sobre la medida[67]. El nivel de importancia que tiene el deber de información y otros elementos del contenido esencial respecto al principio de proporcionalidad, es una de las cuestiones más relevantes que queremos destacar en este trabajo. En este sentido opina la profesora Terradillos que hay que hacer un uso adecuado del principio de proporcionalidad debido a que su errónea aplicación supone tergiversar la razón para la que se planteó, pasando de ser un héroe a ser un villano para los derechos laborales[68].

2.3 Doctrina del Tribunal Supremo

Pasaremos ahora a analizar sentencias recientes del Supremo para ver cómo aplican estos principios. La STS 119/2018, conocida como caso *Inditex*, nos describe el supuesto de una trabajadora que es despedida por usar el correo electrónico corporativo para hacer transferencias de dinero sin compras a otro negocio, es decir, por transgresión a la buena fe contractual. En este caso el TS se pronuncia a favor de la empresa, estimando el recurso de casación y estableciendo que se cumple el principio de proporcionalidad y los criterios fijados en el test de Barbulescu. Considera el tribunal que el deber de información se ha llevado a cabo correctamente, dado que cada vez que los trabajadores hacían uso del ordenador de la empresa, se recordaban en la pantalla las reglas de uso (la prohibición de usar el correo con fines que no fuese la prestación laboral), al igual que la posibilidad del supervisión de los correos por parte de la empresa y cuando se planteaban, el trabajador debía

[67] *Ibid*
[68] *Ibid*

aceptarlo. Sin duda alguna, esta sentencia nos demuestra que el empleador tiene muchas maneras de llevar a cabo el deber de información, siempre que esta sea clara, expresa y previa, unas características que pueden resultar interpretables según el caso.

Por otra parte, a diferencia de las medidas de videovigilancia, en los conflictos de mensajería y correos electrónicos no se exige una sospecha razonable y previa para acceder a los correos, sino que una vez cumplidos los requisitos de información, el empleador puede acceder a todos los correos de esa cuenta.

La STSJ Cataluña 1208/2023 del 20 de febrero de 2023 es la sentencia más reciente que hemos podido encontrar en nuestro empeño de que este trabajo quede actualizado a la jurisprudencia de hoy en día. En ella hemos podido comprobar que se siguen aplicando los criterios del test Barbulescu y también hemos podido verificar el increíble avance tecnológico de las empresas en cuanto al control de los trabajadores. El TS avala en esta sentencia la capacidad del empresario para recuperar correos electrónicos ya borrados a través del acceso al servidor de la empresa. En la sentencia se expone el caso del despido a una trabajadora por transgresión de la buena fe contractual y competencia desleal puesto que la trabajadora utilizó información de la empresa para favorecer a la empresa de la competencia que era de su marido. El tribunal se pronuncia a favor de la empresa y desestima la vulneración de los artículos 18.1, 18.3 y 18.4 que alegaba la actora debido al acceso de la empresa a los correos electrónicos que verificaban sus actuaciones. El tribunal confirma que la actora ya conocía la prohibición de utilizar los recursos de la empresa con otra finalidad que no fuesen las prestaciones laborales, se había entregado una circular al respecto. De esta manera, confirma que la empresa ha cumplido con las exigencias del test Barbulescu, además de que hubo una sospecha por parte de la empresa, derivada de un hallazgo casual de un trabajador que le permitía sin lugar a dudas acceder al correo corporativo de la trabajadora.

Por último, la intromisión hecha por la empresa fue mínima, ya que se limitaron a buscar tan solo los correos respectivos al caso(al igual que se hizo en la STS 119/2018). La empresa contrató a otra compañía especializada para encargarse de reunir las pruebas. Resulta increíble la precisión con la que se describe en la sentencia sobre cómo se accede a los archivos. Sin duda alguna, el incremento de las herramientas tecnológicas facilita al empresario llevar a cabo un control de los trabajadores.

3. Las grabaciones de audio como medida de control de los empresarios

Más que medidas de control, muchas veces en este trabajo nos hemos referido a medios de prueba para el empresario para una posible sanción o despido. No hemos querido abarcar el lado procesal de las sentencias, dado que nos hemos centrado en el desarrollo de los derechos fundamentales, sin embargo cabe decir que los aspectos procesales tienen una enorme relevancia para determinar la validez de una medida y la vulneración o no de derechos fundamentales. Así ocurre también con las escuchas telefónicas y grabaciones de sonido realizadas por el empresario y utilizadas como medio de prueba.

