UNIVERSIDAD COMPLUTENSE DE MADRID
FACULTAD DE DERECHO

TESIS DOCTORAL

La privacidad del trabajador y el control tecnológico de la actividad laboral

MEMORIA PARA OPTAR AL GRADO DE DOCTOR

PRESENTADA POR

Antonio-Felipe Delgado Jiménez

Directores

Ignacio García Vitoria
Vicente J. Navarro Marchante

Madrid

© Antonio-Felipe Delgado Jiménez, 2020

UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO CONSTITUCIONAL

TESIS DOCTORAL

LA PRIVACIDAD DEL TRABAJADOR Y EL CONTROL TECNOLÓGICO DE LA ACTIVIDAD LABORAL

ANTONIO – FELIPE DELGADO JIMÉNEZ

DIRECTORES

Dr. D. Ignacio García Vitoria

Dr. D. Vicente J. Navarro Marchante

Madrid, 2020

ÍNDICE

ABREVIATURAS ..... pág. 5

RESUMEN ..... pág. 7

1.- Título de la Tesis Doctoral ..... pág. 7
2.- Introducción ..... pág. 7
3.- Síntesis ..... pág. 7
3.1.- Objetivo de la Tesis ..... pág. 7
3.2.- Estructura de la Tesis ..... pág. 8
4.- Conclusiones ..... pág. 9

INTRODUCCIÓN ..... pág. 13

1.- Los derechos fundamentales de los trabajadores en el marco de la relación laboral por cuenta ajena ..... pág. 13
1.1.- La recepción de los derechos fundamentales en el contrato de trabajo ..... pág. 13
1.2.- Los derechos fundamentales de los trabajadores en la sociedad digital ..... pág. 17
2.- Los derechos fundamentales en cuanto límites al poder empresarial ..... pág. 24
3.- Límites a los derechos fundamentales en el marco de la relación laboral ..... pág. 28
4.- La ponderación legal y jurisprudencial del poder de dirección del empresario y de la privacidad del trabajador en las relaciones laborales tecnificadas ..... pág. 33
5.- Estructura de la Tesis Doctoral ..... pág. 40

CAPÍTULO I.- EL CONCURSO DE DERECHOS FUNDAMENTALES EN EL ÁMBITO LABORAL ..... pág. 45

1.- Derecho a la intimidad ..... pág. 45
1.1.- Instalación de sistemas audiovisuales de control y sus implicaciones con respecto a la intimidad del trabajador ..... pág. 45
1.2.- Control del ordenador y derechos fundamentales del trabajador ..... pág. 54
1.2.1.- Existencia de expectativa razonable de privacidad ..... pág. 61
1.2.2.- El acceso a contenidos privados mediando consentimiento del trabajador

afectado ..... pág. 69
2.- El derecho a la vida privada en Europa: un contenido ampliado del derecho a la intimidad ..... pág. 73
2.1.- La sucesiva ampliación del contenido del derecho a la vida privada en el CEDH: de Halford a Libert ..... pág. 79
2.1.1.- La primera doctrina del TEDH: los casos Halford y Copland c. Reino Unido y Köpke c. Alemania ..... pág. 80
2.1.2.- La reciente doctrina del TEDH: el caso Barbulescu c. Rumanía; Antovic y Mirkovic c. Montenegro; López Ribalda *et alii* c. España; Libert c. Francia . pág. 84
3.- Derecho al secreto de las comunicaciones ..... pág. 100
3.1.- Interceptación del correo electrónico y su incidencia sobre el secreto de las comunicaciones y la intimidad personal ..... pág. 109
3.1.1.- Comunicaciones protegidas por el secreto de las comunicaciones..... pág. 122
3.1.2.- Contenidos protegidos por el secreto de las comunicaciones ..... pág. 123
3.1.3.- El acceso a mensajes que estén en posesión de los comunicadores ..... pág. 127
3.1.3.1.- Mensajes en poder del emisor ..... pág. 128
3.1.3.2.- Mensajes en poder del destinatario ..... pág. 131
3.1.4.- La finalización del proceso de comunicación ..... pág. 134
3.1.5.- Relevancia o no del conocimiento efectivo del contenido del mensaje por parte del destinatario ..... pág. 136
3.1.6.- Secreto de las comunicaciones y medios digitales de titularidad del trabajador ..... pág. 139
4.- El derecho a la protección de datos personales ..... pág. 140
4.1.- Su autonomía frente al derecho a la intimidad ..... pág. 140
4.2.- Sus diferencias respecto al derecho a la intimidad ..... pág. 144
4.3.- Afectación del derecho a la protección de datos personales ..... pág. 146

CAPÍTULO II.- LA CONFIGURACIÓN LEGAL DE LAS MEDIDAS DE CONTROL EMPRESARIAL ..... pág. 157

1.- Artículo 8.2 CEDH: la necesidad de previsión legal. La calidad de la ley ..... pág. 157
2.- El principio de legalidad en la Constitución Española ..... pág. 163
3.- La normativa laboral ..... pág. 167
3.1.- Artículo 20.3 ET: el poder de dirección y control del empresario..... pág. 167

3.2.- Artículo 18 ET: el registro en la persona del trabajador, su taquilla y efectos personales ..... pág. 172
3.3.- Los Convenios Colectivos de condiciones de trabajo ..... pág. 181
4.- Fijación unilateral de reglas por parte de las empresas: la autorregulación ..... pág. 188
4.1.- Códigos de Conducta que no contienen referencias al uso de las TIC por parte de los trabajadores ..... pág. 190
4.2.- Códigos de Conducta que sí regulan el uso de las TIC por los trabajadores ..... pág. 191
4.2.1.- Prohibición del uso personal ..... pág. 191
4.2.2.- Admisión del uso particular ..... pág. 193
5.- La protección de datos personales y la garantía de los derechos digitales en el ámbito laboral ..... pág. 197
5.1.- La Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales ..... pág. 197
5.2.- Normativa supranacional ..... pág. 201
5.2.1.- Derecho Comunitario ..... pág. 201
5.2.2.- Normativa de la Organización Internacional del Trabajo (OIT) y otras Organizaciones ..... pág. 203
6.- Marco jurídico de la video vigilancia privada ..... pág. 206
7.- ¿Una legislación suficiente? ..... pág. 210

CAPÍTULO III.- LA NECESIDAD DE AUTORIZACIÓN JUDICIAL PARA ACCEDER AL CONTENIDO DEL CORREO ELECTRÓNICO DEL TRABAJADOR ..... pág. 223

1.- Necesidad de resolución judicial ..... pág. 223
2.- La aplicabilidad de los arts. 76.4 y 90.4 LRJS en el acceso a los datos privados del trabajador contenidos en el ordenador de la empresa ..... pág. 237
3.- Consecuencias de la prueba obtenida con lesión del derecho al secreto de las comunicaciones. ..... pág. 257

CAPÍTULO IV.- EL DEBER DE INFORMACIÓN DEL EMPRESARIO ..... pág. 261

1.- Jurisprudencia del Tribunal Supremo ..... pág. 271
1.1.- Video vigilancia con fines distintos a los estrictamente laborales (STS de 13 de

mayo de 2014) ..... pág. 271
1.2.- Cambio de doctrina. Video vigilancia en zonas restringidas al público (STS de 7 de julio de 2016) ..... pág. 272
1.3.- Sistema de video vigilancia. Alcance del deber informativo previo (STS de 31 de enero de 2017) ..... pág. 274
2.- Jurisprudencia del Tribunal Constitucional ..... pág. 278
2.1.- El deber de información previo (STC 29/2013, de 11 de febrero) ..... pág. 278
2.2.- Debilitamiento del deber de información previo (STC 39/2016, de 3 de marzo) ... pág. 285
2.2.1.- Voto particular del Magistrado Fernando Valdés Dal-Ré ..... pág. 295
2.2.2.- Voto particular del Magistrado Juan Antonio Xiol Ríos ..... pág. 296
3.- De López Ribalda I a López Ribalda II ..... pág. 298

CAPÍTULO V.- LA PROPORCIONALIDAD DE LAS MEDIDAS DE CONTROL . pág. 307

1.- El poder de dirección del empresario y el derecho a la intimidad del trabajador: la necesidad de ponderación ..... pág. 307
2.- El juicio de ponderación: su articulación y presupuestos ..... pág. 309
3.- La proporcionalidad en la instalación de cámaras de video vigilancia ..... pág. 312
3.1.- Jurisprudencia europea (TEDH) ..... pág. 316
3.2.- Jurisprudencia constitucional ..... pág. 317
3.2.1.- Primera etapa: admisión generalizada de mecanismos de control tecnológico (STC 142/1993, de 22 de abril) ..... pág. 317
3.2.2.- Segunda etapa: admisión del principio de proporcionalidad (SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio) ..... pág. 318
4.- La utilización del correo electrónico para fines extra laborales y la proporcionalidad en su control ..... pág. 325

VI.- CONCLUSIONES ..... pág. 333

BIBLIOGRAFÍA ..... pág. 341

ANEXO I.- REPERTORIO DE JURISPRUDENCIA MÁS REFERENCIADA..... pág. 371

ANEXO II.- CONVENIOS COLECTIVOS ..... pág. 377

ABREVIATURAS

AL	Actualidad Laboral
AP	Audiencia Provincial
BOP	Boletín Oficial de la Provincia
CC	Código Civil
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CE	Constitución Española de 1978
CEDH	Convenio Europeo de Derechos Humanos de 1950
ET	Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores
GTPD	Grupo de trabajo sobre protección de datos, cuya creación se prevé en el artículo 29 de la Directiva 95/46/CE, de 24 de octubre
JS	Juzgado de lo Social
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LSP	Ley de Seguridad Privada
LRJS	Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social
OIT	Organización Internacional del Trabajo
PIDESC	Pacto Internacional de Derechos Económicos, Sociales y Culturales
RD	Real Decreto
RDS	Revista de Derecho Social
REDT	Revista Española de Derecho del Trabajo
RGD	Revista General de Derecho
RMTAS	Revista del Ministerio de Trabajo y Asuntos Sociales
RPS	Revista de Política Social

RSP	Reglamento de Seguridad Privada
RTSS	Revista de Trabajo y Seguridad Social
SAN	Sentencia de la Audiencia Nacional
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de la información y comunicación
TRLISOS	Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
TFUE	Tratado de Funcionamiento de la Unión Europea
TUE	Tratado de la Unión Europea

RESUMEN.

1.- Título de la Tesis Doctoral: “La privacidad del trabajador y el control tecnológico de la actividad laboral”.

2.- Introducción.

La implantación de las TIC en las organizaciones empresariales ha determinado una radical transformación de la prestación laboral tradicional que, si bien ha supuesto indudables avances desde el punto de vista de la eficiencia productiva y el ahorro de costes, también ha determinado la acumulación de una enorme batería de datos que, adecuadamente tratados, suponen la obtención de una radiografía, no sólo de la actividad laboral *stricto sensu*, sino de la persona del trabajador.

De modo paralelo se ha venido operando un proceso de fortalecimiento del poder empresarial vinculado a la implantación de las TIC en las empresas cuyo impacto se ha dejado notar especialmente respecto de los derechos fundamentales del trabajador, lo que exige retomar el debate sobre los derechos fundamentales en el ámbito del contrato de trabajo y sus relaciones con respecto al poder de dirección y control del empresario.

3.- Síntesis.

3.1.- Objetivo de la Tesis.

Partiendo de las anteriores premisas, el objetivo del presente trabajo consiste en analizar la problemática que conlleva el control tecnológico de la

actividad laboral por parte del empresario y sus implicaciones respecto a los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales, para lo cual habrá que individualizar en primer lugar los derechos en juego; analizar, acto seguido, su regulación legal (si existiere) para, finalmente, escudriñar la doctrina jurisprudencial sobre el tema en cuestión al objeto de extraer las conclusiones pertinentes.

3.2.- Estructura de la Tesis.

Para alcanzar el objetivo señalado se ha dividido la obra en cinco capítulos, cada uno de los cuales responde a una pregunta objeto de investigación, a saber:

a) el análisis del concurso de derechos fundamentales que puede generarse en los supuestos de video vigilancia empresarial y control del correo electrónico por parte del empresario;

b) la necesidad de previsión legal de la medida de injerencia en la privacidad del trabajador y la denominada “calidad de la ley”;

c) la necesaria autorización judicial para conocer el contenido del correo electrónico del trabajador;

d) la proporcionalidad de la medida de vigilancia y control empresarial;

e) y, por último, el deber de información - específico y concreto- al trabajador respecto de las medidas de vigilancia decididas por el empresario.

4.- Conclusiones.

Con independencia de las Conclusiones generales obtenidas con el presente estudio, las cuales figuran al final de la obra, sí podemos adelantar que una de las principales conclusiones extraídas del presente trabajo ha sido que la vida social privada del trabajador en el seno de las empresas no puede en ningún caso reducirse a cero, teniendo el Estado la obligación positiva (obligación de hacer) de procurar que se respete la vida privada de los empleados en el seno de las organizaciones empresariales (caso Bărbulescu c. Rumanía), debiendo el legislador cumplir con esa obligación positiva mediante la fijación del marco normativo adecuado que determine la protección de los diversos intereses en juego y, en defecto de regulación legal, corresponderá a los órganos judiciales nacionales asegurar que la adopción empresarial de medidas de vigilancia de la correspondencia y de otras comunicaciones se efectúe con las garantías adecuadas y suficientes contra los abusos y las arbitrariedades.

SUMMARY.

1.- Title of the Doctoral Thesis: "Privacy and technological control at work”

2.- Introduction.

The implementation of IT in business organizations has determined a radical transformation of the traditional work that although it has led larges advances in order to improve the productive efficiency and cost savings, has also determined the accumulation of a huge battery of data that, properly treated, involve obtaining an x-ray, not only of the work activity stricto sensu but of the worker's person.

In parallel, a process of strengthening business power linked to the implementation of IT in companies has been operating whose impact has been particularly noticeable regarding the fundamental rights of the worker, which requires to rethnk of the debate on fundamental rights in the scope of the employment contract and its relations with respect to the power of direction and control of the employer.

3.- Synthesis.

3.1.- Objective of the Thesis.

Based on the above premises, the objective of this work is to analyze the problem that involves the technological control of the labor activity by the employer and its implications regarding the rights to privacy, the secrecy of communications and data protection personal, for which we must first identify the rights at stake; analyze, immediately, its legal regulation (if it exists) to, finally, scrutinize the jurisprudence on the subject in order to draw the pertinent conclusions.

3.2.- Structure of the Thesis.

To achieve these objectives, the work has been divided into five chapters, namely:

a) the analysis of the fundamental rights at stake in cases of corporate video surveillance and email control by the entrepreneur;

b) the need of a law which rules of the interference in the privacy of the worker and the so-called “quality of the law”;

c) the necessary authorization by the judge in order to know the content of the worker's email;

d) the proportionality of the business surveillance and control measure;

e) and, finally, the duty of information - specific - to the worker regarding the surveillance measures decided by the employer.

4.- Conclusions.

Regardless of the general conclusions obtained with the present study, which appear at the end of the work, we can say that one of the main conclusions drawn from this work has been that the private social life of the worker within companies can´t be reduced to zero, having the State a positive obligation to ensure that the private lives of employees are respected within business organizations (Bărbulescu v. Romania case), and the legislator must comply with this positive obligation by setting the appropriate regulatory framework that determines the protection of the various interests at stake and, in the absence of legal regulation, it will be up to the national judicial bodies to ensure that the business adoption of measures to monitor correspondence and other communications be carried out with adequate and sufficient guarantees against abuses.

INTRODUCCIÓN.

1.- Los derechos fundamentales de los trabajadores en el marco de la relación laboral por cuenta ajena.

1.1.- La recepción de los derechos fundamentales en el contrato de trabajo.

1. El estatuto del trabajador por cuenta ajena se encuentra integrado por un conjunto de derechos la mayor parte de los cuales aparecen en la actualidad reconocidos en las cartas y declaraciones internacionales especializadas en materia laboral y social[1], habiendo llegado muchos de ellos a adquirir la cualificación de derechos fundamentales en los correspondientes sistemas nacionales por mediación de sus respectivos textos constitucionales[2].

No obstante, el impacto en esta materia de las Constituciones modernas, propias del Estado Social y Democrático de Derecho, no se ha limitado a la mera recepción de derechos específicamente laborales, sino que ha ido más allá y ha supuesto también, como no podía ser de otro modo, la transmisión al ámbito del contrato de trabajo de los derechos de ciudadanía. Es decir, del conjunto de derechos propios de la persona en su condición de miembro de una sociedad libre, habiendo sido esta recepción la consecuencia de un proceso histórico de incorporación de los derechos fundamentales al ámbito de las relaciones jurídico-privadas[3], lo que implica que, en el ámbito del contrato

1 GARCÍA MURCIA, J., "Los derechos de la persona en el ámbito del trabajo asalariado", en *Derechos del trabajador y libertad de empresa. 20 casos de Jurisprudencia Constitucional*, Dir. GARCÍA MURCIA, J., Thomson Reuters Aranzadi, Pamplona, 2013, pág. 27.

2 VALDÉS DAL-RÉ, F., "Los derechos fundamentales de la persona del trabajador: un ensayo de noción jurídico-formal", *Relaciones Laborales*, núm. 18, 2003, pág. 3.

3 RIVERO LAMAS, J., "Derechos fundamentales y contrato de trabajo: eficacia horizontal y control constitucional", AAVV, *El trabajo en la Constitución. Estudios homenaje al Profesor Alonso Olea*, MTSS, Madrid, 2003, págs. 497 y

de trabajo, no pueda haber suspensión ni pérdida alguna de los derechos fundamentales de la persona.

2. A esta concepción o doctrina se la denomina *Drittwirkung*[4] o, lo que es lo mismo, eficacia *inter privatos* de los derechos fundamentales, y supone que éstos contienen principios ordenadores de la vida social que tienen un significado inmediato en el tráfico jurídico privado[5], radicando su importancia en el abandono que esta construcción constitucional supone de la idea de que los derechos fundamentales son únicamente eficaces frente al Estado (concepto originario), para acoger una nueva concepción que los dota de eficacia *erga omnes*. La *Drittwirkung*, en definitiva, nos pone de manifiesto que los derechos fundamentales operan tanto en una relación vertical (frente al Estado) como horizontal (frente a los otros ciudadanos).

Nuestro Tribunal Constitucional ha aceptado la *Drittwirkung* y lo ha hecho recordándole al legislador y a los poderes públicos la obligación que tienen de respeto y garantía de los derechos fundamentales en todos los ámbitos[6], siendo ello expresión del mandato constitucional explícito contenido en el art. 9.1 CE, que prescribe la obligatoriedad de sujeción a la misma a los ciudadanos y a los poderes públicos. Como el propio Tribunal Constitucional afirma, la sujeción al art. 9.1 CE se traduce en un deber diferente según se trate de ciudadanos o de poderes públicos, dado que mientras que sobre los

---

sigs. y MOLINA NAVARRETE, C., "Bases jurídicas y presupuestos políticos para la eficacia social inmediata de los derechos fundamentales", *RTSS*, julio-septiembre, 1991, págs. 101 y sigs.

4 Su formulación se debe a Ipsen en 1954, si bien es Nipperdey quien configura doctrinalmente el concepto de *Drittwirkung.* Asimismo, Tribunal Federal de Trabajo de Alemania *(Bundesarbeitsgerich)*, en sentencia de 3 de diciembre de ese mismo año, afirma que los derechos fundamentales contienen "principios ordenadores para la vida social" y que los mismos tienen significación inmediata en el tráfico jurídico privado.

5 REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*, Dykinson, Madrid, 2005, pág. 144.

6 La STC 129/1989, de 17 de julio, recuerda respecto de los derechos fundamentales que la importancia que los mismos tienen dentro del orden constitucional determina que se imponga a los poderes públicos el deber de garantizar su vigencia, obligándose al legislador a proteger los valores incorporados al ordenamiento jurídico a través de los derechos fundamentales. En idéntico sentido se pronuncia la STC 120/1990, de 27 de junio.

primeros pesa un deber negativo de abstención respecto de cualquier actuación que pudiera vulnerar la Constitución, por el contrario, los titulares de los poderes públicos tienen, además, un deber positivo de adecuar sus funciones a lo previsto constitucionalmente[7].

3. La eficacia horizontal de los derechos fundamentales supone que éstos no puedan ser desconocidos[8] en el ámbito del contrato de trabajo, de modo que el trabajador por cuenta ajena puede ejercitar en el seno de la relación laboral todos los derechos que, como persona, le corresponden, lo cual no obsta a que los mismos puedan ser objeto de modulaciones dadas las especificidades propias de aquélla[9].

En este sentido se ha dicho habitualmente que los derechos fundamentales no son cláusulas de excepción de las obligaciones contractuales ni pueden ser invocados para su incumplimiento[10], lo que significa que la sujeción a un contrato de trabajo puede afectar al ejercicio de los mismos, aunque no siempre ocurra con la misma intensidad, de modo que aquéllos y éste habrán de adaptarse mutuamente. O dicho en otros términos: los derechos fundamentales del trabajador habrán de ser respetados en el seno del contrato de trabajo, si bien su ejercicio podrá ser modulado en función de la carga contractual asumida en aquél, con la precisión de que la

7 STC 101/1983, de 18 de noviembre, FJ 3.

8 Así lo establece la STEDH (Gran Sala) de fecha 5 de septiembre de 2017 (caso Barbulescu c. Rumanía), que considera que la normativa interna de las empresas no puede reducir la vida privada social dentro de las empresas a cero, sino que siempre subsiste una expectativa de privacidad pese a la existencia de una prohibición expresa del uso de los medios informáticos de la empresa con fines extra laborales.

9 En el mismo sentido GARCÍA MURCIA, J., "Los derechos de la persona…, *op. cit.*, pág. 37. Asimismo, la idea de la modulación es aceptada prácticamente sin reservas por la práctica judicial y la doctrina científica, aunque no siempre con unanimidad de criterio y con el mismo grado de adhesión, seguramente porque no se traduce tan sólo en un recurso técnico para resolver controversias, sino también en una fórmula conceptual que encierra una notable carga valorativa.

10 BORRAJO DACRUZ, E., "Derechos fundamentales y relación de trabajo: casos judiciales significativos", *AL*, núm. 3, 2004, págs. 267 y sigs.

modulación no significa, en modo alguno, negación ni devaluación del derecho, sino, lisa y llanamente, que el mismo habrá de conjugarse con otras exigencias jurídicas. Es decir, modulación como sinónimo de cohabitación[11].

Pasadas ya más de tres décadas desde sus primeras manifestaciones, la jurisprudencia constitucional sobre la proyección de los derechos fundamentales en el marco del contrato de trabajo ha alcanzado una notable madurez, habiendo gozado el TC de la oportunidad de pronunciarse sobre todos los derechos susceptibles de amparo constitucional consiguiendo proporcionar criterios útiles para preservar la eficacia de los mismos en el ámbito del contrato de trabajo, siendo afirmaciones consagradas del TC las de que los derechos fundamentales rigen también en el ámbito de las relaciones laborales; que el trabajador goza de los derechos propios del ciudadano aun cuando se comprometa a la prestación de servicios por cuenta ajena; o que la celebración de un contrato de trabajo no genera para el trabajador una sujeción absoluta a los intereses de la empresa.

No obstante, también ha dejado ver el TC, por otro lado, que el ejercicio de esos derechos por parte del trabajador ha de cohonestarse con las obligaciones que derivan del contrato de trabajo y que los derechos e intereses de la empresa son dignos, asimismo, de tutela, habiéndose reforzado a través de esta labor la eficacia de la Constitución en el medio laboral y promovido la dignidad del trabajador en el ámbito de la empresa[12].

11 GARCÍA MURCIA, J., "Los derechos de la persona…, *op. cit.*, pág. 42.

12 VALDÉS DAL-RÉ, F., "Poderes del empresario y derechos…", *op. cit.*, pág. 46.

1.2.- Los derechos fundamentales de los trabajadores en la sociedad digital.

1. La aparición de las nuevas tecnologías y su implementación en las empresas ha generado una profunda transformación de la prestación de trabajo tradicional dado que en la mayoría de las actividades empresariales se utilizan, cada vez en mayor medida, herramientas informáticas que, si bien suponen una simplificación de la prestación de trabajo, también de modo paralelo permiten la acumulación de una minería de datos[13] que no sólo se guardan, sino que también se relacionan y analizan obteniéndose, de este modo, un mosaico de aquéllos que permiten una exhaustiva radiografía tanto de la actividad laboral en sentido estricto como de la persona del trabajador[14], al tiempo que limitan decididamente los derechos de éste, haciéndose, pues, necesario proponer métodos que limiten aquél y garanticen éstos.

Piénsese, por ejemplo, en un instrumento tan común como es un ordenador cuya simple utilización permite conocer tanto la actividad realizada por el trabajador como también el comportamiento observado por éste a lo largo de la jornada laboral, de modo que, a través de las TIC, el empresario puede pasar a controlar tanto la actividad laboral propiamente dicha como también la propia persona de quien ejecuta aquélla.

13 CARDONA RUBERT, Mª. B., "Control del correo electrónico de los empleados. Transgresión de la buena fe contractual", *Aranzadi Social* nº 17, 2001, pág. 31. Sobre el problema de la retención de datos de tráfico de comunicaciones y su injerencia en el derecho la intimidad, en la protección de datos, en el secreto de las comunicaciones y en a libertad de circulación, véase FERNÁNDEZ RODRÍGUEZ, J. J., "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional*, 108, septiembre-diciembre 2016, 93-122.

14 ALARCÓN CARACUEL, M. R., "La informatización y las nuevas formas de trabajo", en ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA, R. (Coords.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004, pág. 15.

Las potencialidades tecnológicas de control a las que nos referimos constituyen un conjunto de medidas sumamente poderosas que van desde los más tradicionales sistemas de video vigilancia[15] o la intervención de las conversaciones telefónicas[16] hasta los más modernos métodos de control y localización remotos mediante tarjetas de identificación personal, datos biométricos o, fuera del ámbito del centro de trabajo, a través de sistemas de localización *Global Positioning System (GPS)* e incluso chips subcutáneos, pasando por los cada vez más habituales registros del ordenador utilizado por el trabajador, ya sea de modo directo o bien indirectamente a través de la instalación de *software* espía capaz de revelar una amplia gama de información.

2. En consonancia con lo anterior, se ha venido operando paulatinamente un proceso de fortalecimiento del poder empresarial vinculado a la introducción de las nuevas tecnologías en las empresas y cuyo impacto se ha dejado notar especialmente respecto de los derechos fundamentales del trabajador, de modo que el respeto a la intimidad, al secreto de las comunicaciones y a la protección de datos personales en el desarrollo de la relación laboral cobra especial protagonismo en nuestros días, lo que exige retomar el debate sobre los derechos fundamentales en el ámbito de la relación laboral y su vinculación con respecto al poder de dirección y control del empresario y, en particular, repensar la ejecución de dicho poder de vigilancia y control cuyas formas de expresión varían con las TIC.

Si bien es cierto que trabajo y cambio tecnológico siempre han ido históricamente de la mano, también lo es que la actual revolución tecnológica y digital (la denominada cuarta Revolución Industrial) presenta determinadas

15 SÁNCHEZ-RODAS NAVARRO, C., "Videocámaras y poder de vigilancia", en *Aranzadi Social*, núm. 19, 2000, pág. 74.

16 TASCÓN LÓPEZ, R., "El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica", en *Aranzadi Social*, núm. 17, 2007, pág. 12.

particularidades[17]. Así, en primer lugar nos encontramos ante un proceso de cambio permanente de modo que lo que era nuevo ayer, hoy se presenta anticuado. En segundo lugar, asistimos a un progresivo descenso del peso del sector industrial en manos del sector servicios. Y, en tercer lugar, ambos procesos se ven culminados con la implantación de la digitalización del trabajo, que se ha extendido a todos los sectores dinamitando el tradicional modelo de empleo y de relaciones laborales.

De este modo, un ordenador o un teléfono móvil son, en el ámbito laboral, instrumentos productivos propiedad de la empresa, pero cuando se conectan a la Red son también algo más: son instrumentos de comunicación e información, lo que determina que las TIC difuminen su uso estrictamente laboral para adentrarse en otros ámbitos más propios de la intimidad del individuo[18]. Ello determina que, derivado de este carácter dual de las nuevas tecnologías, el ordenador siga siendo propiedad del empresario, pero a éste no le pertenezcan, sin embargo, los contenidos derivados del derecho a la información y a la comunicación del trabajador[19], lo cual puede generar en ocasiones problemas de colisión entre los citados derechos de los trabajadores y el poder directivo empresarial.

17 Como pone de manifiesto la "Declaración Deusto Derechos Humanos en Entornos Digitales" (https://www.deusto.es/cs/Satellite/deusto/es/universidad-deusto/sobre-deusto-0/derechos-humanos-en-entornos-digitales) *"en esta cuarta revolución industrial las tecnologías digitales convergen con disciplinas como la física, la química, la biología y otras ciencias naturales en la automatización total de los procesos productivos y los servicios que tienen lugar tanto en el terreno empresarial ("empresa 4.0") como en la vida cotidiana ("internet de las cosas"). Este fenómeno revolucionario tiene implicaciones profundas y radicales en muchos órdenes y espacios sociales (economía, política, o cultura entre otros). Además, se está produciendo con una aceleración temporal, una extensión espacial y una profundidad de consecuencias tales que dificulta enormemente la asimilación de los cambios por la sociedad y, lo que es más importante, produce una práctica imposibilidad de ofrecer respuestas éticas, legales y sociales adecuadas a los ritmos y alcances del proceso de transformación"*.

18 FERRANDO GARCÍA, F., "Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías", *Revista de Trabajo y Seguridad Social*, nº 399, junio 2006, págs. 37-68.

19 FALGUERA BARÓ, M. A., "Nuevas tecnologías y trabajo (I): perspectiva contractual", *Trabajo y Derecho*, núm. 19-20, julio-agosto 2016, págs. 31-34.

3. Lo manifestado hasta ahora ha determinado que las denuncias por violación de derechos fundamentales de los trabajadores se hayan incrementado ante los tribunales de justicia en los últimos años. Conflictos derivados del control del correo electrónico corporativo de la empresa y de la video vigilancia empresarial se han ido sucediendo hasta el punto de que los medios de comunicación se han ido haciendo eco paulatino de los mismos, de modo que podemos afirmar que estamos en presencia de un problema jurídico real, no sólo teórico, que necesita de una aproximación, no sólo ya desde el Derecho del Trabajo, sino también y, primordialmente, desde el Derecho Constitucional habida cuenta de que lo que está en entredicho son los derechos fundamentales del trabajador.

4. Sin olvidar que estamos en presencia de una materia de índole sustancialmente laboral de la que habitualmente conocen los tribunales de este orden, no obstante el conflicto presenta una vertiente de primerísima relevancia constitucional dado que se están viendo seriamente comprometidos derechos fundamentales del trabajador como lo demuestra el hecho de que los conflictos mencionados están siendo sometidos al conocimiento y decisión del Tribunal Constitucional, primero, y del Tribunal Europeo de Derechos Humanos, después.

A modo meramente ejemplificativo cabe citar, en materia de video vigilancia empresarial en el orden interno, las Sentencias del Tribunal Constitucional 142/1993, de 22 de abril (reconocimiento generalizado de los mecanismos de control tecnológico); la 98/2000, de 10 de abril y 186/2000, de 10 de julio (admisión del principio de proporcionalidad); la 29/2013, de 11 de febrero (consagradora del deber de información previo al trabajador) y la 39/2016, de 3 de marzo (debilitadora de ese deber de información previo al trabajador); y en cuestión de control de las comunicaciones electrónicas cabe, asimismo, mencionar el más antiguo precedente constituido por la STC 114/1984, de 29 de noviembre (grabación de sonido) hasta las más actuales SSTC 241/2012, de 17 de diciembre (caso Programa “Trillian”, que aborda el

supuesto de un ordenador de uso común sin clave de acceso y su relación con el derecho al secreto de las comunicaciones) y la 170/2013, de 7 de octubre (caso “Alcaliber, S. A.”, que considera el correo electrónico de la empresa un canal de comunicación abierto en determinados casos).

Y, en el plano europeo, el Tribunal Europeo de Derechos Humanos ha tenido ocasión de pronunciarse en diferentes ocasiones sobre cuestiones sometidas a su consideración que versaban sobre las materias referidas. Así, por ejemplo, cabe referenciar en lo que a la video vigilancia empresarial se refiere, su sentencia de 5 de octubre de 2010 (inadmisibilidad de la demanda presentada en el caso Köpke c. Alemania) y las SSTEDH de 28 de noviembre de 2017 (caso Antovic y Mirkovic c. Montenegro) que aborda un caso de video vigilancia en el lugar de trabajo y la más reciente de 9 de enero de 2018 (caso López Ribalda *et alii* c. España I y de 17 de octubre de 2019, López Ribalda II) que analiza un supuesto de video vigilancia encubierta e indiscriminada de trabajadores en el lugar de trabajo; y en materia de control de comunicaciones electrónicas podemos referenciar desde la Sentencia de 25 de junio de 1997 (caso Halford c. Reino Unido), que analiza la interceptación de llamadas telefónicas en despacho profesional y en domicilio particular, o la de 3 de abril de 2007 (caso Copland c. Reino Unido) que estudia el seguimiento de las llamadas telefónicas, correo electrónico y uso de Internet, hasta las más recientes de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía), trascendental resolución del TEDH que analiza el control del correo electrónico de un trabajador rumano que prestaba sus servicios para una empresa privada y que va a obligar casi con toda seguridad al Tribunal Constitucional a modificar su doctrina judicial referida a este tipo de cuestiones[20], y la de 22 de febrero de 2018 (caso Libert c. Francia) relativa también a un caso de control del uso del ordenador y del correo electrónico de un trabajador de una empresa pública francesa.

20 RODRÍGUEZ-RICO ROLDÁN, V., “Las facultades empresariales de vigilancia y los derechos fundamentales de los trabajadores: su difícil equilibrio en la era tecnológica”, *ReDCE*, núm. 29, enero-junio 2018., pág. 23.

Aún más: que estamos en presencia de una cuestión de índole constitucional lo demuestra el hecho de que la misma afecta también al funcionamiento interno de los partidos políticos y a las relaciones entre afiliados a éstos, más allá de las relaciones contractuales de trabajo, como pone de manifiesto la STC 26/2018, de 5 de marzo, relativa a sanciones dentro de los partidos políticos, si bien el objeto de nuestro estudio se circunscribe por razones metodológicas al ámbito de la constitucionalización de los derechos fundamentales en el seno de la relación laboral.

5. Asimismo, de modo paralelo a la cuestión judicial referida, existe en torno al objeto de análisis un debate doctrinal de notable alcance que presenta un indudable interés desde la perspectiva constitucional dado que en el mismo se entrelazan dos temas de suma importancia, a saber: de un lado, uno clásico como es la eficacia de los derechos fundamentales en el ámbito de las relaciones laborales (libertad de expresión[21], derecho a la propia imagen, etc.) sobre los que ya ha tenido ocasión de pronunciarse el Tribunal Constitucional afirmando, entre otras, en su Sentencia 88/1985, de 19 de julio, que la celebración de un contrato de trabajo no supone, en ningún caso, la privación para el trabajador de sus derechos constitucionales de ciudadano, entre los que cabe señalar el derecho a expresar y difundir libremente los pensamientos, ideas u opiniones y, de otro, un tema algo más novedoso cual es el relativo a los derechos de la personalidad y las TIC (intimidad, secreto de las comunicaciones y protección de datos personales) sobre el que nos adentraremos en páginas sucesivas.

6. De cuanto antecede se infiere que estamos en presencia de problemas jurídicos reales en los que se ven involucrados derechos fundamentales (intimidad, secreto de las comunicaciones y derecho a la protección de datos personales desde la perspectiva constitucional interna o derecho a la vida privada y familiar desde la óptica de la jurisprudencia europea), produciéndose,

21 Sobre la libertad de expresión vid. ROJAS RIVERO, G. P., *La libertad de expresión del trabajador*, Universidad de La Laguna, 1990.

en ocasiones, un concurso de derechos, por lo que surge la conveniencia de erigir límites y garantías a la utilización por parte del empresario de las TIC[22] al objeto de que la empresa no se convierta en una especie de cárcel de paredes transparentes, en palabras de González Ortega[23].

Entre esos instrumentos tecnológicos nos centraremos, primordialmente, en el análisis de la video vigilancia en la empresa y en el control del correo electrónico y su potencial vulneración de derechos constitucionales del trabajador por tratarse ambos de los medios tecnológicos sobre cuya utilización por parte del empresario existe una jurisprudencia constitucional y europea reciente que aborda el conflicto de intereses generado, dejando al margen otras modalidades de vigilancia y control tales el uso de detectives privados, los ficheros médicos, las redes sociales y el *GPS*, entre otros, los cuales no serán objeto de análisis en este estudio.

22 Muestra de cuanto decimos es la reciente Resolución de 27 de julio de 2018, de la Subsecretaría del Ministerio de Trabajo, Migraciones y Seguridad Social, por la que se publica el Acuerdo del Consejo de Ministros de 27 de julio de 2018, por el que se aprueba el Plan Director por un Trabajo Digno 2018-2019-2020 (BOE de 28 de julio de 2018), cuyo ANEXO señala que *"la experiencia nos enseña que el crecimiento económico por sí solo no es suficiente. Debemos hacer más para empoderar a las personas gracias al trabajo decente y apoyarlas a través de la protección social"*.

Uno de los objetivos del Plan es la "Protección de derechos fundamentales y promoción de la igualdad", a cuyo efecto establece que *"el ordenamiento jurídico español contiene la prohibición de cualquier tipo de atentado a la intimidad y honor de las personas trabajadoras, así como la prohibición de cualquier clase de discriminación"* y ordena a tal fin a la Inspección de Trabajo y Seguridad Social actuar ante *"cualquier situación de la que tenga conocimiento que pueda suponer una vulneración de derechos fundamentales en su ámbito de competencias, en particular para la protección del derecho a la intimidad frente a la utilización extensiva de tecnologías de la información"*.

23 GONZÁLEZ ORTEGA, S., "La informática en el seno de la empresa. Poderes del empresario y condiciones de trabajo", en Alarcón Caracuel, M. R. y Esteban Legarreta, R. (edits.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004, pág. 48.

2.- Los derechos fundamentales en cuanto límites al poder empresarial.

1. En la presente obra nos centraremos en el análisis de los límites que los derechos fundamentales provocan respecto del poder de dirección y control del empresario en el marco del contrato de trabajo dado que, como es obvio, los mismos modulan el ejercicio regular del poder directivo empresarial[24], siendo así que, en este sentido, para los poderes empresariales la interiorización de los derechos fundamentales en el seno de la empresa implica que la racionalidad económica deja de ser el único factor legitimador de las decisiones empresariales cuando las mismas afectan a derechos fundamentales de los trabajadores[25], de modo que el ejercicio de éstos obliga a ponderar intereses dada la necesidad de tener en cuenta los mismos[26], siendo así que la titularidad empresarial sobre la organización no implica, en modo alguno, la sistemática prevalencia de sus intereses sobre cualquier otro interés contrapuesto[27].

Y, en este sentido, el Tribunal Constitucional no duda en reconocer la legitimidad de los poderes empresariales en el seno de la relación laboral siempre que se ajusten al fin para el que han sido reconocidos[28] y respeten los

24 DEL REY GUANTER, S., "Derechos fundamentales de la persona y contrato de trabajo. Notas para una teoría general", en *Relaciones Laborales: revista crítica de teoría y práctica*, nº 1, 1995, pág. 205 y ROMÁN DE LA TORRE, Mª. D., *Poder de dirección y contrato de trabajo*, Grapheus, Valladolid, 1992, págs. 302 y sigs.

25 GUTIÉRREZ PÉREZ, M., *Ciudadanía en la empresa y derechos fundamentales inespecíficos*, Ediciones Laborum, Murcia, 2011, pág. 166.

26 Afirma RODRÍGUEZ PIÑERO Y BRAVO FERRER, M., "Poder de dirección y derecho contractual", *Relaciones Laborales*, nº 19-20, 2005, pág. 23, que en el ejercicio de los poderes empresariales se pone en juego, frente a intrusiones provenientes del medio empresarial, la persona del trabajador, su libertad y su dignidad.

27 RODRÍGUEZ PIÑERO Y BRAVO FERRER, M., "La integración de los derechos fundamentales en el contrato de trabajo", en *El modelo social en la Constitución Española de 1978*, (Dir., Sempere Navarro, A. V.; Coord., Martín Jiménez, R.,), Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003, pág. 210.

28 STC 34/1984, de 9 de marzo, FJ 5, que señala que *"…como toda medida en que se manifiestan los poderes empresariales, la licitud dependerá de un ejercicio dirigido hacia los fines por los cuales tales poderes se reconocen"*.

derechos fundamentales de los trabajadores[29], lo que nos lleva inexorablemente a analizar las modulaciones que los derechos fundamentales van a imponer al poder de dirección y control del empresario, a cuyo efecto hemos de partir de la noción de dependencia acuñada por el art. 1.1 ET en el sentido de inserción del trabajador en el ámbito de dirección del empresario, la cual lleva implícita la atribución a éste de un poder de organización y de dirección de las singulares prestaciones laborales de los trabajadores por él contratados, los cuales vienen obligados a realizar el trabajo acordado bajo la dirección de aquél o persona en quien delegue, según literal dicción del art. 20.1 ET, norma que es bien expresiva de la actitud del legislador ante el poder directivo del empresario (actitud de reconocimiento, pero simultáneamente de limitación), situándolo dentro del marco de lo convenido con el trabajador.

Precisamente, es la propia Constitución española la que determina la imposibilidad, aun cuando ni siquiera haya dado comienzo la ejecución de la prestación laboral, de que en el contrato de trabajo se puedan fijar estipulaciones contrarias al respeto debido a los derechos fundamentales del trabajador, siendo nulas aquellas cláusulas contractuales incompatibles con los mismos[30] y, una vez iniciada la ejecución de aquélla, el poder de dirección del empresario vendrá limitado tanto por el contrato de trabajo como por el convenio colectivo aplicable y, sobre todo, por los derechos fundamentales[31], los cuales constituyen un límite externo a la relación laboral operando como prohibiciones o límites que suponen un verdadero orden público constitucional que veda intromisiones o injerencias[32] injustificadas.

29 STC 166/1988, de 26 de septiembre, FJ 6, que afirma que el poder de control del empresario *"encuentra un límite insuperable en los derechos fundamentales del trabajador, que no pueden ser vulnerados por el empresario"*.

30 En este sentido, entre otras, STC 19/1985, de 13 de febrero, FJ 4.

31 MARÍN ALONSO, I., *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Tirant lo Blanch, Valencia, 2004, pág. 87.

32 Como expresamente recalca la STC 292/1993, de 18 de octubre, FJ 2, *"el poder de dirección y gestión de la empresa tiene como límite infranqueable el respeto a los derechos fundamentales de los trabajadores"*.

2. En este sentido, los derechos fundamentales ejercen una función de límites negativos –*ius resistentiae* del trabajador - al poder de dirección del empresario obligando a éste a ofrecer un motivo razonable sobre su decisión de modular aquéllos, lo que conducirá inevitablemente a un enjuiciamiento de ese motivo desde la perspectiva del derecho fundamental en cuestión[33]. Pero los mismos también operan como límites positivos a aquél, en el sentido de imponer al empresario la obligación de adoptar medidas positivas en orden a impedir o corregir el menoscabo de los mismos en virtud de lo dispuesto por el art. 20.2 ET, a cuyo tenor el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe, quedando el juzgador vinculado en su aplicación a las relaciones laborales entre particulares[34], de modo que la misma se erige en comportamiento exigible al empresario pudiendo incluso condicionar el ejercicio de su poder de dirección, no sólo en cuanto deber negativo de respeto de los derechos fundamentales del trabajador, sino también en cuanto deber positivo de tutela y protección de los mismos[35].

Así, por ejemplo, por lo que respecta a la violencia de género, una muestra sobre las obligaciones positivas que pesan sobre el empresario al objeto de respetar los derechos fundamentales del trabajador, es la Ley Orgánica 1/2004, de 26 de diciembre, de medidas de Protección Integral contra la Violencia de Género, que supone exigir a la empresa una racionalidad adicional a la estrictamente profesional con la finalidad de acoger en sus decisiones la toma en consideración de vicisitudes estrictamente personales de

33 GUTIÉRREZ PÉREZ, M., *Ciudadanía en la empresa…, op. cit.*, pág. 170.

34 GIL Y GIL, J. L., *Principio de la buena fe y poderes del empresario*, Consejo Andaluz de Relaciones Laborales, 2003, págs. 196 y sigs.

35 GUTIÉRREZ PÉREZ, M., *Ciudadanía en la empresa…, op. cit.*, pág. 176. No obstante, el Tribunal Constitucional ha venido afirmando que la conducta del empresario ha de hallarse presidida por el principio de neutralidad, argumentando al respecto que las actividades productivas no pueden verse alteradas para potencia fomentar o facilitar el ejercicio de derechos fundamentales (STC 19/1985, de 13 de febrero). Por sí mismos, los derechos fundamentales no constituyen cláusulas ilimitadas de excepción que justifiquen el incumplimiento de los deberes asumidos en el contrato de trabajo. La sujeción del empresario a los derechos fundamentales no justifica, por sí sola, un menoscabo de los principios de seguridad jurídica y *pacta sunt Servanda* (SSTC 88/1985, de 19 de julio y 129/1989, de 17 de julio).

las trabajadoras a su servicio que pueden aconsejar modificaciones en su prestación que no se adoptan por la evidencia de necesidades empresariales[36], sino por la necesidad de respetar los derechos fundamentales de las trabajadoras afectadas. O, en cuestión de acoso sexual, se impone al empresario la obligación de prevenir el mismo en la empresa y de mantener un ambiente de trabajo adecuado, la cual se materializa en las obligaciones de mantener unas instalaciones seguras en el centro de trabajo y de adopción de todas las medidas necesarias contra los comportamientos de acoso sexual y de protección de la vida privada de los trabajadores que han sido víctimas de acoso. Y, más recientemente, hemos de reseñar el Real Decreto-ley 6/2019, de 1 de marzo, de medidas urgentes para garantía de la igualdad de trato y de oportunidades entre mujeres y hombres en el empleo y la ocupación.

En el marco de los límites impuestos al poder de dirección y control del empresario en virtud de los derechos fundamentales del trabajador nos referiremos exclusivamente a los límites que éstos imponen a aquél en el desarrollo de la relación laboral *stricto sensu*, dejando al margen tanto la fase pre-laboral como el ámbito extra laboral del trabajador, a cuyo efecto hemos de partir de la afirmación sostenida por el Tribunal Constitucional referida a la necesidad de mantener un adecuado equilibrio entre las obligaciones del trabajador y la facultad de control empresarial, pero siempre teniendo presente que los derechos fundamentales que el trabajador ostenta prevalecen sobre el derecho de control del empresario[37], por lo que aquéllos constituyen límites negativos para el poder de control empresarial y operan como derechos de defensa frente a un ejercicio ilegítimo del mismo por parte del empleador.

Y es precisamente en este sentido en el que los arts. 20.3 y 18 ET aluden al respeto de la dignidad del trabajador como base de todos los derechos fundamentales, de modo que la proyección de la dignidad de la

36 FERNÁNDEZ LÓPEZ, Mª. F., *La dimensión laboral de la violencia de género*, Ed. Bomarzo, Albacete, 2005, págs. 21 y sigs.

37 STC 6/1998, de 21 de enero.

persona en general y los derechos fundamentales en particular en el control por parte del empresario no sólo va a permitir superar una visión patrimonialista de la relación laboral, sino que va a situar a la actividad de control empresarial en sus justos términos, erigiéndose los derechos fundamentales del trabajador en límites a la discrecionalidad del ejercicio del poder de control del empresario.

No obstante, no podemos obviar que el principal problema de los derechos fundamentales, en cuanto límites del poder de control empresarial, reside en que se parte de una ambigua e imprecisa regulación en el Estatuto de los Trabajadores, hasta el punto de que el art. 20.3 de ese texto legal otorga al empresario un alto grado de permisividad al objeto de controlar como crea oportuno la prestación laboral, procurando preservar en gran medida el interés mercantil del mismo[38]. No obstante, las exigencias impuestas por los derechos fundamentales al poder de control impedirán, como se ha dicho, un ejercicio ilegítimo del mismo, obligándose al empresario a motivar la medida de control adoptada, lo que conduce inexorablemente a un enjuiciamiento de ésta desde la perspectiva del derecho fundamental en cuestión[39], habiendo sido resueltos estos conflictos por el Tribunal Constitucional en el sentido de reconocer la facultad de control del empresario ejercida con respeto de los derechos fundamentales del trabajador.

3.- Límites a los derechos fundamentales en el marco de la relación laboral.

1. Si bien es afirmación pacífica la de que el trabajador sigue siendo titular de sus derechos fundamentales aunque se encuentre vinculado al empresario a través de un contrato de trabajo, no obstante los derechos fundamentales no son derechos ilimitados o absolutos, sino que pueden ceder

38 MARÍN ALONSO, I., *El poder de control empresarial…, op. cit.*, pág. 200.

39 A este respecto, vid. GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial*, Civitas, Madrid, 1988.

ante otros intereses y/o derechos constitucionalmente relevantes[40]. Y, en este sentido, se ha venido afirmando tanto por la doctrina[41] como por la jurisprudencia la existencia de límites específicos al ejercicio de aquéllos por parte del trabajador en el seno del contrato de trabajo habida cuenta de que éste despliega un conjunto de derechos y obligaciones recíprocas que condicionan su ejercicio, de modo que manifestaciones de los mismos que pudieran ser legítimas en otro contexto pueden no serlo en el ámbito de la relación laboral[42], lo que significa que, aunque no se niegue su reconocimiento, sí puede, sin embargo, modalizarse su alcance en el marco de aquella relación[43].

2. El fundamento de los límites a los derechos fundamentales en el ámbito del contrato de trabajo se encuentra, como apunta el Tribunal Constitucional[44], en el hecho de que aquéllos se desenvuelven en el seno de una organización que refleja otros derechos consagrados en los arts. 33 y 38 CE (derecho de propiedad y libertad de empresa, respectivamente), lo que implica una necesaria adaptabilidad para el ejercicio conjunto de todos ellos, de modo que se hace necesario modular el contenido de los derechos fundamentales con el objeto de respetar esos otros derechos constitucionalmente consagrados, como son la libertad de empresa y el

40 Entre otras, SSTC 57/1994, de 28 de febrero; 143/1994, de 9 de mayo y 98/2000, de 10 de abril.

41 Entre otros, MARTÍN VALVERDE, A., "Contrato de trabajo y derechos fundamentales", *Revista de Derecho Social*, núm. 6, 1999, pág. 19.

42 En este sentido el propio Tribual Constitucional ha afirmado desde la sentencia 18/ 1981, de 8 de junio, refiriéndose en este caso al derecho de reunión, que éste *"puede ejercerse en la relación laboral (…) pero que se pueden contemplar especialidades de su ejercicio cuando se efectúa en el ámbito laboral"*. Por parte, en la STC 120 /1983 de 15 de diciembre, se afirmaba que el contrato entre trabajador y empresario genera un conjunto de derechos y obligaciones recíprocas que condicionan junto a otros el ejercicio del derecho fundamental en cuestión. En el mismo sentido, SSTC 19/1985, de 13 de febrero; 170/1987, de 30 de octubre; 129/ 1989, de 17 de julio; 126 /1990, de 5 de julio; 186/ 1996, de 25 de noviembre, etc.

43 PEDRAJAS MORENO, A., *Despido y derechos fundamentales: estudio especial de la presunción de inocencia*, Ed. Trotta, Madrid, 1992, pág. 86-87.

44 Entre otras, SSTC 99/1994, de 11 de abril; 6/1995, de 10 de enero; 106/1996, de 12 de junio; 136/1996, de 23 de julio; 14/2003, de 30 de enero, etc.

derecho de propiedad, los cuales son reflejo de la organización empresarial a la que se incorpora el trabajador[45].

3. No obstante, la buena fe también puede desempeñar un papel limitador de los derechos fundamentales del trabajador en lógica correspondencia con las obligaciones que la misma puede entrañar para el empresario en el ámbito de los derechos fundamentales en el marco de la relación laboral, como se ha visto con anterioridad. En este sentido, la jurisprudencia constitucional ha venido afirmando desde sus comienzos que los derechos fundamentales no sólo se limitan por otros derechos o intereses constitucionalmente protegidos[46], sino que también pueden verse condicionados por bienes que gozan de una protección infraconstitucional, como es la buena fe contractual[47], lo que significa que el principio de buena fe puede llegar a erigirse en elemento modulador del ejercicio de aquéllos en el marco del contrato de trabajo con el fin de permitir la satisfacción de legítimos intereses empresariales[48].

45 No obstante, hay que apuntar que un amplio sector de la doctrina laboralista viene criticando que los derechos fundamentales del trabajador puedan venir limitados por la concurrencia en la relación laboral con otros derechos fundamentales menos plenos, como serían el derecho de propiedad y, en especial, la libertad de empresa, al carecer ambos de ciertas garantías sí reconocidas a los derechos fundamentales del trabajador, como la reserva de Ley Orgánica y la posibilidad de acceder al Recurso de Amparo, llegando en ocasiones a disfrutar incluso de un mayor reconocimiento la libertad de empresa y el derecho de propiedad del empresario cuando entran en fricción con los derechos fundamentales del trabajador en cuanto ciudadano. En este sentido, OJEDA AVILÉS, A., "Equilibrio de intereses y bloque de constitucionalidad personal en la empresa", *Revista de Derecho Social*, núm. 35, 2006, pág. 19.