Las grabaciones de sonido como medida y prueba son mas inusuales de ver, que las que hemos abordado previamente y suelen considerarse más intromisivas para el derecho de intimidad, debido a que es más difícil cumplir con el requisito del deber de información. Por lo tanto, se exigirá el principio de intervención mínima y proporcionalidad[69]. En este aspecto veremos un caso de micrófonos ocultos y de llamadas telefónicas grabadas por la empresa La grabación de audios queda consolidada como posible medida de control en el artículo 89.3 LOPD. En este precepto se establece la posibilidad de utilizar la grabación de sonido en el trabajo solamente cuando existan riesgos relevantes para la seguridad de las instalaciones, bienes y personas debido a la actividad desarrollada en el lugar de trabajo. Añadiendo también la necesidad de respetar el principio de proporcionalidad. Podemos apreciar que se hace un tratamiento parecido al de la medida de videovigilancia, sin embargo no se hace mención alguna sobre el deber de información en este caso. Además se establece en el artículo 22.3 de la LOPD que la eliminación de los datos se llevará a cabo en un período no superior a un mes a partir de su recopilación, a menos que sea necesario conservarlos para demostrar la comisión de actos que pongan en peligro la integridad de personas, bienes o instalaciones.

La STC 98/2000 es una sentencia que ya hemos citado en este trabajo. La cual junto con la 186/2000, fue clave para delimitar el contenido esencial del derecho a la intimidad y proteger las circunstancias y lugares en los que no podía el empresario llevar a cabo la instalación de medidas para controlar a los trabajadores. Al ser una sentencia relevante, se aplica a todo tipo de medidas, no solo grabaciones de sonido. El TC cuenta como el Casino de La Toja, S.A

[69] BALAGUER LÓPEZ, M y MORAGUES RAMOS, F. Op. cit.

utilizó como medio de prueba las grabaciones hechas en la caja y la ruleta del casino. Para cuando se publica esta sentencia, ya había quedado consolidado que no se podían instalar medios en aseos, comedores, ni lugares privados. Sin embargo, ello no quita el hecho que la instalación de micrófonos en otro lugar sea válida y no vulnere el derecho de intimidad del trabajador. En este caso, la instalación de los micrófonos en la zona de la ruleta y la caja registradora. El tribunal hace ciertas consideraciones sobre el derecho de intimidad que ya hemos mencionado en este trabajo, como es la necesidad de proteger las relaciones entre los trabajadores. Termina dando la razón al trabajador y declara la vulneración del derecho a intimidad. La medida no fue proporcional debido a que la empresa no terminó de justificar que esta fuese indispensable para la seguridad y el buen funcionamiento de la empresa.

La problemática de las interceptaciones de las escuchas telefónicas ha sido tratada por la jurisprudencia del TEDH afirmando que las llamadas telefónicas que proceden de locales profesionales pueden incluirse en los conceptos de "vida privada" del artículo 8 del CEDH[70]. La cuestión de las escuchas telefónicas se consideran grabaciones de sonido y por tanto también afectan al derecho de intimidad y al de secreto de las comunicaciones. Además, en la La STC 160/2021 se plantea por primera vez en el TC una vulneración del derecho a la protección de los datos (en la STC 98/2000 habíamos analizado las grabaciones desde la perspectiva de vulneración al derecho de intimidad y en esta se alega la vulneración del artículo 18.4 CE).En ella la recurrente trabajadora alega que no se ha cumplido con el deber de información. La empresa sí le advirtió de que las grabaciones podían servir para la supervisión de su trabajo (queda constatado la multitud de reiteraciones que le hizo el empleador en cuanto a correcciones sobre su forma de trabajo) . Pero por otra parte, la empresa había firmado un acuerdo con los representantes en el que se establecía que no se podían usar los datos personales de las grabaciones para imponer sanciones. Debido a ese acuerdo, expresa la trabajadora que la sanción además de ser nula, vulnera el derecho a la protección de datos por usar las grabaciones para un fin distinto.

De esta manera, el tribunal se centra en delimitar si ha habido una vulneración del derecho de protección de datos en relación a el uso de las grabaciones por parte de la empresa, tras haber sido el trabajador renuente a las indicaciones de la empleadora y por tanto ser esa actitud la que supone la aplicación de sanciones. El tribunal resuelve el supuesto desestimando la

[70] STEDH de 3 de abril de 2007, caso *Copland v. Reino Unido.*

vulneración del derecho de protección de datos, dado que, como hemos dicho, en un principio la intención de la empresa era mantener el servicio y visto que la trabajadora no hacía caso, tomar medidas. Además, afirma que el empresario dejó clara la posibilidad de grabar para el control de los trabajadores. Indica también que la determinación de la nulidad o no del despido no corresponde al tribunal. Por lo tanto, concluimos que el tribunal no considera vulnerado el deber de información.

4. La Geolocalización de los trabajadores

Hay una clara conexión entre el poder de dirección de los empresarios y las nuevas tecnologías. En este trabajo no nos hemos referido todavía a ellas expresamente, puesto que considero que las medidas tratadas hasta ahora son problemáticas clásicas. La videovigilancia es la cuestión de fondo que se trató en la trascendental STC 186/2000 que fue una de las sentencias que sirvió para delimitar los derechos de intimidad y protección de datos. Asimismo el acceso del empresario a los correos electrónicos o mensajería mediante medios digitales, si que son más recientes que la videovigilancia, pero hay sentencias antiguas que ya nos muestran la problemática del acceso a correspondencia, líneas telefónicas o las grabaciones de sonidos. Aunque la tecnología, cada vez más precisa afecta a todas las medidas, suponiendo un mayor control para el trabajador, hay medidas que se pueden considerar completamente nuevas y tecnologizadas, como pueden ser los controles biométricos de los trabajadores o la geolocalización, la cual es en la que nos centraremos en este trabajo.

Los datos de localización se definen como "*cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público"*[71]. Estos datos son usados por los GPS(Global Position System) y GSM (Global System for Mobile Communications) para obtener una información más exhaustiva de la ubicación del trabajador[72]. No cabe duda de que cada vez más las empresas se interesan en obtener e implantar sistemas de localización como medida de control, dado que en muchos casos el trabajador opera fuera del centro de trabajo, como suele suceder en los trabajos que consisten

[71] Artículo 2.c). Directiva 2002/58/CE, del Parlamento Europeo y del Consejo de 12 de julio, sobre la privacidad y las comunicaciones electrónicas. (Diario Oficial de las Comunidades Europeas)
[72] ORRICO FERNÁNDEZ, F. J. (2021) *Criterios sobre usos de dispositivos tecnológicos en el ámbito laboral : hacia el equilibrio entre el control empresarial y la privacidad del trabajador.* Tirant Lo Blanch. Pág. 331

en conducir con un coche de la empresa. Resulta una medida óptima para los empresarios, pero si esta no se establece de la forma correcta, puede vulnerar los derechos de intimidad y protección de datos del trabajador.[73] La geolocalización se consolida como posible medida de control en el artículo 90 de la LOPD. En el apartado segundo de dicho artículo se establece el deber de información para los casos de geolocalización. Se indica en la disposición que la información debe ser clara, expresa e inequívoca, igual que con el resto de medidas que hemos mencionado, veremos cómo opera este requisito en la práctica en los casos de geolocalización. Por otra parte, como en todas las medidas que hemos visto se requerirá un juicio de proporcionalidad que veremos cómo se ejerce.

La sentencia 163/2021, de 8 de febrero relata el conocido caso Telepizza. En ella se expone que la empresa Telepizza obliga a los repartidores a poseer un dispositivo móvil personal con conexión a internet para poder acceder a la aplicación de la empresa con el fin de conocer su localización para saber cómo iba el reparto de las pizzas. Se trata de una demanda conflicto colectivo (sobre el que no entraremos demasiado, dado que nos centraremos en los aspectos respectivos a la geolocalización, el derecho a la intimidad y el de protección de datos) que se resolvió con la SAN 13/2019, la cual estimó la demanda y declaró la nulidad del proyecto de la empresa. La sentencia desestima el recurso de casación de la empresa Telepizza y confirma el fallo de la SAN 13/2019.