46 El tema de los límites a los derechos fundamentales es complejo. Sobre el particular puede verse MARTÍN RETORTILLO, L. y DE OTTO PARDO, I., *Derechos fundamentales y Constitución*, Ed. Civitas, Madrid, 1988.

47 En este sentido, la STC 120/1983, de 15 de diciembre, fue la que vino a señalar la trascendencia de la buena fe contractual en la vigencia de los derechos fundamentales en el contrato de trabajo, señalando que *"…la exclusión del deber de lealtad no exime de la necesidad de un comportamiento mutuo ajustado a las exigencias de la buena fe, como necesidad derivada del desenvolvimiento de todos los derechos y específica de la relación contractual, que matiza el cumplimiento de las respectivas obligaciones y cuya vulneración convierte en ilícito o abusivo el ejercicio de los derechos, quedando al margen de su protección".*

48 En este sentido, el TC ha venido sosteniendo que *"surge un condicionamiento o límite adicional en el ejercicio del derecho constitucional, impuesto por la legislación laboral que se deriva del principio de buena fe entre las partes del contrato de trabajo y al que éstas han de ajustar su comportamiento mutuo"* (STC 88/1985, de 19 de julio). No obstante, parte de la doctrina iuslaboralista muestra sus reticencias acerca de la posibilidad de que un principio

En esta línea, la jurisprudencia constitucional ha llegado a afirmar que la buena fe tiene reflejo constitucional, aunque no ha dicho en qué precepto concreto, y que aquélla conforma el ejercicio de todos los derechos, incluidos los constitucionales[49], por lo que, en torno a la exigencia de fundamento constitucional de la buena fe en aras a poder limitar los derechos fundamentales del trabajador, se afirma por la doctrina iuslaboralista[50] que es necesario reconducir la exigencia de la buena fe a la Constitución[51].

4. Asimismo, otro principio general que pudiera utilizarse en orden a limitar el ejercicio de los derechos fundamentales en las relaciones privadas es el abuso de derecho (art. 7.2 C.C.), si bien hay que señalar que rara vez se alude por parte de la jurisprudencia constitucional al posible abuso del derecho fundamental por parte del trabajador[52], al tiempo que se han planteado muchas dudas acerca de la viabilidad jurídica de la aplicación de esta cláusula a un derecho fundamental, sobre todo teniendo en cuenta que la figura del abuso de los derechos fundamentales no se encuentra regulada en la Constitución

---

infraconstitucional, como es la buena fe, pueda limitar los derechos fundamentales de los trabajadores dado el rango constitucional que éstos presentan. En este sentido, entre otros, GARCÍA-PERROTE ESCARTÍN, I., "Ley, convenio colectivo, contrato de trabajo y derechos fundamentales del trabajador", *Revista de Derecho Social*, núm. 4, 1988, págs. 46 y sigs.; DEL REY GUANTER, S., "Derechos fundamentales de la persona y contrato de trabajo: notas para una teoría general", *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 1, 1995, pág. 209; VALDÉS DAL RE, F., "Poderes del empresario y derechos de la persona del trabajador", *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 1, 1990, pág. 291.

En contra se manifiestan, entre otros, MONTOYA MELGAR, A., *La buena fe en el Derecho del Trabajo*, Tecnos, Madrid, 2001, págs. 86 y sigs.; MARTÍN VALVERDE, A., "Contrato de trabajo y derechos fundamentales", *Revista de Derecho Social*, núm. 6, 1999, pág. 20, que entienden que la buena fe viene desencadenada por la suscripción del contrato de trabajo y, por tanto, el derecho fundamental no puede actuar como excusa para alterar lo que aquélla viene a exigir a cada uno de los contratantes.

49 SSTC 34/1981, de 10 de noviembre; 120/1983, de 15 de diciembre; 6/1988, de 21 de enero; 214/1991, de 11 de noviembre.

50 GORELLI HERNÁNDEZ, J. e IGARTÚA MIRÓ, M. T., "Libertad de información y contrato de trabajo. El problema de sus límites", *Aranzadi Social*, núm. 15, septiembre 1999, págs. 73-74.

51 En este sentido, la STC 126/2003, de 30 de junio, parece configurar la buena fe como expresión contractual de la libertad de empresa.

52 GUTIÉRREZ PÉREZ, M., *Ciudadanía en la empresa y derechos…, op. cit.*, pág. 219.

española, como sí sucede con la Constitución alemana y en el CEDH, cuyo art. 18 incluye expresamente este límite para determinados derechos fundamentales, si bien referido a la perturbación de valores supremos como la libertad, la justicia, la igualdad o el pluralismo político.

5. Por lo que se refiere a la posibilidad de modular el contenido de los derechos fundamentales en el seno del contrato de trabajo como consecuencia del consentimiento de su titular merced al principio de autonomía de la voluntad (art. 1255 C.C.), hemos de señalar que no resulta admisible la auto renuncia total por parte del trabajador al derecho fundamental del que es titular. Baste recordar, a este respecto, la STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía) en la que el Tribunal de Estrasburgo sostiene que el ejercicio de los derechos fundamentales en el seno de las empresas no puede reducirse a cero[53], de modo que en la relación laboral no se puede admitir indiscriminadamente la auto restricción por parte del titular del derecho fundamental, reconociendo carta de naturaleza al principio de autonomía de la voluntad con la consecuencia de ignorar la desigualdad de las partes en el contrato de trabajo y sin reparar en que el acto de disposición de un derecho fundamental puede afectar a la dignidad de la persona del trabajador[54].

53 Concretamente señala la sentencia del TEDH que la normativa interna de las empresas no puede reducir la vida privada social en el marco de la relación laboral a cero, sino que subsiste en todo momento una expectativa razonable de privacidad a pesar de la existencia de una prohibición expresa y reiterada de uso de los medios informáticos de la empresa con fines personales.

54 RIVERO LAMAS, J., "Derechos fundamentales y contrato de trabajo: eficacia horizontal y control constitucional", en MONTOYA MELGAR, A. (Coord.), *El trabajo y la Constitución. Estudios en homenaje al profesor Alonso Olea*, Academia Iberoamericana de Derecho del Trabajo y de la Seguridad Social-Ministerio de Trabajo y Asuntos Sociales, Madrid, 2003, pág. 521.

No obstante, como sostiene GUTIÉRREZ PÉREZ, M., *Ciudadanía en la empresa y derechos…, op. cit.*, pág. 223, establecer con carácter general normas limitadoras al principio de autonomía de la voluntad puede comportar una sensible limitación de la autonomía privada modificando de forma esencial el significado del derecho privado, de modo que pueden resultar viables jurídicamente renuncias parciales por parte del trabajador al ejercicio de alguno de sus derechos fundamentales siempre que las mismas expresen realmente su voluntad, esto es, siempre y cuando el trabajador esté actuando libremente a la hora de expresar su consentimiento y no se vea condicionado en ese momento por el mayor poder de la parte empresarial, si bien la validez de esas renuncias exigirá, además, una operación de balance por la que se contraste la admisibilidad o no de las mismas respecto de otros bienes o valores

4.- La ponderación legal y jurisprudencial del poder de dirección del empresario y de la privacidad del trabajador en las relaciones laborales tecnificadas.

1. La controversia jurídica en torno a la ponderación legal y jurisprudencial del poder directivo empresarial y la privacidad del trabajador carece de tratamiento específico en nuestro ordenamiento jurídico dado que no existe norma alguna al respecto que contemple expresamente esta problemática. Sólo contamos en nuestro haber con el art. 20.3 ET que, en su dicción literal, permite al empresario adoptar las medidas de control que considere más convenientes en orden a la verificación del cumplimiento por parte del trabajador de sus obligaciones laborales, siempre con el límite del respeto a la dignidad e intimidad de éste.

Una idea presente en toda la lógica de las relaciones laborales pasa por considerar que la firma del contrato de trabajo y su ulterior desarrollo confiere al empleador un poder legal de dirección tendente a la ordenación de la prestación laboral y asegurar de este modo el normal desarrollo del proceso productivo[55], derivando de dicha prerrogativa un amplio[56] haz de facultades entre las que se cuenta la posibilidad que tiene aquél de adoptar las medidas que considere más oportunas para comprobar el adecuado cumplimiento de la

---

constitucionales dignos de protección, destacando, sobremanera, en este aspecto, como es lógico, los derechos constitucionales de titularidad empresarial, como son el derecho de propiedad y, en especial, la libertad de empresa.

Precisamente, un campo en el que se proyecta con especial relevancia el papel del consentimiento, en lo que a la renuncia de un derecho fundamental se refiere, es en el relativo al tratamiento automatizado de datos de carácter personal y, en particular, los llamados datos sensibles (ideología, religión, salud, etc.), dado que la existencia o no de consentimiento por parte del trabajador va a determinar la accesibilidad o no parte por parte del empresario a determinados datos que afectan directamente a algunos derechos fundamentales de aquél, entre ellos, el derecho a la intimidad

55 MONTOYA MELGAR, A., *El poder de dirección del empresario*, Madrid (IES), 1965, págs. 44 y ss., o, del mismo autor y más reciente, "El poder de dirección del empresario", *Revista Española de Derecho del Trabajo*, núm. 100, 2000, págs. 507 y ss. También, ROMÁN DE LA TORRE, M.ª D., *Poder de dirección y contrato de trabajo*, Valladolid, Grapheus, 1992, pág. 351.

56 Por todos, LUQUE PARRA, M., *Los límites jurídicos de los poderes empresariales*, Barcelona, 1999, Bosch, págs. 16 y sigs.

prestación laboral por parte del trabajador, guardando siempre en su adopción la consideración debida a la dignidad humana (art. 20.3 ET).

En definitiva, este poder de control, complemento del de dirección,[57] pese a conceder un amplio y poco preciso[58] margen de actuación al empresario, lleva aparejado consigo tanto el deber de utilizar medios respetuosos con los derechos fundamentales de los trabajadores[59] como la obligación de circunscribir la actividad de control a la exclusiva comprobación de aquellos aspectos estricta y directamente vinculadas con la prestación del trabajo[60], a lo que hay que añadir, además, que las medidas adoptadas habrán de ser oportunas (es decir, adecuadas) en orden a verificar el cumplimiento por parte del trabajador de sus obligaciones laborales.

Como se ha dicho, la introducción de las TIC en la empresa, además de alterar sustancialmente el modelo de producción y la forma de trabajo, presenta en su impacto sobre el poder directivo del empresario una de sus manifestaciones más vistosas[61] dado que habilitan, cada vez en mayor medida,

57 Para un estudio exhaustivo del tema véase GOÑI SEIN, J. L., *El respeto de la esfera privada del trabajador*, Civitas, 1989, Madrid, pág. 109; DE VICENTE PACHÉS, F., *El derecho del trabajador al respeto de su intimidad*, CES, 1998, Madrid, págs. 299 y ss.

58 VALDÉS DAL-RÉ, F., "Poderes del empresario y derechos de la persona del trabajador", *Relaciones Laborales*, tomo I, 1990, págs. 284 y sigs.; FERNÁNDEZ LÓPEZ, M.ª F., "Libertad ideológica y prestación de servicios", *Relaciones Laborales*, núm. 7, 1985, págs. 421 y sigs.

59 DE VICENTE PACHÉS, F., *El derecho del trabajador al respeto de su intimidad*, *op. cit*, pág. 301; GARCIA NINET, J. I. y VICENTE PALACIO, A., "Los derechos fundamentales como límite a las facultades organizativas del empresario (libertad sindical y movilidad funcional)", *Aranzadi Social*, tomo IV, 1999, págs. 687 y sigs.; FERNÁNDEZ VLLLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral*, Pamplona, 2003, Aranzadi, págs. 34 y sigs. y 61 y sigs., o SAMPEDRO GULLÓ, V., "Facultades empresariales de vigilancia y control en el centro de trabajo", *Tribuna Social*, núm. 160, 2004, pág. 14.

60 Sin embardo, no es fácil hacer una separación entre la persona del trabajador y las implicaciones derivadas de la prestación por él realizada. MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, CES, 2002, Madrid, pág. 54.

61 PÉREZ DE LOS COBOS ORIHUEL, F., *Nuevas tecnologías y relación de trabajo*, 1990, Tirant lo Blanch, Valencia, pág. 72, o SEMPERE NAVARRO, A. V. y SAN MARTIN MAZZUCONI, C., *Nuevas tecnologías y relaciones laborales*, Aranzadi, Pamplona, 2002, págs. 42 y sigs.

medios capaces de intensificar las posibilidades de fiscalización de la actividad laboral por parte del empresario[62].

De este modo, el control presencial del trabajador forma ya parte del pasado del Derecho del Trabajo[63], habiendo cedido el mismo su paso al control tecnológico, de forma que aquel control periférico y discontinuo realizado por el ser humano deja paso a uno centralizado y verificado en tiempo real[64].

A ello hay que unir el hecho de que los mercados de trabajo que conocemos y el empleo cambiarán tan decisiva y rápidamente por diversos condicionantes imparables de la robotización y la mecanización que hacen urgente la preparación de normas, políticas e instituciones jurídicas capaces de acoger las nuevas realidades en orden a que el trabajo con derechos fundamentales y valores sociales sea un elemento de transformación social propio de una democracia constitucional[65].

Tan es así que el propio TEDH ha dicho en la sentencia Barbulescu II que las formas de prestación del trabajo y de organización de las relaciones laborales evolucionan rápidamente en el ámbito de las tecnologías digitales. Sin embargo, ese cambio acelerado y las singularidades del mundo virtual no

62 MARTINEZ FONS, D., *El poder de control del empresario en la relación laboral*, *op. cit*., pág. 54. Recientemente, una magnífica labor de síntesis en ALONSO, D., "Protection of employees' privacy and personal information in Spain: General patterns and case law trends", en AA. VV.: *Protection of employees' personal information and privacy*, Lon• don, 2015, Wolters Kluwer, págs. 163 y sigs.

63 CASAS BAAMONDE, M.ª E., BAYLOS GRAU, A. y ESCUDERO RODRIGUEZ, R., "El Estatuto de los Trabajadores. Diez años después: pervivencias, insuficiencias desviaciones y reformas", *Relaciones Laborales*, núms. 6-7, 1990, págs. 139 y sigs.

64 PÉREZ DE LOS COBOS ORIHUEL, F., *Nuevas tecnologías y relación de trabajo*, cit., pág. 72, o RODRÍGUEZ ESCANCIANO, S., *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015, págs. 45 y sigs.

65 CASAS BAAMONDE, Mª. E., "Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral, *Derecho de las Relaciones Laborales*, I2, 2018, pág. 103.

puede dar lugar a espacios laborales sin derechos fundamentales de los trabajadores, declarando que la proporcionalidad y las garantías procedimentales son elementos esenciales.

2. Lo expuesto nos conduce, ineludiblemente, a poner en valor la necesidad de garantizar, mediante su protección, los derechos fundamentales, no sólo frente a los poderes públicos sino también, fundamentalmente, frente al empleador, no habiendo permanecido impasible el TC ante esta cuestión, sino que ha venido manteniendo a lo largo del tiempo una jurisprudencia constante e invariable a partir de la Sentencia 88/1985, de 19 de julio.

En efecto, en esta sentencia se deja asentado de modo categórico que la celebración de un contrato de trabajo no implica ni supone, en ningún caso, que se prive al trabajador de los derechos que, como persona, la Constitución le reconoce, entre los que se cuentan el derecho de expresión reconocido en su art. 20.1.a), y cuya protección se encuentra garantizada también en el ámbito laboral, como no podía ser de otra forma, dado que las organizaciones empresariales no constituyen mundos separados y estancos al margen de la sociedad, así como tampoco la libertad de empresa consagrada en el art. 38 CE legitima, en ningún caso, que los trabajadores puedan sufrir despojos injustificados, siquiera sean transitorios, de sus derechos fundamentales y libertades públicas, los cual sería expresión de un feudalismo industrial que repugna y choca frontalmente con los postulados del Estado social y democrático de Derecho y los valores supremos de libertad, justicia e igualdad consagrados en el art. 1.1 del texto constitucional.

Pero, como ha quedado dicho, existe un poder directivo del empresario que supone, o puede suponer, una injerencia en el ámbito de los derechos fundamentales de sus empleados, habiendo sido examinado este conflicto de intereses por el TC en su sentencia 98/2000, de 10 de abril, sosteniendo que el ejercicio de los derechos fundamentales sólo admite limitaciones por el hecho

de que se desenvuelven en el seno de una organización empresarial que refleja también otros derechos e intereses reconocidos constitucionalmente en los arts. 33 y 38, lo cual obliga a una necesaria adaptabilidad de los mismos al objeto de hacer factible el ejercicio de todos ellos.

Es, pues, en este aspecto en el que se palpa la pulsión entre la posibilidad absoluta de vigilancia por parte del empresario y los derechos fundamentales de los trabajadores, en particular, los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales y, ante este conflicto de derechos e intereses, se hace necesario acotar el ámbito o alcance de los mismos y la necesaria adaptación o modulación que, en su ejercicio, puede suponer la existencia de otros derechos o intereses cuyo titular es precisamente la otra parte de la relación laboral.

Y es que, como es evidente, si por una parte resulta claro que el trabajador, titular de derechos fundamentales en la vida social, no se despoja de estos al ingresar en la empresa, por la otra lo es también que el empresario ostenta poderes organizativos y directivos que, aun teniendo una base contractual, encuentran igualmente respaldo constitucional, en este caso a través de la libertad de empresa.

Ello determina que nos encontramos ante dos pretensiones dotadas de respaldo constitucional, las cuales de ser llevadas hasta sus últimas consecuencias terminan por ser incompatibles, pues no cabe duda de que un ejercicio ilimitado de los poderes empresariales de dirección y control puede acabar anulando toda posibilidad de ejercicio de los derechos fundamentales por parte de los trabajadores, al tiempo que un celo igualmente absoluto por parte de éstos en el ejercicio de sus derechos vaciaría de contenido esos poderes, siendo en esta confluencia de situaciones jurídicas contrapuestas entre sí donde radica la gran dificultad que entraña la garantía de los derechos fundamentales de la persona en el seno de las relación laboral, lo cual nos

permite apreciar cómo la afirmación de la vigencia de los derechos fundamentales del trabajador constituye más una fuente de interrogantes que de afirmaciones concluyentes en la medida en que deja sin resolver el problema de la relación entre estos derechos y las obligaciones que dimanan del contrato de trabajo[66].

3. Para resolver este conflicto la jurisprudencia constitucional ha adoptado el denominado principio o test de proporcionalidad, el cual ha terminado por erigirse en el criterio dirimente básico de los conflictos derivados del ejercicio de los derechos fundamentales entre particulares, incluyendo, obviamente, los que se presentan en el seno de la relación laboral.

Desde esta perspectiva, la idea de modulación o adaptación remite principalmente a una operación de contraste entre el derecho fundamental en cuestión y los otros derechos presentes en la lógica del contrato de trabajo, de modo que dicha operación será el resultado de articular el adecuado encaje entre el poder de dirección y control del empresario y el derecho fundamental invocado por el trabajador, los cuales delimitan el marco jurídico de actuación de dichos actores[67], desplegando los derechos fundamentales de los trabajadores en todo momento su clásica función de contención frente a los poderes empresariales[68].

De este modo, aquéllos sólo podrán experimentar modulación en los términos estrictamente necesarios para la protección de los otros derechos implicados[69], por lo que la operación de contraste referida entraña un proceso

66 SANGUINETI RAYMOND, W., "Poderes empresariales y derechos de la persona del trabajador: el difícil equilibrio", *Trabajo y Derecho*, Monográfico 7/2018, nº 7, 1 de junio de 2018, Ed. Wolters Kluwer, págs. 2-3.

67 CASAS BAAMONDE, Mª. E., "La plena efectividad de los derechos fundamentales: juicio de ponderación (¿o de proporcionalidad?) y principio de buena fe", *RL*, I, 2004, pág. 145.

68 MARTÍN VALVERDE, A., "La Constitución como fuente del Derecho del Trabajo", *REDT*, núm. 33, 1988, pág. 63.

69 GARCÍA MURCIA, J., "Los derechos de la persona…, *op. cit.*, pág. 44.

de reflexión que habrá de desarrollarse necesariamente en tres pasos sucesivos, a saber: (i) la identificación del derecho empresarial (que será generalmente el poder de control y dirección del empresario); (ii) la delimitación del derecho fundamental del trabajador afectado por la medida empresarial impuesta (es decir, la determinación de su contenido); y (iii) la búsqueda de criterios proporcionales para la adecuada resolución del conflicto, debiendo señalarse que la operación de modulación de los derechos fundamentales en el ámbito del contrato de trabajo presenta una dimensión eminentemente casuística, estando su capacidad de respuesta notablemente condicionada por las circunstancias concretas de cada caso[70], de forma que existen serias dificultades para que dicho proceso modulador pueda traducirse en una fórmula general con validez universal capaz de ofrecer un sentido predecible a la hora de su aplicación práctica dado que, de un lado, cada derecho fundamental presenta rasgos particulares y, de otro, el legislador apenas ha abordado la tarea de la modulación de los derechos fundamentales en el seno de las relaciones jurídico-laborales, habiéndose limitado a reconocer derechos o poderes, pero sin descender a sus problemas de articulación[71].

4. En estas condiciones, todos los esfuerzos de la doctrina y de la jurisprudencia se han dirigido exclusivamente a la búsqueda de procedimientos tendentes a aquilatar la eficacia de los derechos fundamentales en el ámbito del contrato de trabajo a la vista de la habitual concurrencia con otros derechos, siendo el procedimiento de mayor uso a tales efectos el de la ponderación de derechos e intereses en juego al objeto de alcanzar un equilibrio razonable entre los mismos, si bien sus resultados prácticos no han dejado de suscitar críticas debido a que la operación de ponderación de

70 DESDENTADO BONETE, A. y MUÑOZ RUIZ, A., "El control de la prestación de trabajo a través de las nuevas tecnologías: un estudio sobre la video vigilancia en la doctrina judicial", *Justicia Laboral*, núm. 44, 2010, págs. 36-37.

71 SAGARDOY BENGOECHEA, J. A., *Los derechos fundamentales y el contrato de trabajo*, Civitas, Pamplona, 2005, pág. 33.

derechos reclama necesariamente una operación de cuantificación no siempre fácil de realizar en intereses de esta naturaleza[72].

No obstante, hay que destacar que cuando el derecho fundamental en juego tenga un pleno encaje en el ámbito del contrato de trabajo (como sucede, por ejemplo, con el derecho a la intimidad, el derecho al secreto de las comunicaciones, la protección de datos personales o la no discriminación), el mismo será merecedor de la máxima tutela y protección con la consiguiente restricción o anulación de las medidas que lo perturben o lesionen. Y lo mismo sucede en los casos en que la ponderación valore situaciones concurrentes entre derechos fundamentales y otros derechos de distinto nivel, los cuales habrán de ser resueltos conforme a criterios de rango normativo habida cuenta de que los derechos fundamentales, en cuanto parte de la norma constitucional que son, gozan de la máxima jerarquía en el sistema jurídico, debiendo prevalecer los mismos sobre aquellas normas que encierren contradicción con el correspondiente mandato constitucional. Piénsese, por ejemplo, en la hipotética contradicción entre los derechos fundamentales y las obligaciones corrientes u ordinarias asumidas en el contrato de trabajo tales como el deber de buena fe, o entre los derechos fundamentales y las reglas dimanantes de disposiciones de rango infraconstitucional[73].

5.- Estructura de la Tesis Doctoral.

1. Para alcanzar el objetivo previsto hemos dividido la Tesis Doctoral en cinco capítulos, cada uno de los cuales responde a las preguntas objeto de investigación, a saber: el análisis del concurso de derechos fundamentales que

72 GARCÍA MURCIA, J., "Los derechos de la persona…, *op. cit*., pág. 50, que señala que una causa de insatisfacción radica en el hecho de que la ponderación presupone una situación de contraste entre derechos que conduce inevitablemente a la inclinación de la balanza hacia uno u otro lado mediante opciones que suelen tener una gran carga valorativa y que se muestran incapaces de proporcionar una salida airosa al contencioso planteado.

73 GARCÍA MURCIA, J., "Los derechos de la persona…, *op. cit*., pág. 50.

puede producirse en los casos de video vigilancia empresarial y control del correo electrónico por parte del empresario; la necesidad de previsión legal de la medida de injerencia en la privacidad del trabajador y la denominada “calidad de la ley”; la necesidad de autorización judicial para conocer el contenido del correo electrónico del trabajador; la proporcionalidad de la medida de vigilancia y control empresarial y, por último, el deber de información - específico y concreto- al trabajador respecto de las medidas de vigilancia decididas por el empresario.

2. En el Capítulo I se analiza el concurso de derechos referido distinguiendo los derechos fundamentales del trabajador afectados por la medida de injerencia empresarial: intimidad personal, secreto de las comunicaciones y protección de datos personales, previstos en el art. 18 CE, y derecho a la vida privada y familiar previsto en el art. 8 CEDH, en cuanto contenido ampliado del derecho a la intimidad personal.

A tal efecto, se hace un análisis de las decisiones judiciales pronunciadas en el orden interno tanto por el Tribunal Constitucional como por el Tribunal Supremo. En concreto, referidas al derecho a la intimidad, se estudian, entre otras, las SSTC 98/2000, de 10 de abril (caso “Casino La Toja, S.A.”, en el que se cuestionaba la instalación por parte de la empresa de micrófonos en ciertas zonas del casino, concretamente en la zona de caja y de la ruleta francesa, por suponer dicha medida una intromisión ilegítima en el derecho a la intimidad de los trabajadores) y 186/2000, de 10 de julio (caso “ENSIDESA”, en el que se analizaba la instalación de cámaras para un circuito cerrado de televisión en las cajas registradoras del economato de la empresa ante la advertencia de que existían irregularidades contables).

Por su parte, en lo referente al control del ordenador y su uso se analiza la STS de 26 de septiembre de 2007 (unificadora de la doctrina jurisprudencial acerca del alcance y forma del control del empresario sobre el uso por parte del

trabajador del ordenador facilitado por aquél como instrumento de trabajo). En punto al derecho al secreto de las comunicaciones se hace un análisis de las SSTC 241/2012, de 17 de diciembre y 170/2013, de 7 de octubre. Y en lo referente al derecho a la protección de datos personales se estudia la STC 292/2000, de 30 de noviembre.

3. En el Capítulo II se profundiza en la configuración legal de las medidas de control empresarial haciéndose un estudio de las exigencias contenidas en los arts. 8 CEDH y 18 CE para, seguidamente, examinar la jurisprudencia del TEDH recaída en la materia, haciéndose especial hincapié en la necesidad de previsión legal de la medida de injerencia en la privacidad del trabajador y en la denominada "calidad de la ley". En concreto, se examinan, entre otras, las SSTEDH de 25 de junio de 1997 (caso Halford c. Reino Unido); de 3 de abril de 2007 (caso Copland c. Reino Unido); de 2 de agosto de 1984 (caso Malone c. Reino Unido); de 24 de abril de 1990 (casos Kruslin c. Francia y Huvig c. Francia); de 30 de julio de 1998 (caso Valenzuela Contreras c. España); de 18 de febrero de 2003 (caso Prado Bugallo c. España) y de 30 de mayo de 2017 (caso Trabajo Rueda c. España), al tiempo que se estudia, asimismo, el estándar europeo exigido respecto de las obligaciones que ha de cumplir el legislador (obligaciones positivas) a partir de la importante STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía).

A continuación se procede al examen de la "calidad de la ley" española en la materia, la cual viene constituida fundamentalmente por el art. 20.3 y 20 bis del ET, la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y la legislación complementaria en la materia al objeto de evaluar su suficiencia con respecto al *standard* establecido al efecto por el Convenio Europeo de Derechos Humanos y la jurisprudencia del TEDH previamente analizados. De igual modo, se analizan los Informes emitidos por la AEPD, si bien se ha de hacer constar que éstos no tienen la consideración de norma jurídica, siendo su valor el de

constituir fórmulas orientativas e interpretadoras de la normativa española de protección de datos personales.

4. En el Capítulo III se aborda la hipotética necesidad de autorización judicial para proceder al conocimiento del contenido del correo electrónico del trabajador para, seguidamente, en el Capítulo IV analizar la necesidad de información previa – concreta y específica- al trabajador en orden a poder vigilar y controlar el cumplimiento de la actividad laboral mediante cámaras de video vigilancia y/o controlar el correo electrónico corporativo de la empresa, analizándose, entre otras, las SSTC 29/2013, de 11 de febrero (caso "Universidad de Sevilla", deber de información previa al trabajador) y la más reciente 39/2016, de 3 de marzo (caso "Bershka", debilitamiento del deber de información previa al trabajador).

5. Por último, el Capítulo V de la Tesis está dedicado a estudiar la proporcionalidad requerida para la instalación de cámaras de video vigilancia en el centro de trabajo y/o poder proceder al control del correo electrónico del trabajador, a cuyo efecto se hace un recorrido por la jurisprudencia tanto europea como constitucional y del Tribunal Supremo para, finalmente, extraer las Conclusiones pertinentes derivadas de este estudio.

6. Queremos, para terminar, señalar que en la presente obra se analiza de forma conjunta tanto el control del correo electrónico como los *chats* o servicios de mensajería instantánea y la navegación por Internet dado que, aunque se advierten algunas diferencias fácticas entre las dos primeras (en las que hay un proceso de comunicación) y la tercera (donde no lo hay), sin embargo, la problemática generada por las mismas es común y las sentencias recaídas sobre los tres temas forman parte de una única línea jurisprudencial.

CAPÍTULO I.- EL CONCURSO DE DERECHOS FUNDAMENTALES EN EL ÁMBITO LABORAL.

1. Tanto en los supuestos de video vigilancia empresarial como de control del uso del ordenador y del correo electrónico por parte del empresario pueden vulnerarse derechos fundamentales del trabajador generándose, en ocasiones, un concurso entre los derechos reconocidos en el art. 18 CE: derecho a la intimidad personal y familiar (art. 18.1); derecho al secreto de las comunicaciones (art. 18.3) y derecho a la protección de datos personales (art. 18.4), lo cual obliga a individualizar las diversas eventualidades en las que puede producirse dicha vulneración de derechos fundamentales con motivo de la instalación en la empresa de cámaras de video vigilancia o del acceso por parte del empresario a los datos almacenados en el ordenador del trabajador, para cuyo análisis nos basaremos en los diferentes pronunciamientos judiciales que, en el orden interno, han dictado tanto el Tribunal Supremo como el Tribunal Constitucional como, a nivel europeo, el Tribunal Europeo de Derechos Humanos.

1.- El derecho a la intimidad.

1.1.- Instalación de sistemas audiovisuales de control y sus implicaciones con respecto a la intimidad del trabajador.

1. El análisis de la intimidad en el seno de las relaciones laborales ha de partir de un hecho evidente, cual es que la Constitución no se detiene a las puertas de la empresa habida cuenta de que los derechos fundamentales no pueden ser ignorados por el clausulado de un contrato de trabajo[74], ejerciendo los derechos fundamentales en el ámbito de la relación laboral una función

74 STC 88/1985, de 19 de julio.

equilibradora entre trabajador y empresario[75] dada la evidente asimetría de dicha relación[76], pudiendo quedar damnificado el derecho a la intimidad en numerosas ocasiones y momentos que se producen en los centros de trabajo como, por ejemplo, con motivo de la instalación de instrumentos de audición o de un circuito cerrado de televisión[77] o con ocasión de la puesta en marcha de cámaras de control de acceso al lugar de trabajo[78] o mediante el control del correo electrónico[79], etc., siendo así que los derechos fundamentales del trabajador adquieren especial relevancia en un ámbito como el laboral en el que el poder de dirección del empresario puede entrar en colisión con aquéllos.

En efecto, de conformidad con lo dispuesto en el art. 20.3 ET *"el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana..."* y, de acuerdo con el art. 20 bis ET, *"los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales"*, siendo evidente que la implementación de tales medidas por parte del empleador no puede hacerse ignorando que la otra parte del contrato de trabajo también es titular de derechos fundamentales[80], de forma que la eficacia de éstos en las relaciones

75 STC 129/1989, de 17 de julio.

76 MIERES MIERES, L. J., "La protección constitucional de los derechos a la intimidad y a la propia imagen en las relaciones laborales: una visión desde la jurisprudencia constitucional", *RVAP*, núm. 99-100 (Especial "Demetrio Loperena Rota, *In memoriam*), mayo - diciembre, 2014, pág. 2085.

77 STC 186/2000, de 10 de julio.

78 STC 29/2013, de 11 de febrero.

79 STC 241/2012, de 17 de diciembre.

80 Como señala la jurisprudencia del Tribunal Constitucional, *"el empresario no se encuentra apoderado para llevar a cabo, bajo el pretexto de las facultades de vigilancia y control que la legislación le asigna, intromisiones ilegítimas en la intimidad de sus trabajadores en la empresa"* (STC 186/2000, de 10 de julio).

jurídicas *inter privatos* proyecta sobre el contrato de trabajo un elemento heterónomo que opera de forma prevalente sobre las obligaciones contraídas por las partes haciendo que la empresa no sea una fortaleza inexpugnable frente a los valores y derechos constitucionales[81], de modo que el extraordinario avance que supone el progreso de las nuevas tecnologías no puede convertirse en un factor de categorización social[82]. Como de forma ilustrativa lo recuerda la jurisprudencia constitucional, las manifestaciones de feudalismo industrial repugnan al Estado social y democrático de derecho[83].

2. No obstante este *obiter dictum* tan significativo, una primera jurisprudencia constitucional consideraba el contrato de trabajo y las obligaciones dimanantes del mismo como elemento clave de la delimitación del derecho fundamental en la medida en que el trabajador ha dado su consentimiento[84], de manera que determinadas manifestaciones del derecho a la intimidad podían quedar desprotegidas en el ámbito laboral[85].

En efecto, durante mucho tiempo los tribunales admitieron la utilización de medidas de control empresarial de índole tecnológico con muy pocas

81 CARRILLO LÓPEZ, M., "Los ámbitos del derecho a la intimidad en la sociedad", *en El derecho a la privacidad en un nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pág. 41.

82 MACAVILCA ROMÁN, Z., "El derecho a la intimidad y las nuevas tecnologías. El derecho a la intimidad en el contexto de las nuevas tecnologías de comunicación e información", en *El derecho a la intimidad. Nuevos y viejos debates,* Dykinson, Madrid, 2017, págs. 181-183.

83 STC 88/1985, de 19 de julio, FJ 5.

84 STC 6/1988, de 21 de enero, FJ 3.

85 SSTC 19/1985, de 13 de febrero y 170/1987, de 30 de octubre -caso del camarero con barba-. No obstante, el punto de inflexión a esta doctrina restrictiva lo supuso la STC 99/1994, de 11 de abril (caso del cortador de jamón), en la que ante las restricciones establecidas por el empresario al ejercicio de un derecho de la personalidad, como era el derecho a la propia imagen, el TC obligó a aplicar el triple test de idoneidad, necesidad y proporcionalidad a la medida restrictiva con el objeto de determinar si la misma estaba plenamente justificada y si las modulaciones ejercidas sobre el derecho fundamental del trabajador eran las estrictamente necesarias.

reservas[86] bajo el entendimiento de que el centro de trabajo constituía un lugar público en donde no existía proyección del derecho de intimidad, salvo los espacios destinados al descanso y al aseo personal[87]. A tal efecto, la STC 142/1993, de 22 de abril, llegó a señalar que la relación de la intimidad con la dignidad personal determina que la esfera de la inviolabilidad de la persona frente a injerencias externas no comprenda, en principio, los hechos relativos a las relaciones sociales y profesionales en que se desenvuelve la prestación laboral.

De acuerdo con este razonamiento, la protección de la intimidad queda sujeta a un criterio meramente espacial regido por una teoría contractualista[88] según la cual los derechos fundamentales del trabajador ceden frente al poder de dirección del empresario dado que la formalización del contrato laboral mitiga la posibilidad de su aplicación en tiempo y lugar de trabajo[89] (STC 142/1993, de 22 de abril).

A pesar de estos precedentes, hoy superados, la realidad indica que en el contexto de las relaciones laborales se presenta la disyuntiva entre el poder de dirección del empleador (art. 20.3 ET) y los derechos fundamentales de los trabajadores, no siendo siempre pacífica la relación entre ambos grupos de

86 MIERES MIERES, L. J., *Intimidad personal y familiar. Prontuario de jurisprudencia constitucional*, Aranzadi, Navarra, 2002, pág.23.

87 GUERRA RODRÍGUEZ, L., "Ejercicio del poder de control a través de cámaras de video vigilancia: análisis de la doctrina constitucional", *Trabajo y Derecho* 29/2017 (mayo), nº 29 de 1 de mayo de 2017, pág. 2.

88 FABREGAT MONFORT, G., "El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave", *Trabajo y Derecho*, nº 5, 2015, pág. 2.

89 En línea con lo establecido en la STC 142/1993, de 22 de abril , la STSJ de Cataluña de 25 de abril de 1994 admite la instalación de un circuito cerrado de televisión con sistema de grabación de imagen y sonido en múltiples espacios del centro de trabajo tras considerar que entender que la medida vulnera el derecho a la intimidad *"(...) supondría extender la protección de tales derechos a instalaciones que suponen la práctica totalidad de espacios públicos del hotel en el que éste presta sus servicios a los clientes y, en consecuencia, donde los trabajadores desarrollan su actividad. La intimidad de éstos no resulta agredida por el solo hecho de que ésta sea objeto de filmación pues no se trata de divulgar su conducta, sino de obtener un conocimiento de cuál es su comportamiento laboral".* En el mismo sentido se pronuncia la STSJ de Galicia de 25 de enero de 1996.

derechos, sino que suelen producirse fricciones sobre todo cuando, derivado del uso de las nuevas tecnologías, se prima la potestad de dirección del primero en detrimento de los derechos fundamentales de los segundos, ofreciendo a tal efecto la jurisprudencia, tanto constitucional como ordinaria[90], numerosos ejemplos en los que se debate la proporcionalidad de la instalación de medidas de control en las empresas.

En este sentido, no hay duda alguna de que atentan contra la intimidad de los trabajadores los circuitos internos de televisión a cuyo través se accede visualmente a los vestuarios del centro de trabajo. Como tampoco, en sentido contrario, la hay respecto de la proporcionalidad de idéntica medida si el sistema de visualización queda circunscrita a las zonas de compra de productos y de pago en las cajas de un supermercado[91].

No obstante, tanto en uno como en otro caso, algunos tribunales ordinarios han continuado entendiendo que en el centro de trabajo no se ejerce el derecho a la intimidad dado que el mismo se ciñe o circunscribe a un conjunto de actividades privadas que, por esencia, permanecen al margen del centro de trabajo. E incluso el Tribunal Supremo en sentencias de 26 de septiembre de 2007 y 6 de octubre de 2011 ha auxiliado un amplio ejercicio de los poderes de control del empresario al que el Tribunal Constitucional se adhirió en la STC 241/2012, de 17 de diciembre (caso del correo electrónico en la empresa), sobre la que se incidirá de forma específica más adelante, pero ya resulta necesario adelantar la contradicción que supone con el precedente sentado con anterioridad en la STC 98/2000, de 10 de abril (caso micrófonos

90 Entre otras, STSJ de Madrid de 25/1/1996; STSJ de Murcia de 18/7/1995; STS de 1176/1990 (Sala IV); STSJ de Galicia, de 21/4/1995; STSJ de Cataluña, de 25/4/1994; STSJ de la Comunidad Valenciana, de 12/3/1993, etc.

91 CARRILLO LÓPEZ, M., "Los ámbitos del derecho a la intimidad…, *op. cit*., pág. 44.

en el casino de La Toja) en la que sostuvo que la libertad de comunicaciones viene protegida instrumentalmente a través del derecho a la intimidad[92].

3. La doctrina establecida en la referida STC 142/1993, de 22 de abril (los derechos fundamentales del trabajador ceden frente al poder de dirección del empleador), fue desautorizada posteriormente por nuestro Alto Tribunal a través de dos importantes sentencias: la 98/2000, de 10 de abril y la 186/2000, de 10 de julio, las cuales vinieron a establecer los principales criterios interpretativos en la materia, sufriendo los mismos posteriormente importantes correcciones, respecto de sus conclusiones, a través de las SSTC 29/2013, de 11 de febrero y, más recientemente, la 39/2016, de 3 de marzo. No obstante, debe advertirse que en las dos primeras el conflicto se plantea exclusivamente desde la perspectiva del derecho a la intimidad (art. 18.1 CE), quedando al margen del debate el derecho a la autodeterminación informativa que se integra en el derecho a la protección de datos personales que es, justamente, el que tuvo en cuenta la STC 29/2013, de 11 de febrero - que será objeto de análisis más adelante- y que definitivamente configura como eje de su jurisprudencia sobre la privacidad del trabajador el TEDH en su importante sentencia de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía).

4. En efecto, en la STC 98/2000, de 10 de abril[93], se rechazó el planteamiento consistente en exacerbar el poder de dirección del empresario mediante la delimitación precisa del alcance del derecho a no ser importunado en el ámbito de la actividad laboral. Esta sentencia traía su causa de la

92 JIMÉNEZ PÉREZ, A., "El derecho a la intimidad en la jurisprudencia constitucional y convencional: el Tribunal Constitucional Español, el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos", en *El derecho a la intimidad. Nuevos y viejos debates*, Dykinson, Madrid, 2017, págs. 103-104.

93 La STC 98/2000, de 10 de abril resuelve el supuesto de la utilización en un casino (Casino de la Toja, S.A.) de micrófonos en algunas dependencias del centro de trabajo (secciones de caja y ruleta francesa) donde se grababan las conversaciones de los trabajadores. La sentencia, estimatoria del recurso de amparo, reconoce la vulneración del derecho a la intimidad personal del trabajador recurrente, y no admite que la actuación empresarial tuviera, en el caso concreto, amparo en las facultades de vigilancia y control reconocidas al empresario por la legislación laboral (art. 20.3 ET).

instalación por parte del Casino de La Toja de diferentes micrófonos en determinadas zonas del centro de trabajo – zona de caja y ruleta francesa -. Un trabajador que ejercía de cajero y el Comité de Empresa demandaron a la empresa por intromisión ilegítima en su derecho a la intimidad. La sentencia, estimatoria del amparo solicitado, entendió que la medida adoptada por la empresa carecía de toda proporcionalidad para alcanzar la finalidad perseguida - cual era la de garantizar la seguridad del casino - y lesionaba, por tanto, la intimidad de los trabajadores cuyas conversaciones eran grabadas de forma permanente.

En esta sentencia se afirma que el derecho a la intimidad, en cuanto derivación que es de la dignidad personal consagrada en el art. 10 CE, supone, también en el ámbito de las relaciones de trabajo, la existencia de un ámbito propio y reservado frente al conocimiento de los demás, necesario, según las pautas de nuestro sistema cultural, para el mantenimiento de una calidad mínima de vida humana, de modo que el trabajador precisa disponer de una expectativa razonable de intimidad dado que, como señala la jurisprudencia del TEDH, en su interpretación del art. 8 CEDH, sería muy restrictivo constreñir la noción de vida privada a un círculo íntimo, de modo que el derecho a la vida privada engloba también el derecho de la persona a entablar y desarrollar relaciones sociales con otras personas[94] y, entre esas relaciones, deben incluirse – obviamente - las relaciones laborales, por lo que la captación de imágenes y sonidos no puede ser en ningún caso indiscriminada[95].

A este efecto, cabe señalar que el art. 7 de la LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad personal y Familiar y a la Propia Imagen, establece que tendrán la consideración de intromisiones ilegítimas : *“1) El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o*

94 STEDH de 16 de diciembre de 1992, caso Niemietz c. Alemania.

95 CARRILLO LÓPEZ, M., “Los ámbitos del derecho a la intimidad…, *op. cit.*, pág. 46.

reproducir la vida íntima de las personas; 2) La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción".

La formulación genérica de esta Ley requiere de la necesaria matización a la luz de la jurisprudencia constitucional, siendo la principal cuestión que cabe plantear la de si el empleador se encuentra legitimado para poder instalar aparatos de escucha en la empresa y si tal decisión conlleva inexorablemente una lesión del derecho a la intimidad del trabajador. Y la primera reflexión que hemos de efectuar al respecto es la de que el derecho a la intimidad de la persona no queda circunscrito espacialmente a su domicilio personal, sino que la empresa es también un escenario físico-espacial de carácter público en el que la persona comparte su actividad con otras, existiendo en la misma zonas en las que el derecho a no ser perturbado le sigue acompañando[96].

Como ha puesto de relieve el TC, la expectativa razonable de privacidad se relaciona con el derecho de la persona a mantener una "barrera de reserva"[97] en sus diversos ámbitos relacionales, incluido – obviamente – el laboral. Así, por ejemplo, forman parte de este ámbito privado el comedor, los vestuarios o las zonas de esparcimiento de la empresa, sin obviarse otros espacios en los que el derecho fundamental a la intimidad sigue vigente aunque se esté desempeñando una actividad laboral, siendo esta precisamente la razón por la que el Tribunal Constitucional rechaza la premisa, de la que parten algunas sentencias de la jurisdicción ordinaria, según la cual el centro de trabajo no es un espacio en el que se ejerza aquel derecho.

96 CARRILLO LÓPEZ, M., "Los ámbitos del derecho a la intimidad…, *op. cit,.* pág. 46.

97 SSTC 99/1994, de 11 de abril; 156/2001, de 2 de julio; 72/2007, de 16 de abril y 77/2009, de 23 de marzo.

5. De este modo, para la determinación de la procedencia de la instalación de sistemas de video vigilancia resulta necesario atender no sólo a las características del centro de trabajo, sino también a otros elementos causales, tales como el hecho de si la instalación del sistema ha sido o no indiscriminada[98] o si ha sido hecha de forma subrepticia[99] o cuál sea la finalidad realmente perseguida, si concurren razones objetivas de seguridad, etc. En suma, habrá que tener en consideración si la instalación de estos sistemas de video vigilancia y control responde a verdaderos criterios de proporcionalidad, dado que, si bien es cierto que son medidas que se insertan en el ámbito del poder directivo empresarial, no pueden, sin embargo, conducir a resultados inconstitucionales[100].

En el caso de la instalación de micrófonos en la zona de caja y ruleta francesa resulta evidente que la misma permite la captación y grabación de conversaciones que se producen en dichos lugares entre los trabajadores y clientes del casino y entre los propios trabajadores. Al margen de que razones de seguridad puedan justificar esta medida - la cual fue adoptada como complemento de otras ya existentes -, resulta obvio que, a través de la misma, es plenamente factible la captación y grabación de cualesquiera conversaciones mantenidas por los trabajadores a lo largo de su jornada laboral que poco o nada tengan que ver con su desempeño profesional y sí, sin embargo, con su intimidad, la cual es y debe de ser inaccesible a terceros.

6. Supuesto diferente es el que nos brinda la decisión de instalar cámaras para un circuito cerrado de televisión en las cajas registradoras del

98 Vid. STEDH de 9 de enero de 2018 (caso López Ribalda *et alii* c. España).

99 En este sentido cabe citar la STS de 13 de mayo de 2014 (Sala IV, Sección 1ª), que considera vulnerado el derecho a la intimidad de una trabajadora derivado de la utilización de cámaras de video vigilancia instaladas, como sistema disuasorio de hurtos por parte clientes, por causa de la falta de información sobre la posibilidad de supervisión laboral de las capturas de imágenes de los trabajadores y sin que por parte del empresario estuviesen previstos dispositivos anunciando su instalación y captación de imágenes, así como la notificación de la creación de ficheros a la AEPD.

100 CARRILLO LÓPEZ, M., "Los ámbitos del derecho a la intimidad…, *op. cit.*, pág. 47.

economato de un centro de trabajo ante la sospecha de irregularidades contables en la sección de textil y calzado (STC186/2000, de 10 de julio, caso de las cámaras en el economato de ENSIDESA). Esta sentencia resuelve el caso de un despido disciplinario en el que se imputa al trabajador la sustracción de dinero de la caja de dicho economato, habiendo utilizado la empresa para acreditar la conducta las grabaciones del sistema de video vigilancia que instaló para comprobar sus sospechas. Los Tribunales declararon la procedencia del despido no apreciando vulneración alguna del derecho a la intimidad del trabajador derivada de la instalación de las cámaras de vigilancia. El TC desestima el recurso de amparo considerando que, en el caso de autos, se respetó por la empresa el derecho a la intimidad del trabajador y que las pruebas video gráficas eran válidas, al tiempo que reitera la doctrina de la STC 98/2000, de 10 de julio, y fija como criterios a tener en cuenta los siguientes:

i) El derecho fundamental a la intimidad despliega toda su eficacia también en el seno de las relaciones jurídico laborales, si bien no se trata de un derecho ilimitado o absoluto, sino que el mismo puede ceder ante intereses constitucionales tal como sucede en los casos en que la modulación que aquél hubiere de experimentar se revelare como necesaria para la consecución del fin legítimo previsto, fuere proporcionada para alcanzarlo, así como respetuosa con el contenido esencial del derecho[101].

ii) El poder de dirección del empleador, contemplado en el art. 20.3 ET, atribuye a éste la facultad de adoptar medidas de control y vigilancia en orden a la verificación del cumplimiento por parte del trabajador de sus obligaciones laborales, respetando, eso sí, en todo momento la dignidad del trabajador (arts. 4.2.c) y 20.3 ET).

iii) El empresario carece de legitimidad para llevar a cabo intromisiones ilegítimas en la intimidad de sus trabajadores en el centro de trabajo bajo el

101 SSTC 57/1994, de 28 de febrero y 143/1994, de 9 de mayo.

pretexto de las citadas facultades de vigilancia y control previstas en el art. 20.3 ET.

1.2.- Control del ordenador y derechos fundamentales del trabajador.

1. El silencio legislativo imperante hasta diciembre de 2018[102] acerca de la cuestión del control del ordenador asignado al trabajador para el desarrollo de su prestación laboral ha dado lugar a un intenso debate hasta finales de la década pasada. Ante el silencio del legislador resultaban posibles diferentes aproximaciones doctrinales. De un lado, era posible pensar que el ordenador era estrictamente una herramienta de trabajo, de modo que había que reconocer una extensa facultad de control a favor del empresario en cuanto titular de los medios de producción. De otro lado, cabía pensar también que, aun siendo titularidad de la empresa, el ordenador es una herramienta peculiar en la medida en que puede contener datos privados del trabajador, de forma que no resulta posible reconocer tan extensas posibilidades de vigilancia de su contenido por cuanto ello puede suponer un sacrificio del derecho a la intimidad de éste, por lo que el control ha de quedar supeditado al cumplimiento de los requisitos materiales y formales establecidos en el art. 18 ET en orden al registro de los efectos personales del trabajador[103].

2. Desembocada la cuestión ante el Tribunal Supremo, éste procedió a unificar doctrina mediante la sentencia de 26 septiembre 2007. El TS se situó en un punto intermedio entre ambas tendencias reconociendo, en línea con la primera, que el ordenador se incluye entre los medios, propiedad de la empresa, que ésta pone a disposición del trabajador para que los utilice en el

102 Esta cuestión ha sido regulada por el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

103 GOERLICH PESET, J. Mª., "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas", en *El derecho a la privacidad en un nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pág. 144.

cumplimiento de su prestación de trabajo, de modo que ese uso cae bajo la órbita del poder de vigilancia y control del empresario, no aplicándose, por tanto, la regla especial del art. 18 ET, sino la general del art. 20.3 ET.

Ahora bien, dadas las dificultades de índole práctico en orden al establecimiento de una prohibición absoluta del uso personal del ordenador y de una cierta tolerancia acerca de un uso moderado de los medios de la empresa, aceptó, alineándose de este modo con la segunda, la existencia de una "expectativa general de confidencialidad" de los eventuales usos privados. La forma de equilibrar ambas ideas se encuentra en el tratamiento de esta expectativa, la cual no puede ser ignorada, pero tampoco erigirse en un impedimento permanente para el control del empresario. De hecho, éste resulta admisible en función de las instrucciones establecidas por éste para el uso del ordenador y de acuerdo con los controles que se hayan previstos para verificar esa utilización.

3. La evolución interpretativa posterior, tanto en la doctrina del TS como en la jurisprudencia constitucional, ha clarificado el alcance de esta doctrina. Y, al hacerlo, ha ampliado las facultades empresariales de control respecto de las que parecían deducirse literalmente del primer pronunciamiento, habiendo seguido esta ampliación diferentes líneas. En primer lugar, en relación con la contribución del trabajador a la generación de la expectativa general de confidencialidad, la STS de 26 de septiembre 2007 no parece condicionar su nacimiento a requerimientos especiales en la conducta del trabajador al señalar que no constituye obstáculo alguno para la protección de la intimidad el hecho de que el ordenador no tuviera clave de acceso ni que el mismo estuviera situado en un despacho sin llaves.

Sin embargo, la posterior STC 241/2012, de 17 de diciembre, valora para excluir la lesión del derecho fundamental, entre otras circunstancias, que las comunicaciones privadas se habían producido al haberse introducido el

programa en un soporte de uso común para todos los empleados de la empresa sin haberse observado la más mínima cautela al efecto.

Por otro lado, la STS de 26 de septiembre 2007 parece pensar en la existencia de un protocolo en cada empresa sobre el uso del ordenador afirmando, al respecto, que lo que ha de hacer el empresario, de acuerdo con las exigencias de la buena fe, es establecer con carácter previo las reglas de uso del mismo – estableciendo prohibiciones absolutas o parciales – e informar a los trabajadores tanto de que se va a proceder a controlar el uso del ordenador como de los medios que se van a utilizar a tal fin. Asimismo, la jurisprudencia social del TS parece pensar en un control limitado mediante monitorizaciones de carácter general, excluyéndose la vigilancia singularizada[104].

Sin embargo, la doctrina posterior ha permitido la prohibición absoluta del uso privado del ordenador, posibilitando un control empresarial completo de su utilización por parte del trabajador, habiendo sido esta la postura sostenida, primero por el TS en sentencia de 6 octubre 2011 y, más recientemente, por el TC en sentencia 170/2013, de 7 octubre[105], si bien esta posición ha quedado en entredicho a raíz de la STEDH de 5 de septiembre de 2017 en el caso Barbulescu c. Rumanía, que proscribe la reducción a cero del ejercicio de los derechos fundamentales del trabajador en el seno de la empresa[106].

En este punto hay que hacer notar que esta evolución ha supuesto una notable ampliación del ámbito al que se aplica la expectativa general de

104 STS de 8 marzo 2011.

105 GOERLICH PESET, J. Mª., "Protección de la privacidad de los trabajadores…", *op. cit.,* pág. 145.

106 Dice expresamente la STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía) que *"sea como fuere, las instrucciones de un empleador no pueden reducir la vida social privada del trabajador a cero. El respeto de la vida privada y de la confidencialidad de la correspondencia siguen existiendo aun cuando éstas pudieran estar restringidas en la medida de lo necesario".*

confidencialidad. Si bien los primeros pronunciamientos se referían al uso por el trabajador del ordenador y de Internet (aplicaciones utilizadas, eventuales archivos privados existentes en él y, sobre todo, secuencia de navegación en la Red tales como sitios visitados, tiempos de visita, etc.), posteriormente la jurisprudencia ha extendido esta categoría a supuestos en los que pudiera ser aplicable una protección constitucional más fuerte como es la derivada del secreto de las comunicaciones. Si históricamente el TS había aceptado la posible intercepción de las comunicaciones telefónicas en los casos en los que la prestación consistía precisamente en hacer o atender llamadas[107], en fecha más reciente se ha extendido la posibilidad de control empresarial a los programas de mensajería instantánea ubicados en ordenadores de la empresa[108] y a las direcciones corporativas de correo electrónico[109].

4. Los conflictos derivados del control, por parte del empresario, del uso de los ordenadores y el derecho a la intimidad de los trabajadores devienen del hecho de que aquéllos pueden ser usados tanto para cuestiones de índole estrictamente laboral como para temas personales, siendo este el punto del cual parte la STS (Sala IV) de 26 de septiembre de 2007 – fundamental en el tema que se analiza – que sostiene que dichos conflictos surgen dada la existencia de un uso personal – y no exclusivamente laboral – del medio facilitado por la empresa[110]. En relación con el correo electrónico cabe señalar que el derecho al secreto de las comunicaciones impide que el empresario

107 STS de 5 diciembre 2003.

108 STC 241/2012, de 17 de diciembre.

109 STS de 6 octubre 2011 y STC 170/2013, de 7 octubre.

110 Para VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*, Universidad Rey Juan Carlos, Madrid, 2011, pág. 81, los archivos derivados del uso laboral del ordenador de la empresa por parte del trabajador no forman parte del ámbito privativo de éste, en tanto que aquéllos otros vinculados al uso personal por parte de aquél sí caerían dentro de la categoría de privados y, por tanto, protegidos por el derecho a la intimidad.

Estamos en desacuerdo con esa apreciación dado que cualquier archivo es susceptible de contener información perteneciente al ámbito privativo del trabajador, de modo que la diferenciación vendría dada por el contenido de la información incluida en el archivo digital de que se trate.

pueda interceptar las comunicaciones que pudieran mantener los trabajadores entre sí, o con personas ajenas a la compañía, vía correo electrónico o chat[111].

5. No obstante, recientemente, el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, reconoce y regula el derecho a la intimidad de los trabajadores en la utilización de dispositivos digitales puestos a su disposición por el empleador autorizando al empresario a acceder al contenido de los dispositivos a los solos efectos de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de dichos dispositivos, debiendo las empresas establecer criterios de utilización de los mismos respetando los estándares mínimos de protección de la intimidad y con la participación de los representantes de los trabajadores.

Por su parte, el acceso a los dispositivos respecto de los que se hubiere admitido una utilización con fines privados requerirá de una precisa y concreta especificación de los usos autorizados y prohibidos, así como del establecimiento de garantías para la preservación de la intimidad, tales como la especificación de los períodos o momentos temporales en los que los dispositivos podrán ser usados para fines privados, debiendo informarse a los trabajadores de esos criterios de utilización.

6. Por lo que respecta a la navegación por Internet, la misma supone la entrada de datos en el ordenador los cuales quedan incorporados en éste pudiendo ser los mismos rastreados de forma que se puede conocer, bien sea

111 Para VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* págs. 82-83, si se trata de mensajes almacenados, ya lo fueran por el remitente como por el destinatario, si ya hubieran sido abiertos y leídos no operaría el derecho al secreto de las comunicaciones, de modo que en relación con los mismos cabría plantear si el acceso a su contenido afecta al derecho a la intimidad y la repuesta que cabe dar a este interrogante es que dependerá siempre del contenido de la comunicación, de modo que sólo los mensajes de correo electrónico cuyo contenido fuere de carácter personal y reservado podrían plantear problemas relativos al derecho a la intimidad.

en tiempo real o con posterioridad, la actividad desarrollada por el usuario del equipo en la Red.

Sobre el particular, el Documento aprobado el 29 de mayo de 2002 por el Grupo de trabajo del artículo 29 de la Directiva 95/46/CE contiene una serie de recomendaciones acerca del control del acceso a Internet en el seno de las organizaciones empresariales, desaconsejando prohibiciones absolutas de la utilización de la Red con fines personales por parte de los trabajadores, al tiempo que insiste en la necesidad de que el empresario informe a los trabajadores sobre las condiciones de uso de Internet y de los posibles sistemas de control que se pudieran establecer para controlar dicho uso.

Por su parte, el TEDH ha entendido que la utilización personal de Internet atañe a los conceptos de "vida privada" y "correspondencia" del artículo 8.1 del CEDH, de modo que la monitorización y/o control de la actividad del trabajador en la Red puede suponer una injerencia en los derechos contemplados en dicho precepto[112] toda vez que la información así obtenida puede albergar datos sensibles relativos a la intimidad de la persona por contener información referida a aspectos de su vida privada tales como su ideología, sus creencias religiosas, su orientación sexual, sus aficiones, etc.

En base a ello, la STS (Sala IV) de 26 de septiembre de 2007 encuadra dentro del concepto de intimidad las huellas derivadas de la navegación en Internet al señalar que esos archivos caen dentro del ámbito de protección de la intimidad, de modo que el acceso a los archivos temporales de Internet y, de modo genérico, a cualesquiera huellas derivadas de la navegación por la Red que queden incorporadas al equipo puede afectar a la intimidad del usuario y generar la ilicitud de las pruebas así obtenidas[113].

112 Vid. STEDH de 3 de abril de 2007 (caso Copland c. Reino Unido).

113 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 83.

7. En definitiva, lo determinante para evaluar si el acceso a un fichero informático puede suponer una afección del derecho a la intimidad es que el contenido del mismo pueda contener o no información perteneciente al "ámbito propio y reservado" del trabajador, a cuyo efecto existe una abundante jurisprudencia delimitadora de las materias que pueden afectar a dicho ámbito. Sin ánimo de exhaustividad, conforme a la jurisprudencia del TC, se puede considerar que afectan al derecho a la intimidad las intromisiones referidas, entre otras, a las siguientes materias[114]:

a) La intimidad corporal, la cual protege frente a intromisiones que pudieran llegar a constituir violación del recato o pudor de la persona[115].

b) Las informaciones referentes a la salud, tanto física como psíquica, de las personas[116].

c) Las informaciones relativas al consumo de drogas y/o alcohol[117].

d) Los datos afectantes a la situación económica de una persona[118].

e) Las informaciones sobre detalles concretos de la vida en el seno del hogar familiar[119], etc.

Como se ha dicho, no se trata de un elenco elaborado con ánimo de exhaustividad, sino de una simple exposición de hipótesis extraídas de casos decididos por el TC, lo cual permite la posibilidad de que otras tantas materias puedan quedar engullidas en el ámbito privativo de la persona y susceptible,

114 VEGAS TORRES, J., *Idem*, págs. 84-85.

115 SSTC 196/2004, de 15 de noviembre; 218/2002, de 25 de noviembre y 57/1994, de 28 de febrero, entre otras.

116 SSTC 159/2009, de 29 de junio y 70/2009, de 23 de marzo.

117 SSTC 206/2007, de 24 de septiembre; 196/2004, de 15 de noviembre y 207/1996, de 16 de diciembre.

118 SSTC 233/2005, de 26 de septiembre y 233/1999, de 16 de diciembre.

119 STC 115/2000, de 10 de mayo.

pues, de afectar al derecho a la intimidad de ésta dado que, como acertadamente señala Rodríguez Piñero y Bravo-Ferrer[120], una de las cuestiones problemáticas que plantea el derecho fundamental a la intimidad es su compleja determinación sustantiva habida cuenta de que el mismo abarca tanto espacios de la vida personal y familiar como cuestiones relativas a la sexualidad, a la dignidad, a la imagen, etc., de modo que la investigación del contenido almacenado en el ordenador del trabajador supondrá una vulneración de su derecho a la intimidad siempre que aquélla se refiera a materias comprendidas en el ámbito "propio y reservado" de aquél, por lo que la aportación a un proceso de dichos materiales probatorios plantearía serios problemas de ilicitud de los mismos.

1.2.1.- Existencia de expectativa razonable de privacidad.

1. El TEDH acota los supuestos en los que el acceso a datos privados puede constituir una intrusión en el derecho al respeto de la vida privada y familiar en función de que exista o no, en el caso concreto, de una "expectativa razonable de privacidad"[121].

Así, en su sentencia de 5 de junio de 1997 (caso Halford c. Reino Unido) el tribunal rechaza la argumentación del Gobierno británico relativa al hecho de que el empresario tuviera derecho a controlar, sin necesidad de advertencia previa, las llamadas telefónicas realizadas por sus trabajadores con el teléfono de la empresa, sosteniendo que, por el contrario, conforme a su reiterada jurisprudencia, resulta evidente que las llamadas telefónicas realizadas desde la oficina – lo mismo que las efectuadas desde el domicilio particular - caen dentro del concepto de "vida privada" y "correspondencia" del art. 8.1 del CEDH, sosteniendo el tribunal que no hay constancia alguna acerca de que se

120 RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., "Derecho a la intimidad del trabajador y contrato de trabajo", en *Diario La Ley*, núm. 6033, de 4 de junio de 2004.

121 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.*, pág. 97.

hubiere advertido a la funcionaria demandante sobre el hecho de que las llamadas realizadas desde los terminales de su despacho oficial pudieran ser objeto de intervención, siendo así que el tribunal entiende que la funcionaria gozaba de una "expectativa razonable de privacidad" respecto de las mismas, la cual se veía incluso reforzada por factores coadyuvantes tales como su elevado rango, que determinaba que pudiera disfrutar de un despacho propio con dos teléfonos, uno de los cuales era para uso privado y, por lo demás, sus superiores jerárquicos habían autorizado de modo expreso que utilizara los teléfonos de su despacho para el mantenimiento de conversaciones relacionadas con la reclamación por discriminación efectuada por ella y con motivo de la cual se produjeron las interceptaciones[122].

Por su parte, en el caso Copland c. Reino Unido (sentencia de 3 de abril de 2007) se resuelve un caso en el que las llamadas telefónicas, así como el correo electrónico y la navegación por la Red de una empleada de un *College* público habían sido controladas por un superior jerárquico, aplicando de nuevo el TEDH el denominado test de la "expectativa razonable de privacidad" en orden a la determinación de si los hechos enjuiciados quedaban o no englobados en el ámbito de aplicación del art. 8 CEDH, a cuyo efecto el tribunal sostiene que su doctrina jurisprudencial referida a las llamadas telefónicas efectuadas desde el lugar de trabajo resulta también de aplicación tanto al uso del correo electrónico de la empresa como a la información derivada del control del uso personal de la Red por quedar ambos comprendidos en la noción de "vida privada" y "correspondencia" del art. 8.1 del CEDH. Y, dicho esto, el tribunal constata que, además, no se advirtió de modo expreso a la demandante acerca de que sus llamadas podían ser objeto de monitorización, de modo que la trabajadora gozó, en todo momento, de una expectativa razonable de privacidad respecto de las llamadas efectuadas desde los

122 VEGAS TORRES, J., *Idem., Ibidem.*

terminales del lugar de trabajo, la cual es extensible también al uso del correo electrónico y a la navegación por Internet[123].

Asimismo, en el caso Peev c. Bulgaria (sentencia de 26 de julio de 2007[124] se vuelve a aplicar el test de la "expectativa razonable de privacidad" para alcanzar la conclusión de que el registro efectuado había defraudado dicha expectativa de la cual gozaba el demandado, suponiendo, por tanto, aquélla una injerencia en los derechos del art. 8.1 del CEDH, argumentando a tal efecto el TEDH que en todo caso debe entenderse existente un acuerdo implícito en las relaciones empresario-trabajador que permite a estos últimos la posibilidad de tener objetos personales en los cajones de las mesas de trabajo y en los archivadores del despacho, asentándose en este acuerdo la expectativa razonable de privacidad que el tribunal reconoce al demandante, la cual determina que se considere que el registro realizado afecta a los derechos del art. 8.1 Convenio, si bien el tribunal admite, asimismo, la posibilidad de que el empresario pueda establecer políticas que prohíban o limiten la posibilidad de tener objetos personales por parte de los empleados en sus mesas y archivadores, lo cual podría excluir la expectativa razonable de privacidad de aquéllos en caso de incumplimiento de tales políticas[125].

2. En línea con lo establecido por la jurisprudencia del TEDH, el Tribunal Supremo en sentencia de 26 de septiembre de 2007 afronta el análisis de un caso sometido a su consideración relacionándolo con la existencia o no de una "expectativa de privacidad" del trabajador con respecto a los contenidos guardados en el ordenador de la empresa, sosteniendo que, en la medida en que se pudiera considerar existente dicha expectativa de privacidad, el acceso por parte del empresario a datos privados del trabajador podría suponer una

123 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.*, pág. 97.

124 El caso Peev c. Bulgaria analiza el caso de un empleado público cuyo despacho había sido registrado por orden de su superior en el marco de unas actuaciones de carácter disciplinario hallándose en dicho registro diferentes efectos de carácter personal del demandante tanto en los cajones del escritorio como en los archivadores.

125 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.*, págs. 98-99.

intromisión en su derecho fundamental a la intimidad, mientras que si, en función de las circunstancias del caso, no se pudiera afirmar que los trabajadores gozaran de una expectativa razonable de privacidad, el derecho a la intimidad de los mismos no podría considerarse afectado[126].

En este sentido, tanto la jurisprudencia del TEDH como del TC y del TS parten de la base de la existencia de una expectativa de privacidad relacionada con los contenidos personales que el empleado tuviere en el ordenador de la empresa. A este respecto, cabe referenciar las sentencias del TEDH relativas a los casos Halford y Copland c. Reino Unido que asumen que, a falta de advertencia expresa acerca del hecho de que tanto las conversaciones telefónicas como el uso personal del correo electrónico y la navegación por Internet realizados con los medios de la empresa pueden ser controlados, hay que entender latente una expectativa razonable de privacidad respecto del contenidos de tales comunicaciones.

En este orden de cosas, hay que recordar la sentencia del TEDH recaída en el caso Peev c. Bulgaria, la cual parte del hecho de que existe un acuerdo implícito, habitual en las relaciones de trabajo, que autoriza a los empleados a almacenar objetos de índole personal en las mesas y archivadores del puesto de trabajo del que deriva una expectativa de privacidad de aquéllos respecto de éstos[127].

Por su parte, el Tribunal Constitucional es determinante en rechazar los planteamientos tendentes a la exclusión de la existencia de cualquier expectativa razonable de privacidad en el ámbito de la empresa, siendo muy expresiva a este respecto la STC 98/2000, de 10 de abril, que rechaza de forma expresa el entendimiento de que el centro de trabajo no constituye un

126 VEGAS TORRES, J., *Idem.*, pág. 96.

127 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.*, pág. 101.

espacio en el que se pueda ejercer el derecho a la intimidad por parte de los empleados.

De igual modo, la referida STS (Sala 4ª) de 26 de septiembre de 2007 analiza de forma expresa el tema de la existencia de una expectativa de privacidad en relación con los datos de índole personal de los trabajadores guardados en el ordenador de la empresa, considerando que el derecho a la intimidad puede verse en entredicho por el acceso por parte del empresario a los siguientes tipos de archivos: i) correo electrónico; ii) archivos personales del trabajador almacenados en el ordenador, y iii) archivos temporales de Internet, así como las huellas de la navegación en la Red, partiendo dicha sentencia de la existencia de un hábito social de tolerancia respecto de determinados usos personales moderados de los medios informáticos facilitados por la empresa y que dicha tolerancia crea también una expectativa de confidencialidad en tales usos[128].

3. No obstante, al fijarse el fundamento de la protección constitucional y europea en la existencia de una expectativa de privacidad, se admite la posibilidad de que dicha protección pueda quedar desactivada cuando el acceso por parte del empleador a los datos de índole personal que contenga el ordenador del empleado no defraudare ninguna expectativa razonable de confidencialidad[129].

En este sentido, la STS de 26 de septiembre de 2007 alude a la posibilidad de que el empresario pueda limitar o modular la expectativa de confidencialidad a través del establecimiento de reglas concretas de uso de los dispositivos informáticos de la empresa que determinen si está permitido o no –

128 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.*, pág. 101.

129 En este sentido, cabe señalar la alusión en las SSTEDH en los casos Halford y Copland c. Reino Unido a la inexistencia de una advertencia previa de carácter expreso al trabajador acerca de que sus comunicaciones y el uso personal de Internet podían ser controlados.

y si no lo está, en qué medida no lo está - el uso privado y las medidas de control que aplicará al efecto, de modo que la existencia y el conocimiento de unas y otras por parte de los trabajadores podrían modular la expectativa de confidencialidad acerca del uso privado de las herramientas informáticas de la empresa, teniendo siempre como límite dichas reglas de uso la dignidad del trabajador, en cuanto fundamento de todos los derechos fundamentales de la persona, así como las prescripciones derivadas de la STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía) que, como se ha dicho, proscribe la reducción a cero del ejercicio de los derechos fundamentales en el seno del contrato de trabajo al establecer expresamente que las instrucciones de un empresario no pueden reducir de modo absoluto la vida social privada del trabajador, sino que el respeto de la vida privada y de la confidencialidad de la correspondencia siguen existiendo aun cuando éstas pudieran estar restringidas en la medida de lo necesario.

En resumen, con base en la doctrina formulada por la STS de 26 de septiembre de 2007 podemos afirmar que:

i) Lo verdaderamente importante de la doctrina que en ella se unifica no es la valoración conductual del trabajador a efectos disciplinarios, sino los límites del poder de control del empresario en relación al uso del ordenador facilitado por la compañía.

Concretamente, son dos los aspectos fundamentales sobre los que se pronuncia la sentencia unificadora de doctrina, a saber: (i) el empleador puede controlar el uso dado por el empleado al ordenador de la empresa, el cual no se regula por el art. 18 ET, sino por el art. 20.3 ET; y (ii) para que ese control sea lícito, el empresario habrá de concretar con carácter previo las reglas de uso del ordenador e informar a los trabajadores acerca de la existencia de

controles, así como de las medidas a aplicar en caso de incumplimiento de tales reglas[130].

ii) El acceso por parte del empleador a archivos personales contenidos en el ordenador del trabajador puede suponer una injerencia en el derecho a la intimidad de éste si, atendidas las circunstancias concretas del caso, el trabajador contara con una expectativa razonable de confidencialidad referida a esos archivos.

A tal efecto, el TS sostiene que la existencia de un hábito social generalizado de tolerancia respecto de ciertos usos personales de carácter moderado de los medios informáticos de la empresa genera para el trabajador una expectativa de confidencialidad en tales usos que no puede ser desconocida a la hora de llevar a cabo el control empresarial, aunque tampoco puede convertirse en un impedimento de tipo permanente para el control del empresario porque, aunque el trabajador tiene derecho a que se respete su intimidad, éste no puede pretender imponer ese respeto cuando utiliza un instrumento suministrado por la empresa en contra de las indicaciones dadas por ésta para su uso[131].

iii) De lo anterior extrae el TS una nueva conclusión señalando que lo que ha de hacer el empresario, de conformidad con las exigencias del principio de buena fe, es establecer con carácter previo las reglas de uso de los medios informáticos y de comunicación de la empresa e informar a los trabajadores de la posibilidad de que existan controles y de los medios que se aplicarán para comprobar la corrección de la utilización de los mismos. De esta forma, si los medios informáticos se utilizaren para usos privados, mediando prohibición

130 PONCE RODRÍGUEZ, S., "El poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador. Sentencia del Tribunal Supremo de 26 de septiembre de 2007", *Revista Actualidad Jurídica Uría Menéndez*, núm. 19, enero-abril 2008, pág. 68.

131 PONCE RODRÍGUEZ, S., *Idem., ibídem.*

concreta al efecto y conociendo el trabajador los controles que se aplicarán, no podrá concluirse que, al realizarse el control, se ha vulnerado una expectativa de intimidad.

iv) Asimismo, extiende el TS la garantía de la intimidad a los archivos temporales, que son copias que se almacenan automáticamente en el disco duro de las páginas web visitadas. En realidad se trata de huellas de la navegación por la Red y no de informaciones de índole personal, si bien el TS entiende que tales archivos también entran dentro de la protección de la intimidad[132]. Así lo establece, por lo demás, la sentencia de 3 de abril de 2007 del TEDH (caso Copland c. Reino Unido) cuando señala que está incluida en la protección del art. 8 del Convenio la información obtenida del seguimiento del uso personal de Internet dado que puede albergar datos sensibles que atenten contra la intimidad en la medida en que puede incorporar información reveladora de determinados aspectos de la vida privada tales como la ideología, las aficiones personales, la orientación sexual, etc.

v) Constituye una carga para el empresario el establecimiento de reglas de uso y control que sean conocidas expresamente por los trabajadores en el sentido de que, si no lo hiciere, no podrá obtener pruebas lícitas en orden a la defensa ante los tribunales de justicia de las medidas disciplinarias que pudiera adoptar.

Señalar que gran parte de esta doctrina ha sido acogida por el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

vi) Por último, aunque la sentencia de casación que comentamos otorgó en su momento una cierta seguridad jurídica respecto de algunos de los puntos

132 PONCE RODRÍGUEZ, S., "El poder de control empresarial sobre los medios informáticos…*op. cit.*, pág. 69.

controvertidos en torno al control del empleador, lo cierto es que también dejó sin respuesta determinados aspectos sobre la materia, siendo la principal cuestión no aclarada la relativa al derecho al secreto de las comunicaciones.

1.2.2.- El acceso a contenidos privados mediando consentimiento del trabajador afectado.

1. En caso de que el trabajador prestare su consentimiento para que el empleador accediere a contenidos referidos a su actividad informática que tuvieren un carácter privado, el derecho a la intimidad de aquél no resultaría afectado y la prueba así obtenida no podría ser tachada de ilícita.

Según reiterada jurisprudencia del TC, el derecho a la intimidad otorga una facultad de exclusión que impone a terceros un deber de abstenerse de realizar intromisiones salvo que las mismas estuvieren fundadas en una previsión legal con base constitucional y fueren proporcionadas o bien existiere un consentimiento eficaz que las autorizara, habida cuenta de que corresponde a cada persona el acotamiento del ámbito de su intimidad personal y familiar que preserva del conocimiento ajeno[133], de modo que el derecho a la intimidad resultará vulnerado cuando la injerencia en el ámbito reservado de la persona no fuere acorde con la ley, no fuese eficazmente consentida o, siendo la misma autorizada, subvirtiera el alcance para el que se otorgó el consentimiento[134].

Por tanto, para que el consentimiento del trabajador a cuya información privada se accediere excluya una hipotética lesión del derecho a la intimidad, el

133 SSTC 196/2004, de 15 de noviembre; 83/2002, de 22 de abril; 44/1999, de 5 de abril; 207/1996, de 16 de diciembre; 292/2000, de 30 de noviembre y 70/2002, de 3 de abril.

134 SSTC 70/2009, de 23 de marzo y 196/2004, de 15 de noviembre.

mismo habrá de reunir la cualidad de la eficacia[135], a lo que hay que unir el hecho de que la información personal así obtenida habrá de ser utilizada para la finalidad para la que se otorgó el consentimiento y no a otra diferente[136].

2. Respecto de la eficacia del consentimiento, la jurisprudencia del TC viene exigiendo que la persona ha de estar previamente informada del alcance y consecuencias de su consentimiento[137], afirmando la STC 196/2004, de 15 de noviembre, que el sujeto afectado habrá de contar con una información adecuada para que el consentimiento sea un acto informado y pleno[138], a lo que hay que añadir el hecho de que el consentimiento se presta para fines concretos, los cuales habrán de ser explicitados en la información previa ofrecida al afectado[139], de modo que, teniendo presente la finalidad para la que se otorgó el mismo, el acceso a datos privados que nada tengan que ver con dicha finalidad no quedará cubierto por el consentimiento prestado por la persona vulnerándose, pues, el derecho a la intimidad.

De cuanto antecede se infiere que para que el acceso por parte del empresario a datos privados del trabajador que estuvieren contenidos en el ordenador de la empresa se considere cubierto por el consentimiento de éste

135 En relación a los mensajes automáticos en pantalla, se entiende que los mismos no suponen prestación del consentimiento: STSJ de Madrid de 21 de noviembre de 2001. En el caso enjuiciado por esta sentencia aparecía un mensaje en la pantalla del ordenador que rezaba lo siguiente: *"La utilización del presente sistema podrá ser objeto de supervisión y registro por razones administrativas o de seguridad. Todo usuario del presente sistema consiente expresamente tal supervisión"*.

136 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 113.

137 VEGAS TORRES, J., *Idem.,* pág. 114.

138 El caso analizado en esa sentencia versaba sobre un reconocimiento médico al que un trabajador se había sometido voluntariamente pero sin haber sido previamente informado de que se iba a analizar un hipotético consumo de estupefacientes. El TC otorgó amparo por considerar que se había vulnerado el derecho a la intimidad del trabajador por haberse invadido *"la esfera privada de la recurrente sin contar con habilitación legal para ello y sin consentimiento eficaz de la titular del derecho, actuando sin autorización sobre ámbitos que exigían una información expresa y previa al consentimiento"*.

139 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit*., pág. 114.

será necesario el concurso de los siguientes requisitos, a saber: i) información previa de carácter expreso al trabajador acerca del alcance y finalidad de la investigación empresarial a realizar; ii) prestación eficaz del consentimiento por parte del trabajador al carácter de la investigación, su alcance y finalidad; y iii) la investigación no podrá exceder del alcance referido, así como tampoco sus resultados podrán ser usados para una finalidad diferente de aquélla para la que el trabajador prestó su consentimiento[140].

Desde esta óptica, en caso de que el trabajador requiriese la intervención de técnicos para reparar deficiencias de funcionamiento del equipo informático del puesto de trabajo no cabrá entender que aquél prestó su consentimiento para acceder a datos pertenecientes al ámbito privado y personal que pudiese contener el equipo ni, mucho menos, a que si la intervención técnica de que se tratare desvelara que el ordenador contiene ese tipo de datos, se utilizaren los mismos con fines disciplinarios, siendo en este contexto en el que hay que situar la argumentación efectuada por la STS (Sala IV) de 26 de septiembre de 2007 excluyendo que la intervención en el ordenador del trabajador para eliminar un virus informático amparase el acceso a datos privados y la ulterior adopción de medidas de carácter disciplinario respecto de aquél.

3. Por lo demás, entendemos que el consentimiento dado por el trabajador a la investigación de su ordenador ha de ser expreso, habiendo de revestir el mismo la forma escrita[141] y estar basado en una información previa plena y veraz acerca del alcance y la finalidad de aquélla y no exceder la misma en ningún caso de dicho alcance ni desviarse de la finalidad referida. Si se cumplen estos requisitos, el consentimiento dado por el trabajador excluiría una hipotética lesión del derecho a la intimidad personal.

140 VEGAS TORRES, J., *Idem., ibídem.*

141 En sentido contrario, VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.*, pág. 116, que entiende que el consentimiento *"puede ser expreso o tácito sin estar sujeto el expreso a especiales requisitos de forma, pudiendo prestarse tanto por escrito como verbalmente"*.

No obstante, hemos de señalar que la STC 196/2004, de 15 de noviembre, establece que la Constitución no prescribe la forma escrita como requisito para la validez del consentimiento, añadiendo, por lo demás, que aquélla no excluye la eficacia del consentimiento verbal o la de la realización de actos concluyentes que manifiesten la voluntad del sujeto afectado, si bien la posterior STC 209/2007, de 24 de septiembre, determina que la falta de oposición, salvo en circunstancias excepcionales, no se considera suficiente para entender prestado eficazmente el consentimiento[142].

4. A la vista de cuanto antecede, la pregunta que hemos de hacernos es: ¿cabe la posibilidad de injerencias justificadas en la intimidad del trabajador en los supuestos de investigación del ordenador de la empresa?

De lo expuesto hasta ahora conviene señalar que resulta de dudosa legalidad que, en ausencia de instrucciones de uso y control de los medios informáticos comunicadas previamente a los trabajadores de modo expreso, pueda invocarse exitosamente la doctrina de la modulación de los derechos fundamentales para justificar hipotéticas injerencias en el derecho a la intimidad de los trabajadores por parte del empresario.

En este sentido, la doctrina jurisprudencial mayoritaria considera que en ningún caso están justificadas las injerencias en la intimidad de los empleados por parte del empresario, de modo que la única posibilidad de evitar que la investigación de los medios informáticos que la empresa pone a disposición del trabajador conduzca a una hipotética tacha de ilicitud de la prueba por vulnerar el derecho a la intimidad personal consistiría en la modulación del juego de este derecho fundamental mediante el establecimiento de reglas de uso y

142 La STC 209/2007, de 24 de septiembre, se refiere al consentimiento prestado para la entrada en el domicilio. No obstante, el criterio que manifiesta ha de entenderse, asimismo, aplicable al consentimiento dado para acceder a datos personales dada la existencia de una clara identidad de razón.

control de los mismos conocidas por los trabajadores[143]. Argumento que, por lo demás, se ve refrendado por la dicción del art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

A ello se ha de añadir que, en clave europea, el TEHD[144] ha señalado que se habrán de justificar expresamente los motivos para establecer medidas de vigilancia (por lo que entendemos que aquéllos habrán de ir más allá de la genérica alusión al poder de control del empresario del art. 20.3 ET), debiendo concretarse en motivos reales y precisos, estableciéndose la necesidad de información previa al trabajador acerca de la vigilancia de su correspondencia electrónica y otro tipo de comunicaciones, así como de la concreta puesta en marcha de las medidas de control, lo cual implica la necesidad de que dicha información haya de ser previa a la efectiva implantación de las medidas de vigilancia y ser, por lo demás, expresa y precisa *("the notification should normally be clear about the nature of the monitoring and be given in advance"*, dice expresamente la STEDH de 5 de septiembre de 2017, caso Barbulescu c. Rumanía*)*, adoptando el TEDH como referencia principal la normativa sobre protección de datos.

2.- El derecho a la vida privada en Europa: un contenido ampliado del derecho a la intimidad.

1. El art. 8 del CEDH consagra el derecho al respeto a la vida privada y familiar, al domicilio y a la correspondencia, presentando el mismo un contenido muy similar al de la Constitución española hasta el punto de defenderse que el concepto "vida privada" del Convenio equivale al de

143 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.*, pág. 117.

144 STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía).

"intimidad personal" del art. 18.1 CE[145] consistente en el derecho a poder establecer ciertas zonas protegidas frente a cualesquiera injerencias exteriores[146].

Tanto el CEDH como la CE ofrecen bastantes semejanzas en este punto concreto, pudiendo afirmarse que los derechos a la intimidad y al secreto de las comunicaciones reciben un tratamiento común[147] en ambos textos normativos en tanto que los bienes jurídicos protegidos por el art. 8 CEDH – vida privada, familia, domicilio y correspondencia- se encuentran íntimamente relacionados entre sí, sirviendo los mismos al objetivo común de garantizar una esfera autónoma de actuación y desarrollo personal[148].

2. No obstante, el TEDH ha renunciado a definir de modo cerrado el concepto "vida privada" incluyendo en su contenido garantías de la "autonomía personal" en sentido amplio, de modo que el art. 8 CEDH ofrece una protección bastante más extensa que la del estricto "derecho a la privacidad" para pasar a comprender la vida privada, la familia, la vida en el domicilio, la integridad física y moral, el honor y la reputación, el secreto de las comunicaciones, la no revelación de hechos irrelevantes o embarazosos, la protección de datos personales[149], etc.

145 SANTOLAYA MACHETTI, P., "El derecho a la vida privada y familiar (un contenido notablemente ampliado del derecho a la intimidad)", en en García Roca, J. y Santolaya Machetti, P. (coords.), *La Europa de los derechos. El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid 2005, pág. 430.

146 Warren, S. D. y Brandeis, L. D., "The Right to Privacy", *Harvard Law Review*, Vol. IV, December 15, 1890. Nº 5. Por su parte, la STC 73/1982, de 2 de diciembre, habla de *"un ámbito o reducto en el que se veda que otros penetren" y la STC 231/1988, de 2 de diciembre, de "un ámbito propio y reservado frente a la acción y conocimiento de los demás"*.

147 SANTOLAYA MACHETTI, P., "Derecho a la vida privada y familiar…", *op. cit.*, pág. 430.

148 ARZOZ SANTISTEBAN, X., "Derecho al respeto de la vida privada y familiar", en LASAGABASTER HERRARTE, I., *Convenio Europeo de Derechos Humanos. Comentario sistemático*, Thomson Civitas, Madrid, 2009, pág. 255.

149 Como pone de manifiesto GARCÍA VITORIA, I., "La protección de datos como eje de la jurisprudencia del Tribunal de Estrasburgo sobre la privacidad del trabajador y el control empresarial", en http://eapc-rcdp.blog.gencat.cat/2018/02/28/la-proteccion-de-datos-como-eje-de-la-jurisprudencia-del-tribunal-de-estasburgo-sobre-la-privacidad-del-trabajador-y-el-control-empresarial-ignacio-garcia-vitoria/, en la STEDH de 5 de septiembre de

3. Desde un punto de vista material existen bastantes parecidos en el tratamiento del derecho a la intimidad por parte del TEDH y el art. 18 CE, como sucede, por ejemplo, con el "concepto de domicilio" y las condiciones que debe reunir la orden judicial de entrada y el consentimiento del afectado[150], lo que incluye la sede de sus actividades profesionales y/o comerciales.

A este respecto razona el TEDH que el trabajo es el entorno en el que las personas articulan la mayoría de sus relaciones sociales; que la correspondencia profesional se encuentra también protegida[151]; que las llamadas efectuadas desde el lugar de trabajo están incluidas en la vida privada, de manera que para que sea posible un control del uso de las conversaciones, correos e Internet es preciso una expresa previsión legal y una finalidad legítima[152] y que el registro de llamadas realizadas es un dato personal protegido por el art. 8 CEDH (STEDH de 1 de marzo de 2007, caso Heglas c. Rep. Checa)"[153], por lo que se ha de ser consciente de que estamos ante dos ordenamientos que tienen una vigencia simultánea y complementaria, constituyéndose el ordenamiento europeo en una especie de subsistema dentro de los distintos ordenamientos de los Estados miembros[154] y operando

---

2017 (caso Barbulescu c. Rumanía) la Gran Sala parte del repaso de su dilatada y asentada jurisprudencia sobre la noción de "vida privada" recordando que dicho concepto debe ser interpretado de forma amplia no siendo el mismo susceptible de una definición exhaustiva y dejando claro que, en todo caso, la esfera de vida privada protegida en el art. 8 no se puede restringir al círculo más próximo de la persona ni excluir el mundo exterior, incluyéndose en el mismo las actividades profesionales de tal forma que restricciones que afecten a la vida profesional de una persona quedan protegidas por el art. 8 del Convenio "cuando repercuten sobre la manera en que el individuo forja su identidad social por el desarrollo de relaciones con otros sujetos", enfatizando que es en el ámbito de las relaciones de trabajo donde tales relaciones se dan en mayor medida.

150 SSTEDH de 9 de diciembre de 2004 (caso Van Rossem c. Bélgica) y de 28 de abril de 2005 (caso Buck c. Alemania).

151 SSTEDH de 16 de diciembre de 1992 (caso Niemietz c. Alemania) y de 24 de agosto de 1998 (caso Lambert c. Francia), entre otras.

152 STEDH de 3 de abril de 2007 (caso Copland c. Reino Unido).

153 SANTOLAYA MACHETTI, P., "El derecho a la vida privada y familiar…", *op. cit*., págs. 431-432.

154 FREIXES SANJUAN, Mª. T., "Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos", en *Los derechos en Europa* (Cood., GÓMEZ, SÁNCHEZ, Y.), UNED, Madrid, 1998, pág. 228.

el mismo tanto configurando contenidos que han de tener vigencia en cada uno de los ordenamientos jurídicos de los Estados miembros como interpretando el alcance general de todos los derechos, siendo el ordenamiento paneuropeo un estándar mínimo y genérico de reconocimiento y garantía para aquéllos[155], si bien, como señala el propio TEDH[156], el contenido del CEDH es también de aplicación directa dado que puede ocurrir que un derecho se encuentre reconocido por el Convenio y no por el derecho nacional, de modo que la invocación expresa de aquél es el único medio apropiado para plantear un asunto y que sea resuelto por los órganos europeos.

4. El CEDH utiliza, pues, el término vida privada en un sentido amplio y sustitutivo del derecho a la intimidad, de modo que el primer concepto es genérico estando constituido por un conjunto de derechos del individuo entre los que destaca la intimidad, que es la especie, e incluyendo en el concepto de vida privada las actividades profesionales y/o comerciales, así como las profesiones liberales, pues las tareas de un miembro de éstas pueden constituir un elemento de vida privada[157], siendo ello consecuencia de la deliberada pretensión del TEDH de no delimitar de forma exacta el derecho dado que se le reconoce un carácter expansivo y mudable, siendo el mismo el resultado de unas aspiraciones sociales que varían con el transcurso del tiempo e incluso de unos lugares a otros dentro de la propia Europa.

De este modo, la vida privada se articula en base a dos ámbitos: uno interno, referido al individuo, que afecta a su pensamiento, moralidad e integridad corporal, y otro externo, en el que se le atribuyen a la persona las mismas facultades que sobre sí mismo pero con referencia a los demás, y formando parte de ambos ámbitos los datos referidos a sus comunicaciones, la familia, su domicilio, sus relaciones personales y afectivas, la protección de sus

155 REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*…, *op. cit.*, pág. 223.

156 STEDH de 6 de noviembre de 1980 (caso Van Oosterwijck c. Bélgica).

157 STEDH de 16 de diciembre de 1992 (caso Niemietz c. Alemania).

datos personales, entre otros, siendo el sujeto soberano y poseedor del derecho a controlar todo lo referido a ambos ámbitos de la vida privada[158].

5. De lo manifestado se deduce con claridad cuál es el significado de vida privada en el ordenamiento jurídico europeo, si bien resulta sumamente difícil distinguirla de la intimidad. Sabemos que ésta última opera en un plano inferior, que su contenido es más restringido que el de vida privada y que se compone de un ámbito *ad intra* y de otro *ad extra*, pero sus límites se nos muestran muy difusos, pese a lo cual deducimos que *privacy* y vida privada se identifican en Europa.

La distinción con la intimidad proviene de la adopción por parte del TEDH de la teoría de las esferas o círculos concéntricos, según la cual existe una primera esfera o ámbito del individuo en el que se desenvuelve lo que él no quiere dar a conocer a los demás. Una segunda esfera o círculo lo constituyen aquellos aspectos que comparte en un ámbito algo más genérico, pero en sí reducido, como es la familia o amigos. Finalmente, el tercer círculo se compone de lo que la sociedad puede conocer del individuo o lo que éste quiere que conozcan de él en su relación social. Pues bien, el primer ámbito se identifica con la intimidad y los dos restantes con la vida privada, siendo el sujeto libre de establecer cuantos niveles desee, cabiendo la posibilidad de que en un sujeto determinado no existan prácticamente diferencias entre las distintas esferas. No obstante, pese a esta distinción, ni el CEDH ni el TEDH utilizan el concepto intimidad y sí el de vida privada.

6. En orden a la protección otorgada al derecho a la privacidad, tal como se deduce claramente de la jurisprudencia del TEDH, ésta no es absoluta sino que, en el contexto del empleo, su alcance último deriva, por un lado, del concepto de "expectativas razonables de privacidad" y, por otro, de la

158 REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*…, *op. cit.*, pág. 224

existencia de intereses legítimos "más relevantes", hasta el punto de que el TEDH a menudo descuida de forma notoria el aspecto normativo/objetivo del criterio “expectativas razonables”, lo que determina que, en la práctica, la privacidad del empleado en el trabajo quede dependiente en gran medida de los términos y condiciones de empleo acordados.

El principio de proporcionalidad, aunque presente en el sistema europeo de protección del derecho a la intimidad, en la mayoría de los casos se limita al análisis de la idoneidad y necesidad de las medidas invasivas en materia de privacidad, por lo que resulta necesario en el contexto laboral una consideración más cuidadosa por parte del tribunal de la proporcionalidad *stricto sensu* (equilibrio del daño) y, en particular, de los fines que deben inspirar el equilibrio de los derechos en competencia[159].

A este efecto, la sentencia del Tribunal de Estrasburgo de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía) determina que el control de proporcionalidad debe modularse en función de la intensidad del control empresarial, resultando determinante en este sentido la necesidad de valorar si se accede al contenido de los mensajes, así como determinar la amplitud de las comunicaciones sometidas a vigilancia, la duración del control o el número de personas que tienen acceso a los resultados. En este aspecto, los controles que supongan un acceso por parte del empresario al contenido de las comunicaciones deberán ser sometidos a un control de proporcionalidad más intenso.

159 OTTO, M., *The right to privacy in employment. A comparative analysis*, Hart Publishing, Bloomsbury, 2016, págs. 118-119.

2.1.- La sucesiva ampliación del contenido del derecho a la vida privada en el CEDH: de Halford a Libert.

1. El art. 8 CEDH tiene como objetivo específico la regulación de la vida privada al señalar en su apartado primero que *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia..."* y establecer en el apartado segundo las excepciones a la vigencia del derecho, que se concretan en las siguientes: que la injerencia *"esté prevista por ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás"*.

En base al art. 8 CEDH, el TEDH ha establecido una clara distinción entre intimidad y vida privada, otorgándole a este último concepto una significación más amplia que al primero, de forma que aquél ha venido ampliando paulatinamente el contenido del concepto vida privada a ámbitos tales como la vida sexual, la familia, el domicilio, la integridad psíquica y moral, las comunicaciones y la protección de datos, entre los más significativos. El presente apartado pretende ser, pues, una aproximación al núcleo del derecho a la vida privada a través del reconocimiento de sus diversas manifestaciones que ampara la legislación y la interpretación que de ella realiza el TEDH.

Si bien nuestro ordenamiento jurídico reconoce la intimidad personal como una de las manifestaciones esenciales de la intimidad (art. 18.1 CE y Ley Orgánica 1/1982, de 5 de mayo), por contra el CEDH no hace una delimitación normativa expresa de la misma, aunque su máximo intérprete - el TEDH – incluye en ella de forma concreta algunos ámbitos entre los que destacan la

vida sexual, en cuanto manifestación que es de la vida privada del ser humano[160], y la integridad psíquica y moral[161], entre otros.

2. Por lo que hace referencia a la doctrina del TEDH en la materia, señalar, como ya quedó dicho en la Introducción, que la misma es muy extensa, existiendo diferentes pronunciamientos en torno al derecho a la intimidad personal y, más concretamente, en relación al control por parte del empleador del uso de los equipos informáticos en el ámbito laboral, si bien con las recientes sentencias en los casos Barbulescu c. Rumanía y López Ribalda *et alii* c. España se da respuesta final a la cuestión reafirmando el Tribunal su jurisprudencia anterior (casos Halford y Copland c. Reino Unido y Köpke c. Alemania) favorable a una interpretación extensiva de la noción de "vida privada" y de los derechos de los trabajadores.

En orden a un mejor análisis dividiremos la exposición en dos apartados comprensivos de la evolución de la jurisprudencia del TEDH en torno a la ampliación del concepto de vida privada.

2.1.1.- La primera doctrina del TEDH: los casos Halford y Copland c. Reino Unido y Köpke c. Alemania.

1. La doctrina anterior a los casos Barbulescu c. Rumanía y López Ribalda *et alii* c. España, favorable a una interpretación benefactora derivada de una interpretación amplia del art. 8 CEDH, se fundamenta en el criterio de la "expectativa razonable de intimidad o confidencialidad", apareciendo el mismo en los pronunciamientos más importantes del TEDH, tales como las SSTEDH de 25 de junio de 1997 (caso Halford c. Reino Unido) y de 3 de abril de 2007 (caso Copland c. Reino Unido) y en la decisión de inadmisibilidad –sección

160 STEDH de 22 de octubre de 1981 (caso Dudgeon c. Reino Unido).

161 STEDH de 26 de marzo de 1985 (caso X e Y c. Países Bajos).

quinta - de fecha 5 de octubre de 2010 (caso Köpke c. Alemania). Los tres casos versan sobre la licitud de los controles efectuados por el empresario en relación con el obligado respecto del art. 8 CEDH.

2. Fue en 1997, en la STEDH de 27 de mayo de ese año (caso Halford c. Reino Unido)[162], cuando se amplió el concepto de vida privada al tiempo que se restringieron en gran medida las excepciones de injerencia contenidas en el apartado segundo del art. 8 CEDH, incluyéndose de este modo en el concepto de vida privada las comunicaciones realizadas desde el lugar de trabajo o desde cualquier otro lugar, sea éste público o privado, y condenándose al Reino Unido por no haber establecido los mecanismos necesarios que posibilitaran la limitación de la actividad de la policía en sus investigaciones (obligación negativa).

No obstante, lo significativo del caso no es tanto la delimitación de las comunicaciones privadas, sino la interpretación restrictiva que se realiza del concepto "necesario en una sociedad democrática", quedando sentado con ello el carácter expansivo del apartado primero del art. 8 CEDH y el carácter restrictivo en su cumplimiento e interpretación del apartado segundo del mismo artículo. En idéntico sentido, el TEDH en sentencia de fecha 25 de marzo de 1998 (caso Kopp c. Suiza) ratifica esta jurisprudencia y entiende como violación del secreto de las comunicaciones la interceptación por parte de la policía suiza de las comunicaciones en el despacho de un abogado[163].

162 El caso Halford c. Reino Unido versa sobre la interceptación de llamadas telefónicas en despacho profesional y en domicilio particular, entendiendo el TEDH que las conversaciones telefónicas procedentes de locales profesionales y del domicilio quedan comprendidas en las nociones de vida familiar y de correspondencia del art. 8.1 CEDH, máxime cuando en el caso concreto no existe ninguna prueba de que se hubiese avisado a la señora Halford, como usuaria de la red interna de telecomunicaciones puesta en marcha en las oficinas de la policía de Merseyside, de que las llamadas entrantes en el sistema podían ser interceptadas, de manera que el TEDH considera que se podía considerar de forma razonable este tipo de llamadas como de carácter privado, por lo que el art. 8 CEDH es aplicable a las denuncias que se refieren a los teléfonos del domicilio y del despacho.

163 En el Caso Haldimann c. Suiza 2015, respecto al lugar de la grabación (párrafo 60), el TEDH también señala que la entrevista no se llevó a cabo en las oficinas del agente u otras dependencias de su trabajo, espacios que sí podrían estar protegidos especialmente como susceptibles de razonables conversaciones confidenciales; y cita varias de sus

3. Asimismo, en el caso Copland c. Reino Unido[164] el TEDH vuelve a considerar que los trabajadores conservan en todo momento su derecho a la intimidad personal en el seno de la empresa incluso cuando los dispositivos informáticos pertenecieren a ésta y se utilizaren durante el tiempo de trabajo, sosteniendo a tal efecto el Tribunal que las llamadas telefónicas que deriven o procedan del ámbito laboral caen dentro del concepto de "vida privada" y "correspondencia" a los efectos del art. 8.1 del Convenio, haciéndose extensible esta protección a los correos electrónicos[165] enviados desde el lugar de trabajo, así como a toda información derivada del seguimiento de la navegación por la Red, de modo que el carácter privado prevalece al no haber sido advertida la trabajadora acerca de que sus llamadas podían ser controladas, de modo que podía razonablemente confiar en el carácter privado de sus comunicaciones[166].

No obstante, el Tribunal no descarta la posibilidad de que puedan realizarse determinados controles "necesarios en una sociedad democrática" y,

STEDH como caso Chappell c. Reino Unido, de 30 de marzo de 1989 o caso Niemetz c. Alemania, de 16 de diciembre de 1992, entre otras.

164 Seguimiento hecho por un *College* público británico de llamadas telefónicas, visitas a Internet y correo electrónico de una profesora.

165 Asimismo, el Documento de Trabajo del "Grupo del Artículo 29", de 29 de mayo de 2002, relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo, entiende que los mensajes electrónicos deben poder beneficiarse de la misma protección que el "correo tradicional", sosteniendo que las comunicaciones electrónicas que procedan de locales profesionales se encuentran amparadas por los conceptos de "vida privada" y de "correspondencia" (según lo dispuesto en el art. 8.1 CEDH).

Cuando el trabajador recibe una cuenta de correo electrónico para uso estrictamente personal, la apertura por el empleador de los mensajes electrónicos de esta cuenta sólo podrá justificarse en circunstancias muy limitadas habida cuenta de que el acceso a este tipo de datos no es necesario para la satisfacción de un interés legítimo del empleador. En este caso, prevalecerá siempre el derecho fundamental al secreto de la correspondencia.

En consecuencia, la cuestión de en qué medida el artículo 7.f) de la Directiva (derogada por el Reglamento de Protección de Datos) autoriza el control del correo electrónico dependerá de la aplicación, caso por caso, de los principios generales sobre protección de datos, sopesando no solo los intereses de las partes, sino también el respeto de la vida privada de las personas ajenas a la organización afectadas por la actividad de vigilancia.

166 No obstante, en ambos supuestos (casos Halford y Copland c. Reino Unido) se estaba analizando no tanto el ámbito de privacidad laboral, sino más bien los límites de los poderes públicos a efectos de injerirse en la vida privada de funcionarios (art. 8.2 CEDH).

por tanto, lícitos, sobre la utilización que pudieran hacer los empleados del correo electrónico o de Internet en el seno de la empresa, si bien las injerencias en el derecho sólo se encontrarían amparadas si se realizaren mediando el consentimiento expreso del titular o si las mismas estuvieran contempladas de forma precisa en la ley, ya que sólo así se cumpliría con la exigencia de previsibilidad y los ciudadanos podrían conocer con suficiente claridad las condiciones de la limitación[167].

Lo novedoso en el caso Copland c. Reino Unido es que el TEDH establece la necesidad de que la empresa haya establecido reglas de utilización de los medios tecnológicos en orden a poder eliminar cualquier expectativa de intimidad que pudiera tener el trabajador, de modo que para el Tribunal la expectativa de intimidad sólo desaparece si la empresa advierte de la posible fiscalización. De la sentencia cabe resaltar, pues, que se reconoce la legitimación empresarial en el control informático, pero a su vez el deber de informar al trabajador para poder eliminar la expectativa de confidencialidad.

4. Por su parte, en el caso Köpke c. Alemania[168] el TEDH sostiene que la video vigilancia encubierta de un trabajador en el lugar de trabajo sin motivo alguno debe considerarse una intrusión en la vida privada de éste, si bien la misma estaría justificada siempre que fuese una respuesta a una situación ilícita, previamente detectada, al objeto de lograr su comprobación y que la misma no se efectúe de manera indiscriminada, sino que deberá circunscribirse a un momento temporal y espacial concreto y determinado.

167 LÓPEZ DE LA FUENTE, G., "La doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos sobre el control de las comunicaciones electrónicas en el trabajo: ¿el fin de una eterna cuestión?", *Revista de Estudios Europeos*, nº 69, enero-junio 2017, pág. 8.

168 El caso Köpke c. Alemania analiza el supuesto de un empresario que procede a llevar a cabo una vigilancia encubierta de los trabajadores mediante un sistema de video vigilancia con la ayuda de una agencia de detectives, fruto de la cual es despedida por robo la actora sin previo aviso.

2.1.2.- La doctrina reciente del TEDH: los casos Barbulescu c. Rumanía; Antovic y Mirkovic c. Montenegro; López Ribalda *et alii* c. España; y Libert c. Francia.

1. Las recientes sentencias del TEDH de 5 de septiembre de 2017, Gran Sala, (caso Barbulescu c. Rumanía)[169] y de su Sección 3ª, de 9 de enero de 2018, (caso López Ribalda *et alii* c. España I)[170] y de Gran Sala de fecha 17 de octubre de 2019 (López Ribalda II) han sentado una doctrina de gran relevancia que va a tener importantes consecuencias para la teoría de los derechos fundamentales de los trabajadores en el marco del contrato de trabajo, al tiempo que han provocado múltiples reacciones dada la importante cuestión que aborda y que viene a poner fin a un interminable debate.