La sentencia de la Audiencia Nacional considera que para que se pueda implantar la geolocalización para los trabajadores se tiene que cumplir con el deber de información y aplicar el principio de proporcionalidad[74]. De esta manera, aunque la medida beneficie al cliente, considera que es una medida de control del empresario para el desempeño del puesto de trabajo. Respecto al principio de proporcionalidad, menciona el tribunal de la Audiencia que no le parece incorrecta la implantación de la medida de geolocalización, dado que otras empresas del sector ya disponen de ella. Sino que esta en concreto no cumple el principio de proporcionalidad, en concreto el criterio de necesidad, dado que se podía haber pensado en sistemas menos intrusivos para los derechos fundamentales, como por ejemplo implantación

[73] Se confirma la posibilidad de utilizar la geolocalización como medida en el artículo 20 bis ET: "*los trabajadores tienen derecho a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales"*

[74] STSJ Andalucía 2269/2017(Sala de lo Social), de 19 de Octubre de 2017(recurso 1149/2017)

de sistemas de geolocalización en los vehículos con los que hacen los repartos, de manera que no supondría aportar medios propios ni datos de carácter personal a la hora de descargar la aplicación. Por otra parte, en cuanto al deber de información, alega que tampoco se cumple el artículo 90 LOPD ni el reglamento 679/2016. Es complicado abordar este tema sin adentrarse en precisiones sobre el comité de empresa, por lo tanto, nos limitaremos a decir que no se realizaron bien los trámites de información al comité (art 64 ET) y por lo tanto considera el tribunal que el derecho de protección de datos de los trabajadores ha sido vulnerado.

La STS 163/2021 desestima el recurso interpuesto por Telepizza y confirma la sentencia de la Audiencia. Respecto al principio de proporcionalidad, confirma que la medida no es conforme a derecho y que el principio que no se ha respetado es el de necesidad, no idoneidad, por lo ya establecido en la sentencia de la AN. Respecto al deber de información, indica que efectivamente no se cumplen con los artículos que regulan el deber de información, ya citados. Efectivamente se incumple con lo establecido en la ley respecto a la información del comité. Considera un abuso de derecho el hecho de que si el trabajador no sigue las instrucciones del proyecto, le supondría una causa de suspensión y extinción del contrato, al igual que también se llevaría a cabo la suspensión en el caso de que los trabajadores no aportasen su propio teléfono móvil o éste no cumpliese las condiciones que se le imponen. Con esta sentencia parece que se está dando más importancia a la información al comité. Se trata de una sentencia sumamente importante en general para la gente que trabaja en plataformas digitales[75].

La STS 766/2020 de 15 de septiembre relata un caso más sencillo y se centra más en los límites del empresario y derechos fundamentales, que es lo que abordamos en el trabajo. En ella se relata el caso de una trabajadora que está en periodo de incapacidad, es decir, no acude al trabajo ni se tendría que desplazar con el coche de la empresa que tenía GPS instalado. El empresario despide a la trabajadora tras detectarse que ha habido un uso excesivo del coche durante los fines de semana y fuera de horario de la trabajadora,contraviniendo la prohibición de usarlo cuando no esté trabajando sin autorización de la empresa. Teniendo en cuenta además que la trabajadora estaba de baja. La sentencia estima el recurso presentado por la empresa, dejando sin validez la STSJ Andalucía 2269/2017 que declara nulo el despido. El

[75] SEMPERE NAVARRO, A. V. Vídeo-comentario a la STS 84/2021, de 8 febrero. Aranzadi. https://webcastlive.es/aranzadi/actualizacion-profesional/2021.htm?id=TS-163-2021_08-02-2021_RJ-2021-672

TSJ de Andalucía hace 3 apreciaciones a tener en cuenta: la geolocalización fuera de la jornada de trabajo, la vulneración del 18.4 y el deber de información contenido en este.
Respecto a la jornada, establece que es un factor a tener en cuenta, y que en un principio el control de geolocalización impuesto en un vehículo es lícito dado que es razonable que el empresario quiera controlar el cumplimiento laboral, siempre que este se lleva a cabo dentro de la jornada laboral[76]. Critica la sentencia que la geolocalización como función de control en la jornada carece de sentido cuando el empresario lo lleva a cabo fuera de jornada. Por otra parte, en relación a la vulneración del derecho a la protección de datos, establece que no se ha cumplido con el deber de información y tampoco hay ninguna justificación de sospecha razonable. Los datos se utilizaron para finalidades distintas y eso requiere un aviso complementario que no se da en el caso.

Respecto a estos elementos, la STS 766/2020 estima que la trabajadora conocía ya que el vehículo estaba geolocalizado y también conocía la prohibición de usarlo fuera de la jornada. La empresa no ha incurrido en vulneración de datos ya que la geolocalización era permanente y estaba dentro de sus funciones. Por otra parte, el seguimiento de la localización de la trabajadora mientras está en el coche, no supone ninguna intromisión a la protección de datos, dado que no se ha desvelado ninguna circunstancia personal suya. De esta manera, se declara el despido procedente. Como conclusión tengo que decir que esta sentencia me han quedado tres cuestiones pendientes: la geolocalización fuera de jornada, los límites a la geolocalización permanente, y si la empresa podría desactivar o no la opción del dispositivo.

Respecto a la geolocalización permanente la STSJ de Madrid, establece que la activación del control geolocalizado en un vehículo las 24 horas del día, todos los días del año era exhaustivo y se extralimita del poder de dirección del empresario, lo que suponía una invasión de la vida privada[77]. Entonces, ¿ puede operar la geolocalización fuera de jornada? Las STSJ Madrid, núm. 739/2014 de 29 de septiembre y la STSJ 3058/2017, de 27 de diciembre establecen que es ilícita la medida porque no hay consentimiento de los trabajadores en usar la geolocalización fuera de la jornada, pero no se dice nada en caso de que haya consentimiento. La argumentación de estas sentencias, debería de ser suficiente para entender la errónea fundamentación de la STS 766/2020 comentada.

[76]STSJ Galicia 668/2014(Sala de lo Social), de 17 de Enero de 2014 (recurso 3483/2013)

[77]STSJ Madrid 763/2019 (Sala de lo Social), de 12 de julio de 2019 (recurso 197/2019)

VI. Conclusiones

Consideramos que debemos dividir las reflexiones realizadas en este estudio en tres apartados: la irrupción de las nuevas tecnologías respecto a las medidas de control que supone para los trabajadores , el argumento de la sospecha razonable como eximente del deber de información y por último abordaremos varias cuestiones sobre el principio de proporcionalidad. Todas estas problemáticas están conectadas a su vez y se han reflejado en muchos de los votos particulares que hemos expuesto.

1. La evolución y el incremento de la tecnología ha supuesto el desarrollo de los medios de control del empresario. En mi opinión, en este trabajo no hemos abordado medidas que entran dentro de la definición nuevas tecnologías (a excepción de la geolocalización) dado que la videovigilancia, el acceso a la mensajería y la grabación de sonidos se consideran medidas más bien clásicas. No obstante, no significa que la tecnología quede al margen a la hora de valorar las medidas, sino que hemos podido ver en varios casos la importancia de este elemento para obtener la prueba. Esto se refleja en el caso sobre acceso a correos electrónicos en la STSJ Cataluña 1208/2023 en la que la empresa pudo acceder a los correos borrados de la trabajadora contratando a una empresa especializada que pudo acceder al software. Además esta tecnología permite la instalación de dispositivos cada vez más sofisticados y novedosos como son la ya mencionada geolocalización o los controles biométricos a los trabajadores.

2. Los tribunales han confirmado que la sospecha razonable de haber cometido un delito flagrante supone una dispensa para no cumplir el deber de información que debe ser previo, claro y expreso. También hemos visto que muchas sentencias, entre ellas la Lopez Ribalda II y la STC 119/2022, han indicado que no cualquier sospecha es suficiente como argumento, sino que estas deben ser previas a la comisión de la infracción y deben ser fundadas (razonables). Respecto a qué se considera una sospecha razonable, la sentencia Lopez Ribalda estableció que en ese caso la sospecha de robo estaba fundada por deberse a varias pérdidas identificadas. El TEDH considera además que el hecho de que la sospecha recayese sobre una acción cometida por parte de varios empleados supone también una razón de interés legítimo al ser una circunstancia que crea una atmósfera general de desconfianza en el lugar de