169 El caso tiene su origen en el despido de un trabajador por realizar un uso personal de una cuenta de mensajería instantánea, *Yahoo Messenger*, abierta a petición de la empresa para uso profesional (atención de clientes y proveedores). Hay que hacer constar que la empresa contaba con una normativa interna, conocida por el trabajador, que prohibía el uso de los recursos de la compañía para fines personales. El empleador despidió al trabajador alegando como causa del despido la infracción de la normativa interna de la empresa.

No estando conforme con la decisión de la compañía, el trabajador impugna el despido alegando que la monitorización de la cuenta de mensajería por parte de la empresa supone una vulneración del derecho a la vida privada y al secreto de las comunicaciones previstas en la Constitución y en el Código Penal de Rumanía. El tribunal de primera instancia rumano declaró la procedencia del despido por considerar que la compañía había informado al trabajador de su normativa interna y de la prohibición de usar los instrumentos de la empresa para fines personales, tras lo cual el trabajador recurre en apelación la sentencia invocando el art. 8 CEDH, fallando el tribunal de apelación a favor de la empresa confirmando nuevamente el despido por entender que la conducta del empresario fue legítima dado que el control de las comunicaciones era la única forma de probar la existencia de la infracción disciplinaria. Agotadas las vías internas, el trabajador recurre ante el TEDH, siendo parte demandada el Estado de Rumanía.

170 Los hechos se remontan a febrero de 2009, fecha en la que el empleador de los solicitantes notó algunas irregularidades entre los niveles de inventario de los supermercados y lo que realmente se vendía a diario. Con el fin de investigar y poner fin a la situación económica de pérdidas, el empleador instaló un sistema de cámaras de vigilancia visibles y ocultas, siendo el objetivo de las primeras registrar posibles robos de clientes, apuntando las mismas hacia las entradas y salidas del supermercado. Por su parte, el objetivo de las cámaras ocultas era registrar posibles robos de empleados, apuntando éstas a los mostradores de salida que cubrían el área detrás de la caja registradora. La compañía dio a sus trabajadores aviso previo de la instalación de las cámaras visibles. Sin embargo, ni ellos ni el comité de personal de la compañía fueron informados de las cámaras ocultas. Los días 25 y 29 de junio de 2009, todos los trabajadores sospechosos de robo fueron convocados a reuniones individuales. Durante esas reuniones, los solicitantes admitieron su participación en los robos en presencia del representante del sindicato y del representante legal de la compañía, siendo despedidos los mismos por motivos disciplinarios.

Se ha de hacer notar que la sentencia de 5 de septiembre de 2017 (caso Barbulescu), ya inapelable, trae su causa de un recurso a una sentencia previa del Tribunal de Estrasburgo, de modo que para proceder al análisis de la argumentación del tribunal resulta necesario detenerse en la sentencia previa objeto de recurso de fecha 12 de enero de 2016, que constituye el primer pronunciamiento sobre este asunto, el cual será posteriormente corregido en la sentencia de la Gran Sala del referido tribunal de fecha 5 de septiembre de 2017.

Como se ha visto, la doctrina anterior (caso Copland c. Reino Unido) había utilizado el criterio de la "expectativa razonable de intimidad o confidencialidad" de la que puede gozar todo empleado por desconocer la posibilidad de una intromisión del empleador en sus comunicaciones, por lo que si éste decide realizar un seguimiento de aquéllas deberá proceder a la destrucción de esa expectativa de intimidad para que su intromisión pueda considerarse legítima, a cuyo efecto habrá de fijar con carácter previo las reglas de uso de tales medios – mediante la aplicación de prohibiciones absolutas o parciales – e informar a los trabajadores de que va a existir un control de los mismos, así como de los medios que se aplicarán para comprobar la corrección de tales usos, sin perjuicio de la implantación de cualesquiera otras medidas de índole preventivo tales como la exclusión de determinadas conexiones. De este modo, si se cumplieren estos requerimientos no podrá concluirse que, al realizarse el control, se ha vulnerado una expectativa razonable de intimidad[171].

Por el contrario, el TEDH en su sentencia de 12 de enero de 2016 (Barbulescu I) parece proceder a un cambio de criterio al considerar que la normativa interna de la compañía era conocida por el trabajador, lo cual permitía destruir cualquier expectativa de privacidad, constituyendo, de este

171 LLUCH CORELL, F. J., "El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador", 2017, pág. 3, en: http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronico-trabajador_11_1045180003.html

modo, la información ofrecida al trabajador en dicha normativa interna un fundamento suficiente para justificar el control del ordenador, que se entiende, por lo demás, proporcional y razonable dado que el empresario accedió a la mensajería en la convicción de que el registro de las comunicaciones sólo contenía mensajes profesionales - no personales -, a lo que hay que añadir el hecho de que al no haberse accedido por parte del empresario al disco duro del ordenador fue entendido por el tribunal como un elemento de mesura y ponderación[172].

En definitiva, el TEDH –sección cuarta- en su sentencia de 12 de enero de 2016 prima el derecho del empresario a controlar y vigilar el cumplimiento de las obligaciones laborales frente al derecho a la intimidad del trabajador, quedando la "expectativa razonable de confidencialidad" anulada por la mera prohibición general *ex ante* de uso[173].

Lo más importante a destacar en este punto tal vez sea que la sentencia considera suficiente una mera prohibición genérica inserta en una normativa interna, sin necesidad de firma ni comunicación previa al trabajador, acerca de la posibilidad de controles por parte del empresario, siendo, asimismo, irrelevante el hecho de que el comportamiento del trabajador no cause perjuicio alguno a la empresa[174].

Por último, señalar que, a juicio del TEDH, la intromisión del empresario se justifica en la creencia de que los datos contenidos en las comunicaciones intervenidas estaban referidos en exclusiva a actividades profesionales, siendo, pues, legítimo el acceso a los mismos, por lo que el tribunal declara - con seis

172 MIRANDA BOTO, J. Mª, "Derecho a la intimidad de los trabajadores y uso del messenger corporativo ante el Tribunal Europeo de Derechos Humanos", *Derecho de las relaciones laborales*, nº 2, 2016, pág. 104.

173 LÓPEZ DE LA FUENTE, G., "La doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos…, *op. cit.*, pág. 10.

174 LÓPEZ DE LA FUENTE, G., *Idem., ibídem.*

votos a favor y uno en contra -[175] que no se ha infringido el art. 8 CEDH. Tras el controvertido pronunciamiento, la sentencia fue objeto de recurso ante la Gran Sala del TEDH que dictó sentencia el día 5 de septiembre de 2017, sobre la que nos detendremos a continuación.

2. La Gran Sala del TEDH revisa en su sentencia de 5 de septiembre de 2017 el criterio establecido en el anterior pronunciamiento de 12 de enero de 2016, examinando la normativa aplicable, a cuyo efecto toma en consideración la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de esos datos[176].

De igual modo, la Gran Sala del Tribunal retoma el examen sobre la posible vulneración del art. 8 del Convenio, entendiendo que el control por parte del empleador de los medios informáticos habrá de ajustarse al patrón establecido en la Recomendación CM/REC (2015) del Consejo de Europa para la protección de datos en el ámbito laboral adoptada por el Comité de Ministros el 1 de abril de 2015 y que, por tanto, aquél no podía acceder al ordenador del trabajador al gozar éste de una "expectativa razonable de confidencialidad no neutralizada"[177]. Seguramente, los aspectos novedosos sean la exigencia de una información clara y precisa al trabajador sobre el sistema de vigilancia y un

175 La STEDH de 12 de enero de 2016 (Barbulescu I) cuenta con un voto particular del magistrado portugués Pinto de Albuquerque en el que se sostiene que la política de uso de Internet en la empresa ha de ser precisa, no bastando con una simple prohibición genérica del uso de los ordenadores para fines personales, al tiempo que es conveniente *"recoger expresamente el conocimiento del trabajador de que está siendo controlado"*. Asimismo, entiende el magistrado *"que las políticas de control sobre empleados han de establecer reglas claras y transparentes sobre los usos permitidos, los controles que pueden llevarse a cabo y su periodicidad o las medidas técnicas que serán implementadas a tales efectos"*.

176 Esta Directiva quedó derogada a partir del 25 de mayo de 2018 con la entrada en vigor del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos.

177 LÓPEZ DE LA FUENTE, G., "La doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos…, *op. cit.*, pág. 11.

control fuerte o intenso de proporcionalidad en el caso del acceso al contenido de los mensajes.

La sentencia, conocida como “doctrina Barbulescu”, proporciona un cambio radical al someter cualesquiera medidas de control al cumplimiento previo de una serie de condiciones, añadiéndose al requerimiento de información previa la necesidad de privilegiar las medidas preventivas sobre las de fiscalización (v. gr. impedir el acceso a determinadas páginas web) y la obligación de asegurar la transparencia en el tratamiento de los datos de carácter personal[178].

En resumen, podemos decir que hasta la sentencia de 5 de septiembre de 2017 en la jurisprudencia del TEDH, y en la de nuestros tribunales internos, se observaba una tendencia que primaba el poder de dirección del empresario sobre los derechos fundamentales del trabajador. En cambio, la STEDH de 5 de septiembre de 2017 procede a una limitación de las facultades de control empresarial al exigir mayores previsiones para poder acceder y controlar legítimamente los instrumentos informáticos puestos a disposición del empleado, alterando en esencia la doctrina judicial del TC español y del TS.

3. Ambas sentencias del TEDH (Barbulescu II y López Ribalda) reconocen el legítimo interés del empleador de asegurar el buen funcionamiento de la empresa, proteger su organización y gestionar sus derechos de propiedad mediante poderes de vigilancia que le permitan el control del adecuado cumplimiento de las obligaciones contractuales de sus empleados, fijando la primera de ellas los principios generales que los Estados han de tener en cuenta para respetar positivamente el art. 8 del CEDH y el justo equilibrio entre los derechos de los trabajadores a su vida privada y a la correspondencia en el lugar de trabajo y de los empresarios al buen

178 LÓPEZ DE LA FUENTE, G., “La doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos…, *op. cit.*, pág. 11.

funcionamiento de la empresa, corrigiendo el juicio de ponderación efectuado por los órganos jurisdiccionales nacionales. Y, al hacerlo, ha puesto límites al poder empresarial y a la subordinación jurídica del trabajador que el ejercicio del poder de control o vigilancia empresarial a través de medios digitales refuerza cualitativamente.

En efecto, las sentencias referidas dejan claro que el poder de vigilancia empresarial no puede ejercerse sin antes poner en conocimiento de los trabajadores cómo, cuándo y a través de qué medios se va a ejercer, consistiendo la gran novedad de la sentencia Barbulescu II en la desautorización que hace del entendimiento de que una política empresarial de prohibición de la utilización por los trabajadores de los medios tecnológicos empresariales para fines privados conlleva o sobreentiende el ejercicio del poder empresarial de vigilancia y sanción sin previa información a los trabajadores[179].

Por su parte, la aportación de la sentencia López Ribalda radica en condenar el ejercicio de la video vigilancia encubierta de los trabajadores en el lugar de trabajo de modo indiscriminado y durante un largo período de tiempo por considerarlo una intromisión ilegítima en la vida privada de aquéllos al incumplir el empresario la obligación de información previa acerca de la existencia y características del sistema de recogida de datos de carácter personal.

4. Asimismo, de gran importancia es la reelaboración que el TEDH hace de los conceptos de “vida privada” y “correspondencia” del art. 8 CEDH y de la “expectativa razonable de confidencialidad” señalada en la sentencia Barbulescu II.

179 CASAS BAAMONDE, Mª. E., “Informar antes de vigilar…”, *op. cit.*, págs. 105-106.

El TEDH recuerda en las Sentencias Barbulescu II y López Ribalda que la noción de "vida privada" del art. 8 del CEDH es un concepto amplio que no se presta a una definición exhaustiva[180], siendo así que esta norma jurídica garantiza un derecho a la "vida privada" en sentido vasto, comprensivo del derecho a llevar una "vida privada social", esto es, de la posibilidad de la persona de desarrollar con plenitud su identidad social en relación con otros, comprendiendo las actividades profesionales o empresariales[181] y las que se desarrollan no sólo en el domicilio de la persona o en espacios privados, sino también en un contexto público[182], siendo en el ámbito del trabajo en el que la mayoría de las personas se relacionan con el mundo exterior.

Por su parte, la noción de "correspondencia" no se califica de "privada" en el art. 8.1 del Convenio, aplicándose tanto a la correspondencia telefónica y profesional como a los correos electrónicos enviados y recibidos en los lugares de trabajo y los procedentes del domicilio, así como a la información derivada del seguimiento del uso personal de Internet, que quedan protegidos también por la noción de "vida privada" del art. 8 del CEDH (caso Barbulescu II con cita de la STEDH de 3 de julio de 2007, caso Copland c. Reino Unido)[183].

5. Por otro lado, el Tribunal también ha sostenido que, incluso cuando las normas del empleador con respecto a la vida social privada de los empleados en el lugar de trabajo sean restrictivas, ésta no puede reducirse en ningún caso a cero, teniendo el Estado la obligación positiva (obligación de hacer) de procurar que se respete la vida privada de los empleados en el seno de la empresa (caso Bărbulescu c. Rumanía)[184], recordando el TEDH que ha exigido

180 STEDH de 27 de julio de 2004 (caso Sidabras et Dziautas c. Lituania).

181 STEDH, Gran Sala, de 12 de junio de 2014 (caso Fernández Martínez c. España).

182 STEDH, Gran Sala, de 7 de febrero de 2012 (caso Van Hannover c. Alemania).

183 El Tribunal señala: 1) que el sistema de mensajería instantánea vía Internet es una forma de comunicación que forma parte del ejercicio de la "vida privada social"; 2) que el envío y recepción de mensajes electrónicos, incluso desde el ordenador del empresario, queda comprendido en la noción de "correspondencia".

184 CASAS BAAMONDE, Mª. E., “Informar antes de vigilar…”, *op. cit.*, pág. 103.

que sea el legislador quien cumpla con esa obligación positiva mediante la fijación del marco normativo que determine la protección de los diversos intereses en juego, lo cual puede hacerse tanto mediante normas de Derecho del Trabajo, como de Derecho Civil y de Derecho Penal, teniendo los Estados un amplio margen para apreciar la necesidad de regular las condiciones en las que los empresarios pueden adoptar políticas sobre las comunicaciones no profesionales, electrónicas y de todo tipo, de sus trabajadores en el trabajo, si bien la laxitud de la que gozan los Estados en este ámbito no puede ser ilimitada.

Y, en defecto de regulación legal, corresponde a los órganos judiciales nacionales asegurar que la adopción empresarial de medidas de vigilancia de la correspondencia y de otras comunicaciones se efectúe con las garantías adecuadas y suficientes contra los abusos y las arbitrariedades, si bien el TEDH no deja a la amplitud de la libertad de configuración legislativa de los Estados ni al azar de los juicios ponderativos de los órganos judiciales nacionales los elementos esenciales que las autoridades nacionales habrán de tener en cuenta para proteger los derechos garantizados por el art. 8 CEDH a los trabajadores frente a las intromisiones en su vida privada y en su correspondencia en el trabajo, sino que determinados “principios generales” han de aplicarse para apreciar el cumplimiento por los Estados y sus órganos judiciales de sus obligaciones positivas en relación con el art. 8 CEDH, señalando al respecto los siguientes:[185]

i) El art. 8 CEDH reclama que las medidas de control empresarial de las comunicaciones de los trabajadores sean informadas o advertidas a través de diversos medios posibles, pero con carácter previo a su establecimiento y con nitidez en cuanto a la naturaleza de la vigilancia.

185 CASAS BAAMONDE, Mª. E., “Informar antes de vigilar…”, *op. cit.*, pág. 112

ii) Por lo que respecta al alcance de la vigilancia del empresario y su capacidad de intromisión en la vida privada de los trabajadores, debe distinguirse entre la vigilancia del flujo de las comunicaciones y la de su contenido, siendo preciso conocer los límites (temporales, espaciales, de contenido, etc.) de la vigilancia empresarial y el número de personas con acceso a sus resultados.

iii) La vigilancia de las comunicaciones de los trabajadores ha de responder a motivos legítimos del empresario, siendo la vigilancia del contenido de dichas comunicaciones una medida evidentemente más intrusiva, por lo que necesita justificaciones "más serias", de forma que, atendiendo al principio de proporcionalidad, ese conocimiento es la última *ratio*, por lo que sólo podrá ser adoptado cuando el empleador no disponga de otro medio posible para comprobar el cumplimiento por parte del trabajador de sus obligaciones profesionales. Y, además, ese conocimiento deberá ser modulado por un principio de necesidad estricto e impeditivo del acceso del control empresarial directo al contenido de las comunicaciones de los trabajadores[186], debiendo, en todo caso, el empresario informar previamente al trabajador afectado de la extensión de su poder de vigilancia respecto de ese contenido y con qué límites.

iv) Dependiendo de las circunstancias concretas de cada caso se habrá de apreciar si el fin perseguido por el empresario puede ser alcanzado sin acceder directamente al contenido de las comunicaciones de los trabajadores.

v) Es importante determinar la manera en que el empresario ha utilizado los resultados obtenidos a través de la vigilancia y, de manera concreta, si tales resultados se han utilizado para alcanzar el fin declarado por la medida empresarial.

186 CASAS BAAMONDE, Mª. E., “Informar antes de vigilar…”, *op. cit.,* págs. 113-116.

vi) Los trabajadores han de contar con garantías efectivas al objeto de impedir que el empresario acceda al contenido de las comunicaciones sin que el trabajador haya sido previamente advertido de tal posibilidad.

vii) Los trabajadores cuyas comunicaciones hayan sido objeto de vigilancia habrán de poder reclamar ante un órgano judicial que pueda decidir sobre la observancia de las exigencias señaladas por el TEDH y sobre la licitud de las medidas empresariales de vigilancia.

viii) Por último, con el objetivo de determinar si la noción de "vida privada" es aplicable, el TEDH ha examinado en diferentes ocasiones si las personas gozaban de una expectativa razonable de privacidad, habiendo declarado al respecto que la misma es un factor significativo, aunque no concluyente para activar la protección del respeto a la vida privada y a la correspondencia que brinda el art. 8 CEDH[187].

6. Dos meses después, el 28 de noviembre de 2017, el TEDH se ratifica en su doctrina dictando una nueva resolución en el caso Antovic y Mirkovic c. Montenegro[188] en la que vuelve a reiterar que el concepto "vida privada" es un

187 Caso Barbulescu II, con cita de la sentencia de 5 de octubre de 2010 - caso Kopke c. Alemania-; López Ribalda, con cita de la sentencia de 25 de junio de 1997 -caso Halford c. Reino Unido-.

188 El caso Antovic y Mirkovic c. Montenegro versa acerca de la instalación de un sistema de video vigilancia en los auditorios donde se imparten clases universitarias con el objetivo de proteger la seguridad de la propiedad y las personas, la seguridad de los estudiantes y la vigilancia de la enseñanza, quejándose los demandantes - la Sra. Nevenka Antović y el Sr. Jovan Mirković, ambos profesores universitarios - en virtud del art. 8 CEDH de que la instalación y el uso ilegítimos de equipos de video vigilancia en los auditorios universitarios en los que se impartían las clases habían violado su derecho al respeto de su vida privada. La resolución no se refiere a un problema laboral, sino a la desestimación de una demanda civil presentada por unos profesores que reclamaban una indemnización por la instalación de unas cámaras de vigilancia en varios auditorios de una facultad de matemáticas. Las cámaras ya habían sido retiradas tras una decisión de la agencia de protección de datos montenegrina.

Los hechos del caso se pueden resumir del modo que sigue: en febrero de 2011, el Decano de la Escuela de Matemáticas de la Universidad de Montenegro informó a los profesores que allí enseñaban, entre los cuales se encontraban los demandantes, la Sra. Nevenka Antović y el Sr. Jovan Mirković, que la video vigilancia se instalaría en los auditorios donde se imparten las clases, al tiempo que emite una decisión especificando que su objetivo era la

término amplio no susceptible de definición exhaustiva, siendo demasiado restrictivo limitar la noción de "vida privada" a un "círculo íntimo" en el que la persona desarrolle su propia vida personal como él elija excluyendo de ella completamente al mundo exterior no abarcado dentro de ese círculo, sino que el art. 8 del Convenio garantiza, a juicio del Tribunal, el derecho a la "vida privada" en sentido amplio, incluido el derecho a llevar una "vida social privada", es decir, la posibilidad de que el individuo desarrolle su identidad social[189].

Recuerda, asimismo, el Tribunal que la Corte ya ha sostenido que la noción de "vida privada" incluye actividades profesionales que tienen lugar en

---

seguridad de la propiedad y las personas, la seguridad de los estudiantes y la vigilancia de la enseñanza. De conformidad con la decisión, el acceso a los datos recopilados estaba protegido por códigos que sólo eran conocidos por el Decano. Los datos debían conservarse durante un año.

En marzo de 2011, los demandantes presentan una reclamación contra la video vigilancia y la recogida de datos sin su consentimiento a la Agencia de Protección de Datos de Carácter Personal solicitando que se retiraran las cámaras y se borraran los datos recogidos, basando su petición en la Ley de Protección de Datos de Carácter Personal de Montenegro.

Con fecha 28 de abril de 2011, el Consejo de la Agencia emite una decisión ordenando a la Escuela de Matemáticas que retirara las cámaras de los auditorios en un plazo de 15 días por no realizarse la video vigilancia de acuerdo con la Ley de Protección de Datos de Carácter Personal. En particular, el Consejo del Organismo consideró que no existían razones que justificaran la introducción de la video vigilancia prevista en dicha Ley, dado que no había pruebas de que la seguridad de las personas y los bienes estuvieran en peligro en los auditorios y que la enseñanza no estaba entre los motivos legítimos para establecer un sistema de video vigilancia. Las cámaras fueron retiradas y los datos recogidos también fueron borrados.

En enero de 2012, los demandantes presentaron una demanda de indemnización contra la Universidad de Montenegro, la Agencia de Protección de Datos de Carácter Personal y el Estado de Montenegro por presunta violación de su derecho a la vida privada, en particular por la recogida y el tratamiento no autorizados de datos, alegando que la injerencia en su vida privada, sin posibilidad de control alguno, no estaba de acuerdo con la ley en el sentido del artículo 8.2 de la Convención, concluyendo el Tribunal de instancia que la instalación y el uso de video vigilancia y la recopilación de datos no violaban el derecho de los solicitantes a la intimidad. Tras sucesivas apelaciones de los demandantes, todas ellas desestimadas, el caso llega finalmente al TEDH, resolviendo el mismo con fecha 28 de noviembre de 2017.

189 Principios sostenidos por el TEDH en los casos Niemietz c. Alemania de 16 de diciembre de 1992; Peck c. Reino Unido; Halford c. Reino Unido de 25 de junio de 1997; Fernández Martínez c. España y Bărbulescu c. Rumania de 5 de septiembre de 2017.

un contexto público[190] dado que, después de todo, en el transcurso de sus vidas laborales la mayoría de las personas tiene una oportunidad significativa, si no la más grande, de desarrollar relaciones con el mundo exterior, no siendo siempre posible distinguir claramente cuáles de las actividades de un individuo forman parte de su vida profesional o empresarial y cuáles no[191].

Por tanto, hay una zona de interacción de una persona con otra u otras que puede estar dentro del ámbito de la "vida privada"[192], siendo la vida profesional parte de ella[193], observando la Corte en el caso Antovic y Mirkovic c. Montenegro que los anfiteatros universitarios son el lugar de trabajo de los docentes, siendo allí precisamente donde enseñan a los estudiantes y también interactúan con ellos haciendo efectiva relaciones mutuas y construyendo su identidad social, al tiempo que recuerda que la video vigilancia encubierta de un trabajador en su lugar de trabajo debe considerarse una intrusión intolerable en la vida privada del empleado[194] y, por consiguiente, considera que constituye una injerencia en el sentido del art. 8 CEDH, no existiendo en este caso razón alguna para que el Tribunal se desvíe de esa conclusión, incluso cuando se trata de casos de video vigilancia no encubierta de un empleado en el lugar de trabajo.

7. Tal vez el interés de la Sentencia Antović y Mirković c. Montenegro radique en el debate que se plantea entre la mayoría y los votos particulares acerca de si la grabación de imágenes en un aula universitaria puede suponer una intromisión en la vida privada, a cuyo efecto el TEDH se apoya de nuevo en la idea de “vida privada social” y en la consideración de que las aulas son un espacio de trabajo para los profesores. La estimación de la demanda se basa

190 Caso Barbulescu II.

191 Caso Niemietz c. Alemania.

192 Caso Peck c. Reino Unido.

193 Caso Fernández Martínez c. España.

194 Caso Köpke c. Alemania.

sencillamente en el hecho de que la instalación de las cámaras de vigilancia no se adecuaba a la legislación nacional, faltando el requisito de que la intromisión esté prevista en la ley.

Por último, reseñar que la STEDH de 28 de noviembre de 2017 (caso Antovic y Mirkovic c. Montenegro) cuenta con dos votos particulares: uno constituido por la opinión conjunta de los jueces Vucinic y Lemmens[195] y otro integrado por la opinión disidente de los jueces Spano, Bianku y Kjolbro[196].

195 Sostienen los jueces Vucinic y Lemmens que están totalmente de acuerdo con la conclusión de violación del art. 8 del Convenio, si bien hubieran preferido un razonamiento ligeramente diferente. Entienden los referidos jueces que el presente caso trata de video vigilancia en auditorio universitario donde los solicitantes, dos profesores, han estado enseñando a sus alumnos. El problema principal ante el tribunal es si el art. 8 es aplicable a los hechos del caso. Si bien la mayoría considera que los auditorios universitarios son "lugares de trabajo" de los docentes y abordan el caso como uno relacionado con una interferencia en la vida privada de un empleado por parte de su empleador, ambos jueces hubieran preferido dar más importancia a la naturaleza de la actividad que se puso bajo video vigilancia. Entienden ambos jueces que en una interacción profesor-alumno, el profesor goza de una expectativa razonable de privacidad en el sentido de que normalmente puede esperar que lo que está ocurriendo en el aula sea seguido sólo por aquéllos que tienen derecho a asistir a la clase. No obstante, puede haber excepciones, como por ejemplo cuando una conferencia se graba con fines educativos o para uso de estudiantes que no pudieron asistir físicamente a la clase, si bien en el presente caso no existía tal propósito. Al propio tiempo, les parece también que en un ambiente académico, donde la enseñanza está cubiertas por la libertad de cátedra, dicha expectativa de privacidad pueda considerarse "razonable".

Ahora bien, lo anterior no significa en modo alguno que la video vigilancia en un auditorio no sea posible. Pero, dado que el art. 8 del Convenio es aplicable, dicha medida habrá de cumplir con los condicionantes establecidos en el art. 8.2, lo que significa, entre otras cosas, que debe existir una base legal adecuada, que el alcance de la vigilancia debe ser limitado y que deben existir garantías contra el abuso. Pero en el presente caso estamos de acuerdo con la sentencia en la medida en que llega a la conclusión de que la injerencia en cuestión no se ajustaba a la ley y, por tanto, constituía una violación del art. 8.

196 Los jueces Spano, Bianku y Kjolbro votan en contra de declarar admisible la solicitud y de encontrar una violación del art. 8 del Convenio. En su opinión, la sentencia amplía el alcance del art. 8.1 del Convenio, entendiendo que la Corte ya ha decidido con anterioridad una serie de casos relativos a la video vigilancia en lugares públicos y se desprende de la jurisprudencia que dicha supervisión no plantea automáticamente una cuestión en virtud del art. 8.1 del Convenio, habiendo tenido incluso ocasión de decidir una serie de casos relativos al control en los lugares de trabajo, incluida la video vigilancia, y de esta jurisprudencia se desprende que la vigilancia de los empleados en el lugar de trabajo por parte del empleador no plantea automáticamente un problema en virtud del artículo 8.1 de la Convención. De conformidad con la jurisprudencia del tribunal relativa a la monitorización, en principio es necesario establecer una distinción entre la video vigilancia como tal y el registro, el tratamiento y la utilización de los datos obtenidos por otra, y ambas situaciones pueden dar lugar a consideraciones sobre la vida privada. De la jurisprudencia existente del tribunal deducen estos jueces que la video vigilancia no constituye en sí misma una injerencia en la vida privada de las personas supervisadas, sino que dependerá de una evaluación de las circunstancias específicas del

8. La misma doctrina la repite el TEDH en sus sentencias de 9 de enero de 2018 (caso López Ribalda *et alii* c. España I) y de 17 de octubre de 2019 (López Ribalda II) en un supuesto de video vigilancia encubierta de los trabajadores en el puesto de trabajo, volviendo a reiterar la Corte que ésta debe considerarse, como tal, una intrusión intolerable en la vida privada de aquéllos, al tiempo que reitera que, aunque el objetivo del art. 8 CEDH es esencialmente proteger al individuo frente a la injerencia arbitraria de las autoridades públicas, no solo obliga al Estado a abstenerse de dicha injerencia, sino que, además, éste tiene la obligación positiva de hacer o procurar que la vida sea respetada en el seno de la empresa.

Por otro lado, recuerda el Tribunal que los datos visuales obtenidos mediante video vigilancia implicaron el almacenamiento y el tratamiento de datos personales, estrechamente relacionados con la esfera privada de las personas, habiendo sido los mismos procesados y examinados por varios miembros de la empresa - entre otros, el representante sindical y el representante legal de la empresa - antes de que los solicitantes fueran informados de la existencia de las grabaciones de video, destacando además

---

caso que tenga en cuenta el lugar en el que se realiza la supervisión, la naturaleza de las actividades monitoreadas, si la supervisión es específica y sistemática, si las personas supervisadas gozaban de una expectativa razonable de privacidad, etc. En otras palabras, depende de una evaluación de la supervisión de la video vigilancia como tal, así como del almacenamiento, procesamiento y uso de los datos o la información recopilada.

Al evaluar la aplicabilidad del aspecto "vida privada" del art. 8.1 del Convenio, la mayoría se centra en la video vigilancia como tal y no en ninguna grabación o uso posterior de la información recopilada. Para la mayoría, basta evocar el art. 8 sobre la base de que la video vigilancia o el monitoreo se llevó a cabo en el lugar de trabajo de los solicitantes, el auditorio donde los profesores enseñaban e interactuaban con los estudiantes. En nuestra opinión, esta es una comprensión muy amplia de la noción de "vida privada" dado que, teniendo en cuenta las circunstancias específicas del presente caso, el monitoreo de la video vigilancia de la universidad en el auditorio donde los solicitantes estaban enseñando como profesores no planteaba un problema con respecto a la vida privada de los solicitantes, considerando concluyente que la monitorización vía video se realizó en los auditorios universitarios, que los solicitantes habían sido notificados acerca de la misma, que lo que se monitoreaba era la actividad profesional, que la vigilancia era remota no existiendo grabación de audio y, por tanto, no se registraron las enseñanzas o discusiones, las imágenes se difuminaron y las personas no pudieron ser reconocidas fácilmente, las grabaciones sólo fueron accesibles para el Decano y se borraron después de 30 días. Sea como fuere, quisiéramos agregar que, en nuestra opinión, el almacenamiento de la video vigilancia no plantea en sí mismo un problema en la "vida privada".

que la legislación nacional vigente en el momento de los hechos contenía disposiciones específicas sobre protección de datos personales[197].

9. Más recientemente, una nueva sentencia, de fecha 22 de febrero de 2018 (caso Libert c. Francia), vuelve a repetir, matizándola, la doctrina del TEDH en la materia sosteniendo que el empleador puede consultar archivos en el ordenador del trabajador a menos que éste los hubiera identificado claramente como "privados"[198] dado que los archivos creados por los empleados que utilizan ordenadores proporcionadas por sus empleadores se presumen de naturaleza profesional a menos que se identifiquen como "personales".

197 De facto, en virtud del art. 5 LOPD – vigente en el momento de los hechos -, los solicitantes tenían derecho a ser *"informados previa y explícitamente, precisa e inequívocamente"* de *"la existencia de un archivo de datos personales o de que los datos serán procesados, su finalidad y la destinatarios de la información; la naturaleza obligatoria u opcional de su respuesta a las preguntas formuladas; las consecuencias de proporcionar o negarse a proporcionar los datos; la existencia de derechos de acceso, rectificación, borrado y objeción; y la identidad y dirección del controlador o, según corresponda, su representante"*.

Asimismo, en virtud del art. 3 de la Instrucción 1/2006 AEPD el empleador tenía la obligación de colocar un letrero distintivo indicando las áreas que estaban bajo vigilancia, y hacer un documento disponible conteniendo la información proporcionada en el art. 5 LOPD, observando el tribunal que aquél no cumplió con la obligación de informar a los interesados sobre la existencia de un medio de recopilación y tratamiento de sus datos personales ni de la instalación de un sistema de video vigilancia encubierta en las cajas registradoras ni de sus derechos en virtud de la Ley de Protección de Datos Personales.

198 En el caso Libert c. Francia el TEDH sostuvo, por unanimidad, que no se había violado el art. 8 de la Convención Europea de Derechos Humanos. El caso se refería al despido de un empleado de la SNCF (compañía nacional de ferrocarriles franceses) después de que la confiscación de su ordenador de trabajo revelara el almacenamiento de archivos pornográficos y certificados falsificados elaborados para terceros. El Tribunal observó que la consulta de los expedientes por parte del empleador del Sr. Libert tenía un objetivo legítimo de proteger los derechos de los empleadores que legítimamente podían querer asegurarse de que sus empleados utilizaran las instalaciones informáticas que habían puesto a su disposición de acuerdo con sus obligaciones contractuales y las regulaciones aplicables. El Tribunal observó que la ley francesa comprendía un mecanismo de protección de la privacidad que permitía a los empleadores abrir archivos profesionales, aunque no podían abrir subrepticiamente archivos identificados como personales. Solo podían abrir el último tipo de archivos en presencia del empleado. Los tribunales nacionales habían dictaminado que dicho mecanismo no habría impedido que el empleador abriera los expedientes en cuestión, ya que no habían sido debidamente identificados como privados. Por último, el Tribunal consideró que los tribunales nacionales habían evaluado adecuadamente la alegación del demandante de una violación de su derecho al respeto de su vida privada y que las decisiones de esos tribunales se habían basado en motivos pertinentes y suficientes.

Es de destacar que la SNCF, compañía en la que prestaba sus servicios el trabajador, es una entidad de derecho público supervisada por el Estado francés, siendo designado su Director por éste. Esa entidad proporcionaba un servicio público, tenía un monopolio y se beneficiaba de una garantía estatal implícita, confiriéndole estos factores la condición de autoridad pública en el sentido del art. 8 CEDH. Por tanto, el presente caso es distinto del caso de Bărbulescu c. Rumania, en el que un empleador del sector privado había infringido el derecho al respeto de la vida privada y a la correspondencia privada. Dado que la interferencia en este caso se debió a una autoridad pública, la queja fue analizada desde el ángulo no de las obligaciones positivas del Estado, sino de sus obligaciones negativas[199].

199 En el momento material de los hechos, la ley positiva francesa establecía que los empleadores podían abrir archivos contenidos en los ordenadores de trabajo de los empleados a menos que dichos archivos se identificaran como personales. Por tanto, la injerencia tenía una base jurídica, y el derecho positivo había especificado con suficiente claridad las circunstancias y condiciones en que se autorizaba tal medida. Por tanto, la injerencia se orientó a garantizar la protección de "los derechos...de otros", en este caso los derechos de los empleadores, que legítimamente podrían querer garantizar que sus empleados utilizaran las instalaciones informáticas que habían puesto a su disposición en línea con sus obligaciones contractuales y las regulaciones aplicables. La ley francesa comprendía un mecanismo para proteger la vida privada: aunque el empleador podía abrir cualquier archivo profesional almacenado en los discos duros de los ordenadores con los que había suministrado a sus empleados en el ejercicio de sus funciones, no podía abrir subrepticiamente archivos identificados como personales "a menos que haya un riesgo grave o en circunstancias excepcionales", de modo que sólo podía abrir dichos archivos en presencia del empleado en cuestión o después de que este último hubiera sido debidamente informado. Los tribunales nacionales aplicaron ese principio. Consideraron que, en el presente caso, ese principio no había impedido que el empleador abriera los expedientes en cuestión, ya que no habían sido debidamente identificados como privados. El tribunal de apelación había tenido en cuenta la constatación de que las fotografías y videos impugnados se habían encontrado en un archivo almacenado en un disco duro con el nombre predeterminado *"D:/données"*, que el personal utilizó para almacenar sus documentos de trabajo y que, en el ordenador del solicitante, se había titulado *"D:/données personnelles"* ("D:/datos personales"). El tribunal consideró que un empleado no podría haber usado un disco duro completo, que se suponía que registraría datos profesionales, para uso privado y que el término genérico "datos personales" podría referirse a archivos de trabajo procesados personalmente por el empleado y podría, por lo tanto, no han designado explícitamente elementos relacionados con la vida privada. El tribunal de apelación había aceptado el argumento de SNCF de que el Estatuto del Usuario establecía que la información privada debería identificarse claramente como tal (opción "privada" en los criterios de Outlook), y que lo mismo se aplicaba a "los medios que reciben esa información ('privada' directorio)". Además, el tribunal de apelación sostuvo que el despido del Sr. Libert no había sido desproporcionado ya que había cometido una violación grave del código deontológico profesional de la SNCF y de las directrices internas pertinentes. Según el tribunal de apelación, sus acciones habían sido particularmente graves porque, como funcionario responsable de la vigilancia general, se esperaba que él sirviera de ejemplo. Por lo tanto, la Corte observó que los tribunales nacionales habían evaluado adecuadamente la alegación del demandante de una violación de su derecho al respeto de su vida privada y que las decisiones de esos tribunales se habían basado en motivos pertinentes y suficientes. Ciertamente, al utilizar la palabra "personal" en lugar de "privado", el Sr. Libert optó por la palabra utilizada

3.- Derecho al secreto de las comunicaciones.

1. Como ha quedado expuesto, con la finalidad última de proteger la vida privada, el apartado tercero del art. 18 CE proclama la inviolabilidad del secreto de las comunicaciones, cuyo concepto es, en la Constitución, rigurosamente formal[200] dado que se predica de lo comunicado con independencia de su contenido y pertenezca o no el objeto de la comunicación al ámbito de lo personal, lo íntimo y lo reservado[201], sosteniendo, de este modo, el TC la existencia de una presunción *iuris et de iure* de que lo comunicado es secreto, pretendiendo de esta manera proteger un ámbito de la vida de la persona frente a injerencias de terceros sin establecer distinciones acerca de qué contenidos de ese ámbito pueden ser afectados[202].

Al margen de su reconocimiento constitucional, el secreto de las comunicaciones presenta un componente internacional de notable importancia, estando el mismo reconocido en tres tratados internacionales suscritos por España: en la Declaración Universal de Derechos Humanos de 1948[203]; en el Convenio Europeo para la Protección de los Derechos Humanos y Libertades

---

en la jurisprudencia del Tribunal de Casación en el sentido de que un empleador no podía, en principio, abrir archivos designados como "personales" por el empleado. Sin embargo, eso no bastaba para poner en tela de juicio la pertinencia de las razones aducidas por los tribunales nacionales, ya que la Carta de los usuarios establecía específicamente que "la información privada (tenía que) estar claramente identificada como tal", de modo que las autoridades nacionales no se han extralimitado en el margen de apreciación de que disponen, por lo que no se ha violado el artículo 8 de la Convención.

200 JIMÉNEZ CAMPO, J., "La garantía constitucional del secreto de las comunicaciones", *Revista Española de Derecho Constitucional*, Año 7, núm. 20, Mayo - Agosto 1987, pág. 41.

201 STC 123/2002, de 20 de mayo.

202 MARÍN ALONSO, I., La facultad fiscalizadora del empresario sobre el uso de correo electrónico en la empresa: su limitación en base al derecho fundamental al secreto de las comunicaciones, *Temas Laborales*, núm. 75/2004, pág. 112.

203 Reza en su art. 12 que *"nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"*

Fundamentales de 1950[204] y, en tercer lugar, en el Pacto Internacional de Derechos Civiles y Políticos de 1966[205].

Por su parte, en nuestra Constitución, el art. 18.3 garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial, sobreentendiéndose el carácter de *numerus apertus* de este enunciado, no estando excluidos otro tipo de comunicaciones tales como el correo electrónico, chats, telefax o teletipo, entre otros, siempre que se efectúen mediante un medio técnico[206].

El TC, en su Sentencia 70/2002, de 3 de abril, se ha manifestado claramente en este sentido señalando que los avances tecnológicos operados en los últimos tiempos en el ámbito de las telecomunicaciones hacen necesario un nuevo entendimiento tanto del concepto de comunicación como del objeto de protección del derecho fundamental capaz de extender la protección a esos nuevos ámbitos, como se deriva del tenor literal del art. 18.3 CE. No está protegida, en cambio, la comunicación directa (verbal o no verbal), ya que aquí depende de los propios comunicantes evitar la interferencia de terceros, si bien ello no obsta a la posible aplicabilidad del derecho a la intimidad, como ocurriría, por ejemplo, en el caso de la instalación ilegal de micrófonos en la casa de una persona.

---

204 Expone en su art. 8.1 que *"toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia"*, añadiéndose en el apartado segundo que *"no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás"*.

205 Proclama en su art. 17 que *"nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia"*.

206 DE LA QUADRA-SALCEDO JANINI, T. y SUÁREZ CORUJO, B., "¿Trabajadores incomunicados?: la deriva de la doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones", en *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social (Actas del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social)*, Varios, Madrid 2014.

2. Los sujetos del derecho al secreto de las comunicaciones son todas las personas, tanto físicas como jurídicas, y vincula a los poderes públicos y a los particulares, consistiendo su contenido en la libertad de comunicarse con otros a través de los medios técnicos a disposición del público y en excluir a los demás de la comunicación. El secreto sólo puede ser excluido mediando dispensación al respecto por parte de uno de los comunicantes, dado que el secreto no rige para ellos, o por resolución judicial. A ello se añade, además, la exigencia de que la comunicación a que hace referencia el art. 18.3 CE es la que se realiza mediante canales cerrados de comunicación, no disfrutando de la protección del referido precepto las comunicaciones realizadas a través de canales abiertos, como es el caso de las transmitidas por radio mediante ondas hertzianas o la carta abierta publicada en un periódico con la intención de crear un estado de opinión[207].

3. Por otro lado, el derecho al secreto de las comunicaciones tiene, pese a ir emparejado al derecho a la intimidad, un significado propio, configurándose como un derecho autónomo y a cuyo concepto se ha referido la STC 114/1984, de 29 de noviembre, sosteniendo que el mismo ampara tanto el contenido de la comunicación como la identidad subjetiva de los interlocutores, no siendo posible la disposición de los datos sin el consentimiento de su titular. El bien jurídico protegido por el derecho al secreto de las comunicaciones es, como indica la Sentencia referida, la libertad de las comunicaciones[208], no la intimidad.

Distinguir debidamente cuándo nos hallamos ante una cuestión concomitante con el secreto de las comunicaciones y cuándo con el derecho a

207 MARÍN ALONSO, I., La facultad fiscalizadora del empresario sobre el uso…, *op. cit.*, pág. 112. En el mismo sentido, RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones: tecnología e intimidad*, Mc Graw Hill, Madrid 1998, págs. 66-67; MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid 1995, pág. 52.

208 PARDO FALCÓN, J., "Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional", *Revista Española de Derecho Constitucional*, Año 12, núm. 34, Enero-Abril 1992, pág. 174.

la intimidad resulta de todo punto necesario tanto por motivos conceptuales como porque la CE somete a un diferente régimen jurídico la protección de ambos derechos.

Así, mientras que la intimidad está sujeta únicamente al régimen general de protección de los derechos fundamentales previsto en el art. 53 CE, para el derecho al secreto de las comunicaciones se añade, además, la exigencia de resolución judicial para poder proceder a cualesquiera injerencias en las comunicaciones protegidas, por lo que se hace necesario identificar los criterios que permitan individualizar, en cada caso concreto, el derecho afectado dado que de esa identificación va a depender el régimen jurídico aplicable[209].

De acuerdo con la doctrina del TC, el derecho al secreto de las comunicaciones consagra la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas[210], de modo que este derecho resultará vulnerado tanto por la interceptación en sentido estricto - aprehensión física del soporte del mensaje, con conocimiento o no del mismo, - como por el simple conocimiento antijurídico de lo comunicado - apertura de la correspondencia ajena guardada por su destinatario o de un mensaje remitido por correo electrónico o a través de telefonía móvil, por ejemplo -[211], tal como reconoce, entre otras, la STC 115/2013, de 9 de mayo, siendo elemento fundamental para entender vulnerado el derecho recogido en el art. 18.3 CE el hecho de que la injerencia en el proceso comunicativo provenga de un tercero ajeno a los comunicantes, de modo que el secreto de las comunicaciones no puede ser opuesto frente a quien tomó parte en la comunicación misma,

209 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 22.

210 DE LA QUADRA-SALCEDO JANINI, T. y SUÁREZ CORUJO, B., "¿Trabajadores incomunicados?: la deriva de la doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones", en *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social (Actas del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social)*, Varios, Madrid 2014.

211 LÓPEZ ANIORTE, Mª. C., "Límites constitucionales al ejercicio del poder directivo empresarial mediante el uso de las TIC y otros medios de vigilancia y seguridad privada en el ordenamiento jurídico español", *Revista Policía y Seguridad Pública*, noviembre 2013-junio 2014, pág. 35

operando el mismo solamente respecto de terceros ajenos a la comunicación[212], de modo que cuando tal intromisión no se produce, sino que es el propio receptor de la comunicación quien divulga la misma[213], el derecho al secreto de las comunicaciones no resulta vulnerado[214], aunque sea posible vulnerar el derecho a la intimidad si el contenido de lo divulgado reviste naturaleza personal o íntima.

Por otro lado, mientras que el derecho a la intimidad presenta fundamentalmente una proyección material, el derecho al secreto de las comunicaciones es, como se ha dicho, más bien formal. En la intimidad lo que se tutela es el área que cada persona reserva para sí y para sus íntimos, alejándola del conocimiento de terceros ajenos. Sin embargo, para el derecho al secreto a las comunicaciones toda comunicación es secreta y sólo algunas comunicaciones serán íntimas[215].

La STC 114/1984, de 29 de noviembre, destacó este carácter formal subrayando que aquél se predica de lo comunicado con independencia de cual fuere su contenido y pertenezca o no el objeto de la comunicación al ámbito de lo íntimo, lo personal o lo reservado, constituyendo esta característica del secreto de las comunicaciones una garantía formal de intangibilidad que

212 FERNÁNDEZ ESTEBAN, Mª L., "Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto de las telecomunicaciones entre particulares, en especial en el ámbito de la empresa", *Revista Aranzadi Doctrinal Civil-Mercantil*, nº 3, 2000, pág. 21.

213 NAVARRO MARCHANTE, V. J., "El recurso a cámaras ocultas en los reportajes periodísticos: el caso Haldimann ante el TEDH" en *Revista Española de Derecho Constitucional*, 2015, pág. 341.

214 STSJ Galicia/A Coruña, de 25 de abril de 2014, (JUR 2014, 207850). Se trata de una enfermera de un geriátrico que, entre otros hechos, le comenta a través de WhatsApp a una compañera de trabajo que una paciente ha consumido una medicación errónea produciéndole una intoxicación medicamentosa, siendo la enfermera la persona encargada de administrar los medicamentos, por lo que, de la conversación, puede deducirse su falta. La compañera de trabajo proporciona el registro de dicha conversación a la empresa que la utiliza como prueba para despedir a la enfermera. El tribunal considera que esta prueba no vulnera el derecho al secreto de las comunicaciones porque la conversación ha sido transmitida a la empresa por la compañera de trabajo e interlocutora de la comunicación.

215 JIMÉNEZ CAMPO, J., "La garantía constitucional del secreto…, *op. cit.*, pág. 41.

determina que cuando el titular del derecho consiente el acceso a la comunicación quede automáticamente excluida la vulneración del derecho al secreto, aunque no una eventual lesión de la intimidad.

4. Un interesante desarrollo de la distinción entre derecho a la intimidad y secreto de las comunicaciones se encuentra, por lo demás, en la STS de 20 de noviembre de 2014, cuyos antecedentes de hecho versan sobre una trabajadora que recoge con su teléfono móvil la conversación sostenida con su empleadora en el mismo momento en que ésta le hace entrega, en la vía pública, de su carta de despido y la invita a retirarse, impidiéndole la entrada al centro de trabajo. El diálogo mantenido se ciñe a cuestiones netamente laborales, sin contener alusión alguna a la vida personal o familiar de las interlocutoras. La empleadora, alegando que la grabación se produjo sin su consentimiento, interpone demanda de protección de su derecho a la intimidad contra la trabajadora.

Atendiendo a los hechos, el Tribunal Supremo resuelve señalando que la conducta de la trabajadora no supuso una intromisión ilegítima en el derecho a la intimidad personal de su empleadora dado que lo contenido en la grabación no puede considerarse referido al ámbito de la intimidad que protege el art. 18.1 CE dado que se trata de cuestiones de índole laboral que la empleadora, en su condición de representante legal de la empresa y en ejercicio de su facultad disciplinaria, transmite a la trabajadora. De ahí que tales actos no puedan calificarse como una manifestación del ejercicio de su derecho a la intimidad[216].

216 APARICIO ALDANA, R. K., *Derecho a la intimidad y a la propia imagen en las relaciones jurídico laborales*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2016, pág. 85. Véase también MUÑOZ RUIZ, A. B., "Instrumentos informáticos de utilización generalizada en la empresa o medios de uso personal y secreto de las comunicaciones: comentario a la STC 241/2012, de 17 de diciembre", *Justicia Laboral*, nº 55, 2013, págs. 93-107; MARTÍNEZ FONS, D., "El control de la correspondencia electrónica personal en el lugar de trabajo (Comentario a la SJS núm. 32 de Barcelona de 16 de septiembre de 2002"), *Relaciones Laborales*, t. I, 2003.

En lo relativo al secreto de las comunicaciones, la sentencia reitera que este derecho se dirige a garantizar su impenetrabilidad por terceros ajenos a la comunicación, de forma que no hay secreto para aquél que es parte en el proceso comunicativo, lo cual es debido, como se ha dicho, a que el concepto de secreto del art. 18.3 CE presenta un carácter formal habida cuenta de que se predica de lo comunicado con independencia de cual fuere su contenido. De ahí que el deber de secreto no pese sobre los comunicantes, sino solamente un deber de reserva cuando el contenido material de lo comunicado se refiera a cuestiones personales o íntimas.

5. El objeto de la protección es, pues, la comunicación, la cual se concibe como un proceso de transmisión de mensajes entre personas concretas, con lo que sólo se protege el intercambio de objetos a cuyo través se transmiten mensajes mediante signos lingüísticos[217] y siempre que se trate de una comunicación indirecta, es decir, a distancia. No obstante, hay que tener presente que se protege no sólo el contenido de lo comunicado, sino también sus aspectos externos, tales como la identidad de los interlocutores, la frecuencia, etc.[218] Las comunicaciones directas no son objeto de protección por la vía del art. 18.3 CE, si bien pueden serlo a través del derecho a la intimidad, explicándose esta exclusión por la mayor vulnerabilidad de la comunicación indirecta.

6. El ámbito temporal de la garantía del secreto no es una cuestión pacífica, pues la STC 114/1984, de 29 de noviembre, amplía la protección al afirmar que el derecho puede conculcarse tanto por la interceptación en sentido estricto durante el proceso comunicativo como por el simple conocimiento antijurídico de lo comunicado, de forma que la garantía del art. 18.3 CE cubre no sólo el proceso de comunicación, sino también el mensaje cuando se materializa en algún objeto físico, planteamiento este que ha sido criticado por

217 STC 281/2006, de 9 de octubre.

218 SSTC 114/1984, de 29 de noviembre y 281/2006, de 9 de octubre.

privar supuestamente de coherencia al secreto de las comunicaciones como derecho autónomo, pues la correspondencia recibida y guardada por su destinatario debería protegerse por la vía del art. 18.1 CE y por la del número 3 de este artículo[219].

Así, la STC 70/2002, de 3 de abril, en el caso de la carta que es intervenida estando fuera del sobre y guardada en una agenda, se inclina por la exclusión de la protección por el art. 18.3 CE al señalar que la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo. Pero, una vez finalizado éste, la protección constitucional de lo recibido se realizará, en su caso, a través de las normas que tutelan la intimidad u otros derechos.

7. Aplicando las anteriores consideraciones al ámbito laboral nos encontramos con que, a efectos del art. 18.3 CE, resulta indiferente la distinción entre comunicaciones privadas o profesionales de los trabajadores pues el empleador, pese a ser el titular de las herramientas de trabajo es, según doctrina del TC, un tercero ajeno a la comunicación ante el que puede oponerse el secreto[220], careciendo el mismo de un derecho a fiscalizar las comunicaciones, sean privadas o profesionales, en las que no participa como interlocutor[221].

8. Por otro lado, protegido por el secreto no están sólo el soporte (carta, línea telefónica, etc.) y el mensaje, sino también las circunstancias de la

219 URBANO CASTRILLO, E., *El derecho al secreto de las comunicaciones*, La Ley, Madrid, 2011, pag. 154. Véase también MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones,* Madrid, Civitas, 1995; ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, Madrid, Iustel, 2007.

220 SSTS de 23 de diciembre de 1994 (RJ 10266) y de 10 de febrero de 1998 (RJ 948). Véase también la STEDH de 26 de octubre de 1998, caso Norris c. Irlanda.