trabajo. En la STC 119/2022 el tribunal se limita a decir que le pareció razonablemente sospechoso y digno de ser comprobado el hecho de encontrar el día anterior del despido una bolsa con el logotipo de una empresa de la competencia que contenía el objeto de la empresa que desapareció (alguien se apropió indebidamente de él). En este sentido, cabe decir que la delimitación de sospecha razonable resulta en mi opinión una cuestión de índole probatoria a la que debe darse importancia y sobre la que deben los tribunales establecer más requisitos para su consideración. Por ejemplo en el caso de Lopez Ribalda II podrían quedar probadas las sospechas con la contabilidad y pérdidas de los productos. En las sentencias que hemos analizado no se le da suficiente importancia a la naturaleza de la sospecha, confundiendo la necesidad del juicio de proporcionalidad con la excepción del deber de información en caso de sospecha razonable. La excepción del deber de información forma parte del juicio de proporcionalidad, pero el deber de información no. Como analizaremos próximamente, el deber de información queda fuera del juicio de proporcionalidad. Por lo tanto, la determinación de sospecha razonable debido a las circunstancias podrá eximir tras el juicio de proporcionalidad el deber de información previa, clara y expresa en su caso, pero siempre mediante una motivación profunda sobre ello teniendo en cuenta todos los factores.

En este sentido cabe mencionar el voto particular formulado en la STC 119/2022 donde algunos magistrados ponen en manifiesto el peligro que entraña la escasa delimitación de las sospechas que deben tenerse en cuenta, ya que se podría hacer uso de la excepción contenida en el del artículo 89.1 LOPD en un número inaceptablemente elevado de casos. Este artículo no debe usarse con el propósito de avalar las meras sospechas y confirmar el debilitamiento del deber de información.

3. Por último, destacaremos algunas consideraciones sobre el principio de proporcionalidad. El magistrado Fernando Valdés hizo una importante crítica sobre en el voto particular de la STC 39/2016, la cual queda analizada en su apartado correspondiente. En resumen, lo que quiere poner de manifiesto el magistrado es la necesidad de respetar el contenido esencial de los derechos fundamentales. Es cierto que la empresa tiene un poder de dirección y control sobre los trabajadores, no obstante los derechos fundamentales pertenecen a todos los ciudadanos y por tanto deben respetarse en el trabajo también. Por lo tanto, a la hora de aplicar el principio de

proporcionalidad es necesario tener en cuenta el contenido esencial de cada derecho fundamental. En este sentido, el empresario sí que puede aplicar medidas cuando sea necesarias, idóneas y proporcionales al derecho fundamental afectado. Sin embargo, en mi opinión, hay elementos que deben respetarse siempre, o al menos tener más en cuenta. Un ejemplo de ello puede ser el debilitamiento del deber de información, el cual se ha rebajado al mismo nivel que el argumento de sospecha razonable, siendo el deber de información parte del contenido esencial del derecho a la protección de datos.

Lo cierto es que la excepción de este deber que tanto rechazaba Valdés, además de aplicarse por los tribunales desde la STC 39/2016, ahora queda legislada en el artículo 89.1 LOPD. Sin duda alguna, es de suma importancia separar el deber de información (que forma parte del contenido esencial) de los elementos que integran el principio de proporcionalidad. El problema con la aplicación del principio de proporcionalidad en las actuales sentencias que hemos examinado es que se ha rebajado este deber al mismo nivel que el argumento de sospecha razonable, siendo el deber de información parte del contenido esencial del derecho a la protección de datos. Es por ello que la profesora Edurne Terradillos indicaba que la mala aplicación del principio podía suponer que éste pasase a ser el peor aliado de los derechos fundamentales.

El voto particular de Fernando Valdés en la STC 39/2016 es de tal importancia que se sigue haciendo mención a él cada vez que se pretende remarcar la relevancia de los derechos fundamentales de los trabajadores frente al poder de dirección. En definitiva, la crítica del magistrado es ajena a la progresiva intervención de la tecnología en los derechos laborales y a los cambios jurisprudenciales sobre el principio de proporcionalidad. De esta manera, nuestra intención con este estudio no se limita a analizar y describir los casos concretos en los que se aplica el principio de proporcionalidad, sino que queremos poner de manifiesto la importancia del conflicto que subyace tras las decisiones de los tribunales que se trata de la necesidad de preservar el contenido de los derechos fundamentales de los trabajadores.