221 El empresario no es un tercero cualificado en orden a la transgresión del derecho al secreto de las comunicaciones. En el mismo sentido, FERNÁNDEZ ESTEBAN, Mª L., "Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto a las comunicaciones entre particulares…", *op. cit.,* págs. 34-36.

comunicación, tales como la duración o la identidad de los comunicantes (STEDH de 2 de agosto de 1984, caso Malone c. Reino). Aunque el Tribunal Constitucional sostuvo inicialmente que la protección de la identidad de los comunicantes es menos intensa, dando por buena la entrega a la policía sin autorización judicial del listado de llamadas efectuadas desde un determinado número de teléfono[222], parece haber cambiado de criterio con la STC 230/2007, de 5 de noviembre, que considera exigible el consentimiento del titular o la autorización judicial para tener acceso a listado de llamadas telefónicas realizadas desde un número.

9. En cuanto al contenido de la comunicación, el secreto es susceptible de graduación en función de las características técnicas del medio empleado para la misma. Así, quien envía una tarjeta postal no puede esperar el mismo nivel de secreto que quien envía una carta en sobre cerrado. Dicho en otros términos: quien intercepta un mensaje sin aprehender o manipular su soporte no vulnera el art. 18.3 CE, siendo indiferente a este respeto que la interceptación sea casual o deliberada e independientemente del contenido de la comunicación.

Por último, señalar que, si bien lo importante en el secreto de las comunicaciones es el continente, no obstante, debe existir una comunicación digna de tal nombre. Así se explica que la STC 281/2006, de 9 de octubre, no apreciara vulneración de este derecho en la interceptación sin autorización judicial de un paquete postal que contenía droga. Al no haber ningún acto de comunicación, no podía decirse violado el art. 18.3 CE.

222 STC 123/2002, de 20 de mayo.

3.1.- Interceptación del correo electrónico y su incidencia sobre el secreto de las comunicaciones y la intimidad personal.

1. El primer pronunciamiento del Tribunal Constitucional que abordó la incidencia del secreto de comunicaciones en el contrato de trabajo fue la Sentencia 114/1984, de 29 de noviembre (por lo que hace a la prueba obtenida a través de una grabación de sonido), en la que se señalaba que el art. 18.3 CE no se limitaba únicamente al contenido de la misiva, extendiéndose asimismo a otros aspectos de la misma, tales como la identidad subjetiva de los interlocutores y que la impenetrabilidad para terceros no se aplicaba únicamente respecto a los poderes públicos, sino que también era postulable en el ámbito *interprivatos*. A lo que se añadía que el concepto de secreto del art. 18.3 presenta un carácter formal, en el sentido de que se predica de lo comunicado, sea cual fuere su contenido y perteneciera o no el objeto de la comunicación al ámbito de lo íntimo, lo personal o lo reservado. Y aunque podían existir algunas dudas en relación a si dichos criterios se aplicaban a las comunicaciones electrónicas, el propio TC en su sentencia 70/2002, de 3 de abril, indicó que los avances tecnológicos hacen necesario un nuevo entendimiento tanto del concepto de comunicación como del objeto de protección del derecho fundamental que sea capaz de extender aquélla a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del art. 18.3 CE.

2. Posteriormente, la STC 173/2011, de 7 de noviembre[223], avanzó en el terreno de la privacidad en el uso de las nuevas tecnologías (aunque en el ámbito de una investigación policial), señalando que cuando su titular navega por Internet, participa en foros de conversación o en redes sociales, descarga archivos, realiza operaciones de comercio electrónico, entre otras actividades, está revelando datos de su personalidad que pueden afectar al núcleo de su intimidad por referirse a orientaciones sexuales, a creencias religiosas, a

223 Una crítica a esta Sentencia en SAIZ ARNAIZ, A., "TC y PC", *Actualidad Jurídica Aranzadi* num.834/2012 parte Cara, Ed. Aranzadi, Cizur Minor, Pamplona 2012.

ideologías, etc. Con esta sentencia el TC perdió una buena oportunidad para fijar de modo sencillo las condiciones de intromisión legítima en el derecho fundamental a la intimidad cuando se trata de un ordenador[224].

Asimismo, son variados los pronunciamientos del TC en los que –también en el ámbito penal– se ha analizado cómo el conocimiento ajeno de los ámbitos de privacidad es susceptible tanto de afectar al derecho al secreto de comunicaciones como al de la intimidad puesto que una cosa es ese conocimiento como tal y otra el contenido del mensaje. El primero, de carácter procedimental, tiene cobijo en el artículo 18.3 CE; el segundo – de carácter sustantivo– en el artículo 18.1 CE[225].

3. Por lo demás, señalar que es criterio constitucional que no existe vulneración del secreto de comunicaciones si una de las partes que interviene en éstas aporta su grabación y/o transcripción como prueba, afirmándose así en la STC 114/1984, de 29 de noviembre, que quien entrega a otro la carta recibida o quien emplea durante una conversación telefónica un amplificador de voz que permite trasladar la conversación a otras personas presentes no está violando el secreto de las comunicaciones. Y ello sin perjuicio de que lo así transmitido a otros pudiese entrar en la esfera íntima del interlocutor y constituir un atentado contra el derecho garantizado por el art. 18.1 CE.

Un criterio similar ha seguido la STS – Sala de lo Civil– de 20 de noviembre de 2014, negando una invasión por una trabajadora de la privacidad de un empresario al hacer pública una conversación mantenida entre ambos en

224 GARCÍA ALBERO, R., "TC y PC", *Actualidad Jurídica Aranzadi* num.834/2012 parte Cruz, Ed. Aranzadi, Cizur Minor, 2012, pág. 1.

225 Por todas, STC 115/2013, de 9 de mayo.

la empresa en un contexto de conflictividad laboral sin que aparecieran en la misma aspectos vinculados con la vida íntima o personal[226].

4. Por lo que respecta al uso del correo electrónico por los trabajadores en la empresa se suscita la cuestión de los límites a la utilización del mismo, así como la legitimidad del empleador para intervenir las comunicaciones en uso de su potestad directiva, así como la incidencia que ello pueda tener en algunos derechos fundamentales de aquéllos, siendo la cuestión de fondo la de si el empresario puede acceder o no al ordenador del trabajador sin violentar derechos fundamentales de éste y, en particular, el derecho al secreto de las comunicaciones y a la intimidad.

La respuesta a este interrogante es que aquél sólo puede acceder a los contenidos almacenados en el ordenador del trabajador cuando dicho acceso no suponga una violación de los derechos fundamentales de éste. Sólo de este modo, lo así obtenido no se vería afectado por la tacha prevista en el art. 11.1 LOPJ y, por tanto, podría ser aportado como prueba en cualquier procedimiento judicial. Aunque la Constitución permite, en determinados supuestos, que el secreto de las comunicaciones pueda ser conculcado para obtener pruebas, dicha posibilidad sólo se contempla para determinadas autoridades públicas, pero no para sujetos particulares como es el empresario[227].

5. A tal efecto, el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, tras afirmar en su apartado 1 que los trabajadores y los empleados públicos tendrán

226 Véase DÍAZ RODRÍGUEZ, J. M., "Las grabaciones ocultas realizadas entre empresarios y trabajadores y su utilización como prueba en juicio", *Trabajo y Derecho* núm. 6/2015; MERCADER UGUINA, J. R., "Nota informativa sobre derecho a la intimidad y secreto de las comunicaciones en la relación de trabajo: dos casos en las jurisdicciones civil y penal", *Trabajo y Derecho*, núm. 2/2015.

227 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 20.

derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador, sostiene en su apartado 2 que el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos, si bien, como prescribe el apartado 3, los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente, debiendo ser informados los trabajadores de dichos criterios de utilización y habiendo de participar en su elaboración los representantes de los trabajadores.

Con este fin deberán elaborarse protocolos de uso, debiendo participar en su elaboración tanto los empresarios como los representantes de los trabajadores. La determinación de dichos criterios no es una opción empresarial, sino se recoge en la ley como una obligación. La utilización del verbo "deber" lleva a concluir que se impone como nueva obligación del empresario la protocolización del empleo de los dispositivos digitales que ponga a disposición de sus trabajadores[228].

6. No obstante, al igual que en todos los casos relativos a decisiones empresariales en el ejercicio del poder directivo, resulta necesario ponderar la proporcionalidad de la medida tendente al control del correo electrónico puesto a disposición del trabajador, siendo necesario distinguir entre el uso profesional y el uso personal del *e-mail*, siendo así que el epicentro de la cuestión reside en el primero y no en el segundo.

228 BLÁZQUEZ AGUDO, E. Mª, "Novedades laborales en la nueva ley orgánica de protección de datos", *Trabajo y Derecho*, 50/2019 (febrero), pág. 5.

Lo ideal es que el uso personal sea acordado en las normas de orden interno de la empresa y, de no existir las mismas, se entiende que existe un derecho a un uso normal no abusivo por parte del trabajador para temas personales. En el contexto laboral resulta evidente que el trabajador no puede vivir aislado de su ámbito privado durante la jornada laboral y, en la medida en que el correo electrónico es una forma de comunicación, parece lógico (lo mismo que ocurre con el teléfono) que ello no le sea impedido radicalmente[229]. No obstante, es en relación al uso profesional del *e-mail* donde el problema se plantea con toda crudeza y para cuya resolución no resulta posible partir de una concepción maximalista de los derechos en colisión, siendo precisamente en este estadio del razonamiento donde procede aplicar las reglas que integran el triple test sobre la proporcionalidad de la medida empresarial (idoneidad, necesidad y proporcionalidad en sentido estricto).

En este sentido, un control indiscriminado del *e-mail* sin mediar acuerdo previo con la otra parte de la relación laboral o una implantación directa por medio de una mera notificación constituirían elementos suficientes para calificar la medida de desproporcionada, de modo que con el objeto de evitar un resultado lesivo para los derechos fundamentales en juego resulta necesario un previo acuerdo.

7. Pero al margen de lo que sería deseable, lo cierto es que la jurisprudencia del Tribunal Constitucional se ha adentrado por una senda en la que la ponderación de derechos se desvanece a favor de un criterio maximalista que exacerba el poder directivo del empresario. En efecto, ésta fue la tesis sostenida en la STC 241/2012, de 17 de diciembre (caso Programa Trillian. Ordenador de uso común sin clave de acceso y secreto de las comunicaciones) de la que se deriva un cambio de criterio sumamente restrictivo para el ejercicio de los derechos fundamentales en el centro de

229 La STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía) sostiene que los derechos fundamentales de los trabajadores en el seno de la empresa no pueden ser reducidos a la nada, teniendo el Estado la obligación positiva (obligación de hacer) de procurar que el ejercicio de los mismos sea efectivo y eficaz.

trabajo con motivo del control informático del uso del correo electrónico como instrumento de comunicación[230].

En esta sentencia, el supuesto de hecho sometido a la consideración del Alto Tribunal se refiere a la empresa *Global Sales Solutions Line, S.L.*, la cual había previsto un ordenador de uso indistinto por todos los trabajadores sin necesidad de contraseña para acceder a la unidad "C". En dicho ordenador instalan dos trabajadoras, sin mediar autorización ni conocimiento por parte de la empresa, que expresamente había prohibido tales prácticas, el programa *Trillian* de mensajería instantánea con el que procedieron a llevar a cabo diferentes conversaciones en las que se proferían comentarios despectivos y críticos acerca de sus compañeros de trabajo, jefes y clientes, las cuales fueron descubiertas "casualmente" por un empleado, que informó a la empresa.

Ésta comunicó tales hechos a las trabajadoras en una reunión en la que se leyeron algunas de las conversaciones mantenidas y se resumieron las demás, tras lo cual amonestó verbalmente a aquéllas, procediendo una de ellas a interponer demanda contra la empresa por violación de derechos fundamentales solicitando que se declarara la vulneración de sus derechos al secreto de las comunicaciones, al honor y a la intimidad, siendo la demanda desestimada por el Juzgado de lo Social Nº 9 de Sevilla en virtud de sentencia de 13 de junio de 2005, presentando la trabajadora recurso de suplicación que también fue desestimado por la Sala de lo Social del Tribunal Superior de Justicia de Andalucía (Sevilla) mediante sentencia de 10 de febrero de 2006.

Seguidamente, la trabajadora interpuso recurso de amparo ante el TC, que dicta Sentencia sobre el asunto con fecha 17 de diciembre de 2012 (STC 241/2012, de 17 de diciembre), la cual diferencia el derecho a la intimidad del derecho al secreto de las comunicaciones señalando que el primero se configura como un derecho fundamental estrechamente vinculado a la propia

230 CARRILLO LÓPEZ, M., "Los ámbitos del derecho a la intimidad…", *op. cit.,* pág. 51.

personalidad y que deriva de la dignidad de la persona habida cuenta de que el mismo reconoce la existencia de un ámbito propio y reservado frente al conocimiento de los demás, necesario, según las pautas de nuestra cultura, para el mantenimiento de una calidad mínima de vida humana.

En el presente caso, el Tribunal Constitucional no apreció vulneración ni del derecho a la intimidad ni del derecho al secreto de las telecomunicaciones desde el preciso momento en que la demandante y su compañera de trabajo realizaron actos de disposición que supusieron la eliminación de la privacidad de las conversaciones al proceder a la inclusión de éstas en el disco duro del ordenador de uso común, de modo que podían ser leídas por cualquier usuario y trascender su contenido a terceras personas, a lo que hay que añadir el hecho de que estaba prohibido por parte de la empresa la instalación de programas en el ordenador, por lo que la pretensión de secreto que alega la trabajadora carece de toda cobertura constitucional.

En definitiva, dado que la empresa no había autorizado la instalación de dicho sistema de comunicación ni, por tanto, el uso personal del ordenador, carece de relevancia lesiva tanto en el derecho al secreto de las comunicaciones como sobre el derecho a la intimidad el hecho de que la empresa, una vez conocida la desobediencia de la empleada, la apercibiese por ello. Pero sí la tiene el hecho de que la empresa fuese más allá y accediese al conocimiento del contenido de los mensajes emitidos y recibidos por la teleoperadora, siendo ello completamente innecesario para imponerle una sanción ante una conducta a todas luces incorrecta. Sin embargo, el TC afirma que para la trabajadora no existía una expectativa de confidencialidad derivada de la utilización del programa instalado dado que éste era de acceso totalmente abierto y, además, había contravenido la orden empresarial[231].

231 “Nuevas tecnologías y trabajo (II): perspectiva constitucional”, *Trabajo y Derecho*, núm. 21, septiembre 2016, pág. 35.

8. Por tanto, la preceptiva autorización empresarial se convierte en el canon empleado en orden a la delimitación del ejercicio de estos derechos fundamentales en el seno de la empresa, lo cual conduce a preguntarse si el poder directivo del empresario puede ser planteado en esos términos. Es decir, si dicho poder puede devenir en el único parámetro para medir el ejercicio legítimo de un derecho fundamental, debiendo ser la respuesta a esta cuestión de índole negativa dado que la premisa basada en la prohibición absoluta del uso personal de los medios de comunicación que ofrecen las nuevas tecnologías conduce a los trabajadores, como ya había advertido anteriormente el TC, a sentirse constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser grabados y escuchados por la empresa (STC 98/2000, de 10 de abril)[232].

En el caso analizado de la teleoperadora, la conducta del empresario hubiese sido jurídicamente correcta si, tras comprobar el incumplimiento de la misma, no hubiese accedido al contenido de los correos contenidos, de modo que al hacerlo ejerció un poder omnímodo y, por tanto, desproporcionado sobre los derechos fundamentales de la trabajadora que, como se ha dicho, no puede vivir aislada de su entorno social durante la jornada laboral.

En la STC 241/2012, de 17 de diciembre[233] se analiza, pues, una situación que bien puede ser calificada como singular en tanto que la

232 A ello hay que añadir que la STEDH de 5 de septiembre de 2017, Gran Sala (caso Barbulescu c. Rumanía) considera que la normativa interna de la empresa no puede reducir la vida privada social dentro del trabajo a cero, por lo que subsiste siempre una expectativa razonable de privacidad a pesar de la existencia de una prohibición expresa y reiterada de uso de los medios informáticos de la empresa con fines personales, lo cual va a obligar al TC a modificar su doctrina judicial al respecto.

233 Para un análisis de este pronunciamiento del TC véase MARÍN ALONSO, I*.,* "La mensajería electrónica en la empresa: un paso atrás en la protección constitucional del derecho al secreto de las comunicaciones: a propósito de la STC 241/2012, de 17 de diciembre", *Relaciones Laborales*: *revista crítica de teoría y práctica*, nº 3, 2013, págs. 89-97; APARICIO ALDANA, R. K., "Las nuevas tecnologías en las relaciones laborales: análisis de la STC 241/2012, de 17 de diciembre", *Revista general de Derecho del Trabajo y de la Seguridad Social*, nº 36, febrero 2014, págs. 279-290.

comunicación entre las trabajadoras afectadas se produjo a través de un programa informático de correspondencia instalado por ellas mismas, sin autorización del empleador, en el ordenador de uso común de la empresa que permitía la libre lectura de mensajes por terceros, siendo esa práctica descubierta "casualmente", siendo precisamente estas características las que determinaron que el TC denegara la existencia de invasión de la privacidad.

Esta sentencia sitúa, pues, la intervención empresarial de las comunicaciones electrónicas en el estricto marco de las facultades de auto-organización, dirección y control empresariales *ex* art. 20.3 ET, de modo que para el TC la expectativa de confidencialidad del trabajador respecto de sus comunicaciones se determina en función de las instrucciones que haya podido impartir el empresario - prohibición de instalar programas de mensajería en un ordenador de uso común -, siguiendo un modelo jurídico-liberal y marcadamente propietario del poder de control, contradiciendo de este modo la garantía social del TEDH, el cual, a diferencia del TC, admite que incluso con normas prohibitivas iniciales de la empresa, pueda existir una expectativa razonable de confidencialidad de las comunicaciones[234].

9. La sentencia que comentamos cuenta con un voto particular formulado por el Magistrado Fernando Valdés Dal-Ré, quien discrepa de la opinión mayoritaria de la Sala al afirmar que la sentencia constituye un paso atrás en la jurisprudencia sobre la materia, en tanto que no tutela el derecho al secreto de las comunicaciones en las relaciones laborales, argumentando al efecto que la intervención empresarial no se limitó a comprobar la instalación del programa en el sistema informático de la empresa, sino que la empresa accedió a todos los mensajes, llegando incluso a exponer el contenido de los mismos en una

234 MOLINA NAVARRETE, C., "El derecho al secreto de las comunicaciones en la relación de trabajo: la dilución en «tópica» y «retórica» de su tutela constitucional", *Trabajo y Derecho*, Monográfico 7/2018, Nº 7, 1 de junio de 2018, Ed. Wolters Kluwer, pág. 6. Y, por su parte, el TS, secundando la devaluación de garantías del secreto de comunicaciones a partir de la visión liberal-contractual del poder empresarial exhibida por el TC, pierde una magnífica oportunidad para establecer una doctrina más correcta y certera en su sentencia 119/2018, de 8 de febrero (caso Inditex).

reunión celebrada a posteriori con las trabajadoras, todo lo cual acredita fehacientemente que manejaron dichos datos.

Por otro lado, el acceso a los correos contenidos en el servicio de mensajería no era fácil, siendo precisa la apertura de hasta siete carpetas diferentes para poder acceder a los mismos y, tras ello, proceder a abrir los ficheros de forma individual para poder acceder al contenido de los mensajes.

Afirma, asimismo, que existe un derecho de los trabajadores a utilizar los sistemas informáticos de la empresa para fines personales dado que el trabajador tiene un derecho fundamental a la libertad de las comunicaciones sin que el uso común del ordenador haga desaparecer la pretensión del secreto de las comunicaciones habida cuenta de que toda comunicación es secreta con independencia de su contenido, no pudiendo ser interceptada por el empresario bajo ninguna circunstancia, salvo que exista autorización judicial para ello o medie el consentimiento expreso de los trabajadores, de modo que lo resuelto por la mayoría del Tribunal Constitucional condiciona seriamente el derecho al secreto de las comunicaciones, pues la efectividad de este derecho fundamental en las organizaciones empresariales dependería no sólo de que no hubiera prohibición expresa, sino de que existiese permiso para ello. Por todas estas razones, entiende el Magistrado Fernando Valdés que la empresa sí vulneró el derecho al secreto de las comunicaciones de la trabajadora, por lo que el TC debió otorgarle el amparo[235].

10. Sin embargo, la posterior STC 170/2013, de 7 de octubre[236] (consideración del correo electrónico de la empresa como canal de

235 Posición favorable a lo manifestado en el voto particular, SANTIAGO REDONDO, K. M., "Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE", *Relaciones Laborales*, 2014, Nº 1, Tomo I, págs. 119 y sigs.

236 TRUJILLO PONS, F., "Revelación de secretos empresariales a terceros por medio del correo electrónico: posición del Tribunal Constitucional ante una supuesta vulneración a los derechos a la intimidad y al secreto de las

comunicación abierto), sí ha sido mucho más clara en la interpretación caracterizada como "patrimonialista". Cabe observar, en este sentido, que este pronunciamiento está analizando un supuesto en el que el trabajador había proporcionado a través del correo electrónico datos sensibles de producción de la empleadora a otra mercantil, existiendo una interdicción del uso de dicha herramienta informática para fines extralaborales en el convenio rector.

En esta sentencia, el demandante de amparo había venido prestando servicios para la empresa *"Alcaliber S.A."*, dedicada a la actividad químico-industrial de obtención de alcaloides, concretamente morfina y codeína. El trabajador fue objeto de un despido disciplinario alegando el empresario transgresión de la buena fe contractual como consecuencia de haber mantenido durante mucho tiempo una conducta desleal consistente en haber proporcionado información confidencial a otra compañía sin contar con autorización y usando, por lo demás, los medio de la empresa (correo electrónico y teléfono).

Se afirma en el pronunciamiento que el acceso por parte del empresario al correo electrónico del trabajador no resultó contrario al derecho al secreto de comunicaciones, pues la prohibición del uso extra laboral del correo electrónico contenida en el Convenio Colectivo llevaba implícita la facultad de aquél de controlar su uso en orden a la verificación del cumplimiento de la prestación laboral por parte del trabajador, a lo que hay que unir el hecho de que la comprobación por parte del empresario no supuso una interceptación de comunicaciones ajenas en canal cerrado por haber sido llevado a cabo aquélla cuando el proceso de comunicación ya había finalizado.

---

comunicaciones: STC 170/2013, de 7 de octubre", *Revista general de Derecho del Trabajo y de la Seguridad Social*, nº 36, febrero 2014, págs. 240- 267; MARTÍN VALVERDE, A., "Uso extralaboral del correo electrónico empleando medios informáticos de la empresa: control empresarial, requisitos. Comentario a la STC 170/2013, de 7 de octubre", *Actualidad Laboral*, nº 2, febrero 2014, págs. 184-192.

Y se descarta, además, que en el supuesto concreto existiera una vulneración del derecho a la intimidad del art. 18.1 CE, en tanto en cuanto el trabajador carecía de una expectativa razonable de privacidad respecto de sus correos electrónicos dado que esa herramienta informática fue habilitada únicamente para fines profesionales y el hecho de que un uso para fines distintos de los estrictamente profesionales estuviese tipificado como infracción en el Convenio Colectivo aplicable impide entender que su uso pudiera quedar al margen del control del empresario.

11. En definitiva, lo que viene a sostener este pronunciamiento es que de no existir una situación de tolerancia del uso personal del ordenador no podrá invocarse la existencia de una expectativa de privacidad, por lo que si existiere una prohibición expresa al respecto por parte de la empresa, ésta podría vigilar el correo electrónico de sus empleados para verificar el cumplimiento de la prestación laboral por parte de éstos.

Así pues, lo que en principio es comunicado vía canal cerrado, como es un correo electrónico, se transforma en canal de comunicación abierto al ejercicio del poder de control de la empresa. Algo verdaderamente inaudito y carente, a mi entender, de cualquier basamento jurídico y que supone una verdadera y completa desnaturalización del derecho al secreto de las comunicaciones y que está en abierta contradicción con la doctrina Barbulescu del TEDH (STEDH de 5 de septiembre de 2017), la cual realiza una importante advertencia - determinante, a mi juicio, para evidenciar el profundo desajuste de la doctrina del TC y también de la jurisprudencia del TS en este punto – señalando que las instrucciones de un empresario no pueden suponer una anulación del ejercicio de la privacidad social en el puesto de trabajo, sino que el respeto a la confidencialidad de las comunicaciones es necesario aunque pueda ser limitada (apartado 80, sentencia Barbulescu), correspondiendo a los tribunales nacionales velar para que el establecimiento por parte de las empresas de medidas de vigilancia de las comunicaciones vaya acompañada de garantías adecuadas para evitar abusos.

12. El carácter abierto del correo electrónico en este caso deriva de la existencia de una previsión convencional que indirectamente prohíbe la utilización del correo electrónico para fines personales (existía un Convenio Colectivo Sectorial de eficacia general que tipificaba como infracción leve el uso para fines particulares del correo electrónico).

Dicha previsión conlleva, a juicio del Tribunal, no sólo la prohibición de usar estos mecanismos en cualquier empresa del sector, sino el reconocimiento genérico de que cualquiera de estas empresas cuenta con la facultad de controlar su uso en orden a comprobar el cumplimiento por parte del trabajador de su prestación laboral. De acuerdo con estos argumentos, la remisión de mensajes efectuada por el trabajador se realizó a través de un canal de comunicación que se encontraba abierto al ejercicio del poder de fiscalización del empresario y, en consecuencia, fuera de la protección constitucional del art. 18.3 CE.

En definitiva, la tipificación como falta leve contenida en el Convenio Colectivo se equipara a la existencia de una prohibición absoluta en la empresa acerca del uso del correo electrónico para fines extra laborales, lo cual lleva al TC a considerar que dicha prohibición permite al empresario el despliegue de medidas de control con el fin de controlar el adecuado cumplimiento de la prestación laboral por parte de los trabajadores y a entender que el trabajador debía conocer esta posibilidad de control dado que, a su vez, era su obligación conocer el convenio colectivo aplicable a la empresa[237].

237 SEPÚLVEDA GÓMEZ, Mª., "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contralímites. Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre", *Temas Laborales* núm. 122/2013, pág. 203.

3.1.1.- Comunicaciones protegidas por el secreto de las comunicaciones.

1. En este apartado procederemos a analizar si el correo electrónico se ha de considerar o no amparado por el derecho al secreto de las comunicaciones previsto en el art. 18.3 CE, a lo que se responderá de modo afirmativo. Refiriéndonos a las comunicaciones operadas vía ordenador se ha de señalar que sólo resulta de aplicación la garantía constitucional del secreto de las comunicaciones a aquéllas en las que concurran las siguientes características:

i) Que la transmisión del mensaje se efectúe a través de un servicio interpuesto entre emisor y receptor y cuya operatividad escape al control de estos sujetos.

ii) Que se trate de comunicaciones cerradas, es decir, dirigidas una o varias personas concretas y determinadas[238].

iii) Que la comunicación se opere a través de servicios específicamente destinados a transmitir mensajes entre personas distantes[239].

Cualquier comunicación en la que concurrieren esas tres condiciones ha de entenderse protegida por el secreto de las comunicaciones, por lo que, *a sensu contrario*, hay que entender que quedan excluidos del ámbito de aplicación del art. 18.3 CE aquellos fenómenos de comunicación que, aun

238 Este criterio permite descartar que se encuentren amparados por el secreto de las comunicaciones los mensajes difundidos a través de las redes sociales a todos los contactos del destinatario (el muro de Facebook, por ejemplo).

239 Es muy significativa, en este sentido, la STC 281/2006, de 9 de octubre, cuando afirma que *"no gozan de la protección constitucional aquellos objetos –continentes– que por sus propias características no son usualmente utilizados para contener correspondencia individual sino para servir al transporte y tráfico de mercancías, de modo que la introducción en ellos de mensajes no modificará su régimen de protección constitucional"*.

valiéndose de redes informáticas, no concurran alguno de los anteriores requisitos. A tal efecto, no resultan protegidas por la garantía del secreto de las comunicaciones las operadas vía Internet que vayan dirigidas a una pluralidad indeterminada de personas.

De lo expuesto se deduce que el acceso por parte del empresario a los contenidos de las comunicaciones de un trabajador que no cumpla alguna de las tres características anteriormente referidas no quebrantaría el secreto de las comunicaciones, lo cual no significa que no pudiera vulnerar otros derechos como, por ejemplo, la intimidad.

3.1.2.- Contenidos protegidos por el secreto de las comunicaciones.

1. Lo primero que se ha de señalar es que el secreto de las comunicaciones protege el mensaje prohibiendo el acceso al mismo por parte de terceros. No obstante, lo que se discute es si la garantía constitucional del secreto de las comunicaciones resulta también extensible a otros contenidos de la comunicación distintos del mensaje.

A este respeto, la STEDH de 2 de agosto de 1984 (caso Malone c. Reino Unido), refiriéndose a las comunicaciones telefónicas, analizó el efecto que, sobre el derecho al respeto de la correspondencia, previsto en el art. 8.1 CEDH, tiene la operación de elaborar un listado de llamadas telefónicas realizadas desde un concreto número de teléfono con expresa indicación de la hora y duración de la llamada *(comptage o metering)*, a cuyo efecto el TEDH no cuestiona el hecho de que las compañías telefónicas lleven a cabo ese tipo de registros a efectos de facturación de los servicios prestados, resolución de quejas de clientes, etc.

No obstante, lo que sí resulta discutible es la utilización de esos listados de llamadas con finalidad probatoria en un proceso penal, entendiendo el TEDH que los datos registrados por el método de *comptage o metering* caen bajo la órbita del art. 8.1 CEDH, de modo que su obtención por una autoridad pública constituye una injerencia en el derecho reconocido en el citado precepto y sólo se considerará legítima aquélla si se ajustare a los requisitos contemplados en el apartado 2 de dicho artículo[240].

Siguiendo esta doctrina, la STC 114/1984, de 29 de noviembre, entiende que la noción de secreto del art. 18.3 CE no comprende solamente el contenido de lo comunicado, sino también otros aspectos de la comunicación, tales como la identidad de los interlocutores.

En idéntico sentido se pronuncia la STC 123/2002, de 20 de mayo, que entiende que el secreto de las comunicaciones telefónicas garantiza a los interlocutores la confidencialidad de la comunicación telefónica, la cual comprende tanto el secreto de su contenido como la confidencialidad de los datos externos de la conexión telefónica – v. gr. momento, duración y destino, entre otros -, considerando, además, que la entrega de un listado de llamadas a la Policía debe estar autorizada por resolución judicial.

Con posterioridad, la STC 230/2007, de 5 de noviembre, extiende el ámbito de protección del art. 18.3 CE al registro de llamadas enviadas, recibidas y perdidas contenido en el teléfono móvil, entendiendo que vulnera el secreto de las comunicaciones el acceso por parte de miembros de la Guardia Civil al citado registro sin contar con el pertinente consentimiento de su titular o con la necesaria autorización judicial.

240 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 45. También llegan a la misma conclusión las SSTEDH de 30 de julio de 1998 *(caso Valenzuela Contreras c. España)* y de 25 de septiembre de 2001 (caso P. G. y J. H. c. Reino Unido).

En suma, se puede decir que, de entre todos los datos de tráfico generados en el transcurso de una comunicación telefónica, merecen la protección reforzada del art. 18.3 CE los datos indicativos del origen y del destino de la comunicación, del momento y duración de la misma y los referidos al volumen de la información transmitida y el tipo de comunicación entablada.[241]

Por su parte, el TS también sigue la doctrina del TEDH sobre la extensión del derecho al secreto de las comunicaciones a los datos externos de la comunicación[242], si bien entiende que no resulta factible considerar que cualquier clase de dato relativo a una comunicación telemática se considere "dato externo" para el secreto de las comunicaciones, sino que es necesario determinar, en cada caso concreto, si el dato de que se trate es merecedor o no de la protección constitucional dispensada por el art. 18.3 CE[243].

2. De este modo, en relación con la dirección IP, la STS de 18 de marzo de 2010 (Sala 2ª) ha entendido que no resulta afectante al secreto de la comunicación la identificación del usuario que tiene asignada una concreta dirección IP por el proveedor de servicios de Internet, lo cual conduce a dicho Tribunal a distinguir dos conceptos, a saber: i) de un lado, los datos personales externos o de tráfico referidos a una concreta comunicación y que coadyuvan a desvelar el secreto protegido por el art. 18.3 CE; y ii) de otro lado, las circunstancias personales referidas a la intimidad de una persona (art. 18.1 CE), pero desconectados de cualquier proceso comunicativo, los cuales caen

241 Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado, sobre Pautas en relación con la Diligencia de Intervención de las comunicaciones telefónicas.

242 Cabe referenciar a este respecto las SSTS (Sala 2ª) de 25 de febrero de 2002 y de 20 de mayo de 2008.

243 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit*., pág. 48.

dentro de la órbita del derecho a la protección de datos informáticos del art. 18.4 CE[244].

Así pues, los rastreos policiales para localizar direcciones IP *(Internet Protocol)* pueden realizarse sin necesidad de autorización judicial dado que no se trata de datos confidenciales preservados del conocimiento público. Pero tras la averiguación del IP, las subsiguientes actuaciones de identificación y localización de quien sea la persona que tiene asignado ese IP se deben llevar a cabo bajo control judicial.

Asimismo, cuando en el marco de una diligencias de investigación desarrolladas por las Fuerzas y Cuerpos Policiales en la persecución de actividades delictivas de cualquier naturaleza resulte necesario dirigirse a una operadora para conocer el IP utilizado es necesario obtener autorización judicial, conforme a las previsiones de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones[245], la cual exige autorización judicial para acceder no sólo a los datos de tráfico (terminales conectados, identificación de los usuarios y datación de la comunicación), sino también a otros que podrían ser calificados como servicios de valor añadido.

En el marco jurídico vigente, toda investigación policial o del Ministerio Fiscal para el esclarecimiento de un hecho delictivo que requiera la cesión de alguno de los datos almacenados por las operadoras a los que se refiere la Ley 25/2007, de 18 de octubre, afecten o no al secreto de las comunicaciones, exigirá autorización del Juez de Instrucción.

244 La STS (Sala 2ª) de 18 marzo de 2010 concluye que los datos relativos a la identificación del usuario que tiene asignada una determinada IP no afectan al secreto de las comunicaciones dado que no interceptan ni tratan de descubrir una concreta comunicación.

245 Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado, sobre Pautas en relación con la Diligencia de Intervención de las comunicaciones telefónicas.

3. Por lo que respecta al IMSI[246] e IMEI[247], señalar que la información contenida en la serie IMSI e IMEI no puede catalogarse como dato externo integrable en el contenido del derecho al secreto de las comunicaciones, de modo que la captación de IMSI e IMEI puede llevarse a efecto por la Policía Judicial sin necesidad de mandamiento judicial.

Sin embargo, para que los operadores telefónicos puedan ceder datos sobre IMSI e IMEI es necesaria autorización judicial.

3.1.3.- El acceso a mensajes que estén en poder de los comunicadores.

1. Entiende el Tribunal Constitucional que el fundamento del secreto de las comunicaciones se encuentra en la especial vulnerabilidad de su confidencialidad en la medida en que son posibilitadas mediante la intermediación técnica de un tercero ajeno a la comunicación[248]. De acuerdo con este razonamiento, la garantía del secreto de las comunicaciones sólo opera en relación con el acceso al mensaje y a los datos de la comunicación protegidos que ataque esa "especial vulnerabilidad"[249] aprovechándose de la intermediación técnica de un tercero ajeno a la comunicación[250].

246 IMSI es el acrónimo de *International Mobile Subscriber Identity* (Identidad Internacional del Abonado Móvil). Es un código de identificación único para cada dispositivo de telefonía móvil, integrado en la tarjeta SIM, que permite su identificación a través de las redes GSM y UMTS.

247 El IMEI (del inglés *International Mobile Equipment Identity*, identidad internacional de equipo móvil) es un código USSD pregrabado en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta.

248 En este sentido, vid. SSTC 123/2002, de 20 de mayo y 281/2006, de 9 de octubre.

249 DÍAZ REVORIO, F. J., "El derecho fundamental al secreto de las comunicaciones", *Derecho PUCP, Revista de la Facultad de Derecho*, nº 59, 2006, pág. 160.

250 VEGAS TORRES, J., Obtención de pruebas en ordenadores personales…*op. cit*., pág. 49.

Dado que el Tribunal Constitucional limita la garantía del secreto de las comunicaciones a los datos obtenidos a través de la interceptación de las comunicaciones[251], de ahí cabe deducir que quedan excluidas del ámbito del derecho al secreto de las comunicaciones el acceso a aquellos contenidos de la comunicación que no se produzcan mediante la interceptación del proceso comunicativo[252], por lo que no puede considerarse vulneración del secreto de las comunicaciones la escucha, sin utilización de ningún artificio, de una conversación telefónica o directa por hallarse el que las oye en las inmediaciones del lugar en que se produce.

Del mismo modo, en caso de llamada telefónica, la visión del número emisor que automáticamente aparece en la pantalla del receptor al margen de la voluntad de quien llama y perceptible por cualquiera que tenga a la vista el aparato no entraña interferencia en el ámbito privado de la comunicación.

Para una mejor exposición distinguiremos entre mensajes en poder del emisor de aquéllos otros que ya están en poder del destinatario.

3.1.3.1.- Mensajes en poder del emisor.

1. El rechazo de la aplicación de la garantía del derecho al secreto de las comunicaciones a aquellos mensajes que aún estén en poder del remitente se establece en la STC 137/2002, de 3 de junio, referida a un caso en el que los agentes de la Guardia Civil detectaron la presencia en una delegación de Correos de una persona que estaba siendo investigada en el preciso instante en el que la misma se disponía a remitir un paquete postal. Dicha persona, al

251 En este sentido, SSTC 70/2002, de 3 de abril, que entiende que la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación, pero una vez finalizado este, la protección constitucional de lo recibido se realiza vía derecho a la intimidad u otros derechos; en idéntico sentido, SSTC 123/2002, de 20 de mayo y 56/2003, de 24 de marzo.

252 VEGAS TORRES, J., Obtención de pruebas en ordenadores personales…*op. cit.*, pág. 49.

ser requerida por los agentes, accede a abrir el paquete postal. En el recurso de amparo se argumentaba que la actuación de la Guardia Civil había infringido el secreto de las comunicaciones, lo que el TC rechaza argumentando al efecto que en dicho caso no se había operado interferencia alguna en el proceso comunicativo dado que el paquete postal se había interceptado y abierto antes de ser depositado el mismo en la oficina de Correos para su remisión al destinatario.

Si bien la lesión del derecho al secreto de las comunicaciones la podría haber descartado el Tribunal Constitucional por el hecho de haber sido abierto el paquete postal mediando consentimiento del portador, aquél atiende, sin embargo, al hecho de que el acceso de los agentes de la Guardia Civil al paquete postal tiene lugar mientras el mismo aún está en poder del remitente antes de ser entregado al personal del servicio de correos, por lo que no hay interferencia alguna en el proceso comunicativo.

Posteriormente, el Tribunal Constitucional vuelve a excluir la aplicación de la garantía del secreto de las comunicaciones a los mensajes mientras estos están poder del remitente en la sentencia 281/2006, de 9 de octubre, la cual aborda las cuestiones suscitadas por el art. 18.3 CE en relación con las comunicaciones postales, señalando la misma que la protección que otorga el derecho al secreto de las comunicaciones abarca a cualquier forma de interceptación mientras dure el proceso comunicativo, citando expresamente la STC 137/2002, de 3 de junio, y precisando que cualquier objeto que pueda servir de soporte de la comunicación postal – v. gr. sobre, carta, paquete, etc. - sólo será objeto de la protección dispensada por el art. 18.3 CE si, atendidas las circunstancias concretas del caso, constituyere instrumento de la comunicación o si el proceso comunicativo hubiera sido ya iniciado.

2. No obstante, entendemos de conformidad con lo señalado en la Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado, sobre

Pautas en relación con la Diligencia de Intervención de las comunicaciones telefónicas,[253] que el acceso a un correo electrónico aún no leído por su receptor, con independencia del momento preciso del proceso comunicativo en que se encontrare - ya estuviere escrito y almacenado en el ordenador personal o en el terminal telefónico pendiente de ser enviado a su destinatario final, o enviado y recibido, hubiere sido o no leído por el destinatario -, supone una injerencia en el secreto de las comunicaciones[254], de modo que debe considerarse necesaria la autorización judicial para acceder a cualquier mensaje enviado por correo electrónico, ya se trate de correo electrónico enviado y recibido pero no leído, correo en fase de transferencia o correo ya enviado, recibido y leído y que se encuentra almacenado.

Y lo mismo sucede con los mensajes almacenados en la carpeta denominada "enviados" una vez que han sido remitidos al destinatario, respecto de los cuales se predica que los mismos forman parte de un proceso de comunicación ya iniciado, de modo que el acceso a los mismos compromete el derecho al secreto de las comunicaciones[255]. No es tan claro, sin embargo, el tratamiento que haya de darse al acceso al contenido de un correo que ya hubiese sido leído por su receptor, habiéndose defendido al efecto que el

253https://www.seguridadpublica.es/2013/03/sobre-pautas-en-relacion-con-la-diligencia-de-intervencion-de-las-comunicaciones-telefonicas/

254 En sentido contrario VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…op. cit.,* pág. 51, que considera que las sentencias referidas hacen referencia al hecho de que el mensaje aún no ha sido enviado. Y esta exclusión de la protección del derecho al secreto de las comunicaciones frente al acceso a mensajes a través de soportes que estuvieren en poder del remitente tiene trascendentales repercusiones en el ámbito de las comunicaciones telemáticas, permitiendo poder resolver en sentido negativo la cuestión de si están protegidos por el referido derecho los mensajes de correo electrónico no enviados mientras se encuentran almacenados en la carpeta denominada "borradores" habida cuenta de que los mismos no forman aún parte de ningún proceso de comunicación, pudiendo aquéllos quedar almacenados sine die, por voluntad del remitente, en la citada carpeta antes de llegar a ser enviados, de modo que en estos casos no se opera ninguna interceptación que esté prohibida por el art. 18.3 CE. No obstante, sí podría existir en este caso una posible vulneración del derecho a la intimidad personal del art. 18.1 CE.

255 En sentido contrario, VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 52, por entender que lo que queda en la carpeta denominada "mensajes enviados" es únicamente una copia de los mensajes remitidos al objeto de que el remitente pueda disponer de un archivo de sus propias comunicaciones con el fin de revisarlas cuando lo estime pertinente, pero en ningún caso el acceso a esos mensajes almacenados supone una interferencia en el proceso comunicativo.

mismo queda fuera del ámbito de protección del art. 18.3 CE habida cuenta de que se entiende concluso el proceso comunicativo, estando sólo protegidos por el derecho a la intimidad (en el mismo sentido, en relación con el correo ordinario, se manifiesta la STC 70/2002, de 3 de abril)[256].

No obstante, razones de prudencia aconsejan solicitar siempre la preceptiva autorización judicial para acceder a cualesquiera mensajes enviados por correo electrónico dado lo difícil de deslindar ambos tipos de correo (Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado), conclusión esta que se refuerza por el hecho de que el propio Tribunal Constitucional ha concedido protección a los datos externos del proceso de comunicación una vez concluso el mismo, de modo que si se protegen éstos, con más razón habrá de protegerse el contenido de la comunicación ya finalizada.

3.1.3.2.- Mensajes en poder del destinatario.

1. Si se atiende únicamente al hecho de que el derecho al secreto de las comunicaciones protege a éstas de su interceptación solamente mientras exista un proceso de comunicación en curso, ello parece dejar fuera del campo de aplicación del art. 18.3 CE a los mensajes que ya obren en poder del destinatario y hayan sido leídos por el mismo.

A tal efecto, el Tribunal Constitucional ha llegado a sostener en diferentes ocasiones que una vez finalizado el proceso comunicativo, la protección de lo recibido no se efectúa a través del secreto de las comunicaciones, sino que se realiza vía normativa que tutela el derecho a la intimidad u otros derechos[257], habiendo aplicado este criterio en su sentencia

256 Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado, sobre Pautas en relación con la Diligencia de Intervención de las comunicaciones telefónicas.

257 SSTC 70/2002, de 3 de abril; 123/2002, de 20 de mayo, y 56/2003, de 24 de marzo.

70/2002, de 3 de abril, al objeto de rechazar cualquier tipo de lesión en el secreto de las comunicaciones postales en un supuesto de aprehensión, por parte de miembros de la Guardia Civil, de una carta que estaba en poder del investigado, la cual fue leída por los agentes sin contar con autorización judicial, sosteniendo en este caso que la intervención objeto de análisis no supone una interferencia del proceso comunicativo por haberse consumado ya el mismo[258].

2. No obstante, cabe señalar la existencia de demasiadas contradicciones en la jurisprudencia del Tribunal Constitucional referente al tema en cuestión como para sostener de modo indubitado que el derecho al secreto de las comunicaciones protege a éstas de su interceptación única y exclusivamente mientras exista un proceso de comunicación en curso.

En este sentido, la STC 114/1984, de 29 de noviembre, afirmaba que el derecho al secreto de las comunicaciones puede resultar vulnerado tanto por la interceptación en sentido estricto – aprehensión física del soporte del mensaje – como por el mero conocimiento antijurídico de lo comunicado –apertura de la correspondencia ajena guardada por su destinatario -, lo cual resulta contradictorio con lo sostenido en la posterior STC 70/2002, de 3 de abril, que sostiene que, finalizado el proceso comunicativo, la protección constitucional de lo recibido se realizará, en su caso, a través de las normas que tutelan la intimidad u otros derechos[259].

Asimismo, también resulta contradictoria la STC 230/2007, de 11 de noviembre, en la que se analizaba la vulneración del secreto de las comunicaciones por los agentes de la Guardia Civil, los cuales, tras detener a los investigados, intervinieron los teléfonos que portaban los mismos para

258 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 49.

259 VEGAS TORRES, J., *Idem.,* pág. 53.

acceder al registro de llamadas y confeccionar un listado de las enviadas, recibidas y perdidas sin contar con el consentimiento de los titulares de los teléfonos ni con la preceptiva autorización judicial[260].

En este caso, el TC consideró que se había producido una vulneración del derecho al secreto de las comunicaciones entendiendo que resulta de todo punto necesario el consentimiento del titular del teléfono móvil para acceder al listado de llamadas enviadas, recibidas y perdidas o bien contar con la debida autorización judicial, corrigiendo de este modo la STC 70/2002, de 3 de abril.

3. Por su parte, el TS también ha tenido ocasión de enfrentarse a casos en los que el acceso a los mensajes tuvo lugar, una vez concluso el proceso de comunicación, a través de soportes que estaban en poder del destinatario del mensaje, mostrándose ambivalente en sus decisiones dado que, si bien en un primer momento entendió que no resultaba vulnerado el derecho al secreto de las comunicaciones[261], posteriormente la STS (Sala 2ª) de 8 de abril de 2008, apreció vulneración del citado derecho en un caso en el que los agentes de la Guardia Civil llevaron a cabo, sin la preceptiva autorización judicial, una diligencia de cotejo de teléfonos móviles y de registro de su agenda de números y mensajes, invocando expresamente el precedente de la STC 230/2007, de 11 de noviembre, para con posterioridad, reafirmar la línea jurisprudencial anterior[262].

No obstante, más recientemente, las SSTS (Sala 2ª) de 5 de febrero de 2010 y de 11 de marzo de 2010, sostienen que el acceso al registro de llamadas de un teléfono móvil sin contar para ello con el consentimiento del titular o sin la preceptiva autorización judicial vulnera el secreto de las

260 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 54.

261 En este sentido, vid., entre otras, las SSTS (Sala 2ª) de 7 de octubre y de 25 de noviembre de 2008.

262 Vid. entre otras, las SSTS (Sala 2ª) de 10 de febrero, 8 de junio, 17 y 18 de diciembre de 2009 y de 26 de enero de 2010.

comunicaciones. Y, con más contundencia, se reafirma en un caso similar la STS (Sala 2ª) de 13 de mayo de 2010, poniendo especial énfasis en que, conforme a la doctrina del TEDH, los datos averiguados son "datos externos" de la comunicación protegidos por la garantía del secreto[263].

Así pues, el acceso a la libreta de contactos de un teléfono móvil no supone una injerencia en el secreto a las comunicaciones. Por el contrario, el acceso a los datos de registro de llamadas de un teléfono móvil supone una injerencia en el secreto de las comunicaciones. Y el acceso a los mensajes contenidos en el teléfono móvil de los detenidos, hayan sido o no leídos, exigirá autorización judicial.

No obstante, me parece necesario precisar dos aspectos que suscitan algunas de las sentencias comentadas, a saber: de un lado, la relevancia que pudiera tener el hecho de que la comunicación haya finalizado y, de otro, tratándose del acceso a mensajes que obren en poder del destinatario, que éste hubiere leído o no el mensaje.

3.1.4.- La finalización del proceso de comunicación.

Como ha quedado dicho, algunas sentencias del TC parecen vincular la operatividad del derecho al secreto de las comunicaciones con el hecho de que el proceso comunicativo haya finalizado o no, lo cual parece deducirse del contenido de las SSTC 70/2002, de 3 de abril; 123/2002, de 20 de mayo, y 56/2003, de 24 de marzo, ya analizadas, en las que se afirmaba que la protección del derecho al secreto de las comunicaciones alcanza al proceso comunicativo, pero una vez finalizado el mismo, la protección constitucional de lo recibido se realizará, en su caso, a través de las normas que tutelan la intimidad u otros derechos.

263 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 59.

Aun no siendo así exactamente[264], el hecho de que el acceso al mensaje protegido haya tenido lugar una vez concluso el proceso comunicativo no excluye de por sí que la fuente de conocimiento del contenido del mismo se hubiere obtenido interceptando la comunicación en su discurrir a través del servicio que la conduce a su destino. Si así fuere habría que entender violado el secreto de las comunicaciones pese a que el acceso a lo comunicado hubiere tenido lugar tras la recepción del mensaje por el destinatario.

A tal efecto, el propio TS, refiriéndose al acceso al listado de llamadas de un teléfono móvil, entiende que si el mismo se solicitare a la compañía telefónica operaría el secreto de las comunicaciones[265], en tanto que si se accediere a él a través del teléfono móvil en poder del usuario no entraría en juego el citado derecho fundamental sino el derecho a la intimidad[266], lo cual no deja de ser paradójico. Pues bien, a tal efecto hemos de señalar que el acceso al listado de llamadas facilitado por la compañía telefónica se produce, obligatoriamente, una vez que las llamadas que aparecen referenciadas en dicho listado han finalizado, lo cual no impide que se considere afectado el derecho al secreto de las comunicaciones.

Sin embargo, la Consulta 1/1999, de 22 de enero, de la Fiscalía General del Estado, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones, referida a la posibilidad de que los Fiscales, en el marco de una investigación pre-procesal, puedan solicitar listados de llamadas a los operadores telefónicos sin necesidad de autorización judicial se opone al argumento de que, finalizada la comunicación, cese el secreto de las comunicaciones, de modo que la entrega de listados de llamadas por las

264 Recuérdese la ambivalencia, antes referida, de la jurisprudencia tanto del Tribunal Constitucional como del Tribunal Supremo al respecto. En concreto, SSTC 114/1984, de 29 de noviembre y 230/2007, de 11 de noviembre; SSTS (Sala 2ª) de 8 de abril de 2008; de 5 de febrero de 2010 (Sala 2ª), de 11 de marzo de 2010 (Sala 2ª) y de 13 de mayo de 2010 (Sala 2ª).

265 STS (Sala 2ª) de 28 de junio de 2007, entre otras.

266 STS (Sala 2ª) de 30 de noviembre de 2005, entre otras.

compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requiere resolución judicial habida cuenta de que la protección constitucional del secreto de las comunicaciones se extiende, con carácter indefinido, al mensaje y resto de datos de la comunicación, los cuales se encuentran protegidos aun después de finalizada ésta[267].

3.1.5.- Relevancia o no del conocimiento efectivo del contenido del mensaje por parte del destinatario.

1. Cuando el contenido del mensaje hubiese sido conocido a través de soportes que ya obraren en poder del destinatario, cierta jurisprudencia del Tribunal Supremo parece conceder relevancia al hecho de que el destinatario hubiere accedido al referido soporte y, por tanto, hubiere tenido conocimiento del contenido de aquél o, por el contrario, aun estando éste a su disposición, no hubiere accedido a su contenido y no conociera aún el mensaje.

Según esta corriente jurisprudencial, el conocimiento de lo comunicado por terceras personas a través del soporte obrante en poder del destinatario no afectaría al secreto de las comunicaciones en el primero de los casos, en tanto que sí lo haría en el segundo[268]. Este criterio ha sido el aplicado al acceso a mensajes tipo SMS almacenados en el teléfono del destinatario, partiéndose de la circunstancia de que el listado de mensajes que exhibe aquél indica, respecto de cada mensaje recibido, si ha sido abierto o no, entendiéndose

267 En sentido contrario VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit.,* pág. 61, que entiende que el criterio a seguir en orden a delimitar si el secreto de las comunicaciones resulta o no afectado es si los datos de la comunicación a los que se accede han sido obtenidos con o sin interferencia del proceso comunicativo. En el primer caso resultaría afectado el derecho al secreto de las comunicaciones aunque el acceso a esos datos tuviere lugar una vez que la comunicación hubiere finalizado, en tanto que en el segundo caso, el secreto de las comunicaciones no se vería afectado. Y ello con independencia de que el acceso a los mismos se hubiere producido antes o después de terminar el proceso comunicativo.