VII. Bibliografía

-LIBROS

-CONTRERAS NÚÑEZ-CORTÉS,P (2012) *Lecciones de contrato de trabajo*. Editorial Dykinson Pág. 125

- FABREGAT MONFORT, G. (2016). *Nuevas perspectivas del poder de dirección y control del empleador*. Editorial Bomarzo

-ORRICO FERNÁNDEZ, F. J. (2021) *Criterios sobre usos de dispositivos tecnológicos en el ámbito laboral : hacia el equilibrio entre el control empresarial y la privacidad del trabajador.* Tirant Lo Blanch.

-UGINA MERCADER, JESÚS R(2019) *Protección de datos y garantía de los derechos digitales en las relaciones laborales.* Ediciones Francis Lefebvre. *https://online-elderecho-com.ehu.idm.oclc.org/seleccionProducto.do;jsessionid=DCF361A1EE34AAB6C42BCA174A271AC9.TC_ONLINE04?producto=DOCTR&javascriptInicial=presentarMarginalMemento(%27*%27,%27ES%27,%272013/900081%27)#%2FpresentarMemento.do%3Fnref%3D2013%2F900081%26producto%3DDOCTR%26marginal%3D%26rnd%3D0.40411201271504504*

-REVISTAS

-ALCALÁ NOGUEIRA, H (2007) "El derecho a la propia imagen como derecho fundamental implícito: Fundamentación y caracterización" *Ius et Praxis*. Vol. 13, Nº. 2. Págs. 245-285

-BALAGUER LÓPEZ, M y MORAGUES RAMOS, F (2020) "Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad" *Lex social: revista de los derechos sociales*. Vol. 10, Nº. 2 . Págs. 506-540

-BONETE DESDENTADO, A y DAROCA DESDENTADO, E (2018) “La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador.” *Revista de información laboral.* Nº. 1, Págs. 19-39

-CARRIÓN DURO, S (2021) “El deber de información en el artículo 87 y 89 lop dgdd. La quiebra de la expectativa de privacidad vinculada al derecho a la intimidad y otros derechos fundamentales en liza en la relación laboral” *Revista de Derecho Laboral vLex.* Núm 2. Pág. 70-93

- CATALÁ POQUET, R. (2022) “Poder de control empresarial a través de sistemas de videovigilancia: alcance y límites” *Revista Aranzadi Doctrinal.* Núm. 5. Pág. 2

- DAL-RÉ VALDÉS, F (2017) “Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa” *Revista de derecho social.* Nº 79 . Págs. 15-35

-Del Cuvillo Álvarez, A. (2020). “La delimitación del derecho a la intimidad de los trabajadores en los nuevos escenarios digitales”. *Temas laborales: Revista andaluza de trabajo y bienestar social.* Núm 151. Págs. 275-292

-Fované, J. (2015). “El poder de dirección del empleador vs. el acceso de los medios tecnológicos e informáticos dentro de la empresa”. *Revista Vía Iuris,* (18), pp. 47-71

-GIMÉNEZ TOSCANI, D (2015) “La vulneración del derecho a la intimidad por delatadores, detectives privados y medios tecnológicos”*Revista de derecho social.* Núm. 71. Pág. 55-78

-GIMENEZ TOSCANI, D. (2017) “Las facultades de la empresa de videovigilancia de sus trabajadores. Comentario a la STC 39/2016, de 3 de marzo” *Revista Boliviana de Derecho* Nº. 23 . Págs. 366-373

-HENRÍQUEZ TILLERÍA, S (2019) “Protección de datos, videovigilancia laboral y doctrina de la sentencia López Ribalda II: un peligroso camino hacia la degradación de la obligación de información.” *IUSLabor*. Nº 3. Págs 55-80

- Jiménez, A. F. D. (2021). “El Derecho a la Intimidad y a la Protección de Datos Personales en el Ámbito Laboral.” *Revista Internacional Consinter De Direito*. Nº 7(13). Págs 357–385

- LAMPARERO ASQUERINO,JOSE Mª. (2012) “El derecho de resistencia frente al poder de dirección” Revista *Doctrinal Aranzadi Social* núm. 8/2012.