268 Este enfoque está presente, por ejemplo, en la STS (Sala 2ª) de 7 de octubre de 2008.

relevante este dato a efectos de considerar o no que el acceso a los mismos pueda afectar al derecho al secreto de las comunicaciones[269].

El soporte jurisprudencial que analizamos parte de la base de que el derecho al secreto de las comunicaciones se circunscribe a la consecución del contenido de la comunicación a través de su interceptación en algún momento de su recorrido desde el remitente hasta el destinatario, entendiendo que aquélla no llega al destinatario hasta que éste accede de modo efectivo al contenido del mensaje y lee el mismo, de manera que el acceso por terceras personas ajenas a la comunicación antes de ese momento supone una interceptación de ésta[270].

2. A nuestro entender resulta completamente desacertado este criterio que vincula la operatividad del secreto de las comunicaciones a la circunstancia de que los mensajes hayan sido o no leídos por el destinatario de los mismos habida cuenta de que el fundamento de la garantía del secreto de las comunicaciones no radica precisamente en el expreso conocimiento del contenido del mensaje por parte de su destinatario, como se ha visto con anterioridad[271]. A tal efecto, cabe recordar la Consulta 1/1999, de 22 de enero, de la Fiscalía General del Estado[272], que rechaza el argumento consistente en

269 Este es, precisamente, el sentido en el que se manifiestan las SSTS (Sala 2ª) de 27 de junio de 2002, de 10 de febrero y de 8 de junio de 2009. Ésta última, por ejemplo, concede relevancia al conocimiento del mensaje por su destinatario afirmando que en los casos en los que el mensaje estuviere almacenado en el terminal de aquél y hubiere sido abierto y leído por él, en la medida en que ya se ha agotado el proceso comunicativo, su protección constitucional tiene lugar vía garantía de la intimidad y no a través del secreto de las comunicaciones.

270 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit*., pág. 63.

271 En sentido contrario, VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…, op. cit*., pág. 63, que entiende acertado el criterio jurisprudencial que vincula la operatividad del secreto de las comunicaciones, en relación con el acceso a mensajes que obren en poder del destinatario, al hecho de que los mensajes hayan sido o no leídos por éste habida cuenta de que el fundamento de la garantía del secreto de las comunicaciones radica precisamente en el expreso conocimiento del contenido del mensaje por parte de su destinatario.

272 La Consulta 1/1999, de 22 de enero, de la Fiscalía General del Estado, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones, hace referencia a la posibilidad de que los Fiscales, en el marco de una investigación pre-procesal, puedan solicitar listados de llamadas a los operadores telefónicos sin necesidad de

considerar que la finalización de la comunicación suponga el cese del secreto de las comunicaciones habida cuenta de que la protección de éste se extiende con carácter indefinido tanto al mensaje como al resto de datos de la comunicación, los cuales se encuentran protegidos aun después de finalizada aquélla.

Por lo demás, señalar que en la jurisprudencia analizada no hay casos que se refieran directa y expresamente a comunicaciones vía correo electrónico, siendo verdaderamente complicado trasladar a este modelo comunicativo cuanto se lleva expuesto hasta ahora en cuanto a la protección constitucional dispensada por el derecho al secreto de las comunicaciones.

Baste recordar que un mensaje de correo electrónico puede ser recibido, abierto y leído por su destinatario y, seguidamente, volverlo a cerrar y colocarle la etiqueta de "no leído", por lo que resulta imposible saber si el contenido del mensaje ha sido conocido o no por su receptor, de modo que podemos concluir señalando que el derecho al secreto de las comunicaciones resulta violado tanto por el acceso a mensajes almacenados en la carpeta de "mensajes enviados" del remitente como por acceder a los mismos vía carpeta de "mensajes recibidos" del destinatario, si bien se ha de reseñar que cierta jurisprudencia del TS diferencia en función de si se trata de mensajes abiertos o no abiertos por éste, entendiendo que, en este último caso, el mensaje sí estaría protegido por el derecho al secreto de las comunicaciones, en tanto que en el primer caso la jurisprudencia se muestra ambivalente[273].

requerir autorización judicial para ello, lo cual dependerá siempre de que la entrega de los listados por dichos operadores telefónicos afecte o no al secreto de las comunicaciones.

273 No obstante, hay que hacer notar que, como se ha dicho, un mensaje de correo electrónico puede ser abierto y leído y, seguidamente, volver a ser cerrado y poner la etiqueta de "no leído" por parte de su destinatario, de modo que este criterio difícilmente ofrece garantía alguna de cara a poder valorar si se ha vulnerado o no el secreto de las comunicaciones.

3.1.6.- Secreto de las comunicaciones y medios digitales de titularidad del trabajador.

1. El progreso de la tecnología está conduciendo al uso creciente por los trabajadores de sus propios dispositivos electrónicos en el puesto de trabajo, fenómeno que se conoce como *BYOD (Bring Your Own Device*: trae tu propio dispositivo). Obviamente, resulta muy complicado desentrañar la complejidad de este fenómeno[274]. Aquí sólo interesa plantear el aspecto relativo al control del secreto de comunicaciones en estos casos, de modo que la cuestión que se plantea es si el control del uso de las herramientas informáticas por parte del empresario puede hacerse del mismo modo e intensidad que respecto de los dispositivos que sean de su titularidad.

De un lado, se puede argumentar que se trata de una cuestión de grado de control, no de modelo de garantías, atendiendo a que la titularidad dominical no desvanece la sujeción del trabajador al poder de control del empresario, de modo que el art. 20.3 ET seguiría manteniendo su vigor en estos casos. Y, de otro lado, se puede entender también que, tratándose de un dispositivo personal, habría que aplicar el art. 18 ET, sobre todo si se realiza sobre una red privada virtual[275].

No obstante, sin desconocer la razonabilidad de esta segunda opción, parece necesario reforzar el papel del consentimiento, tanto del trabajador como del empleador, en orden a su utilización a fin de evitar situaciones de empleos no consentidos de la tecnología personal - que plantearía problemas análogos a los suscitados por los usos privados de las tecnologías en la

274 INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE), Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario, Madrid, 2017.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

275 MOLINA NAVARRETE, C., "El derecho al secreto de las comunicaciones en la relación de trabajo…", *op. cit.,* pág. 17.

empresa-[276]. Y ello no sólo por la titularidad del dispositivo, sino también por la coexistencia con informaciones estrictamente privadas, volviéndose éstas vulnerables de no existir ese consentimiento previo o, alternativamente, la autorización judicial[277].

En consecuencia, toda implantación del *BYOD* - hoy minoritaria, pero en un futuro cercano muchas empresas la tendrán - requiere ponderar, junto a los mayores riesgos de inseguridad, el menor poder de control sobre los contenidos de las comunicaciones en estos dispositivos, viendo los trabajadores incrementados, consecuentemente, su disposición sobre tales recursos tecnológicos mixtos - personales y profesionales -. En todo caso, esto no significa que el empleador pierda su poder de ejercer el poder disciplinario ante eventuales infracciones con este tipo de dispositivos, dentro o fuera del trabajo (v. gr. STSJ Aragón 350/2016, 18 de mayo, FJ 5º).

4.- El derecho a la protección de datos personales.

4.1.- Su autonomía frente al derecho a la intimidad.

1. La protección del derecho a la intimidad se ve acompañada por otro derecho fundamental, cual es el derecho a la de autodeterminación informativa, que implica el consentimiento y control de la utilización de datos personales[278]. Este derecho pretende garantizar a la persona un poder de disposición y control sobre sus datos personales, así como sobre su uso y destino con el objetivo de impedir su tráfico ilícito y/o lesivo para su dignidad y derechos, no

276 Vid. ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 2/2017 on data processing at work, Brussels (Belgium), (17/EN – WP 249), págs. 6-8.

277 Para un análisis global vid. PUYOL MONTERO, J., *Una aproximación a la técnica BYOD y al control estratégico de las nuevas tecnologías en la empresa*, Tirant lo Blanch, Valencia, 2015.

278 OLLERO TASSARA, A., ¿Son jurídicos los derechos humanos?, *Revista SCIO*, nº 4, 2009, págs. 141-142.

reduciéndose el mismo únicamente a datos íntimos, sino que abarca cualquier tipo de dato personal cuyo conocimiento por terceros pueda afectar a sus derechos, sean o no fundamentales[279]. No obstante, hemos de señalar que el derecho a la protección de datos excede al derecho a la intimidad, pues su ámbito instrumental de aplicación no sólo está referido al ejercicio de este derecho, sino también al de otros derechos fundamentales, siendo, pues, el derecho a la protección de datos un derecho específico y distinto al derecho a la intimidad.

Ello se debe a que, como el propio TC reconoce en su sentencia 292/2000, de 30 de noviembre –que resuelve recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra determinados preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal–, tanto el derecho a la intimidad o el derecho a la vida privada, como otros derechos fundamentales, tienen una dimensión positiva que reclama un control sobre los datos relativos a la propia persona, sobre su uso y destino con el fin de impedir su trato ilícito y lesivo para la dignidad de la persona cuyos datos se tratan. De ahí, como señala la sentencia referida, la singularidad y especificidad del derecho a la protección de datos, cuyo objeto es más amplio que el del derecho a la intimidad, ya que aquél extiende sus garantías no sólo a la intimidad, sino a cualquier ámbito de los bienes de la personalidad, que puedan verse vulnerados con el uso inadecuado de estos datos.

Por ello, todo dato de carácter personal que identifique o permita la identificación de una persona debe ser protegido por el derecho a la protección de datos[280], pues dichos datos pueden servir para la confección de su perfil

279 STC 292/2000, de 30 de noviembre.

280 A este respecto, la AEPD ha señalado que si es posible deducir de las listas que contienen los resultados obtenidos por productividad, proporcionadas por el empleador a los trabajadores y que son publicadas a través del tablón de anuncios o en Internet, la identidad de los empleados, sin realizar para ello esfuerzos desproporcionados, deben ser elaboradas y difundidas únicamente son el consentimiento de los trabajadores involucrados, salvo que el Comité de Empresa se pronuncie considerando estas medidas como controles que efectúa el propio empresario a su trabajador al amparo del art. 20.3 ET, en cuyo caso la cesión vendría amparada en el mencionado artículo. *Vid.*

ideológico, económico, sexual, racial o de cualquier otra índole que, usado en ciertas condiciones o circunstancias, puede llegar a constituir una amenaza para el individuo, por lo que este derecho otorga a su titular un haz de facultades que le confieren la potestad de ejercer un poder de disposición y control sobre sus datos personales, facultándolo para decidir cuáles de estos datos proporciona a un tercero, ya sea el Estado o un particular, pudiendo conocer aquél en todo momento quién posee esos datos personales y para qué, así como oponerse a esa posesión o uso[281].

De este modo, aunque el derecho a la protección de datos tiene sus propias peculiaridades que lo convierten en un derecho con un contenido específico y con un sistema de protección propio, dichas características coexisten con la función de garantía instrumental de otros derechos en razón de los riesgos de lesión de determinados derechos fundamentales que, por ejemplo, el tratamiento de datos personales a través de la introducción de las nuevas tecnologías pueden producir en sus titulares[282].

2. En cuanto a los caracteres del derecho a la protección de datos, señalar que se trata de un derecho fundamental relacionado con la vida privada, pero independiente y distinto de ésta, tiene carácter universal, está vinculado a la dignidad humana y, por tanto, de titularidad de las personas físicas, sean nacionales o extranjeras[283], que tiene por objeto garantizar la libertad del individuo en relación a su autodeterminación respecto del tratamiento de sus datos personales por terceros y que presenta como contenido un conjunto de facultades consistentes, en su mayoría, en el poder jurídico de imponer a terceros la realización u omisión de determinados

---

Agencia Española de Protección de Datos, *Informe Nº 0529-2009: Comunicaciones de la productividad de los trabajadores a otros trabajadores*, AEPD, Madrid, 2009. En http://www.agpd.es.

281 APARICIO ALDANA, R. K., *Derecho a la intimidad y a la propia imagen…*, *op. cit.,* pág. 88.

282 DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, pág. 81.

283 SSTC 292/2000, de 30 de noviembre y 17/2013, de 31 de enero.

comportamientos clasificables como acceso, rectificación, cancelación u oposición[284].

Por ello, el uso empresarial de los datos personales de los empleados ha de ir acompañado de un control, por parte de los trabajadores, sobre su uso, más aún cuando, con el surgimiento de las nuevas tecnologías, los empresarios, para facilitar sus actividades de gestión del personal, cuentan con soportes informáticos que les facilitan almacenar gran cantidad de datos, cruzarlos y tratar información, lo que les permite ir más allá de lo que el propio dato revela, haciendo más sencilla la labor de entrelazar datos no íntimos o que aislados no tengan mayor importancia, pero que entrecruzados pueden ofrecer un retrato de la personalidad o de la historia del individuo que éste tiene derecho a mantener en reserva[285].

3. El derecho a la protección de datos no es, por lo demás, un derecho absoluto, sino limitado[286] (art. 52.1 CDFUE y art. 8 CEDH)[287], estando sujeto a limitaciones de origen legal por norma con rango de ley accesible y previsible. Limitaciones que, por otro lado, han de responder a una necesidad imperiosa, debiendo ser adecuadas y proporcionadas al logro de ese propósito, en definitiva, indispensables en una sociedad democrática[288]. Entre tales limitaciones la jurisprudencia ha considerado legítimas la seguridad del

284 PRECIADO DOMENECH, C. H., *El derecho a la protección de datos en el contrato de trabajo*, Thomson Reuters Aranzadi, Pamplona, 2017, pág. 36.

285 PÉREZ DE LOS COBOS ORIHUEL, F., *Nuevas tecnologías y relación de trabajo*, Tirant lo Blanch, Valencia, 1990, pág. 73.

286 SSTJUE de 24 de noviembre de 2011 (caso Asociación Nacional de Establecimientos Financieros de Crédito, Asuntos C-468/10 y C-469/10) y de 9 de noviembre de 2010 (caso Volker und Markus Schecke GbR y Hartmut Eifert c. Land Hessenm, Asuntos acumulados C-92/09 y C-93/09, de 9 de noviembre de 2010).

287 Sobre las limitaciones del derecho en el nuevo Reglamento *vid.* Art. 24 Reglamento 679/2016, que se corresponde con el art. 13 de la Directiva 95/46.

288 SSTEDH de 26 de marzo de 1985 (caso X e Y c. Países Bajos), de 26 de marzo de 1987 (caso Leander c. Suecia), de 7 de junio de 1989 (caso Gaskin c. Reino Unido) y de 25 de febrero de 1983 (caso Funke c. Francia).

Estado[289], la persecución de infracciones penales o la distribución equitativa del sostenimiento del gasto público, entre otras.

4.2.- Sus diferencias respecto al derecho a la intimidad.

1. La protección de datos personales ostenta, en el ordenamiento jurídico español, la naturaleza de derecho fundamental. Así, el Tribunal Constitucional estableció la existencia de este derecho fundamental en diferentes sentencias -desde la STC 254/1993, de 20 de julio, hasta la mencionada STC 292/2000, de 30 de noviembre-, configurándolo como un derecho de naturaleza instrumental de textura abierta que se relaciona con el entero sistema de derechos fundamentales[290] y fundamentándolo en el art. 18.4 de la CE, siendo en esta última resolución en la que se perfilan las características más importantes de su régimen jurídico, distinguiéndolo del derecho a la intimidad en base a tres criterios diferenciales: diferencias en la función, en el objeto y en el contenido[291].

2. Por otro lado, el Tribunal Constitucional establece que tanto el derecho a la intimidad como el derecho a la protección de datos no son derechos incompatibles, si bien los mismos presentan perfiles diferentes, residiendo la peculiaridad del derecho a la protección de datos respecto del derecho a la intimidad en su distinta función, ya que si bien éste protege al individuo frente a cualquier acto de injerencia que pudiera efectuarse en aquellos aspectos de su vida personal y familiar que desee excluir de intromisiones de terceros en contra de su voluntad, aquél, por el contrario, lo que persigue es garantizar al

289 STEDH de 26 de marzo de 1987 (caso Leander c. Suecia).

290 MARTÍNEZ MARTÍNEZ, R., ¿Minusvaloramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales?, *La Ley*, nº 9329, Sección Tribuna, 3 de enero de 2019.

291 LÓPEZ JIMÉNEZ, D., "Los Códigos Tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el Derecho español", en *Estudios Constitucionales*, año 11, nº 2, 2013, Centro de Estudios Constitucionales de Chile Universidad de Talca, pág. 587.

individuo un poder de disposición y control sobre sus datos personales, su uso y destino, con la finalidad de impedir su tráfico ilícito y/o lesivo para su dignidad[292].

3. Asimismo, la distinción que se advierte obedece también a la especialidad del objeto que protege, el cual es más amplio en el caso de la protección de datos habida cuenta de que el objeto de protección no se circunscribe solamente a los datos más íntimos o privados del individuo, sino a cualquier tipo de dato de carácter personal, íntimo o no, cuyo conocimiento o uso por terceros pudiere afectar a sus derechos, sean o no estos fundamentales.

4. Por último, existe también una importante diferencia en cuanto al elenco de facultades que atribuyen ambos derechos. Así, mientras el derecho a la intimidad confiere a su titular el poder jurídico de imponer a terceros un deber de abstención de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo conocido, el derecho a la protección de datos atribuye a aquél un haz de facultades que engloba diversos poderes jurídicos cuyo ejercicio impone, a su vez, a terceros deberes jurídicos que no se incluyen en el anterior[293].

5. Obsérvese que no estamos hablando tanto de la privacidad de los ciudadanos en su esfera de intimidad personal frente a terceros o en sus comunicaciones, sino ante las garantías constitucionales de que sus datos personales, integrados en cualquier soporte no puedan ser destinados, sin su consentimiento, a fines distintos de aquéllos para los que fueron revelados. Sin embargo, en la práctica –como la experiencia judicial y constitucional pone en evidencia– no siempre resulta fácil diferenciar en el mundo laboral, cuando

292 LÓPEZ JIMÉNEZ, D., "Los Códigos Tipo como instrumento para la protección de la privacidad…, *op. cit*, pág. 588.

293 LÓPEZ JIMÉNEZ, D., *Idem., Ibidem.*

existen grabaciones, los límites entre los apartados 1 y 4 del art. 18 CE, estándose, generalmente, en estos casos ante un concurso real de derechos.

En efecto, un registro video gráfico en un vestuario afecta, sin duda, al derecho a la intimidad en forma absoluta. De similar manera, una grabación en el puesto de trabajo también puede hacerlo –tal y como se desprende de la STC 98/2000, de 10 de abril–. Ahora bien, si como es la práctica habitual, las imágenes así obtenidas se almacenan en una base de datos, aparecen también las dudas de la posible afectación al derecho a la protección de datos, como antes se ha indicado[294].

4.3.- Afectación del derecho a la protección de datos personales.

1. Para poder determinar la naturaleza de la injerencia en el derecho a la protección de datos derivados de la captación de imágenes y sonidos mediante videocámaras resulta necesario la reunión de todos los elementos del supuesto de hecho de la norma constitucional. Es decir, habrá que examinar si los dispositivos de video vigilancia recogen datos de carácter personal protegidos por el derecho fundamental a la protección de datos, de modo que la relevancia iusfundamental de la video vigilancia dependerá del tipo de dispositivo utilizado[295].

294 FALGUERA BARÓ, M. A., "Nuevas tecnologías y trabajo (II): perspectiva constitucional", *Trabajo y Derecho*, núm. 21, septiembre 2016, pág. 45. Es conveniente indicar que esa base de datos con imágenes supone la creación de un "fichero de datos" (art.3.b) LOPD y, por tanto, sometida a la LOPD. Respecto a la consideración de una imagen como dato y la transmisión de imágenes de trabajadores en su lugar de trabajo mediante una webcam e internet, ver la SAN de 24 de enero de 2003, Sala de lo Contencioso. Asimismo, para una mejor comprensión del problema, véase NAVARRO MARCHANTE, V. J., *El derecho a la información audiovisual de los juicios*, CEPC, 2011, pág. 142.

295 ARZOZ SANTISTEBAN, X., *Videovigilancia, seguridad ciudadana y derechos fundamentales,* Civitas, Madrid, 2010, pág. 137.

Los datos amparados por el derecho a la protección de datos frente a la informática son todos aquellos que identifiquen o permitan identificar a una persona y puedan valer para confeccionar su perfil ideológico, sexual, racial, económico, social o de cualquier otra índole o puedan servir para cualquier otra utilidad que constituya una amenaza para el individuo[296]. La clave está, pues, en la identificación o identificabilidad de la persona, de modo que si las grabaciones de imágenes y los sonidos que captan los dispositivos de video vigilancia identifican o permiten identificar a las personas constituirán datos de carácter personal y se estará penetrando en el ámbito de protección del derecho a la protección de datos personales. Por el contrario, si las imágenes captadas no permitieren identificar personas concretas, la utilización de las cámaras está fuera del ámbito de protección constitucional del citado derecho.

2. Pero la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, requiere algo más para considerar que una grabación de imágenes y sonidos contiene datos de carácter personal en el sentido de la legislación de protección de datos. Así, según su art. 2.1, lo dispuesto en sus Títulos I a IX y en los arts. 89 a 94 de se aplicará a cualquier tratamiento, total o parcialmente automatizado, de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Y, por su parte, el art. 4.6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) define el concepto de “fichero” como todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica, de manera que el criterio decisivo es el de

296 STC 254/1993, de 20 de julio.

conjunto organizado registrado en un soporte físico, por lo que la obtención de imágenes mediante sistemas de grabación digital, bajo el control de un ordenador, puede considerarse tratamiento automatizado en el sentido del art. 2.1 de la Ley Orgánica 3/2018, de 5 de diciembre.

3. En el ámbito de la video vigilancia empresarial, la AEPD ha interpretado que las grabaciones tomadas en el lugar de trabajo constituyen un conjunto organizado porque sabiendo el horario de trabajo de una persona se puede acceder a las imágenes referidas a la persona en cuestión. En este ámbito, las imágenes captadas se pueden relacionar fácilmente con personas determinadas, de modo que la captación de la imagen de los trabajadores a través de cámaras de video vigilancia constituye un dato de carácter personal ya que toda la información captada concierne a la persona y proporciona información sobre la imagen personal de ésta, su lugar de captación y la actividad desarrollada por aquél a quien la imagen se refiere, por lo que la misma se encuentra sometida a las prescripciones previstas en la legislación sobre protección de datos en la medida en que sea objeto de tratamiento[297].

4. Dado que las actividades de video vigilancia laboral caen dentro de la órbita de las facultades de control del empresario reconocidas a éste en el art. 20.3 ET, la captación y tratamiento de imágenes de los trabajadores para controlar el cumplimiento de su prestación laboral serán lícitos, de conformidad con lo dispuesto en el art. 6.1 del Reglamento Europeo de Protección de Datos, si se cumple al menos una de las siguientes condiciones:

a) Que el interesado hubiere prestado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

297 DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B., *Control informático, video vigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, pág. 62.

b) Que el tratamiento resultare necesario para la ejecución de un contrato en el que el interesado fuese parte o para la aplicación, a petición de éste, de medidas precontractuales.

c) Que el mismo fuera necesario para cumplir una obligación legal aplicable al responsable del tratamiento.

d) Que resultara necesario en orden a la protección de intereses vitales del interesado o de otra persona física.

e) Que fuese necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

f) Que el tratamiento deviniera necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

No obstante, lo dispuesto en la letra f) no será de aplicación al tratamiento que realicen las autoridades públicas en el ejercicio de sus funciones.

Por su parte, el art. 6.3 de la Ley Orgánica 3/2018, de 5 de diciembre, al hablar del tratamiento basado en el consentimiento del afectado, impide supeditar la ejecución de un contrato al consentimiento por parte del afectado para tratar sus datos personales para finalidades que no tengan relación directa con el desarrollo de la relación contractual, al disponer expresamente que *"no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual"*.

5. Ahora bien, el hecho de que pueda no resultar necesario el consentimiento expreso de los trabajadores acerca de la video vigilancia, ello no quiere decir que el empresario no deba informar expresamente a los mismos de la instalación de los medios de control en la empresa con el fin de evitar vulnerar derechos fundamentales. A tal efecto, la AEPD ha dejado claro que lo importante es que el trabajador esté debidamente informado acerca de la finalidad de la vigilancia, al tiempo que sugiere que se aclare cuál es la política de la empresa acerca de la utilización de los medios electrónicos, qué conductas están autorizadas y cuáles no y qué herramientas de inspección se van a utilizar[298]. En esta misma línea, si se trata de la instalación de cámaras de video vigilancia, es necesario que en las zonas video vigiladas se coloque un distintivo informativo, poniéndose en conocimiento de los representantes de los trabajadores, sin que puedan ser utilizados para fines distintos de los declarados.

En este sentido, el art. 89 de la Ley Orgánica 3/2018, de 5 de diciembre, establece que el empresario podrá tratar las imágenes obtenidas a través de sistemas de cámaras de video vigilancia para el ejercicio de las funciones de control previstas en el art. 20.3 ET siempre que las mismas se ejerzan dentro del marco legal y con los límites inherentes al mismo, debiendo el empleador informar con carácter previo y de forma expresa a los trabajadores y, en su caso, a sus representantes, acerca de esta medida.

6. En el ámbito de la jurisprudencia del Tribunal Constitucional referida al terreno de las relaciones de trabajo por cuenta ajena hay que destacar que, hasta la STC 29/2013, de 11 de febrero (caso Universidad de Sevilla. Cámaras de video vigilancia en centro de trabajo), el TC había venido estableciendo los principios en esta materia sobre la base de la colisión de las facultades de control del empresario con el derecho a la intimidad de los trabajadores sin hacer referencia alguna al derecho de autodeterminación informativa que

298 Informe Jurídico 0247/2008: Acceso por el empresario al correo electrónico de los trabajadores.

consagra art. 18.4 CE. En cambio, la STC 29/2013, de 11 de febrero, sí atiende específicamente a las exigencias derivadas del respeto al contenido esencial del derecho en materia de protección de los datos de carácter personal.

El caso que accedió al amparo en esa ocasión no fue un despido disciplinario, sino la imposición de tres sanciones de suspensión de empleo y sueldo por infracciones muy graves a un Director de Servicio de la Universidad de Sevilla por incumplir el horario y la jornada de trabajo. Ante las sospechas de la empleadora procedió a reproducir las grabaciones efectuadas por las cámaras de seguridad en donde se veía como el trabajador firmaba a unas determinadas horas, aunque entraba al establecimiento en otras diferentes[299]. Consta también en el relato de los hechos que el Convenio Colectivo aplicable preveía la posibilidad de que el empresario efectuase control sobre los medios informáticos y audiovisuales. El Comité de Empresa había sido informado sobre la adopción de estas medidas y existían incluso carteles informativos en donde se avisaba de la existencia de cámaras. Sin embargo, los trabajadores no habían sido informados, previa y expresamente, de la finalidad para la que podían ser recabados esos datos personales derivados de las grabaciones.

La STC 29/2013, de 11 de febrero, estima el recurso de amparo al apreciar que se había violado el derecho del art. 18.4 CE por incumplimiento del deber de información a los trabajadores acerca de la existencia de las cámaras de seguridad y de la finalidad a la que podían destinarse los datos personales[300]. Es necesario destacar que en la determinación del contenido esencial del derecho de autodeterminación informativa sigue aquí la doctrina de la STC 292/2000, de 30 de noviembre.

299 Se declaró probado en la sentencia del Juzgado de lo Social que en la mayor parte de los días laborables existía una demora en la hora de entrada al trabajo de entre treinta minutos y varias horas.

300 Declara la nulidad de las sanciones porque habiéndose acordado las mismas con base en una violación del art. 18.4 CE, no pueden dejar de tacharse como nulas de acuerdo con la calificación nacida de las SSTC 88/1985, de 19 de julio y 134/1994, de 9 de mayo.

La doctrina que establece la STC 29/2013, de 11 de febrero, cabe resumirla del siguiente modo:

i) La habilitación legal para recabar datos personales sin necesidad de consentimiento del interesado en el seno de las relaciones laborales no exime del deber de informar al trabajador, dado que es complemento del derecho del art. 18.4 CE la facultad de saber, en todo momento, quién dispone de los datos personales y a qué uso los está sometiendo. Una cosa es la necesidad o no de autorización por parte del afectado y otra, distinta, es el deber de informarle sobre su poseedor y el propósito del tratamiento[301].

ii) El derecho de información del trabajador solo puede venir limitado por Ley y, en el ámbito de las relaciones laborales, no existe habilitación legal expresa que permita su omisión[302].

iii) El citado derecho de información no puede sustituirse por la existencia de anuncios acerca de la instalación de cámaras o porque se hubiera notificado la creación del fichero a la AEPD.

iv) Lesiona el derecho del art. 18.4 CE la utilización, para verificar el cumplimiento de las obligaciones laborales, de medios encubiertos que niegan al trabajador la información debida.

301 Señala la STC 29/2013, de 11 de febrero, que el deber informativo es exigible también cuando el control empresarial incide en el derecho a la intimidad personal (art. 18.1 CE) y no sólo cuando está en juego el derecho a la protección de datos de carácter personal (art. 18.4 CE).

302 Para la STC 29/2013, de 11 de febrero, tampoco puede situarse el fundamento de la exención del deber de información al trabajador en el interés del empresario en controlar la actividad laboral a través de sistemas no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de la vigilancia.

v) Respecto del alcance del deber de información, señala que es necesaria una información previa, expresa, precisa, clara e inequívoca a los trabajadores acerca de la finalidad de control de la actividad laboral, debiendo concretar dicha información tanto las características como el alcance del tratamiento de datos que vaya a realizarse. No obstante, sobre este particular se incidirá más adelante en el Capítulo IV de esta obra cuando se analice el deber de información.

7. La diferencia entre los pronunciamientos contenido en las SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio y el expresado en la STC 29/2013, de 11 de febrero, reside en que en las dos primeras sentencias el Tribunal analiza el deber de preavisar desde la perspectiva del art. 18.1 CE, mientras que esta última lo hace aplicando el art. 18.4 CE, a lo que cabe añadir que la STC 186/2000, de 10 de julio, lo que analiza es un supuesto de instalación de sistemas de grabación con el único fin de perseguir un posible ilícito de autor indeterminado, en tanto que la STC 29/2013, de 11 de febrero, se refiere al uso laboral de un sistema de grabación de carácter general, ajeno a la prestación laboral en cuanto tal[303].

En suma, el Tribunal Constitucional tras estimar que las imágenes grabadas en un soporte físico constituyen datos de carácter personal protegidos por el derecho de protección de datos, sostuvo que la solución del recurso se encontraba en la STC 292/2000, de 30 de noviembre, pronunciamiento referido específicamente al art. 18.4 CE y, en base a ella, se reafirmó en que el derecho de información es parte del núcleo esencial del derecho de autodeterminación informativa habida cuenta de que es complemento indispensable del mismo la facultad de saber en todo momento quién dispone de los datos personales y qué uso le está dando[304].

303 FALGUERA BARÓ, M. A.: "Nuevas tecnologías y trabajo (II): perspectiva constitucional", *Trabajo y Derecho*, núm. 21, septiembre 2016, pág. 36.

304 STC 292/2000, de 30 de noviembre.

De este modo, el afectado tiene derecho a ser informado sobre los referidos extremos, incluso en los casos en los que la recogida de datos no requiera consentimiento del titular, ya que una cosa es la necesidad o no de autorización del afectado y otra, distinta, es el deber de informarle sobre su poseedor y el destino del tratamiento[305]. No obstante, el propio TC reconoció que la exigencia informativa no es absoluta, dado que caben limitaciones al derecho de información previa por razones constitucionalmente admisibles y legalmente previstas, las cuales deberán ser necesarias y proporcionadas.

En aplicación de dicha doctrina se concluyó que, al no existir habilitación legal expresa para omitir el deber de información previo en el ámbito de las relaciones laborales, no cabe que éste sea desconocido. De donde deriva la proscripción de cámaras ocultas[306] así como la utilización de grabaciones para finalidades distintas mientras no exista norma legal que las ampare, no siendo suficiente que el tratamiento de datos esté amparado en la Ley o que pueda resultar proporcionado en el caso concreto de que se trate. Siguiendo esta doctrina, el derecho de información previa prohibiría el empleo de sistemas de video vigilancia encubierta aunque pudiera estar justificados los mismos en orden a detectar incumplimientos contractuales graves o, incluso, actividades fraudulentas[307].

En este marco, en el caso de autos hubiera sido necesario que los trabajadores hubiesen sido informados de manera previa, precisa, expresa, clara e inequívoca acerca de la posibilidad de utilizar las grabaciones provenientes de cámaras instaladas en vestíbulos y zonas públicas con la finalidad de controlar la actividad laboral, debiendo contener dicha información tanto las características como el alcance del tratamiento de datos que se iba a

305 STC 29/2013, de 11 de febrero. Recuérdese, además, lo afirmado por el TEDH en su sentencia de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía).

306 STEDH de 9 de enero de 2018 (caso López Ribalda *et alii* c. España).

307 GALLARDO MOYA, R.: "El derecho fundamental a la protección de datos y la videovigilancia empresarial", *Revista de Derecho Social*, nº 62, 2013, págs. 169-170.

realizar[308], no bastando con que existieran distintivos sobre la instalación de cámaras en el centro de trabajo ni que se hubiera notificado la creación del fichero a la AEPD.

8. Más recientemente, el TEDH en sentencia de fecha 5 de septiembre de 2017 (caso Barbulescu c. Rumanía), ha planteado el debate en torno a las obligaciones de las autoridades administrativas y judiciales para situar el foco sobre los jueces de lo laboral e incidir de modo especial en que los jueces nacionales deben examinar si el trabajador ha sido informado previamente de la posibilidad de que el empresario pueda aplicar medidas de control de las comunicaciones, al tiempo que precisa que la notificación debe ser clara y precisa acerca de la naturaleza de las medidas de control, adoptando el Tribunal[309] como referencia principal la normativa sobre protección de datos -que adquiere un papel preponderante en el ámbito de las relaciones laborales - al objeto de exigir que el trabajador tenga información previa, clara y concreta sobre los sistemas de vigilancia, apoyándose para ello en el principio de transparencia que respaldan el Comité de Ministros del Consejo de Europa –Recomendación CM/REC (2015)– y el Grupo de Trabajo del art. 29 sobre Protección de Datos que existe en la Unión Europea.

A tal efecto, señala expresamente la sentencia que los tribunales nacionales habrán de velar para que el establecimiento, por parte de una empresa, de medidas de vigilancia de la correspondencia y otras comunicaciones, vaya acompañada de las garantías adecuadas y suficientes contra los abusos, al tiempo que hace un llamamiento expreso a que la proporcionalidad y las garantías procesales contra el carácter arbitrario sean elementos esenciales de valoración.

308 STC 29/2013, de 11 de febrero.

309 GARCÍA VITORIA, I., “La protección de datos como eje de la jurisprudencia del Tribunal de Estrasburgo sobre la privacidad del trabajador y el control empresarial”, en http://eapc-rcdp.blog.gencat.cat

Y, referida a la video vigilancia empresarial, la STEDH de 9 de enero de 2018 (caso López Ribalda *et alii* c. España), destaca cómo la legislación española sobre protección de datos (la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) obligaba sin excepción a los empresarios a informar del establecimiento de sistemas de vigilancia, incluida la existencia de cámaras ocultas -al tiempo que proscribe la video vigilancia indiscriminada- y recuerda que los datos visuales obtenidos mediante video vigilancia implican el almacenamiento y procesamiento de datos de carácter personal, estrechamente vinculados a la esfera privada de las personas - lo que iría en línea con la doctrina de nuestro Tribunal Constitucional, que afirma que las imágenes grabadas en un soporte físico constituyen un dato de carácter personal que cae íntegramente bajo el ámbito de aplicación del art. 18.4 CE -.

Por ello, continúa el TEDH, conforme al art. 5 de la derogada Ley Orgánica 15/1999, de 13 de diciembre, las demandantes tenían derecho a ser informadas con carácter previo y de modo expreso, preciso e inequívoco acerca de la existencia de un fichero de datos de carácter personal, la finalidad de la recogida de éstos y de los destinatarios de la información. La existencia de la norma implicaba que las demandantes tenían una expectativa razonable de respeto a su privacidad y la empresa no cumplió con los requisitos del citado art. 5 de la derogada Ley Orgánica 15/1999, de 13 de diciembre, lo que lleva al TEDH a considerar que se vulneró el art. 8 del Convenio.

CAPÍTULO II.- LA CONFIGURACIÓN LEGAL DE LAS MEDIDAS DE CONTROL EMPRESARIAL.

1.- Artículo 8.2 CEDH: la necesidad de previsión legal. La calidad de la ley.

1. Del hecho de que las diferentes formas de control empresarial de la actividad laboral pueden incidir, vulnerándolos, en los derechos fundamentales del trabajador deriva la exigencia constitucional de la necesidad de previsión legal de las medidas de injerencia empresarial en la privacidad del trabajador (casos Halford y Kopland c. Reino Unido), la cual deviene requisito imprescindible tanto a nivel europeo vía art. 8.2 CEDH[310], como a nivel interno vía art. 9.1 y 3[311].

Que dicha injerencia esté prevista por la ley es algo que viene exigido por el art. 8.2 CEDH habida cuenta de que las medidas en él contempladas para la afectación del derecho habrán de justificarse en *"la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás"*. No falta casi nada en este elenco de conceptos jurídicos, si bien la jurisprudencia del TEDH ha ido progresivamente precisando que las medidas previstas en la ley habrán de ser proporcionadas al fin legítimo en ella perseguido[312] y que aquélla ha de articularse de forma tal que proporcione al individuo la suficiente certeza y previsibilidad sobre la

310 Establece el art. 8.2 CEDH que *"No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley"*.

311 Señala el art. 9.1 CE que *"Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico". Por su parte el párrafo 3 del art. 9 CE prescribe que "La Constitución garantiza el principio de legalidad…"*.

312 SSTEDH en los casos Dudgeon y Silver y otros, de 22 de octubre de 1981 y 25 de mayo de 1983, respectivamente.

hipótesis a la que se une la posibilidad de adoptar una medida de interceptación de las comunicaciones[313].

En todo caso, el requisito de la previsión legal previsto en el CEDH ha sido detallado en todas sus manifestaciones por la jurisprudencia del TEDH, pudiendo deducirse de la misma que la previsión legal encierra tres requisitos, el primero de los cuales afectaría a la previsión en sentido propio, y los otros dos a lo que el TEDH denomina "calidad de la ley"[314]. Dichos requisitos son los siguientes: i) existencia de una base en el derecho interno; ii) accesibilidad de la ley para la persona implicada; iii) previsibilidad de la ley en cuanto al sentido y la naturaleza de las medidas aplicables (entre otras, sentencias del TEDH de 24 de abril de 1990, casos Kruslin y Huvig c. Francia y de 25 de marzo de 1998, caso Kopp c. Suiza)[315].

2. La exigencia de que la injerencia en la vida privada del trabajador haya de estar prevista por la ley significa que la misma ha de estar contemplada por el Derecho interno de que se trate. Aunque el término "ley" ha sido interpretado por el TEDH con un criterio flexible, utilizándolo en sentido material y no formal[316], es decir, que no exige el rango normativo de ley, sino que admite que pueda tratarse de una disposición general de rango infralegal[317], lo verdaderamente fundamental a este respecto es que exista una norma de carácter general en el ordenamiento estatal que establezca los límites y garantías para adoptar, implementar y controlar la medida limitadora del derecho fundamental de que se trate, no importando que la norma en cuestión

313 STEDH de 2 de agosto de 1984 (caso Malone c. Reino Unido).

314 STEDH de 30 de julio de 1997 (caso Valenzuela Contreras c. España).

315 DÍAZ REVORIO, F. J., "El derecho fundamental al secreto de las comunicaciones: una visión desde la jurisprudencia europea y su influencia en el Tribunal Constitucional español", Instituto de Investigaciones Jurídicas UNAM, www.juridicas.unam.mx, 2006, pág. 133.

316 Así lo señalan las SSTEDH de 24 de abril de 1990 (casos Kruslin y Huvig c. Francia).

317 STEDH de 18 de junio de 1971 (caso De Wilde c. el Reino Unido).

sea escrita o consuetudinaria[318], pues no se puede olvidar que la doctrina del TEDH ha de resultar aplicable tanto en los Estados con ordenamientos propios del sistema continental como en aquellos otros, de cultura anglosajona, que han optado de manera primordial por el Derecho consuetudinario[319].

3. No obstante, en la doctrina del TEDH lo verdaderamente importante no es tanto la constatación de que la injerencia en la vida privada esté contemplada en una norma de Derecho Interno como que ésta ostente una concreta y determinada "calidad", siendo a este requisito al que le dedica mayor atención el Tribunal a la hora de proceder a la valoración de la norma interna aplicable al caso concreto de que se trate.

La expresión "calidad de la ley" es acuñada por la jurisprudencia del TEDH, la cual exige estrictas condiciones de previsibilidad al legislador de los derechos fundamentales, en particular, al legislador de determinadas medidas especialmente rigurosas puestas a disposición de los poderes públicos, como son la prisión provisional y la intervención de la correspondencia[320], presuponiendo a esta exigencia de "calidad de la ley", de modo coetáneo, la necesaria constatación de que la norma cumpla tres requisitos necesarios, a saber:

i) En primer lugar, que sea accesible a los ciudadanos, es decir, que los términos en que se manifiesta la ley hayan de ser lo suficientemente claros o expresivos como para que aquéllos puedan comprender sin demasiados esfuerzos intelectuales los supuestos en los cuales está tolerada la injerencia

318 Así lo pone de manifiesto, también, en las SSTEDH de 26 de abril de 1979 (caso Sunday Times); de 22 de octubre de 1981 (caso Dudgeon) y de 30 de marzo de 1989 (caso Chappel), todos ellos contra el Reino Unido.

319 SSTEDH de 24 de abril de 1990 (casos Kruslin y Huvig contra Francia), entre otras.

320 CRUZ VILLALÓN, P., "Control de la calidad de la ley y calidad del control de la ley". *Derecho Privado y Constitución*, núm. 17, enero-diciembre 2003, pág. 149.

en su vida privada. En definitiva, que su derecho fundamental a la privacidad u otro derecho fundamental puede quedar limitado.

ii) En segundo lugar, que las consecuencias que pudieran derivarse de la injerencia en la vida privada sean "previsibles" para el sujeto afectado.

iii) Y, finalmente, que la norma contemple las garantías necesarias para controlar el ámbito y aplicación de la concreta medida limitadora. O, dicho en otros términos, que las injerencias sean compatibles con la preeminencia del derecho.

Analicemos cada uno de estos requisitos aisladamente:

1ª) Accesibilidad de la norma. Es ésta justamente la exigencia menos elaborada por la doctrina del TEDH dado que éste se limita única y exclusivamente a exigir que la concreta norma que contemple la medida restrictiva del derecho fundamental de que se trate sea "accesible" para los sujetos afectados por aquélla[321].

Así, por ejemplo, en la STEDH de 2 de agosto de 1984 (caso Malone c. Reino Unido) se destaca con precisión esta exigencia al declarar que el ciudadano deberá poder disponer de la suficiente información acerca de las normas jurídicas aplicables a un determinado caso[322].

321 SSTEDH de 25 de marzo de 1998 (caso Kopp c. Suiza) y de abril de 2004 (caso Doerga c. Países Bajos).

322 El TEDH reproduce en este caso su anterior doctrina contenida en las sentencias referentes a los casos The Sunday Times y Silver, ambos c. Reino Unido.

De donde parece deducirse que lo verdaderamente determinante de este requisito es la necesidad de que los ciudadanos destinatarios de la norma en cuestión tengan garantizado el acceso a su conocimiento mediante los correspondientes sistemas de publicación de aquélla, circunstancia ésta que, obviamente, tiene lugar con una mayor facilidad en los ordenamientos continentales dado que en ellos predomina el Derecho escrito y publicado en los Boletines Oficiales correspondientes, en tanto que en los sistemas jurídicos propios del *Common Law* prevalece la tradición consuetudinaria no escrita y, por tanto, existe una mayor dificultad a la hora de proceder al conocimiento de aquélla[323].

2ª) Previsibilidad de sus consecuencias. Con esta exigencia el TEDH está poniendo de manifiesto que la concreta norma que habilite la injerencia en el derecho fundamental de que se trate debe ser, además, muy precisa en la fijación del ámbito y límites de tal o cual medida limitadora de éste, de forma que la misma habrá de expresarse en términos lo suficientemente claros y precisos como para permitir al ciudadano medio conocer, de manera suficiente, bajo qué condiciones y en qué circunstancias habilita a los poderes públicos a adoptar tales medidas[324].

Es decir, la tesis del TEDH, patente por lo demás en tres condenas contra España[325], es que las garantías para los ciudadanos y los poderes de apreciación de las autoridades, incluidas las judiciales, deben estar claramente previstas y delimitadas en la ley, siendo insuficiente a tales efectos la mera

323 DE LLERA SUÁREZ-BÁRCENA, E., *La observación o escucha de las comunicaciones telefónicas.* Estudios Jurídicos del Ministerio Fiscal, Tomo VI, Centro de Estudios Jurídicos de la Administración de Justicia, 1997, pág. 471.

324 Fueron las SSTEDH de 24 de abril de 1990 (casos Kruslin y Huvig c. Francia) las primeras que aludieron precisamente a este requisito. Con posterioridad, las SSTEDH de 25 de junio de 1997 (caso Halford c. Reino Unido); de 25 de marzo de 1998 (caso Kopp c. Suiza); de 30 de julio de 1998 (caso Valenzuela Contreras c. España) y de 16 de febrero de 2000 (caso Amann c. Suiza) han continuado insistiendo en el cumplimiento de este requisito para que la norma resulte compatible con las exigencias derivadas del art. 8 del Convenio.

325 Casos Valenzuela Contreras c. España, de 30 de julio de 1998; caso Prado Bugallo c. España, de 18 de febrero de 2003; caso Trabajo Rueda c. España, de 30 de mayo de 2017.

fijación de criterios jurisprudenciales[326], estando orientado todo el sistema del Convenio hacia un nivel ascendente de protección de los derechos humanos en Europa[327].

En definitiva, la exigencia de previsión legal coincide con el principio de legalidad de los ordenamientos internos, entendido el mismo como la necesidad de que la injerencia tenga un fundamento jurídico en el derecho interno, no bastando a tal efecto únicamente con que sea compatible con aquél. A tal efecto, la doctrina contenida en la STEDH de 26 de abril de 1979 (caso Sunday Times c. Reino Unido) referida a la expresión *"prescribed by the law"*, utilizada en el art. 10, resulta aplicable en el ámbito del art. 8, debiendo entenderse la exigencia de fundamento jurídico en sentido material y no formal. Idea ésta que se completa dando por buena la posible precisión que pudiera introducir al respecto la jurisprudencia aplicativa. Así, en la STEDH de 25 de mayo de 1993 (caso Kokkinakis c. Grecia) se sienta la doctrina de que aunque en ocasiones la ley sea un tanto vaga o indefinida, es suficiente con que haya habido una concreción jurisprudencial que la complete, siempre que haya sido publicada y resulte accesible[328].

3ª) Compatibilidad de las medidas con la preeminencia del derecho. Se refiere esta exigencia a la necesidad de que la norma habilitante delimite con precisión las facultades de los poderes públicos a los que se les hubiere atribuido la potestad de acordar tales medidas limitativas del derecho fundamental de la manera necesaria como para garantizar la interdicción de la

326 SANTOLAYA MACHETTI, P., "Derecho a la vida privada y familiar: un contenido notablemente ampliado del derecho a la intimidad (art. 8 CEDH)", en García Roca, J. y Santolaya Machetti, P. (coords.), *La Europa de los derechos. El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid, 2005, pág. 492.

327 ARZOZ SANTISTEBAN, X., "Derecho al respeto de la vida privada y familiar", en LASAGABASTER HERRARTE, I.: *Convenio Europeo de Derechos Humanos. Comentario sistemático*, Madrid, 2009, Thomson Civitas, pág. 259.

328 MARTÍN-RETORTILLO BAQUER, L., "La calidad de la Ley según la jurisprudencia del Tribunal Europeo de Derechos Humanos (Especial referencia a los casos "Valenzuela Contreras" y "Prado Bugallo", ambos contra España"), *Derecho Privado y Constitución*, núm. 17, enero-diciembre 2003, págs. 390-391.

arbitrariedad. En realidad, se trata de dos requisitos englobados en uno: de un lado, la ley ha de señalar cuáles han de ser las circunstancias que permitan el establecimiento de la medida (las denominadas "garantías mínimas" que fueren necesarias para evitar los abusos y arbitrariedades de los poderes públicos). Y de otro lado, se refiere también a la exigencia de que los Ordenamientos Internos establezcan sistemas de control eficaces y de impugnación de todas las fases en que se estructure la aplicación de la medida[329].

2.- El principio de legalidad en la Constitución Española.

1. Por expreso mandato de la Constitución, toda injerencia en el ámbito de los derechos fundamentales y de las libertades públicas que incida directamente en su desarrollo (art. 81.1 CE) o limite o condicione su ejercicio (art. 53.1 CE), precisa de una habilitación legal[330]. Aunque la propia Constitución contiene, con carácter general, tal habilitación legal, el art. 18 CE no hace referencia alguna a los presupuestos y condiciones que la Ley ha de reunir como garantía de la seguridad jurídica. La regulación de los derechos fundamentales y su desarrollo directo corresponde, pues, sólo a la ley, ordinaria y orgánica, respectivamente (arts. 53.1 y 18.1 CE), y esta garantía no decae en los casos en que la propia Constitución identifica el medio a través del cual el objeto del derecho pueda resultar afectado por los poderes públicos[331].

329 NARVÁEZ RODRÍGUEZ, A., "Tutela de la privacidad e interceptación de las comunicaciones", en *Cuadernos Penales Jose María Lidón*, núm. 4, Delito e informática: algunos aspectos, Bilbao, 2007, Universidad de Deusto, pág. 321.

330 MONTAÑÉS PARDO, M. A., *La intervención de las comunicaciones. Doctrina jurisprudencial*, Aranzadi Editorial, Pamplona 1999, pág. 31; VEGAS TORRES, J., VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…op. cit.*, pág. 120.

331 JIMÉNEZ CAMPO, J., La garantía constitucional del secreto de las comunicaciones, *Revista Española de Derecho Constitucional,* año 7, nº 20, mayo-agosto 1987, pág. 58.

2. Por su parte, la jurisprudencia del TC admite injerencias en los derechos fundamentales siempre que se cumplan determinados requisitos. Partiendo de la base de que los derechos fundamentales carecen de carácter absoluto, el Tribunal Constitucional admite que el contenido de cualquier derecho fundamental se encontrará delimitado por el de otros derechos constitucionales, siendo desde esta óptica admisibles injerencias en el derecho a la intimidad que encuentren su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales[332].

3. Respecto de la previsión legal, el Tribunal Constitucional insiste en que cualquier limitación del derecho a la intimidad habrá de estar fundamentada en una previsión legal de carácter constitucional, debiendo ser la misma proporcionada y expresar todos los presupuestos materiales de la medida limitadora[333], de modo que la limitación de aquel derecho sólo será admisible si encuentra amparo en una norma de rango legal, afirmando, en este sentido, la STC 233/2005, de 26 de septiembre, que la condición de la legitimidad constitucional de una medida limitativa de un derecho fundamental es su previsión legal. Se trata, pues, de una reserva de ley que impide que la injerencia en derechos fundamentales pueda ser autorizada por normas de rango reglamentario[334].

4. Ahora bien, no se considera bastante con que confluya la necesidad formal de que la injerencia en el derecho fundamental a la intimidad esté autorizada por una norma de rango legal, sino que se necesita también que la disposición legal de que se trate cumpla determinados requisitos en cuanto a su contenido, de tal modo que la jurisprudencia constitucional exige al respecto que la ley concrete las restricciones, alejándose de criterios de delimitación imprecisos, pues vulnera el derecho fundamental a la intimidad personal el

332 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…op. cit.*, pág. 119.

333 SSTC 159/2009, de 29 de junio; 70/2009, de 23 de marzo y 206/2007, de 24 de septiembre.

334 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…op. cit.*, pág. 120.

establecimiento de límites de forma tal que hagan impracticable el derecho fundamental afectado (SSTC 70/2009, de 23 de marzo)[335].

5. Pero además de tener suficiente cobertura legal, en los términos señalados, las injerencias en los derechos fundamentales están también sujetas a otras exigencias que habrán de ser observadas en la ejecución de las medidas limitadoras, planteándose a este respecto, en primer lugar, la necesidad o no de resolución judicial que permita la injerencia en el derecho a la intimidad en cada caso concreto, debiendo ser la respuesta deducida de la jurisprudencia del Tribunal Constitucional a esta cuestión de tipo negativo, de manera que sólo respecto de injerencias que tuvieren lugar en el curso de investigaciones penales la resolución judicial habrá de ser necesaria, si bien únicamente como regla general, ya que derivado de la falta de reserva constitucional a favor del Juez, se reconoce la posibilidad de que la Ley pueda autorizar a la Policía judicial para poder llevar a cabo medidas limitativas del derecho a la intimidad siempre que concurran acreditadas razones de urgencia y necesidad y se respeten los principios de proporcionalidad y razonabilidad[336].

6. La principal exigencia en materia de ejecución de medidas restrictivas del derecho a la intimidad es el respeto del principio de proporcionalidad[337], el cual exige, con arreglo a la jurisprudencia constitucional, el cumplimiento de los tres postulados siguientes: i) que la medida sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad); ii) que sea, además, necesaria, en el sentido de que no exista otra medida más moderada para la consecución del tal propósito con igual eficacia (juicio de necesidad); iii) y, finalmente, que la

335 En el mismo sentido, STC 206/2007, de 24 de septiembre.

336 SSTC 206/2007, de 24 de septiembre; 70/2002, de 3 de abril y 207/1996, de 16 de diciembre. En idéntico sentido, la STC 233/2005, de 26 de septiembre – referida a medidas limitativas de la intimidad adoptadas por la Administración tributaria – afirma que *"no es constitucionalmente exigible que sea el Juez quien tenga que autorizar esta medida limitativa, pudiéndola adoptar, siempre que una ley expresamente la habilite, la autoridad que, por razón de la materia de que se trate, sea la competente"*.

337 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…op. cit.*, pág. 121.

medida adoptada sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en un juicio estricto de proporcionalidad[338]. Por lo demás, el respeto al principio de proporcionalidad es una exigencia común y constante para la constitucionalidad de cualesquiera medidas restrictivas de derechos fundamentales[339].

7. Por otro lado, como exigencia formal vinculada al principio de proporcionalidad el Tribunal Constitucional viene exigiendo la motivación de la resolución –judicial o administrativa– que adopte la medida limitativa[340], debiendo hacer referencia la misma tanto a la previsión legal que ampara la afectación de la intimidad como al juicio de ponderación entre el derecho fundamental afectado y el interés constitucionalmente protegido y perseguido, del cual se evidencie la idoneidad, la necesidad y la proporcionalidad de la adopción de la medida[341], considerando a estos efectos el Tribunal Constitucional que la ausencia de motivación de la adopción de la medida limitativa de derechos fundamentales supone la vulneración del derecho fundamental afectado por la medida de que se trate[342].

338 Entre otras muchas, STC 159/2009, de 29 de junio.

339 STC 207/1996, de 16 de diciembre.

340 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…op. cit.*, pág. 122.

341 STC 70/2009, de 23 de marzo.

342 SSTC 70/2009, de 23 de marzo y 207/1996, de 16 de diciembre.

3.- La normativa laboral.

3.1.- Artículo 20.3 ET: el poder de dirección y control del empresario.

1. Lo primero que hemos de destacar en este apartado es que el poder de dirección del empresario constituye el elemento más característico de las relaciones laborales, fruto de la situación de dependencia jurídica del trabajador en el contrato de trabajo. Esta idea la recoge el art. 20 ET que, bajo la rúbrica "Dirección y control de la actividad laboral", establece que el trabajador está obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien éste delegue, debiendo, pues, el mismo cumplir las órdenes e instrucciones de aquél en el ejercicio regular de sus facultades directivas (art. 5.c) ET), concretándose, a su vez, ese poder directivo dentro del ámbito de organización y dirección de un empleador y aplicándose sólo a los trabajadores que voluntariamente presten sus servicios retribuidos por cuenta ajena (art. 1.1 ET). Y, por su parte, el apartado 3 del art. 20 ET autoriza al empresario a adoptar cuantas medidas de vigilancia y control estime oportunas en orden a la verificación del cumplimiento por parte del trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a la dignidad humana de éste.

A esta prescripción hay que unir lo dispuesto por el nuevo art. 20 bis ET introducido por 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, a cuyo tenor los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empresario, a la desconexión digital y a la intimidad frente al uso de dispositivos de video vigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

Como puede observarse, los artículos referidos no concretan las medidas de control que pueden ser utilizadas por el empresario en orden a verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, limitándose a señalar el art. 20.3 ET que aquél está facultado para utilizar las que estime más oportunas. Por tanto, corresponde al empresario definir las medidas de vigilancia, siempre que las mismas guarden la consideración debida a la dignidad del trabajador, lo que significa que las mismas no podrán ser arbitrarias, sino que el empleador deberá adoptar las más acordes con la tutela de la dignidad del trabajador e ir dirigidas única y exclusivamente a verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, de modo que quedan excluidas medidas tendentes a la averiguación de extremos de índole personal, o de cualquier otra clase, del trabajador. Se trata, pues, de una prescripción de índole finalista, evidenciada por la preposición “para” seguida del objeto “verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales”, que no da cabida a vigilancias o controles tendentes a finalidades distintas a las reseñadas.

2. De lo expuesto cabe señalar que las facultades de ordenación del empresario incluyen, en principio, la posibilidad de vigilar y controlar el cumplimiento de la actividad laboral de los trabajadores. No se trata de vigilar y controlar a los trabajadores, sino que la norma se refiere única y exclusivamente a la vigilancia y control del cumplimiento de la actividad laboral, lo que significa que el empleador sólo podrá proceder a la captación y grabación de imágenes y sonido del entorno laboral con el único y exclusivo objeto de verificar si la prestación laboral resulta adecuadamente desarrollada y cumplida, lo que excluye, de principio, la posibilidad de adoptar medidas de vigilancia y control tendentes a otros fines, al tiempo que el uso de herramientas audiovisuales encaminadas a tal fin habrá de ajustarse en todo momento al respeto de los derechos fundamentales de los trabajadores a fin de evitar formas propias de un feudalismo virtual.

Por último, el referido art. 20.3 ET supedita la facultad de vigilar y controlar del empleador a su deber de respeto de la dignidad del trabajador en cuanto persona, previamente reconocida en el art. 10.1 CE, lo cual obliga a aquél a la adopción de las medidas de control con respeto, en todo momento, al derecho al honor, a la intimidad, a la propia imagen, al secreto de las comunicaciones y a la protección de datos personales en cuanto derechos fundamentales reconocidos en el art. 18 CE.

En definitiva, el art. 20.3 ET ofrece cobertura material a la pretensión empresarial de vigilancia y control del uso que el trabajador hace de los medios informáticos puestos a su disposición para el desarrollo de su prestación laboral siempre y cuando a través de esos medios se ejecute y desarrolle la misma, si bien, para ejercitar legalmente sus facultades habrá de moverse dentro de los límites y coordenadas que protegen el ejercicio de los derechos fundamentales de los trabajadores en el medio laboral.

Dicho de otro modo, la decisión empresarial deberá someterse a los rigores del test de proporcionalidad[343] sin imponer el sacrificio injustificado de los derechos fundamentales de los trabajadores (cfr. SSTC 98/2000, de 10 abril y 186/ 2000, de 10 julio), por lo que, ante cada caso concreto, habrá que decidir, en primer lugar, si existen indicios o razonables sospechas de uso abusivo; seguidamente, determinar si la concreta medida de control es idónea para la finalidad pretendida, esto es, para verificar si el trabajador cometía o no las irregularidades sospechadas; en tercer lugar, valorar la necesidad de la medida, considerando la posible existencia de otras medidas alternativas menos dañosas e invasivas en el derecho fundamental de que se trate; y, finalmente, decidir a través de un juicio de proporcionalidad en sentido

343 Acerca del principio de proporcionalidad véase GAVARA DE CARA, J. C., "El principio de proporcionalidad como elemento de control de la constitucionalidad de las restricciones de los derechos fundamentales", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 16, 2003, págs. 16-20. GONZÁLEZ BEILFUSS, M., *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*, Pamplona, 2003, Aranzadi.

estricto, atento a los medios y a los fines sobre la razonabilidad, el equilibrio y la objetividad de la medida.

A este efecto, se cuestionan por, supuestamente, ser violadores de los derechos al honor y a la intimidad de los trabajadores, el sometimiento de éstos a controles mediante cámaras de vigilancia, micrófonos y otras técnicas audiovisuales de los lugares de trabajo con la finalidad de comprobar el adecuado cumplimiento de la prestación laboral por parte de los mismos o el control empresarial efectuado sobre los ordenadores puestos a disposición de aquéllos para llevar a cabo su prestación laboral, conductas fiscalizadoras éstas que se consideran lícitas siempre que fueren idóneas, necesarias y proporcionadas, según prescribe la doctrina constitucional, y que han generado una riquísima doctrina y jurisprudencia al respecto que será objeto de análisis a lo largo de este estudio.

3. Por otro lado, de cuanto antecede se deduce, asimismo, que la regulación contenida en el art. 20.3 ET se revela, por sí sola, insuficiente para evitar arbitrariedades, quedando sometido el trabajador a la incertidumbre de desconocer qué aspectos de su vida privada son grabados y conservados o cedidos y tratados, considerándose la misma como un "parvo instrumental jurídico"[344] o, dicho en otros términos, como un instituto jurídico muy limitado para dar respuesta satisfactoria a los nuevos retos planteados por las TIC, si bien con las SSTC 98/2000, de 10 de abril[345] y 186/2000, de 10 de julio[346], se

344 GOÑI SEIN, J. L., "Controles empresariales: geolocalización, correo electrónico, Internet, video vigilancia y controles biométricos", *Justicia Laboral*, núm. 39, 2009, pág. 15.

345 La STC 98/2000, de 10 de abril, analiza la constitucionalidad de la instalación en la ruleta francesa y en la caja de un casino, de un sistema de control microfónico, junto a otro sistema de video vigilancia ya existente con anterioridad, con el fin de registrar las conversaciones entre clientes y trabajadores. El TC considera que la facultad de instalar los medios audiovisuales no es un poder omnímodo del empresario, sino que el mismo se encuentra condicionado por el derecho a la intimidad, y declara que la instalación de micrófonos en las referidas zonas del casino constituye una intromisión ilegítima en el derecho a la intimidad por entender que el uso de los micrófonos permitía la audición continuada e indiscriminada de todo tipo de conversaciones tanto entre los propios trabajadores como con los clientes y

produjo un punto de inflexión importante al concretar el TC la doctrina sobre la extensión de los poderes de vigilancia y control del empresario en el contexto laboral, en el sentido de aplicar el triple test de idoneidad, estricta necesidad y proporcionalidad para determinar si el control empresarial estaba vulnerando o no los derechos fundamentales de los trabajadores.

Esta ausencia de una regulación que especifique cuál haya ser el uso por el trabajador y cómo debe desarrollarse el control empresarial no se produce solamente a nivel heterónomo, sino también en el plano colectivo, evidenciándose de este modo la lentitud de la que adolece el Derecho para acomodarse a las nuevas realidades sociales. La consecuencia de todo ello ha sido el elevado grado de judicialización de esta materia que ha generado una abundante casuística en las respuestas ofrecidas por los Tribunales de Justicia que, sin embargo, debe relativizarse tras los pronunciamientos del TS en unificación de doctrina y las SSTC 241/2012, de 17 de diciembre y 39/2016, de 3 de marzo, sobre las que se incidirá más adelante.

4. Para salvar las dificultades que comporta esa indeterminación normativa, han sido dos las respuestas que se han adoptado. De un lado, las empresas han procedido a adoptar de forma unilateral normas de uso y control de los instrumentos tecnológicos puestos a disposición de los trabajadores. De otro lado, cabe destacar también el papel que han desempeñado los representantes de los trabajadores en la negociación colectiva alcanzando

---

porque no quedó acreditado que dicha medida resultase indispensable para la seguridad y el buen funcionamiento del casino.

346 La STC 186/2000, de 10 de julio, juzga la corrección de la instalación en un economato, ante las sospechas de comportamiento irregular de las trabajadoras, de un circuito de televisión para controlar las cajas registradoras y el mostrador de paso de las mercancías. El TC analiza el sistema de video vigilancia instalado y considera que la empresa tiene razón porque la medida es legítima, no es arbitraria ni caprichosa por pretenderse verificar si el trabajador cometía las irregularidades sospechadas para adoptar, en ese caso, las medidas disciplinarias pertinentes, siendo, además, necesaria dado que la grabación serviría de prueba de dichas irregularidades, y equilibrada, habida cuenta de que la grabación de imágenes se limitó exclusivamente a la zona de caja y a una duración temporal limitada, la suficiente en orden a comprobar que no se trataba de un hecho aislado, sino de una conducta ilícitareiterada.

acuerdos específicos en la materia, si bien, como se verá más delante, la mayor parte de los convenios que han contemplado la irrupción de las TIC en seno de las empresas han regulado el fenómeno desde una perspectiva fundamentalmente reactiva mediante su inclusión en el catálogo de faltas laborales, salvo para los supuestos atinentes al ejercicio de la acción sindical en el seno de las mismas.

En definitiva, lo primero, pues, que se advierte en clave netamente jurídica es que, a falta de regulación en convenio colectivo o en normativa interna, el ordenamiento jurídico español carece de una norma que expresamente contemple y regule el conflicto de intereses entre trabajador y empresario subyacente a este tipo de situaciones, como sucede, sin embargo, con el registro operado en la persona del trabajador, su taquilla y efectos particulares, el cual está pormenorizadamente regulado en el art. 18 ET bajo la rúbrica "Inviolabilidad de la persona del trabajador".

3.2.- Artículo 18 ET: el registro en la persona del trabajador, su taquilla y efectos personales.

1. El art. 20.3 ET, regulador del poder de vigilancia y control del empresario, puede verse completado con la previsión establecida en el art. 18 ET[347] que, bajo la rúbrica "Inviolabilidad de la persona del trabajador", faculta al empresario para realizar un determinado control sobre la persona de aquél, sus taquillas o efectos personales siempre que exista un riesgo para el patrimonio del empresario, de otros trabajadores o de terceros. No obstante, este precepto ha sido criticado por parte de la doctrina que ha analizado el mismo[348],

347 El art. 18 ET establece que *"sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible".*

348 ALONSO OLEA, M. y BARREIRO GONZÁLEZ, G., *El Estatuto de los Trabajadores. Texto, comentarios, jurisprudencia*, Madrid, 1995, Civitas, pág. 104.

calificándolo más de limitación de los derechos del trabajador que de protección, ya que no cabe duda de que, con esta facultad, el empresario puede incidir sobre la persona del trabajador de forma más directa, violándose con ella, en cierta medida, el derecho del art. 18.1 CE y también el art. 14 CE en tanto que somete a los trabajadores a una mayor incidencia en la vida privada que el resto de los ciudadanos[349].

En verdad, con esta facultad se trata de proteger la propiedad privada y el patrimonio empresarial[350] y el de los demás trabajadores de la empresa o de terceras personas, por lo que comúnmente se entiende que las facultades del art. 18 ET son exorbitantes[351], situando el derecho de propiedad[352] por encima de la dignidad del trabajador y reconociendo al empresario unos poderes policiales propios de una autoridad pública, sosteniéndose que supone el vaciamiento en el ámbito laboral de las garantías que la ley exige normalmente para el registro del ciudadano, al reconocer al empresario la posibilidad de realizar pesquisas sobre el trabajador sin mandato judicial previo en defensa del patrimonio empresarial y de los intereses propios de los demás trabajadores o de clientes[353].

349 POQUET CATALÁ, R., *El actual poder de dirección y control del empresario*, Cuadernos de Aranzadi Social, Navarra, 2013, Thomson Reuters Aranzadi, pág. 157.

350 DURÁN LÓPEZ. F., "Inviolabilidad de la persona del trabajador", en AA VV, *Comentarios a las Leyes Laborales*, Madrid,1983, Edersa, pág. 538.

351 Entre otros, DEL VALLE VILLAR, J. M., "El derecho a la intimidad del trabajador durante la relación de trabajo", en *Actualidad Laboral*, núm. 39, 1991, pág. 487; MONTOYA MELGAR, A., *Comentario al Estatuto de los Trabajadores*, Pamplona, 1998, Aranzadi, pág. 81; GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador*, Madrid, 1988, Civitas, pág. 161.

352 Sobre el derecho de propiedad, véase FERNÁNDEZ MÁRQUEZ, O., "La utilización por los trabajadores de los bienes de la empresa: un enfoque desde el derecho de propiedad", *Revista Española de Derecho del Trabajo* num.148/2010 parte Estudios, Pamplona, 2010, Civitas, págs. 1 y sigs.

353 GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador*, *op. cit.*, pág. 184; CARDONA RUBERT, Mª. B., "Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás. Comentario a la STC 241/2012, de 17 de septiembre", *Revista de Derecho social*, nº 60, 2012, págs. 169-180.

2. En cuanto a su ámbito objetivo, la doctrina mayoritaria[354] coincide en interpretar de forma amplia el concepto de efectos personales, si bien sostiene que los efectos personales son aquellos que previamente hayan sido introducidos en el centro de trabajo, incluido el vehículo del trabajador, siempre que el mismo hubiera sido introducido en el recinto de la empresa. No obstante, Goñi Sein[355] sostiene una concepción más estricta entendiendo que sólo son los bienes que posee el trabajador en el lugar de trabajo, de tal forma que todos los efectos personales que no estén en posesión de la persona del trabajador cuando éste se encuentre en el centro de trabajo quedan automáticamente excluidos de la previsión del artículo 18 ET.

Respecto de la necesidad de que los efectos personales objeto de control empresarial se hallen en el centro de trabajo, ello deriva del propio precepto estatutario que sólo permite el registro para evitar la salida de los bienes sustraídos a la empresa, estando, por tanto, prohibido el registro fuera del centro de trabajo. En segundo lugar, por lo que se refiere al requisito de que se trate de efectos de uso personal del trabajador, lo determinante es la conexión de los mismos con la esfera de la intimidad del trabajador[356], de forma que los efectos que pueden ser registrados son aquéllos que se encuentren en posesión del trabajador en el momento del registro o aquéllos otros que sean utilizados por éste.

3. Por otro lado, de conformidad con lo dispuesto en el art. 18 ET, el registro habrá de practicarse dentro del centro de trabajo, de modo que si algún registro hubiera de practicarse fuera de aquél siempre habrá de hacerse a través de los órganos legalmente habilitados para ello, no pudiendo ser

354 Por ejemplo, DURÁN LÓPEZ, F., "Artículo 18. Inviolabilidad de la persona del trabajador", en Borrajo Dacruz, E. (Dir.), *Comentarios a las Leyes Laborales*, Madrid, 1983, Edersa, pág. 544.

355 GOÑI SEIN, J. L., *El respeto a la esfera privada*…ídem. pág. 169.

356 AGUT GARCÍA, C., "Las facultades empresariales de vigilancia y control sobre útiles y herramientas de trabajo y otros efectos de la empresa", *Tribuna Social*, nº 163, 2004, pág. 14.

efectuado por el empresario, dado que de ser así estaríamos otorgando poderes de policía a éste[357]. A todo ello hay que añadir que el mismo habrá de realizarse dentro de la jornada laboral, siendo ilegales los registros efectuados fuera de aquélla, debiéndose contar, además, con la asistencia de un representante legal de los trabajadores o, en su ausencia, de otro trabajador de la empresa, al objeto de evitar manipulaciones y falsedades. A tal efecto, la STSJ Navarra, de 18 de abril de 2006 señala que el vaciado de la taquilla del trabajador viola el derecho a la intimidad de éste puesto que se efectuó sin la presencia del trabajador ni de ningún representante legal, habiendo sido razonablemente fácil localizar su paradero para comunicar al trabajador dicha operación empresarial.

De cualquier modo, si la ausencia de representante legal o de tercero no es por causa imputable al empresario, sino por el rechazo del trabajador a su presencia, la doctrina científica y judicial se ha mostrado conforme con dicha posibilidad[358].

4. Asimismo, se ha de señalar que el objeto del registro ha de ajustarse al fin pretendido, de forma que sólo se podrán llevar a cabo registros cuando sean necesarios para proteger el patrimonio empresarial o el de los demás trabajadores (art. 18 ET), de manera que, en primer lugar, se requiere que el mismo sea necesario y, en segundo lugar, el citado precepto lo pone en relación con el patrimonio empresarial o de los demás trabajadores, de modo que el registro se configura como una medida de carácter excepcional (principio de proporcionalidad) a utilizar sólo cuando los objetos sustraídos

357 GARCÍA NINET, I., *El control empresarial en el ámbito laboral*, Bilbao, 2005, CISS, pág. 206.

358 Véase HIERRO HIERRO, F. J., *Registros sobre la persona del trabajador, Libertad de empresa y poder de dirección del empresario en las relaciones laborales*, Abril, 2011, Aranzadi, pág. 56; STSJ Cataluña, de 14 de enero de 2009, que señala que *"…la exigencia legal de que en el registro de taquillas del trabajador en la empresa concurra un representante legal de los trabajadores viene exigido por el art. 18 ET en el caso de que se realice con carácter forzoso, unilateralmente por la empresa, pero no en el caso de que el trabajador voluntariamente acceda al mismo, mostrando su contenido, tal como se declara probado que sucedió en el presente caso"*.

pudieran llegar a poner en peligro el referido patrimonio (principio de necesidad), si bien, también se puede proceder al registro con el fin de proteger la seguridad de la empresa.

5. Establece también el art. 18 ET una exigencia de carácter finalista o teleológico al señalar que se habrá de respetar, en todo momento, la dignidad e intimidad del trabajador, en el sentido de que la práctica del registro se habrá de realizar de forma lo menos gravosa posible para aquél, cobrando ello especial sentido en relación con determinadas formas de practicar el mismo, como puede ser el despojo de la ropa o el cacheo. En estos casos, para legitimar la medida se deben observar las siguientes reglas: la primera es que el registro se practique ante personas del mismo sexo que el trabajador afectado cuando ello pueda implicar algún tipo de contacto físico o despojo de la ropa. En segundo lugar, la medida debe realizarse en un lugar discreto, no accesible al conjunto de los trabajadores. En tercer lugar, no se puede practicar el registro por la fuerza física, dado que ello transgrede los límites de los arts. 10 y 17 CE, pudiendo incurrirse en un ilícito penal.

6. No obstante, se ha de indicar que las garantías del art. 18 ET no resultan aplicables a los supuestos de control de los medios informáticos facilitados a los trabajadores para la ejecución de su prestación laboral por mor de lo establecido en la STS de 26 de septiembre de 2007, que entiende que el supuesto regulado por el art. 18 ET es completamente distinto del que se produce con ocasión del control de los medios informáticos en el trabajo, considerando éstos de propiedad de la empresa, la cual los facilita al trabajador para el cumplimiento de la prestación laboral, por lo que su uso cae dentro del ámbito del poder de vigilancia del empresario contemplado en el art. 20.3 ET[359] y no por el art. 18 del mismo cuerpo legal.

359 GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos de trabajo", *Revista Española de Derecho del Trabajo* num.164/2014 parte Comentario de Jurisprudencia, Ed. Aranzadi, Cizur Minor, 2014, págs. 12-15.

Es decir, para el TS no cabe la aplicación, siquiera sea analógica, del art. 18 ET a los supuestos de control del uso del ordenador por los trabajadores dado que no hay ni semejanza de los supuestos ni identidad de razón en las regulaciones[360]. En efecto, para el Alto Tribunal el supuesto de hecho es distinto del que tiene lugar con ocasión del control de los medios informáticos en el trabajo dado que el art. 18 ET atribuye al empresario un control que excede del que deriva de su posición en el contrato de trabajo, quedando, por tanto, el mismo fuera del marco regulador del art. 20 ET toda vez que el ordenador es un instrumento de producción cuya titularidad corresponde al empresario, teniendo éste facultades de control de la utilización del mismo[361], a lo que hay que unir el hecho de que con el ordenador se ejecuta la prestación laboral y, por tanto, el empresario está facultado para verificar y controlar su adecuado cumplimiento, lo cual no sucede en los supuestos del art. 18 ET.

En definitiva, entiende el TS que las garantías del art. 18 ET no resultan aplicables al control de los medios informáticos por las siguientes razones: en primer lugar, la necesidad de control de los citados medios no tiene que justificarse por la protección del patrimonio de la empresa ni del de los trabajadores de ésta dado que la legitimidad del mismo deriva de su carácter de instrumento de producción, de modo que el empresario tiene que controlar el uso del ordenador porque en él o a través de él se ejecuta la prestación laboral y, por tanto, habrá de comprobar si su uso es el adecuado. Con toda claridad, señala el TS que es evidente que el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del art. 18 ET, una justificación específica caso por caso, sino que, por el contrario, su legitimidad deriva directamente del art. 20 ET[362].

360 LUJÁN ALCARAZ, J., "La vigilancia empresarial sobre el uso de los medios informáticos puestos a disposición de los trabajadores", en *Libertad de empresa y poder de dirección del empresario en las relaciones laborales*. Estudios ofrecidos al Profesor Alfredo Montoya Melgar, Navarra, 2011, Thomson Reuters Aranzadi, Cizur Minor, pág. 133.

361 LUJÁN ALCARAZ, J., "La vigilancia empresarial…", *op. cit.,* pág. 133.

362 Así lo especifica la STS de 26 de septiembre de 2007.

En segundo lugar, la exigencia de respeto de la dignidad humana en el control no es requisito exclusivo de los registros del art. 18 ET, sino que esta exigencia es genérica para todas las formas de control empresarial, como se advierte a partir de la propia literalidad del art. 20.3 ET.

En tercer lugar, la necesidad de que el registro se haya de practicar en el centro de trabajo y en las horas de trabajo cobra virtualidad en el marco del art. 18 ET, el cual se refiere a facultades empresariales que, dado su carácter excepcional, no pueden ser ejercidas fuera del ámbito de la empresa, siendo evidente que el empresario no puede proceder al registro del trabajador o sus efectos personales fuera del centro de trabajo y del tiempo de trabajo ya que, en ese caso, sus facultades de policía privada resultarían desproporcionadas.

Y, finalmente, en cuarto lugar, la presencia de un representante de los trabajadores o de un trabajador de la empresa no se relaciona con la protección de la intimidad del trabajador registrado, sino que es, más bien, una garantía de objetividad y de eficacia de la prueba[363].

7. En suma, entendemos que la diferencia entre el artículo 18 y 20.3 ET reside, desde nuestro punto de vista, en la finalidad perseguida por ambos preceptos. La capacidad de vigilancia ordinaria o rutinaria del empleador deriva del peculiar régimen de derechos y obligaciones del sinalagma contractual laboral y la situación de subordinación del trabajador, siendo su límite la dignidad del trabajador. Por su parte, el art. 18 ET está regulando una cosa diferente como es el ámbito de privacidad de la persona asalariada, permitiendo la intromisión del empleador si se cumplen determinadas tutelas legalmente prescritas, siendo ésta una lógica que deriva claramente del contenido de la STS de 26 de septiembre de 2007.

363 LUJÁN ALCARAZ, J., "La vigilancia empresarial…", *op. cit.*, págs. 134-135.

Es decir, al ordenador, los archivos informáticos y el correo electrónico, de acuerdo con la doctrina jurisprudencial, no les resulta de aplicación el art. 18 ET, sino el art. 20 ET, por tratarse de medios que son propiedad de la empresa y, en consecuencia, su vigilancia entra dentro de las facultades normales de control del empresario[364], pudiendo decirse que no se trata de objetos de carácter personal, sino de herramientas de trabajo cuyo destino es facilitar la labor profesional[365].

8. Ahora bien, a tales efectos, parte de la doctrina[366] entiende que es necesario que la empresa haya establecido previamente las reglas de uso del correo electrónico de la empresa, siendo necesario, para poder vigilar el contenido de los mismos, que haya establecido previamente, de forma inequívoca, la prohibición total y absoluta del correo electrónico de la empresa para uso personal de los trabajadores[367], de modo que no exista ninguna expectativa razonable de confidencialidad, sino que el trabajador tenga conciencia que se le puede vigilar el uso que haga de los medios informáticos y sancionar un uso incorrecto del mismo, para así superar el pertinente juicio de proporcionalidad. En consecuencia, no se puede considerar una comunicación confidencial a través de un canal cerrado[368], pudiendo establecerse dicha prohibición de modo verbal, contractual o convencional, siempre que sea expresa y nítida[369].

364 STS de 26 de septiembre de 2007 y STC 241/2012, de 17 de diciembre.

365 TALENS VISCONTI, E., "La expectativa razonable de confidencialidad como presupuesto de vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario", en *Revista Doctrinal Aranzadi Social*, nº 51, 2013, pág. 2.

366 Entre otros, TOSCANI GIMÉNEZ, D. y VALENCIANO SAL, A., *Derechos fundamentales inespecíficos de los trabajadores*, Ed. Bomarzo, Albacete, 2016, pág. 76.

367 STS de 6 de octubre de 2011.

368 STC 241/2012, de 17 de diciembre. Tampoco existiría dicha expectativa razonable de confidencialidad cuando el ordenador utilizado no sea de uso personal, sino colectivo. STS de 6 de octubre de 2011. Vid. TALENS VISCONTI, E., "La expectativa razonable de confidencialidad...", *op. cit.*, *Revista Doctrinal Aranzadi Social*, nº. 51, 2013, pág. 3.

369 STC 170/2013, de 7 de octubre.

9. No obstante, este planteamiento resulta en la actualidad difícil de mantener a raíz de la doctrina sentada en las SSTEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía) y de 9 de enero de 2018 (caso López Ribalda *et alii* c. España) dado que el Tribunal de Estrasburgo entiende, de un lado, que la mensajería electrónica enviada desde una cuenta profesional debe considerarse correspondencia a todos los efectos y, de otro lado, que la normativa interna de las empresas no puede reducir la vida privada social en el marco de la relación laboral a cero, sino que subsiste en todo momento una expectativa razonable de privacidad a pesar de la existencia de una prohibición expresa y reiterada de uso de los medios informáticos de la empresa con fines personales.

Asimismo, sostiene que los controles que supongan un acceso por parte del empresario al contenido de las comunicaciones deberán ser sometidos a un control de proporcionalidad más intenso, debiendo someterse, asimismo, a ponderación la severidad de las medidas disciplinarias adoptadas por el empresario, de modo que entendemos que el empresario podrá constatar, de forma genérica, el uso indebido del correo electrónico mediante, por ejemplo, la revisión y control del historial o la bandeja de entrada de los correos recibidos y remitidos, pero que en ningún caso está facultado para abrir los correos, facultad, esta última, que sólo podrá hacerse previa autorización judicial debidamente fundamentada al efecto (argumento *ex* art. 18.3 CE y 90.2 y 4 LRJS)[370].

370 En idéntico sentido, SEPÚLVEDA GÓMEZ, M., "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites", en *Revista Temas Laborales*, nº 122, 2013, pág. 210.Por su parte, TOSCANI GIMÉNEZ, D. y VALENCIANO SAL, A., *Derechos fundamentales inespecíficos*…, op. cit, págs. 78-79, entienden que en este caso, o existe una normativa específica convencional o contractual o códigos de conducta internos o protocolos sobre el uso del correo electrónico, prohibiendo el uso por razones personales específicamente o, de lo contrario, los trabajadores tienen unas expectativas de derecho que obligará a la empresa a informar expresamente y con carácter previo, antes de poder acceder al correo electrónico, y además la información obtenida sólo se podrá utilizar para la finalidad comunicada al trabajador. Ahora bien, es preciso destacar a continuación que, en este supuesto concreto, no sólo se incide sobre el derecho a la intimidad del trabajador (art. 18.1 CE), sino también sobre el derecho al secreto de las comunicaciones (art. 18.3 CE) y que en este ámbito, en concreto, el texto constitucional exige una autorización judicial previa para poder acceder a las comunicaciones y para que, en consecuencia, la prueba sea lícita. Sin embargo, la jurisprudencia ha mantenido que tal

3.3.- Los Convenios Colectivos de condiciones de trabajo.

1. La negociación colectiva no ha mostrado históricamente demasiado interés por regular el uso de las tecnologías de la información en el seno de la relación laboral, si bien el mismo ha ido incrementándose progresivamente en las últimas negociaciones colectivas, siendo ejemplo de ello la previsión de constitución de comisiones para estudiar el fenómeno y regular su uso[371] o la llamada a las empresas bajo el ámbito funcional de aplicación de un determinado convenio para que entablen procesos de negociación con los representantes de los trabajadores tendentes al establecimiento de medidas para que puedan utilizarse los medios electrónicos de comunicación por los trabajadores sin que ello afecte al normal desenvolvimiento del proceso productivo[372].

2. Un análisis detallado de la negociación colectiva en la materia nos conduce a la identificación de cuatro grandes contenidos de convenios, a saber:

a) Un primer grupo de convenios incluyen una regulación de la materia, si bien referida principalmente a la utilización de las TIC con fines sindicales (el mismo no será objeto de análisis en este estudio por no constituir su objeto).

---

condicionante sólo es exigible en el ámbito del procedimiento penal. En efecto, el TS distingue entre el ámbito penal y el ámbito social o laboral. En el primero, los principios y las garantías que caracterizan el procedimiento penal exigen, en opinión de la Sala Segunda del TS, la aplicación de criterios más rigurosos en orden a poder justificar la injerencia en el derecho al secreto de las comunicaciones de los imputados, y evitar una vulneración de los derechos que éstos tienen reconocidos en el proceso penal.

371 Convenio Colectivo del sector de la industria siderometalúrgica de Madrid, código de convenio número 28003715011982 (BOCM de 2 de enero de 2016).

372 Convenio Colectivo de las Cajas de Ahorro, código de convenio nº 99000785011981 (BOE de 12 de agosto de 2016).

b) Un segundo grupo norma el uso de las TIC en el seno de la empresa para uso personal, si bien lo hace utilizando fórmulas abiertas, carentes de seguridad jurídica al objeto de evitar posibles conflictos.

c) Un tercer grupo, minoritario, destaca por ofrecer un modelo de regulación detallada del uso de las TIC en el seno de la empresa. Se trata, generalmente, de convenios de empresa.

d) Y, por último, un cuarto conjunto que regula el fenómeno solamente desde un plano meramente sancionador mediante su inclusión en el catálogo de faltas laborales[373].

3. Dentro del tercer grupo cabe mencionar el I Convenio Colectivo de empresas vinculadas a Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones, SAU, código de convenio nº 90100303012015, (BOE de 21 de enero de 2016) que, bajo la rúbrica "Utilización del correo electrónico e Internet", regula en su Capítulo XVI (art. 168) la actuación de la empresa y de los trabajadores y sus representantes cuando utilicen los medios técnicos que se ponen a su disposición para el desarrollo de la actividad laboral y las funciones de representación, respectivamente, bajo los siguientes principios:

a) Con carácter general, los empleados no podrán utilizar el correo electrónico, la Red Corporativa, ni Internet para fines particulares.

b) La Empresa, en ejercicio de su poder de organización y dirección y en defensa de sus legítimos intereses, podrá controlar el uso de las herramientas y medios técnicos que pone a disposición del trabajador para realizar su actividad laboral, en los términos que se contemplan en dicho Convenio Colectivo, debiendo realizarse el control empresarial de

373 COLÁS NEILA, E., *Derechos fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia,* Albacete, Bomarzo, 2012, págs. 121-127.

las herramientas informáticas y medios técnicos respetando los derechos fundamentales de los trabajadores.

A tal efecto, se pondrá especial atención en la protección de aquellos derechos más fácilmente vulnerables, en particular el derecho al secreto de las comunicaciones y a la intimidad y dignidad de los trabajadores, de modo que las medidas adoptadas por el empresario para el control de los sistemas informáticos habrán de ser proporcionadas al riesgo existente y necesarias para alcanzar un propósito específico, explícito y legítimo.

En orden a la consecución de dichos objetivos, se acuerda el establecimiento de una serie de normas de funcionamiento tendentes, por un lado, a regular las actuaciones de la empresa y, por otro, a establecer las normas de uso de los medios técnicos puestos a disposición de los trabajadores para la realización de su prestación laboral. Dichas normas podemos resumirlas del modo que sigue:

1.- Utilización del correo electrónico e Internet por los empleados:

- Los empleados pueden utilizar tanto el correo electrónico como la red corporativa e Internet con total libertad, en el sentido más amplio posible, para el desempeño de las actividades normales y habituales de su puesto de trabajo y en su relación con las organizaciones sindicales y el comité intercentros.

- Siempre que precisen realizar un uso de estos medios que exceda el habitual o se trate de envíos masivos o de especial complejidad, se utilizarán los cauces adecuados, de acuerdo con su jefe inmediato, para no causar daños en el desarrollo normal de las comunicaciones y en el funcionamiento de la red corporativa.

- Con carácter general, los empleados no podrán utilizar el correo electrónico, la red corporativa ni Internet para fines particulares.

a) Usos terminantemente prohibidos:

Bajo ningún concepto podrán los empleados falsificar mensajes de correo electrónico, enviar por correo mensajes o imágenes de material ofensivo, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, etc., así como aquéllos que promuevan el acoso sexual o moral o inciten a la violencia.

b) Utilizaciones en perjuicio de la Empresa:

También se prohíbe utilizar estos medios para realizar envíos masivos de mensajes, así como enviar mensajes con anexos de gran tamaño (capacidad) y realizar cualquier tipo de envío sin relación alguna con el desempeño profesional que interfiera las comunicaciones del resto de empleados o perturbe el normal funcionamiento de la red corporativa.

c) Otros usos no permitidos:

En particular, quedan prohibidas las siguientes conductas: el envío de cadenas de mensajes electrónicos; la utilización de listas de distribución para fines ajenos a la actividad del puesto de trabajo, así como el uso de la red para juegos de azar, sorteos, apuestas, descarga de vídeo, audio u otros materiales no relacionados con la actividad profesional. El incumplimiento de estas normas determinará la utilización de las restricciones que se consideren oportunas en el uso de estos medios y la aplicación del régimen disciplinario, en su caso.

Cuando existieren indicios de un uso ilícito o abusivo por parte de un empleado, la empresa podrá realizar las comprobaciones oportunas y, si fuere necesario, realizará una auditoría en el ordenador de éste, la cual habrá de hacerse en horario laboral y en presencia de algún representante de los trabajadores o de la organización sindical que proceda en caso de afiliación, si el empleado lo desea, y con total respeto a su dignidad e intimidad.

Obsérvese que resultan aplicables en este caso las garantías previstas en el art. 18 ET en lo relativo a la realización de la auditoría en horario laboral y con presencia de representante sindical.

4. Por su parte, son muy numerosos los convenios colectivos que se pueden incluir dentro del cuarto grupo. Así, por ejemplo, el sector de la madera aporta numerosos ejemplos de este tipo tanto en los convenios de ámbito provincial como en el estatal[374], previéndose en todos ellos, como falta grave, el uso reiterado o perjudicial para el proceso productivo del teléfono móvil o de aparatos multimedia (aun propiedad del trabajador) para fines personales durante la jornada laboral, así como el uso no autorizado para fines particulares de las herramientas de la empresa. También constituye falta grave el uso no autorizado y para fines particulares de las herramientas de la empresa

374 Así sucede con el Convenio Colectivo del Sector de la Madera de Almería, Código Convenio 04000395011982, (BOP Almería de 16 de septiembre de 2011); Convenio Colectivo del Sector de Industrias de Carpintería y Ebanistería de Ávila, Código del Convenio Actual n°05000482012000, (BOP Ávila de 28 de febrero de 2014); Convenio Colectivo de Actividades de Carpintería y Molduras, Cestería y Artículos de Mimbre y Junco; Ebanistería y Tapicería, Carrocerías y Carreterías, Chapa y Tableros y Aglomerados y Almacenistas de Madera de Guadalajara, código de convenio 19000225011981, (BOP Guadalajara de 14 de agosto de 2013); Convenio Colectivo de fabricantes de muebles, carpintería, tapicería y ebanistería de Ourense, código de convenio 32000185011982 (BOP Ourense de 11 de diciembre de 2013); Convenio Colectivo para Industrias de la Madera de Salamanca, código de convenio 37000325011981, (BOP Salamanca de 16 de agosto de 2013); Convenio Colectivo del sector de Aserraderos y Almacenistas de Madera de Cantabria, Código de convenio 39000655011982, (BO de Cantabria de 28 de abril de 2011); Convenio Colectivo del sector de industrias y almacenes de la madera de Cádiz, Código de convenio 11000485011982, (BOP Cádiz de 29 de agosto de 2013); Convenio Colectivo Provincial para las Industrias de la Madera de Toledo, Código de Convenio 4500265, (BOP Toledo de 28 de enero de 2008); Convenio Colectivo estatal de la Madera, código convenio 99010175011996, (BOE de 27 de noviembre de 2012).

(incluidos los equipos informáticos). Estas previsiones no son de aplicación a la representación sindical de los trabajadores en el ejercicio de sus funciones.

Por otro lado, se consideran faltas muy graves en todos ellos la reiteración en el uso no autorizado y con carácter personal de las herramientas de la empresa (incluidos los equipos informáticos), dentro o fuera de la jornada laboral, siempre que ese uso sea contrario a los usos y costumbres.

Otros ejemplos de este tratamiento exclusivamente punitivo se encuentran también en el Convenio Colectivo de Grandes Almacenes (BOE de 8 de abril de 2013), que incluye diversas infracciones en sus diferentes grados: señala como falta leve el uso de los medios de comunicación empresariales con fines distintos a aquéllos para los cuales se encuentre habilitado, sin mayor precisión al respecto, así como el empleo de teléfonos móviles durante la jornada laboral; como falta grave, proporcionar la clave personal de acceso a un tercero, simular la identidad de un compañero o realizar copias de ficheros sin previa autorización empresarial; y como falta muy grave la violación de las normas sobre seguridad informática o la transgresión de la confidencialidad de los datos.

En cambio, tanto el Convenio Colectivo del sector de Industrias Transformadoras de Plásticos de la Comunidad de Madrid -código de convenio 28003155011981- como el XVIII Convenio colectivo de la Industria Química -código de convenio 99004235011981- (BOCAM de 14 de mayo de 2016 y BOE de 19 de agosto de 2015, respectivamente), regulan únicamente como falta leve la utilización para fines distintos a los relacionados con la prestación laboral de los medios informáticos propiedad de la empresa, tales como correo electrónico, intranet, Internet o cualesquiera otros para fines personales. Por otro lado, el Convenio Colectivo del Sector del Comercio Textil de Valencia -Código de convenio 46000555011982- (BOP de Valencia de 20 de octubre de 2017) incluye como falta grave el uso personal de los medios telemáticos (teléfono, Internet, correo electrónico, etc.), siempre y cuando ello no origine un

perjuicio grave a la empresa, en cuyo caso la falta se calificará como muy grave.

Por su parte, el Convenio Colectivo de "Consum, Sociedad Cooperativa Valenciana"- código de convenio 90012062012002- (BOE de 15 de diciembre de 2014) tipifica también como falta muy grave el uso particular de los medios de comunicación electrónica de la empresa, estableciendo la facultad de ésta para poder acceder a las comunicaciones con el objeto de verificar si se produce una utilización desviada de los mismos, siempre que existan indicios razonables de uso indebido.

Asimismo, el Convenio Colectivo del sector del comercio en general de las comarcas de Lleida –Código de convenio 2500065011993- (BOP Lleida de 22 de junio de 2017) prevé como falta grave un uso desproporcionado, contrario a la buena fe contractual o no razonable, del correo electrónico, intranet o extranet.

Finalmente, en el XVI Convenio Colectivo de la empresa ONCE y su personal – Código de convenio 90003912011984- (BOE de 18 de enero de 2018), se establece como falta leve el uso de los medios telemáticos para actividades no relacionadas directamente con el puesto de trabajo y como falta grave compartir o facilitar el identificador de usuario y contraseña con otras personas, el *spam* o envío masivo de correos electrónicos con fines comerciales sin consentimiento de la organización, la instalación de cualquier software sin consentimiento de la empresa, leer, borrar o modificar los mensajes de correo electrónico o archivos de otros usuarios, excepto las personas autorizadas a ello por la empresa, etc.

5. En definitiva, la negociación colectiva –salvo en contadas ocasiones, fundamentalmente en los denominados convenios de empresa – está desaprovechando la oportunidad de regular minuciosamente la potestad de

vigilancia del empresario del uso de las TIC por parte de los trabajadores en el seno de las empresas proporcionando a ambos reglas claras y proporcionadas, lo que unido a los inconvenientes derivados de la indeterminación de la normativa heterónoma ha supuesto un notable incremento del papel que desempeña en este ámbito la jurisdicción laboral, constitucional y europea.

En suma, no existe un verdadero interés en regular minuciosamente esta problemática más allá de la preocupación mostrada por los sindicatos en regular el uso del correo electrónico para usos sindicales. No obstante, la publicación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales hará con toda seguridad que, en las sucesivas negociaciones colectivas, se incremente el interés por regular una materia que afecta de manera decisiva a derechos fundamentales de los trabajadores.

4.- Fijación unilateral de reglas por parte de las empresas: la autorregulación.

1. La fijación de reglas unilateralmente por parte de las empresas mediante el establecimiento de códigos de conducta internos es una práctica cada día más arraigada en empresas de carácter multinacional, presentando las mismas, con carácter general, un marcado acento restrictivo[375].

La vía de los códigos de conducta es aconsejada por diversas organizaciones tales como la *EEMA – The European Association for e-Identity & Security*[376], que establece entre las recomendaciones formuladas el recurso a avisos sobre la política empresarial en la pantalla del ordenador, cuya aceptación es requisito previo e imprescindible para acceder al sistema y, por tanto, para el desarrollo de la actividad laboral. Esta misma línea restrictiva al

375 MCINTOSH, D., "E-monitoring@workplace.com: the future of communication privacy in the Minnesota Private-Sector Workplace", *Hamline Law Review*, núm. 23, 2000, pág. 542.

376 https://www.eema.org/

uso de los medios electrónicos en la empresa es seguida, por ejemplo, por la patronal italiana *Confindustria* en su documento *Linee Guida per l´utilizzo dei sistema informatici aziendali*[377]. Entre las recomendaciones contenidas en este último documento cabe señalar la necesidad de dotar a los trabajadores de una cuenta de correo electrónico personal o privada, en paralelo a la cuenta empresarial o profesional destinada en exclusiva al desarrollo de la actividad laboral. Esta solución técnica es sugerida también por el Grupo de Trabajo sobre Protección de Datos (GTPD)[378] [cuya creación se prevé en el art. 29 de la Directiva 95/46/CE, de 24 de octubre], que aboga por que el trabajador pueda disponer de una cuenta de correo de carácter exclusivamente profesional y otra de uso estrictamente privado, o bien permitir la utilización del correo web.

2. Los Códigos de Conducta, en cuanto manifestación que son del poder de dirección, se encuentran sujetos a los mismos límites que cualquier otra manifestación del referido poder empresarial, concretamente, a los límites internos derivados del contrato de trabajo y a los límites externos derivados del respeto a los derechos fundamentales[379].

Un análisis de la diferente tipología de Códigos de Conducta internos de las empresas nos lleva a distinguir entre aquéllos que no contienen referencia

377 https://www.avis.it/emilia-romagna/repository/off_legge/6_up_allegato.pdf

378 GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS – ARTÍCULO 29 (2002), "Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo", Bruselas: 5401/01/ES/Final (WP 55). Señalar que el Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, es un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea, que realiza funciones de secretariado. Las funciones del GT29 reconocidas por la Directiva incluyen estudiar todas las cuestiones relativas a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva; la emisión de dictámenes sobre el nivel de protección existente dentro de la Comunidad y en países terceros; el asesoramiento a la Comisión sobre cualesquiera proyectos de modificación de la Directiva, así como formular recomendaciones sobre cualquier asunto relacionado con la protección de datos en la Unión Europea.

379 CALVO GALLEGO, F.J., *Códigos Éticos y Derecho de los Trabajadores*, Bomarzo, Albacete, 2008, págs. 72-80.

alguna al uso de las TIC por parte de los trabajadores y los que sí contienen una referencia expresa a las mismas regulando su uso por parte de aquéllos.

4.1.- Códigos de Conducta que no contienen referencias al uso de las TIC por parte de los trabajadores.

Esta tipología de Códigos de Conducta que no contienen referencia alguna al uso de las TIC por parte de los trabajadores suelen ser, más bien, protocolos operativos de la actividad de la empresa[380], en tanto que otros están ligados a la responsabilidad social corporativa de la compañía, desarrollando en su seno cuestiones de diversa índole tales como ética, medio ambiente, conciliación de la vida laboral y familiar[381], etc.

En la misma línea se mueven otros Códigos que contienen referencias genéricas a los "bienes de la empresa" o a los "recursos empresariales" sin contener mención alguna al uso de las tecnologías de la información por parte de los trabajadores. Así, el Código de Conducta de LM Wind Power A/S contiene una escueta referencia a la utilización de los recursos de la empresa para fines profesionales. Y en el mismo sentido, el Código de Endesa o del de Enagás que, al contemplar el uso de los recursos de ésta, establece la obligación de un uso eficiente de los mismos, al tiempo que expresa un deber de protección frente a cualquier uso inadecuado de los que pudieran derivase perjuicios para los intereses de la compañía, pero sin referirse en ningún momento al uso de las TIC por parte de los trabajadores.

380 En este sentido, los Códigos de Conducta de BBVA Mercado de Valores y de Abertis establecen las normas relativas a cómo se deben efectuar las operaciones en una actividad donde la confidencialidad de la información es primordial.

381 En este grupo cabe incluir los Códigos de Conducta de Nestle, Adolfo Domínguez, Gas Natural, Inditex, Ferrovial, etc.

En idéntico sentido se pronuncia el Código de Conducta de ACS, que tras indicar que se pone a disposición de los empleados los recursos necesarios para el desempeño de su actividad laboral, establece de modo genérico que éstos deberán utilizar los recursos de la empresa de forma responsable, eficiente y apropiada al entorno de su actividad profesional y el de Acciona que también, de forma poco concreta, al hablar del uso y protección de activos empresariales, señala que los recursos de la empresa deberán ser utilizados de forma responsable y apropiada en el entorno de su actividad profesional.

En líneas generales, cabe señalar que este conjunto de Códigos de Conducta sólo contienen formulaciones generales carentes de precisión y seguridad jurídicas que permiten el uso de todas las TIC por parte de los trabajadores.

4.2.- Códigos de Conducta que sí regulan el uso de las TIC por los trabajadores.

Existen Códigos que sí contienen una regulación exhaustiva del uso de las tecnologías de la información y comunicación en el seno de la empresa concretando esa regulación bien en sentido prohibitivo, bien en sentido permisivo.

4.2.1.- Prohibición del uso personal.

Ejemplo de Código prohibitivo es el de la empresa Cepsa, el cual contiene precisiones concretas de carácter restrictivo acerca del uso de las nuevas tecnologías por parte de los empleados considerando dicho uso como no ético o inmoral. A tal efecto, se establece, respecto de los recursos informáticos puestos a disposición por la empresa, que los mismos deben

sujetarse a un uso autorizado, que es el que tiene por finalidad el desarrollo de las actividades del puesto de trabajo, incluyéndose en la expresión “recursos informáticos” los equipos informáticos, así como los programas y aplicaciones, comunicaciones de voz y servicios de acceso a la red.

Es de destacar que este protocolo regula los usos prohibidos de los recursos informáticos agrupándolos en cuatro grandes categorías: usos ilegales, no éticos o inmorales, usos abusivos, usos sindicales distintos a los previstos en el convenio colectivo y usos maliciosos. Así, por ejemplo, si los recursos son utilizados con fines de lucro personal se considerará una utilización no ética o inmoral, mientras que si la utilización se hace con fines extra laborales, pero sin apreciarse un lucro personal, se calificará como uso abusivo.

Por lo que respecta al uso del correo electrónico, se establece que las cuentas de correo electrónico son puestas a disposición de los empleados con la finalidad exclusivamente laboral; y, por otro, se advierte de la posibilidad de control empresarial sobre el correo electrónico, al señalarse el derecho de la empresa de acceder a las cuentas, los archivos, buzones y direcciones de correo electrónico por razones organizativas, de seguridad o del puesto de trabajo, al tiempo que también se contextualizan los usos prohibidos en las cuatro grandes categorías antes referidas: usos ilegales, no éticos o inmorales, usos abusivos, usos sindicales distintos a los previstos en el convenio colectivo, usos indebidos.

Dentro de las medidas de privacidad se establece, por un lado, que los mensajes podrán ser registrados y analizados por la empresa, de acuerdo a los procedimientos operativos de seguridad y auditoría establecidos en la empresa; y, por otro lado, no se permite la utilización desde el puesto de trabajo de servicios proporcionados por otros proveedores de correo electrónico, correo

web o mensajería instantánea, así como el uso de cuentas de correo personales que no hayan sido autorizadas por la empresa.

En lo referente al uso de Internet, el Código vuelve a marcar las mismas pautas anteriores, señalando que el acceso a Internet queda limitado a sitios que contengan información relacionada con la actividad de la empresa o de las actividades del puesto de trabajo, reservándose la empresa el derecho de acceso, reasignación, cancelación o modificación por razones organizativas, de seguridad o del puesto de trabajo.

4.2.2.- Admisión del uso particular.

1. En el ámbito de la Administración de Justicia, la Instrucción 2/2003, de 26 de febrero (BOE nº 59, de 10 de marzo de 2003) contiene el Código de Conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia, siendo la regla general la de una inicial utilización para fines profesionales de las nuevas tecnologías que es matizada al permitirse un uso personal excepcional u ocasional. Este Código es modelo de regulación exhaustiva y profusa del uso de las nuevas tecnologías en el ámbito de la Administración de Justicia, pudiendo servir el mismo de ejemplo para otras Administraciones Públicas y empresas privadas.

En lo relativo a los equipos informáticos, dado que se afirma que son puestos a disposición para la realización del trabajo, se declara que no son idóneos para un uso personal o extraprofesional, si bien, dicha prohibición queda matizada al permitirse su utilización excepcional para actividades personales no reservadas y siempre de conformidad con la normativa reglamentaria desarrollada por la Administración competente (Estado y/o Comunidades Autónomas), sin que en ningún caso se puedan alterar o conectar elementos externos sin la autorización expresa.

Respecto de la utilización de los programas y archivos informáticos, sigue la misma pauta que para los equipos, de forma que deben ser utilizados solo con fines profesionales, no siendo idóneos para un uso personal o privado. No obstante, de manera excepcional, los documentos personales que se confeccionen podrán guardarse en el archivo personal del disco duro del ordenador asignado a cada empleado.

En cuanto al acceso a Internet, éste debe estar vinculado a los fines profesionales, si bien se permite el acceso para fines personales ocasionales, que deberán restringirse al máximo, quedando prohibido el acceso a páginas de contenido ofensivo o atentatorio a la dignidad humana.