-ORMAECHEA TERRADILLOS, M. E. (2017) “El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español” *Revista de derecho social.* Nº 80. Págs. 139-162

-REVORIO DÍAZ, F. JAVIER (2006) “El derecho fundamental al secreto de las comunicaciones” *Derecho PUCP: Revista de la Facultad de Derecho.* Nº. 59. Págs 159-175

-OTROS

- Ripollés Rastrollo, A.(2017) Sinopsis artículo 38 de la Constitución Española. https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=38&tipo=2

- Diccionario panhispánico del español jurídico. https://dpej.rae.es/lema/derecho-a-la-propia-imagen

- SEMPERE NAVARRO, A. V. Vídeo-comentario a la STS 84/2021, de 8 febrero. Aranzadi. https://webcastlive.es/aranzadi/actualizacion-profesional/2021.htm?id=TS-163-2021_08-02-2021_RJ-2021-672

-SEIN GOÑI, J. LUIS (2014) *Los derechos fundamentales inespecíficos en la relación laboral individual ¿necesidad de una reformulación?* XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Pamplona

-JURISPRUDENCIA

- **Tribunal Constitucional**

-STC 11/1981, 8 de Abril

- STC 83/1984, 24 de Julio de 1984

-STC 19/1985, de 5 de marzo

-STC 88/1985, 19 de Julio de 1985

- STC 225/1993, 8 de Julio de 1993

-STC 254/1993, de 20 de julio

-STC 57/1994, de 28 de febrero

- STC 99/1994 de 11 de Abril

-STC 94/1998, de 4 de mayo

- STC 17/2000, de 31 de enero

-STC 98/2000, 10 de Abril

-STC 186/2000, de 10 de julio.

-STC 292/2000 de 30 de noviembre

-STC 281/2006, de 9 de octubre

-STC 159/2009, de 29 de junio

- STC 12/2012, de 30 de enero

-STC 241/2012 de 17 de diciembre

- STC 29/2013, de 11 de febrero

-STC 170/2013, de 7 de octubre

-STC 39/2016, de 3 de marzo

-STC 160/2021 de 4 de octubre

- STC 119/ 2022 de 29 de septiembre

- **Tribunal Supremo**

- STS 26 de septiembre de 2007

-STS (Sala de lo Social), de 6 de octubre de 2011(recurso 4053/2010)

-STS 77/2017 (Sala de lo Social), de 31 de enero de 2017 (recurso 3331/2015)

-STS 96/2017 (Sala de lo Social), de 2 de febrero de 2017 (recurso 554/2016)

-STS 119/2018 (Sala de lo Social), de 8 de Febrero de 2018 (recurso 1121/2015)

-STS 766/2020 (Sala de lo Social), de 15 de Septiembre de 2020 (recurso 528/2018)

-STS 163/2021 (Sala de lo Social), de 8 de Febrero de 2021 (recurso 84/2019)

- **Tribunal Superior de Justicia**

-STSJ Galicia 668/2014(Sala de lo Social), de 17 de Enero de 2014 (recurso 3483/2013)
-STSJ Andalucía 2269/2017(Sala de lo Social), de 19 de Octubre de 2017(recurso 1149/2017)
-STSJ Madrid 763/2019 (Sala de lo Social), de 12 de julio de 2019 (recurso 197/2019)
-STSJ Cataluña 1208/2023, de 20 de febrero de 2023

- **Tribunal Europeo de Derechos Humanos**

-STEDH de 3 de abril de 2007, caso *Copland v. Reino Unido.*
-STEDH de 5 de septiembre de 2017, caso *Barbulescu II*
-STEDH de 17 de octubre de 2019, caso *López Ribalda II*

-LEGISLACIÓN

- **ESPAÑOLA**

- Constitución Española de 1978, (BOE núm. 311, de 29 de diciembre de 1978)

-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. (BOE núm. 255, de 24 de octubre de 2015)

-Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (BOE núm. 294, de 6 de diciembre de 2018)

- **COMUNITARIA**

-Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convención Europea de Derechos Humanos) (BOE número 243, de 10 de octubre de 1979)

-Directiva 2002/58/CE, del Parlamento Europeo y del Consejo de 12 de julio, sobre la privacidad y las comunicaciones electrónicas. (Diario Oficial de las Comunidades Europeas)

- 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). (Diario Oficial de la Unión Europea)