Sin embargo, en relación al correo electrónico la pauta de uso que se establece, aunque se permite un uso personal, no despliega una expectativa de intimidad, posibilitando su control empresarial al establecerse que debe utilizarse para fines profesionales, quedando prohibido el uso para actividades personales restringidas en las que pudiera haber una expectativa de privacidad o secreto en las comunicaciones.

2. De similar contenido, aunque algo más limitativo en lo relativo al uso personal de las nuevas tecnologías, es el Código de Conducta Telemático para los empleados de CaixaBank, el cual norma el uso de la intranet, el acceso a Internet, el uso de los equipos informáticos, correo electrónico, etc., siendo los aspectos más importantes que regula en cuanto aquí interesa los siguientes:

a) La navegación por Internet habrá de responder a fines profesionales, facultándose a la empresa para acceder a los datos de conexión a Internet almacenados en los servidores de la empresa, así como revisar los datos de las conexiones y su contenido hechos desde los ordenadores utilizados por los empleados.

b) En cuanto al correo electrónico, se pone a disposición de los empleados una cuenta de correo inscrita en el servidor y con nombre de dominio de la propia empresa, insistiéndose que para esta herramienta no existe expectativa alguna de privacidad en su utilización, estando facultada la empresa para auditar todas las comunicaciones que tengan lugar entre empleados, profesionales, clientes, proveedores, etc. Es sumamente relevante que, adicionalmente a este correo de uso profesional, la entidad se comprometa a facilitar una cuenta de correo para uso personal, gratuito y gestionado por empresa externa, cuyo uso será responsabilidad exclusiva del trabajador. La utilización de esta cuenta personal no podrá afectar al normal desenvolvimiento de la actividad productiva. Para ambas cuentas de correo se establecen determinadas pautas comunes: no podrán enviarse mensajes ilegales, ilícitos, atentatorios contra la dignidad humana, prohibiéndose, asimismo el uso del correo electrónico de otros compañeros. Una vez finalizada la relación laboral, la empresa puede mantener las relaciones con clientes a través del correo electrónico profesional, pero queda desvinculada totalmente del correo personal, pudiendo mantenerlo el empleado, asumiendo los costes que ello suponga. En cuanto a las posibilidades de realizar auditorías en ambas cuentas, la profesional podrá ser revisada periódicamente, y la personal sólo cuando lo determine la autoridad judicial.

c) Se establecen, asimismo, unas pautas generales aplicables al uso de todos los equipos informáticos y de los medios de comunicación previéndose, en primer lugar, que el uso no puede repercutir en el normal desarrollo de la actividad laboral, especialmente en lo que al correo electrónico e Internet se refiere. En segundo lugar, se pone a disposición un correo de Seguridad Informática al que los empleados podrán formular dudas relacionadas con el código de conducta y plantear sugerencias.

3. Se puede o no estar de acuerdo con estos Códigos de Conducta. A su favor cabe decir que ofrecen, al menos, seguridad jurídica al trabajador, si bien, para la determinación de su contenido considero imprescindible la participación de los representantes de los trabajadores, encargándose la negociación colectiva de establecer las posibilidades de utilización de las TIC en la empresa por los trabajadores y, en su caso, los límites y procedimientos de control. Ello a pesar de que algunos autores[382] han sostenido que, por encontrarnos ante derechos fundamentales como la intimidad, las soluciones colectivas no pueden ser nunca la respuesta. Igualmente se plantea la cuestión de si es posible la renuncia de derechos en esta sede y, en cualquier caso, de ser posible la misma, con qué extensión y requisitos.

En cualquier caso debe tenerse en cuenta que nos hallamos ante derechos fundamentales y, en este sentido, según la jurisprudencia constitucional, en la línea de lo establecido por el TEDH, la renuncia a los mismos, cuando fuere posible, debe ser expresa y formulada en términos inequívocos[383]. De cualquier modo, se corre el peligro de que si únicamente se exige el establecimiento de una política empresarial de prohibición absoluta del uso de los medios informáticos de la empresa para fines privados para poder realizar el control de los mismos, la empresa pueda, sin demasiados escorzos, desnudar la intimidad del trabajador en la empresa, al colocar en sus manos una potente herramienta, tal cual serían los códigos de conducta o normas de uso emanadas de aquellas y comunicadas fehacientemente a los trabajadores,

382 OLIVER, H., "Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out", *Industrial Law Journal*, vol. 31, núm. 4, 2002, pág. 351. En relación a la regulación por la negociación colectiva de aspectos relativos a derechos fundamentales inespecíficos, puede verse el trabajo colectivo dirigido por SEMPERE NAVARRO A. y SAN MARTÍN MAZZUCONI, C., *Derechos fundamentales inespecíficos y negociación colectiva*, Thomson Reuters, Navarra, 2011.

383 SSTEDH de 6 de diciembre de 1998 (caso Barberá, Messegué y Jabardo); de 23 de mayo de 1991 (caso Oberschlick); de 29 de agosto de 1991 (caso FCB contra Italia) y de 23 de noviembre de 1993 (caso Poitrimol).

donde se prohíba terminantemente el uso de los medios informáticos para fines privados[384].

5.- La protección de datos personales y la garantía de los derechos digitales en el ámbito laboral.

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

1. El derecho a la protección de datos se encuentra regulado, a nivel interno, en la Ley Orgánica 3/2018, de 5 de diciembre, Protección de Datos Personales y garantía de los derechos digitales y por las regulaciones de la Agencia Española de Protección de Datos.

Esta Ley se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (art. 2.1), entendiéndose por datos personales toda información sobre una persona física identificada o identificable (el interesado), por persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (art. 4.1 Reglamento Europeo de Protección de Datos) y por tratamiento cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos

384 GUTIÉRREZ PÉREZ, M., "Prohibición expresa del uso privado del ordenador de la empresa como fundamento para su control", *Revista Española de Derecho del Trabajo* num.165/2014 parte Comentario de Jurisprudencia, Aranzadi, Cizur Minor, 2014, pág. 3 y sigs.

personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (art. 4.2 Reglamento Europeo de Protección de Datos).

Dato personal es, pues, aquél que permite la identificación de una persona y que debe ser objeto de tratamiento manual o automatizado, lo que supone realizar ciertas actividades como el almacenamiento o archivo de los datos o la conexión de los datos entre sí. De tal forma que el dato personal se define, por un lado, por la información y, por otro, por la identificación, entendiéndose como persona identificable toda aquélla cuyos datos razonablemente asociados puedan dar lugar, sin mayores esfuerzos, a su identificación[385].

Dichos datos habrán de ser utilizados por el empresario, de conformidad con el principio de buena fe, respetando unas exigencias mínimas que garanticen que, en el procedimiento seguido para su obtención, tratamiento y clasificación no se han empleado técnicas engañosas que pudieran inducir a error al trabajador. Así, por ejemplo, no se puede condicionar la firma del contrato de trabajo a la entrega, por parte del trabajador, de determinados datos de carácter personal para ponerlos a disposición del empleador, tales como el número de teléfono móvil o el correo electrónico, cuando tales datos no son necesarios para el mantenimiento o cumplimiento del contrato, pues ello, en realidad, es una forma de obligar al trabajador a desvelar información personal, en su afán de conseguir el empleo, para uso y disfrute del empresario, lo que constituye una conducta abusiva por parte del empleador y,

385 Sentencia de la Audiencia Nacional de 8 de marzo de 2003.

en consecuencia, una vulneración del derecho del trabajador a la protección de datos[386].

Los datos, por lo demás, deben ser recogidos y conservados con exactitud, lo que significa que tanto el responsable como el encargado del fichero deben ajustar la información a la situación real, precisa, completa y actual del trabajador[387], realizando las correcciones o cancelaciones que considere oportunas para mantener la información actualizada[388].

2. Por otro lado, en el caso de las relaciones laborales es muy importante tener en cuenta que el fichero de datos tiene una finalidad laboral determinada, explicita y legítima y, por ello, el empleador únicamente podrá recabar aquella información que resulte pertinente y no excesiva para tal efecto, a cuyo objeto habrá de tener en cuenta el tipo de empleo y las necesidades evolutivas de información de la empresa. Asimismo, el tratamiento de los datos que realice la empresa deberá abocarse exclusivamente a cumplir las finalidades laborales determinadas, explicitas y legítimas para las cuales tal información fue recogida, pues es la finalidad laboral la que legitima el uso y tratamiento de datos personales de los trabajadores por parte de la empresa, de modo que el empleador no se encuentra facultado para recabar información cuya finalidad sea indeterminada, ilícita o contraria al ordenamiento jurídico.

De ahí que exista una especial protección para las denominadas "categorías especiales de datos personales" (afiliación sindical, religión, orientación sexual, ideología, creencias u origen racial o étnico y salud) recogidos en el art. 9 Ley 3/2018, de 5 de diciembre y art. 9 Reglamento (UE) 2016/679. En principio, salvo el caso de empresas de tendencia o la existencia

386 Sentencia de la Audiencia Nacional de 28 de enero de 2014.

387 CARDONA RUBERT, Mª. B., *Informática*…, *op. cit.,* pág. 112.

388 DEL REY GUANTER, S., "Tratamiento automatizado de datos de carácter personal y contrato de trabajo: una aproximación a la intimidad del trabajador", *Relaciones Laborales*, nº 15, 1993, pág. 20.

de previa habilitación legal y con el respeto a las garantías precisas, estos datos no tienen relevancia o interés alguno para el adecuado desarrollo de la prestación laboral, por lo que el empresario no se encuentra facultado para indagar y, mucho menos, almacenar, tratar o retener las informaciones del trabajador relativas a tales extremos[389] y, por tanto, incluso con el consentimiento del trabajador, el tratamiento de estos datos especiales por parte del empresario resultaría ilícito dada la irrenunciabilidad de este tipo de derechos (art. 9.1 Ley 3/2018, de 5 de diciembre).

También son considerados datos sensibles los relativos a la comisión de infracciones penales por parte del trabajador, de modo que el empresario no puede hacer acopio o tratamiento de esta información. Así lo entiende la Recomendación sobre Protección de Datos Personales de la OIT cuando afirma en su art. 6.5.1 que los empleadores no deberían recabar los datos relativos a antecedentes penales de los trabajadores y, de ser necesario su acopio, este debe limitarse exclusivamente a los que guardan una relación manifiesta con el puesto de trabajo.

Esta limitación no alcanza a las infracciones laborales, las cuales sí podrán ser registradas por el empresario. Ello se debe a que esta información es necesaria para el desarrollo de la relación laboral o del contrato de trabajo, por ejemplo, a efectos de valorar la reincidencia del trabajador en la comisión de faltas laborales, su cambio positivo de actitud o su participación o no en determinados conflictos. Obviamente, ello no supone que el empleador pueda hacer público estos datos, pues esto resultaría una actuación a todas luces arbitraria, impertinente y contraria al derecho a la intimidad del trabajador[390].

389 TASCÓN LÓPEZ, R., "La protección de datos personales de los trabajadores", *Revista Jurídica de Castilla y León*, nº 16, 2008, pág. 475.

390 CASTRO ARGÜELLES, Mª. A., *El régimen disciplinario en la empresa. Infracciones y sanciones laborales*, Aranzadi, Pamplona, 1993, págs. 41-42.

5.2.- Normativa supranacional.

5.2.1.- Derecho Comunitario.

1. En cuanto al marco normativo en el ámbito de la Unión Europea, el mismo encuentra reflejo, en el derecho originario, en la Carta de Derechos Fundamentales de la Unión Europea, hecha en Estrasburgo, de 12 de diciembre de 2007 (art. 8), en el Tratado de Funcionamiento de la Unión Europea (art. 16) y en el Tratado de la Unión Europea (art. 39) y, a nivel de derecho derivado, en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016[391], relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

2. Asimismo, en el ámbito de la Unión Europea destaca el Dictamen 8/2001, de 13 de septiembre de 2001, sobre el tratamiento de datos personales en el contexto laboral, adoptado por el Grupo de Trabajo del Artículo 29, que insiste en la idea de que la recopilación, almacenamiento y uso de información sobre los trabajadores por medios electrónicos, así como las herramientas informáticas de uso común en las empresas, tales como el correo electrónico o el acceso a Internet, implican de modo general el tratamiento de datos personales de los trabajadores, a los que hay que añadir otras potenciales formas de control del trabajador entre las que destacan los sistemas de video vigilancia, a los que se debe aplicar la normativa sobre protección de datos.

En este Dictamen, el Grupo enumera los Principios Fundamentales de la Protección de Datos que los empresarios deberán siempre tener en cuenta en

391 Esta norma, pese a ser un Reglamento, cuya entrada en vigor se retrasó dos años, fue una norma con forma de Reglamento y alma de Directiva.

el ámbito laboral, destacando al respecto los principios de Finalidad y Transparencia, referidos a la necesidad de un uso legítimo de los datos, adecuados a un fin propio de la actividad laboral, así como a la obligación de que los trabajadores hayan de conocer qué datos recoge el empresario acerca de ellos.

A su vez, el principio de legitimidad se vincula al de proporcionalidad, debiendo ser los datos recabados adecuados, pertinentes y no excesivos en relación con la necesidad de su recogida, estableciéndose la obligación de que los trabajadores sean adecuadamente informados sobre la existencia de dicho tratamiento legítimo y proporcionado, lo que referido a la vigilancia de los trabajadores a través del correo electrónico, Internet, cámaras de vídeo o datos de localización, se traduce en la necesidad de que el control habrá de ser una respuesta proporcionada del empleador ante riesgos ciertos, y teniendo siempre en cuenta el derecho a la vida privada de los trabajadores.

Por otro lado, recae sobre el empresario la responsabilidad inexcusable de velar por la exactitud, actualización y conservación de los datos, adoptando al efecto las medidas de seguridad pertinentes en orden a preservar la información obtenida en el ámbito de la empresa e impidiendo el acceso indebido y la difusión no autorizada de dichos datos.

Especial referencia merecen dos importantes aspectos abordados por el Dictamen, como son el tratamiento del “consentimiento” del trabajador en el ámbito laboral y la “interacción entre la legislación laboral y la legislación sobre protección de datos”. Por lo que respecta al “consentimiento”, el Grupo de Trabajo del Artículo 29 entiende que si un empresario debe tratar datos personales como consecuencia de la relación laboral, no debería legitimar este tratamiento a través del consentimiento, sino que el recurso al consentimiento habrá de limitarse a los casos en los que el trabajador pueda expresarse de

forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.

Finalmente, el "Grupo de trabajo" sostiene que la legislación sobre protección de datos no debe aplicarse de forma autónoma e independiente del Derecho del Trabajo y que éste, a su vez, no puede aplicarse aisladamente sin tener en cuenta la legislación sobre protección de datos, sino que esta interacción es necesaria y valiosa, debiendo contribuir la misma al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores.

5.2.2.- Normativa de la Organización Internacional del Trabajo (OIT) y otras Organizaciones.

1. En el terreno laboral existen diversos documentos internacionales que abordan la problemática de la protección de datos en dicho ámbito. Entre ellos destacan el Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores de la OIT de 1 de septiembre de 1997[392], el cual establece un exhaustivo elenco de aquéllas tendentes a proporcionar orientaciones para la protección de los datos personales de los trabajadores. El mismo carece de carácter obligatorio y no suple la legislación nacional, si bien puede ser utilizado para la elaboración e interpretación de leyes, reglamentos, convenios colectivos, directivas y políticas laborales a nivel de empresa, extendiéndose su aplicabilidad tanto a los sectores privado como público y al tratamiento manual y automatizado de los datos personales de un trabajador.

En lo que nos concierne, señalar que el Repertorio de recomendaciones prácticas de la OIT se refiere expresamente a la vigilancia de los trabajadores señalando al respecto que los medios tradicionales de vigilancia, tales como la

392 https://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf

intervención de teléfonos o la video vigilancia, se complementan con otros métodos más sutiles y tecnológicamente avanzados como el registro del correo electrónico, a lo que hay que añadir que los trabajadores son objeto, cada vez en mayor medida, de una vigilancia indirecta que permite recabar datos que pueden transformarse con facilidad en medios de vigilancia.

El Repertorio no prohíbe la vigilancia de los trabajadores, si bien fija límites muy precisos, debiendo cumplir aquélla con dos premisas, a saber: en primer lugar, sólo podrá realizarse si los trabajadores afectados han sido previamente informados, de modo preciso y expreso, acerca de las intenciones al respecto del empresario, de modo que con anterioridad a la puesta en marcha de las actividades de vigilancia los trabajadores habrán de tener un conocimiento expreso tanto de las finalidades de ésta como de los lugares y períodos temporales en que la misma se llevará a cabo. En segundo lugar, el empresario no tienen la libertad de elegir el método y los medios de vigilancia que considere como los mejor adaptados a sus objetivos, sino que habrá de tener en cuenta en todo momento las consecuencias que, para la vida privada de los trabajadores, puede tener aquélla, debiendo dar preferencia a los medios que tengan los menores efectos en ese orden.

En cuanto a la vigilancia secreta o permanente, el Repertorio adopta un enfoque marcadamente restrictivo dado que se ha probado que la misma es causa de ansiedad constante que, a su vez, puede originar enfermedades físicas y perturbaciones psicológicas, por lo que se habrá de limitar exclusivamente a los casos en los que la vigilancia fuere absolutamente necesaria para hacer frente a problemas concretos relacionados con la salud y la seguridad o la protección de los bienes, siendo solamente aceptable en la medida en que esté prevista por ciertas disposiciones de la legislación nacional.

Puede también ser necesaria en orden a la investigación de actividades delictivas u otras infracciones graves, si bien el Repertorio subraya que no basta con meras sospechas acerca de tales actividades o infracciones, sino que habrá de tratarse de sospechas razonablemente justificadas de actividades delictivas u otras infracciones graves, mencionándose como ejemplo de infracción grave el acoso sexual.

Asimismo, en orden a garantizar la transparencia del tratamiento de los datos, los empresarios deberían suministrar con regularidad a los trabajadores las informaciones generales acerca del modo de tratamiento, los tipos de datos conservados, los usos internos dados a los datos personales y los terceros a los que se hubieren comunicado datos sobre los trabajadores.

2. De igual modo, cabe referenciar la Recomendación (89) 2 del Comité de Ministros del Consejo de Europa, sobre la protección de los datos de carácter personal utilizados con fines de empleo, la cual contiene una serie de consideraciones generales sobre las condiciones que ha de reunir un tratamiento leal y legítimo de los datos de los trabajadores, así como referencias específicas a diversos tipos de problemas que pueden surgir con la protección de dichos datos en el entorno laboral, estableciendo que sólo mediando el consentimiento del interesado, o con otras garantías previstas en el Derecho interno, se podrán realizar pruebas o análisis destinados a evaluar el carácter o definir la personalidad de una persona, al tiempo que también señala el derecho del afectado a conocer el resultado de dichas evaluaciones si así lo deseare.

Y, a su vez, el “Grupo de Berlín”, constituido en el seno de la Conferencia Internacional sobre Protección de Datos, también se ha posicionado abiertamente acerca de la necesaria protección de los datos en el ámbito laboral a través de su documento “Informe y Recomendaciones sobre

las Telecomunicaciones y la Privacidad en las relaciones laborales", de agosto de 1996.

En dicho documento, el Grupo analiza los riesgos inherentes a la vigilancia y control de los empleados a través de las modernas Tecnologías de la Información y de las Comunicaciones (TIC) e informa sobre los métodos de recogida de datos más utilizados en el seno de las empresas, mencionando al respecto los dispositivos de video vigilancia y comunicaciones electrónicas, al tiempo que alerta de los riesgos que un uso desviado de los mismos puede ocasionar al trabajador, recomendando la necesidad del establecimiento de controles a fin de conseguir que dicho uso sea legítimo, necesario, adecuado, pertinente y proporcionado a la finalidad que lo justifica, debiendo implicarse en él a los representantes de los trabajadores.

Así, tanto los trabajadores como sus representantes habrán de ser informados del tipo de tecnología utilizada por el empleador en relación con la vigilancia de su actividad laboral, debiendo abstenerse éste de recoger datos personales que resulten excesivos. A su vez, los representantes de los trabajadores deberán contar con cumplida información acerca de la introducción de cualquier nuevo sistema de registro de datos que afecte al conjunto de los trabajadores de la empresa, teniendo estos últimos el derecho de acceso y de rectificación de los datos que se procesen sobre ellos.

6.- Marco jurídico de la video vigilancia privada.

1. La instalación de sistemas de video vigilancia en establecimientos privados habrá de cumplir con los requisitos legales predeterminados por la legislación vigente en la materia que, en este caso, viene constituida por la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y

garantía de los derechos digitales (art. 22)[393], tal como señala el Informe del Gabinete Jurídico de la AEPD nº 0630/2009[394], el cual resulta de extraordinario interés para el caso dado que en él se enfatiza el marco normativo regulador de las cámaras de video vigilancia privadas, estableciéndose en el mismo que la Agencia Española de Protección de Datos carece de competencias para la autorización de sistemas de video vigilancia privadas, siendo su competencia la de velar para que el tratamiento de datos derivado de dichos sistemas resulte conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (esta referencia hay que entenderla sustituida por la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales), y la Instrucción 1/2006, de 8 de noviembre de esta Agencia.

Señala, asimismo, el Informe referido que la competencia para la instalación de videocámaras en lugares públicos corresponde en exclusiva a las Fuerzas y Cuerpos de Seguridad del Estado, rigiéndose el tratamiento de dicha imágenes por su legislación específica contenida en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos[395], sin perjuicio de que les sea aplicable, en su caso, lo especialmente previsto por la derogada

393 Es decir, las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones, cumpliendo las prescripciones establecidas en la Ley Orgánica 3/2018, de 5 de diciembre y resto de legislación complementaria, así como las Instrucciones de la AEPD.

394 https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2009-0630_Instalaci-oo-n-de-c-aa-maras-de-seguridad-en-un-ayuntamiento.pdf

395 Según lo previsto en dicha normativa, la instalación de videocámaras en las vías públicas sólo estará permitida cuando fuere realizada por las Fuerzas y Cuerpos de Seguridad del Estado en los términos previstos en la Ley Orgánica 4/1997 y su Reglamento de desarrollo aprobado por Real Decreto 596/1999, de 16 de abril, figurando entre las atribuciones del Delegado del Gobierno en la Comunidad Autónoma correspondiente la autorización para dicha instalación. A tal efecto, dispone el artículo 3.2 de la Ley 4/1997 que *"las instalaciones fijas de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y de las Corporaciones Locales serán autorizadas por el Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de la misma Comunidad. La composición y funcionamiento de la Comisión, así como la participación de los municipios en ella, se determinarán reglamentariamente"*.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (hoy, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

A tal efecto, prescribe el art. 22.6 de la referida Ley Orgánica 3/2018, de 5 de diciembre que el tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica, añadiendo el apartado 7 de dicho art. 22 que lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

No obstante, la captación de imágenes a través de cámaras de video vigilancia no realizada por las Fuerzas y Cuerpos de Seguridad del Estado en el ámbito de la referida Ley Orgánica 4/1997, de 4 de agosto, quedará plenamente sometida a la normativa vigente en materia de protección de datos en tanto en cuanto se trate de imágenes de personas que puedan ser susceptibles de identificación, al ser la imagen de una persona un dato personal. La Instrucción 1/2006, de 8 de noviembre[396], de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, establece en su artículo primero, al delimitar su ámbito de aplicación, que la presente

396 BOE de 12 de diciembre de 2006.

Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras o videocámaras.

2. En consecuencia, si una empresa va a instalar cámaras de seguridad a través de una empresa de seguridad privada, dichas cámaras sólo podrán captar imágenes de la vía pública en la medida en que resulte imprescindible para preservar la seguridad de las personas y bienes, así como de sus instalaciones (art. 22.2 Ley Orgánica 3/2018, de 5 de diciembre). No obstante, es posible la captación de la vía pública en una extensión superior cuando sea necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado (art. 22.2 *in fine* Ley Orgánica 3/2018, de 5 de diciembre).

La instalación de cámaras que realice la empresa de seguridad privada deberá adecuarse a los términos previstos en la vigente Ley Orgánica 3/2018, de 5 de diciembre y en la Instrucción 1/2006, de 8 de noviembre. A tal efecto, el Informe del Gabinete Jurídico de la Agencia de fecha 15 de diciembre de 2008 en el que se analizan los requisitos que debe de cumplir una instalación de sistemas de video vigilancia para adecuarse a la normativa antes señalada, establece que si la decisión es instalar unas cámaras de video vigilancia para otorgar mayor seguridad a las instalaciones, dicha instalación habrá de respetar lo dispuesto tanto en la Ley Orgánica 15/1999, como en la Instrucción 1/2006, para que la injerencia en la imagen de los afectados sea mínima[397].

3. Una vez que las cámaras hayan sido instaladas correctamente, habrá de distinguirse si la cámara graba o no las imágenes. En el caso de que las

397 Las referencias efectuadas a la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, hay que entenderlas referidas a la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que deroga a la primera.

grabe resulta necesario cumplir con el deber de informar a los afectados en los términos establecidos en el art. 22.4 de la Ley Orgánica 3/2018, de 5 de diciembre, a cuyo tenor el deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

Asimismo, deberán respetarse los plazos y procedimiento de almacenamiento de imágenes, resultando de aplicación el art. 22.3 Ley Orgánica 3/2018, de 5 de diciembre, que establece que los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

7.- ¿Una legislación suficiente?

1. Llegados a este punto, se trata de analizar si la legislación española cumple el *standard* europeo respecto de las obligaciones que ha de observar el legislador. En definitiva, si el art. 20.3 ET en combinación con el art. 20 bis del mismo cuerpo legal y las normas de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, constituyen *per se* base legal suficiente para permitir al empresario un control

tecnológico de la actividad laboral teniendo presente los requerimientos que, a tal fin, establece la legislación y jurisprudencia europeas.

2. A tal efecto, hemos de recordar que de la exigencia de que la ley debe emplear términos lo suficientemente claros como para informar a todos bajo qué circunstancias y en qué condiciones se habilita a los poderes públicos a tomar medidas restrictivas de los derechos fundamentales[398] deriva la necesidad de usar reglas claras y detalladas referidas a los supuestos de intervenciones telefónicas y, por extensión de correos electrónicos, que incluyan las siguientes garantías:

a) La definición de los grados o categorías de personas susceptibles de sometimiento a vigilancia telefónica (o intervención del correo electrónico) judicial.

b) El tipo o clase de infracción a que pueda dar lugar.

c) El establecimiento de un límite temporal de duración de la medida.

d) Las condiciones de los atestados que registren las conversaciones interceptadas.

e) Las precauciones que se deban adoptar para comunicar intactas y completas las grabaciones realizadas al objeto de ser controladas eventualmente por el juez y la defensa.

f) Las circunstancias en las que se puede realizar el borrado de las cintas de grabación, sobre todo tras el sobreseimiento o la absolución.

Y a la luz de estas garantías mínimas y de los requisitos establecidos por la legislación y la jurisprudencia europeas se había venido sosteniendo que el art. 20.3 ET, aisladamente considerado, no cumplía con los estándares

398 entre otros, casos Malone, Kruslin, Kopp y Valenzuela Contreras, citados, y sentencias de 24 de abril de 1990, casos Kruslin y Huvig c. Francia

europeos de previsibilidad mínimos exigidos. Baste, como botón de muestra, citar los casos Kruslin c. Francia (STEDH de 24 de abril de 1990), Huvig c. Francia (STEDH de 24 de abril de 1990) o Copland c. Reino Unido (STEDH de 3 de abril de 2007) en los que se dice que, para cumplir con la exigencia de la previsibilidad, la ley debe emplear términos lo suficientemente claros para que todos puedan conocer en qué circunstancias y en qué condiciones pueden las autoridades recurrir a medidas restrictivas de derechos[399].

De modo expreso, en los Casos Kruslin y Huvig c. Francia afirma el TEDH que las escuchas y demás procedimientos de interceptación de conversaciones telefónicas constituyen un grave ataque a la vida privada y a la correspondencia, por lo que deberán siempre fundarse en una ley de singular precisión, siendo absolutamente indispensable que las normas que las regulan sean claras y detalladas.

3. E idéntica argumentación cabe sostener respecto del art. 20.3 ET, norma cuya vaguedad y generalidad hacen imposible una mínima exigencia de previsibilidad respecto de las circunstancias y condiciones en que pueden los empresarios recurrir a medidas restrictivas de derechos[400]. La principal dificultad que encuentra la justificación de las injerencias del empleador en la intimidad de sus empleados es la ausencia de una previsión legal que ampare con claridad y precisión la adopción por aquél de medidas que impliquen la limitación del derecho fundamental. El art. 20.3 ET, aisladamente concebido, no puede ser considerado en este sentido un precepto habilitante de injerencias

399 La STEDH de 24 de abril de 1990 (caso Kruslin c. Francia) señala que *"las palabras "prevista por la ley", en el sentido del artículo 8, exigen ante todo que la medida impugnada tenga algún fundamento en el Derecho interno; pero también se refieren a la calidad de la norma de que se trate: debe ser accesible a la persona afectada, que ha de poder prever sus consecuencias, y compatible con la preeminencia del Derecho"*.

400 Conviene recordar que en España, la ley española se ha considerado insuficiente para cumplir las exigencias del art. 8 CEDH en dos ocasiones: en el Caso Valenzuela Contreras y el en Caso Prado Bugallo, ambos en relación con el art. 579 LECr., habiendo sido subsanadas dichas insuficiencias por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

del empresario en la intimidad ni en ningún otro derecho fundamental de los trabajadores[401].

4. Como se ha visto con anterioridad, el límite "previsto por la ley" busca en primer lugar que la medida imputada tenga base en el derecho interno. No obstante, dicha expresión no se limita a remitir al derecho interno, sino que se refiere también a la calidad de la ley, exigiendo que sea compatible con la preeminencia del derecho, exigiendo de este modo que el derecho interno deba ofrecer protección contra atentados arbitrarios de los poderes públicos a los derechos consagrados por el párrafo 1 y derivando de esta exigencia la necesidad de accesibilidad de la ley para la persona implicada que, por añadidura, debe poder prever las consecuencias para ella.

Así, tratándose de medidas secretas de vigilancia o de interceptación de comunicaciones por las autoridades públicas, la exigencia de previsibilidad implica que el derecho interno deba emplear términos suficientemente claros para indicar a todos de manera suficiente en qué circunstancias y bajo qué condiciones habilita a los poderes públicos a tomar tales medidas, siendo indispensable la existencia de reglas claras y detalladas en la materia, aún más cuando los procedimientos técnicos no cesan de perfeccionarse[402]. Y es obvio que la generalidad de los términos con que se expresa el art. 20.3 ET impide al mismo cumplir con el requisito de exigencia de previsibilidad mencionado.

---

401 VEGAS TORRES, J., *Obtención de pruebas en ordenadores personales…op. cit.*, pág. 128. En idéntico sentido, GOÑI SEIN, J. L., "Controles empresariales: geolocalización, correo electrónico…, *op. cit.* y PRECIADO DOMENECH, C.H., *El derecho a la protección de datos en el contrato de trabajo*, *op. cit*., entre otros.

Asimismo, resulta necesario también traer a colación en este apartado la STEDH de 30 de julio de 1998 (caso Valenzuela Contreras c. España) en la que se pone de manifiesto de forma palpable la insuficiencia en el ámbito del secreto de las comunicaciones de la LECr., al tiempo que el Tribunal establece una serie de criterios aplicables en la interceptación de conversaciones telefónicas que deduce del art. 8 CEDH. Para mayor detalle vid. Ocón, J. (2018), "Derecho a la intimidad y registro de dispositivos informáticos: a propósito del asunto Trabajo Rueda c. España", *Revista Española de Derecho Constitucional*, 113, 327-343.

402 SSTEDH de 24 de abril de 1990 (casos Kruslin y Huvig c. Francia).

5. En lo que se refiere específicamente a la video vigilancia privada, coincidimos con Arzoz Santisteban cuando señala que la Instrucción 1/2006 constituye un paliativo, pero no la solución constitucionalmente satisfactoria de una utilización con cobertura deficiente y sin regulación legal. El eje de una regulación de la video vigilancia mediante cámaras fijas de seguridad privada o mediante cámaras móviles empleadas por detectives privados deben ser los derechos fundamentales del art. 18.1 CE: derecho a la intimidad personal y derecho a la propia imagen[403].

En suma, la legislación española carece de una norma legal específica, más allá de la LOPDGDD, que regule el uso de cámaras de video vigilancia por establecimientos privados. Aún más: la legislación española no regula con precisión la facultad de instalación y utilización de dispositivos de video vigilancia por empresas privadas, ni el tratamiento de las imágenes resultantes. Teniendo en cuenta, por un lado, los importantes derechos fundamentales en juego y, por otro, la proliferación actual de los dispositivos de video vigilancia, resulta discutible que la ausencia de regulación legal se pueda considerar compatible con el debido respeto al contenido constitucional de los derechos fundamentales. El régimen jurídico del uso de la video vigilancia privada, así como las garantías para las personas, deben estar claramente regulados en una norma de rango legal específica, como ocurre en otros Estados, como por ejemplo Alemania, Francia o Suecia.

Esta ausencia de cobertura legal y de regulación jurídica se ha procurado paliar desde instancias institucionales y doctrinales con un recurso intenso a los principios y normas de protección de datos y a las Instrucciones emitidas a este respecto por las agencias de protección de datos, lo cual es, sin duda, lícito desde la perspectiva material del derecho fundamental a la protección de datos personales, pero está muy lejos de resolver el problema en

403 ARZOZ SANTISTEBAN, X.: Videovigilancia, seguridad ciudadana…op. cit. pág. 264.

términos constitucionales[404]. La importancia de los derechos fundamentales afectados obliga a una regulación mediante Ley Orgánica, que aclare en qué supuestos la utilización de cámaras de video vigilancia en el ámbito de la seguridad privada no se considerará intromisión ilegítima en los derechos fundamentales a la intimidad, al honor y a la propia imagen, de modo que cabe ir más allá y preguntarse si los ciudadanos gozan de una protección constitucionalmente adecuada de sus derechos fundamentales frente a la utilización de videocámaras en el ámbito privado.

Ciertamente, el legislador ha dispuesto una cierta protección mediante normas civiles (en concreto, el art. 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen)[405], penales (el art. 197 del Código Penal)[406] y administrativas (arts. 22 y 89 LOPDGDD). Pero la cuestión es si la Constitución obliga al legislador a proporcionar una mayor y más adecuada protección frente a la video vigilancia privada, cabiendo señalar que no existe aquí una ausencia de regulación legal de una actividad que comporte la prohibición de una acción que es ejercicio de un derecho fundamental, sino una insuficiencia de las normas y garantías existentes para proteger plenamente los derechos fundamentales a la intimidad y a la propia imagen frente a la video vigilancia privada.

404 ARZOZ SANTISTEBAN, X.: Videovigilancia, seguridad ciudadana…op. cit. pág. 264.

405 El art. 7 LO 1/1982 considera intromisión ilegítima *"el emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas"* (apartado 1) y *"la captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2"* (apartado 5).

406 El art. 197.1 CP establece que *"el que, para descubrir secretos o vulnerar la intimidad de otro, sin su consentimiento (…) utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses"*.

Tradicionalmente se ha entendido que la protección frente a injerencias privadas en los derechos fundamentales no necesita estar configurada de forma tan precisa como la protección frente a las injerencias estatales en los mismos derechos fundamentales, los cuales han tenido históricamente una función primordialmente defensiva, añadiéndose con posterioridad las obligaciones de protección positiva, si bien con un contenido abierto que determina que no se pueda establecer de antemano hasta dónde llegan las obligaciones de protección positiva.

La doctrina de las obligaciones positivas dimanantes de los derechos fundamentales ha tenido acogida en la jurisprudencia del TEDH. De acuerdo con su jurisprudencia, aunque la finalidad del art. 8 sea principalmente la protección de los individuos frente a la injerencia arbitraria de los poderes públicos, dicha disposición no se limita a compeler al Estado a que se abstenga de tales injerencias, sino que además de esta medida negativa pueden existir también obligaciones positivas inherentes al respeto efectivo de la vida privada o familiar[407], las cuales pueden implicar la adopción de medidas dirigidas a asegurar el respeto de la vida privada incluso en el ámbito de las relaciones entre particulares[408].

En principio, el legislador tiene una amplio margen de maniobra tanto en la selección de los instrumentos de reacción posibles como en la ponderación de las posiciones iusfundamentales confrontadas de dos o más particulares. Salvo en los casos excepcionales en que se puede deducir un mandato inequívoco aplicable a las relaciones entre particulares, la protección de los derechos fundamentales frente a otros particulares en conductas que no están prohibidas de antemano (como la utilización de video cámaras) se encauza a través de la ponderación de bienes e intereses, a cuyos efectos el particular afectado por la utilización de video cámaras en el ámbito privado se coloca en

407 STEDH de 9 de octubre de 1979 (caso Airey c. Irlanda).

408 SSTEDH de 24 de febrero de 1998 (caso Botta c. Italia); de 13 de febrero de 2003 (caso Odicure c. Francia); de 4 de diciembre de 2003 (caso M.C. c. Bulgaria) o de 24 de junio de 2004 (caso von Hannover c. Alemania).

el mismo plano que el individuo que las utiliza. El primero invocará los derechos fundamentales a su propia imagen, al respeto de su vida privada o a la autodeterminación informativa, en tanto que el segundo aducirá su derecho fundamental a la seguridad y la protección de su propiedad privada. El conflicto aparente de derechos se resuelve mediante técnicas de ponderación, la delimitación previa de los derechos en cuestión y el principio de proporcionalidad.

Por su carácter indeterminado, la especificación de la protección resultante de las obligaciones positivas corresponde al legislador, el cual ha optado por proteger a los particulares frente al uso de videocámaras en el ámbito privado mediante normas civiles y, más recientemente, mediante normas de protección de datos. La cuestión que se plantea es si el legislador ha cumplido con el mínimo exigible constitucional e internacionalmente. Las normas civiles son cláusulas generales que necesitan de interpretación y aplicación por los jueces. Solamente cabría fundamentar una violación de las obligaciones positivas si la aplicación de las normas legislativas no proporcionara protección suficiente. El particular no tiene derecho a una forma determinada de protección, sino a que se le proporcione protección suficiente como resultado de los diversos instrumentos previstos en el ordenamiento.

El problema estriba en la dificultad de valorar si la protección dispensada es suficiente. Las vigentes normas civiles no desconocen la problemática de la captación de la imagen por terceras personas mediante dispositivos ópticos, si bien en el contexto de la Ley Orgánica 1/1982 las injerencias en los derechos fundamentales a la intimidad y a la propia imagen son excepcionales y no generales. Mientras existe una amplia jurisprudencia en la jurisdicción social en relación con la video vigilancia empresarial, que sigue la particular jurisprudencia constitucional existente en la materia, en la jurisdicción civil las resoluciones judiciales sobre conflictos entre particulares respecto a la

utilización de videocámaras en el ámbito privado, de conformidad con la referida LO 1/1982, parecen ser inexistentes[409].

Por otra parte, si bien es cierto que las Agencias de Protección de Datos se han tomado en serio el problema de la captación de imágenes a través de videocámaras en el ámbito privado mediante la adopción de Instrucciones al respecto, sin embargo su labor no puede proporcionar una protección plena de los derechos afectados dado que las mismas velan exclusivamente por la correcta aplicación de su legislación específica, básicamente la LOPD y su Reglamento de desarrollo.

Las Agencias pueden sancionar a quienes incumplan los requisitos establecidos en su normativa, pero no pueden poner fin a la intromisión ilegítima, ni restablecer el pleno disfrute del derecho fundamental vulnerado. Sólo la vía civil puede ofrecer protección a este respecto, si bien en la práctica resulta ineficaz, por lo que cabe concluir que el Estado no cumplirá plenamente sus obligaciones dimanantes del art. 8 CEDH mientras no determine los supuestos de utilización legítima de la video vigilancia por los particulares, no proporcione una habilitación legal al respecto y no establezca los criterios para garantizar que los diversos intereses en juego sean debidamente ponderados. Y para conciliar los derechos en juego es necesario también regular las normas técnicas a las que deberían sujetarse los sistemas de video vigilancia instalados en establecimientos privados, de forma que se especificara qué tipo de cámaras se pueden instalar, en qué establecimientos y para qué supuestos, al tiempo que se establecieran las condiciones de uso y la atribución de la función de supervisión a alguna autoridad administrativa.

En definitiva, pues, cabe concluir señalando que en la jurisprudencia constitucional española la categoría de la inconstitucionalidad por omisión parece restringida a aquellos supuestos en los que la ausencia de regulación

409 ARZOZ SANTISTEBAN, X.: Videovigilancia, seguridad ciudadana…op. cit. pág. 268.

legal de una actividad conduzca a la prohibición lisa y llana de una actividad ligada al ejercicio de un derecho fundamental (STC 31/1994, de 31 de enero), no siendo éste el caso de la falta de regulación legal de la video vigilancia privada, por lo que de acuerdo con el orden constitucional español no cabe sostener que el legislador haya incurrido en inconstitucionalidad por no regular adecuadamente la instalación de videocámaras en el ámbito de la seguridad privada[410].

6. Por otro lado, la promulgación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, tampoco ha venido a resolver el problema cuando lo podía haber solventado perfectamente. El nuevo art. 20 bis ET, introducido por la ley referida, que intenta fijar los términos en que han de entenderse delimitados los derechos a la intimidad digital mediante la técnica del reenvío al art. 87 LOPDPGDD, no aporta ninguna novedad relevante desde el punto de vista práctico. Así, su apartado 1 es meramente declarativo del derecho a la intimidad de los trabajadores en el uso de dispositivos digitales proporcionados por la empresa, que ya estaba reconocido por el Tribunal Constitucional y por el Tribunal Supremo[411].

Por su parte, el apartado 2 del mismo precepto legal tampoco merece valoración más positiva. El mismo permite al empresario, de forma genérica, acceder a los contenidos de la comunicación digital de los trabajadores, remitiendo al artículo 20.3 del ET. No se entiende, pues, la utilidad de este apartado, por cuanto el art. 20 bis ET remite al art. 87.2 de la LOPDGDD y, éste, a su vez, al art. 20.3 ET. De este modo, el interés legítimo del empleador al control sigue garantizándose, con respeto en todo caso a los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente.

410 ARZOZ SANTISTEBAN, X.: Videovigilancia, seguridad ciudadana…op. cit. pág. 270.

411 Vid. SSTS 119/2018, de 8 de febrero (Sala IV) y de 23 de octubre de 2018 (Sala II).

La cuestión es que es la LOPDGDD, precisamente, el instrumento que debería haber fijado tales estándares de protección y, sin embargo, ni tan siquiera clarifica si el empleador puede establecer una prohibición absoluta de uso extra laboral o si debe respetar cierto uso privado. En este punto, parece que el TEDH ha evolucionado en la dirección de admitir un uso privado mínimo -asuntos Barbulescu y Libert-. Con todo, el Documento de Trabajo del Grupo de Trabajo del artículo 29 (GT29), relativo al control o vigilancia de las comunicaciones electrónicas en el trabajo (WP 55, de 29 de mayo de 2002), parece reconocer potestad al empresario para prohibir a los trabajadores todo uso privado de estos dispositivos digitales.

El tema es relevante dado que si no se acepta que sea posible el establecimiento de dicha prohibición absoluta, decaería la posibilidad de realizar controles ocultos sin mediar información previa[412]. Si bien la jurisprudencia nacional admitió tal posibilidad de vetar todo uso particular (STS de 6 de octubre de 2011), y esta posición ha tenido algún apoyo en la práctica administrativa (AEPD, procedimiento E-01017/2015), se considera que debe descartarse atendiendo a la línea marcada por la Sentencia Barbulescu. Al margen de que debe aceptarse cierto uso mínimo extra laboral, la garantía de transparencia debe ser un elemento esencial para superar todo juicio previo de legitimidad[413].

Con todo, la valoración aún puede ser menos favorable desde la perspectiva laboral. Así, la versión definitiva de la norma establece un "derecho de participación" de la representación de los trabajadores en el establecimiento de la política de uso de los dispositivos digitales en la empresa, aunque sin concretar la modalidad -información, audiencia, consulta-[414]. Por lo demás,

412 MIÑARRO YANINI, M., "La Carta de derechos digitales de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación", *Revista de Trabajo y Seguridad Social, CEF*, 430 (enero 2019), pág. 8.

413 STS de 23 de octubre de 2018 (Sala II).

414 De este modo, esta garantía colectiva se ha devaluado durante el proceso de tramitación parlamentaria, pues la versión originaria se refería al "derecho a acordar" el protocolo de uso razonable de los dispositivos digitales, si bien

carece de novedad que se reconozca el deber de información previa –AEPD, informe 0464/2013; Recomendación (2015) 5, del Consejo de Europa, punto 10-, al tiempo que sorprende que se prescinda de toda referencia al principio de proporcionalidad, exigido por el acervo normativo – Dictamen del GT29 2/2017; Recomendación (2015) 5, del Consejo de Europa, punto 14 -.

7. Por lo que respecta a las prácticas de video vigilancia y grabación de sonidos en el lugar de trabajo, la valoración tampoco puede ser positiva[415]. El art. 89 LOPDPGDD, rubricado "Derecho a la intimidad frente al uso de dispositivos de video vigilancia y de grabación de sonidos en el lugar de trabajo", mantiene la misma actitud permisiva para tal tratamiento de datos -imágenes y sonidos- que el precedente, asumiendo el enfoque liberal del art. 20.3 ET, al que nuevamente se remite. Resulta sorprendente la nueva remisión dentro de su marco legal y con los límites inherentes al mismo, pues esta fórmula, vacía de contenido regulador, contrasta con el copioso cuerpo de doctrina administrativa que ilustra perfectamente cómo debe articularse[416].

8. Como reconoce la STS 489/2018, de 23 de octubre (Sala II), hasta ahora hemos convivido con una legislación laboral obsoleta (arts. 18 y 20 ET) y con lecturas jurisprudenciales extremadamente inciertas, nada uniformes ni lineales en su evolución[417]. Como afirma gráficamente, la solución al conflicto entre derechos fundamentales e intereses en juego del empresario y del trabajador se sitúa en una encrucijada en la que confluyen líneas de fuerza en

preveía la posibilidad de que éste no existiera, permitiendo la aprobación unilateral con un deber de información a los trabajadores del contenido de las pautas adoptadas. Se reduce, además, el contenido obligatorio del protocolo, pues en la versión originaria se incluían indicaciones sobre cómo debería hacerse, así como su contenido mínimo, mientras que en la versión adoptada se permite que sea fijado libremente por el empresario.

415 MOLINA NAVARRETE, C., "Celebrando los 40 años de Constitución (social). Tres temas sociolaborales de hoy, sendos retos de modernización promovidos por la Constitución de 1978", *Revista de Trabajo y Seguridad Social, CEF*, diciembre 2018.

416 Vid. AEPD informes 0495/2009 y 0475/2014.

417 Tampoco es casual que el acuerdo de PGE entre PSOE y Podemos se repare expresamente en la necesidad de abrir un debate profundo, político, social y sindical sobre "un nuevo marco de relaciones laborales más democrático".

tensión y múltiples cuestiones a las que la jurisprudencia no siempre ha ofrecido respuestas uniforme.

9. El desvaído art. 20.3 ET sigue siendo, pues, el referente jurídico fundamental, lo que es una sorprendente contradicción dado que la finalidad de la nueva regulación contenida en la LOPDGDD debía ser, precisamente, la de poner en el centro del eje regulador los derechos fundamentales, no la potestad empresarial. Por tanto, aquí la norma legal pierde su principal sentido garantista para mantener el que hoy tiene el art. 20.3 ET, primando el interés empresarial. Naturalmente, el legislador podrá continuar estableciendo condiciones a su ejercicio. Pero, nuevamente, la opción técnico-legislativa se muestra manifiestamente deficiente, por cuanto se limita a dos remisiones genéricas[418].

418 MOLINA NAVARRETE, C., "Poder de geolocalización, intimidad y autodeterminación digital en las relaciones de trabajo: ¿un nuevo orden eficaz de garantías y límites?, *Diario La Ley*, Nº 9319, Sección Tribuna, diciembre 2018.

CAPÍTULO III.- LA NECESIDAD DE AUTORIZACIÓN JUDICIAL PARA ACCEDER AL CONTENIDO DEL CORREO ELECTRÓNICO DEL TRABAJADOR.

1.- Necesidad de resolución judicial.

1. De la naturaleza de garantía formal de intangibilidad que tiene el secreto de las comunicaciones se desprenden tres características fundamentales de este derecho que lo diferencian de cualesquiera otros. La primera característica es la reserva de jurisdicción, la cual viene dada por la cláusula "salvo resolución judicial" que aparece en el apartado tercero del art. 18 CE, siendo su finalidad última la de excluir de raíz cualquier intromisión gubernativa o administrativa en ese derecho, de modo que la misma habrá de ser siempre acordada por un juez, que puede valorar imparcialmente las circunstancias del caso.

Dicho de otro modo, se trata de un derecho fundamental con respecto del que existe un alto riesgo de arbitrariedad por parte de la autoridad gubernativa y, por tanto, al ordinario control judicial de la actuación administrativa, que es potestativo y sucesivo (art. 106 CE), se añade un control judicial necesario y preventivo (STC 160/1991, de 18 de julio), debiendo ser la resolución judicial que autoriza la interceptación de las comunicaciones suficientemente motivada con respecto a las circunstancias del caso. Es decir, no puede ser genérica ni desproporcionada[419].

De conformidad con lo dispuesto por el art. 18.3 CE se requiere resolución judicial expresa para que resulte admisible el sacrificio del derecho

419 SSTC 139/1999, de 22 de julio; 171/1999, de 27 de septiembre; 299/2000, de 11 de diciembre; 139/2004, de 13 de septiembre; 136/2006, de 8 de mayo; 253/2006, de 11 de septiembre y STEDH de 9 de diciembre de 2004 (caso Van Rossem c. Bélgica).

al secreto de las comunicaciones, lo que parece excluir de principio que un empresario pueda lícitamente, por propia iniciativa y sin contar con autorización judicial, obtener pruebas mediante actos que supongan un sacrificio de aquél[420].

2. Al atribuir sólo a la autoridad judicial el poder de disponer el levantamiento del secreto de las comunicaciones, se alinea el Derecho español junto a los ordenamientos que nos son más próximos y en los que, con la excepción del Derecho británico, la medida que se considera escapa a las potestades administrativas[421].

En nuestro ordenamiento jurídico la intervención en el derecho que se considera ha de responder siempre, sin más quiebra que la prevista en el art. 55.1 CE, a una decisión judicial y a una decisión, además, típica, es decir, prevista en la ley en cuanto a sus condiciones de adopción y en cuanto a su contenido[422], debiendo estar la resolución judicial motivada, pese al silencio al respecto del art. 18.3 CE, dado que la jurisprudencia del Tribunal Constitucional es inequívoca en cuanto a la necesidad de que toda resolución que limite el ejercicio de un derecho fundamental habrá de estar motivada, de forma que la razón determinante de la decisión pueda ser conocida siempre por el afectado (STC 62/1982, de 15 de octubre). La solución adoptada por el Derecho español es, pues, la misma que la recogida en la Ley Fundamental de Bonn (art. 10)[423]

420 Como señala FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones en Internet*, Thomson Civitas, Madrid, 2004, pág. 167, *"tal y como se configura en España el régimen de intervención lícita de las comunicaciones que se realizan por canal cerrado, las injerencias que en las mismas lleven a cabo agentes privados serán siempre ilícitas y, por ende, vulnerarán el derecho al secreto de las comunicaciones del art. 18.3 CE"*.

421 JIMÉNEZ CAMPO, J., La garantía constitucional del secreto…, *op. cit.*, pág. 64.

422 JIMÉNEZ CAMPO, J., La garantía constitucional del secreto…, *op. cit.*, pág. 65.

423 Art. 10 Ley Fundamental de Bonn: 1. *"El secreto epistolar, así como el secreto postal y de las telecomunicaciones son inviolables. 2. Las restricciones sólo podrán ser ordenadas en virtud de una ley. Si la restricción está destinada a proteger el régimen fundamental de libertad y democracia o la existencia o seguridad de la Federación o de un Land, la ley podrá disponer que no se informe al afectado y que el recurso jurisdiccional sea reemplazado por el control de órganos y de órganos auxiliares designados por los representantes del pueblo"*.

o en la Constitución italiana (art. 15)[424], quedando sometida a reserva de ley la previsión de los supuestos en los que pueda procederse por la autoridad judicial al levantamiento del secreto de las comunicaciones.

3. Cuando la norma fundamental prevé que un determinado ámbito de libertad puede ser constreñido o negado mediante una resolución judicial está creando sólo una regla competencial que habrá de ser integrada, para poder actuarse en concreto, a través de la regulación legislativa que establezca los supuestos y los procedimientos para el efectivo despliegue de la competencia de este modo nombrada. Si así no fuera, el reconocimiento del derecho subjetivo sería sólo teórico: se garantizaría el derecho frente al Estado, a salvo de que por uno de sus órganos, el juzgado competente, se resolviera lo contrario[425].

4. Se ha de señalar, asimismo, que el requisito de la motivación de la resolución judicial tiene carácter sustantivo en cuanto que es instrumento indispensable para juzgar si la limitación de un derecho fundamental supera o no un juicio de razonabilidad, de la razonabilidad de una ponderación entre este derecho y los principios constitucionales con los que está en conflicto[426]. Los detalles de este juicio los encontramos desarrollados en la jurisprudencia del Tribunal Constitucional relativa al art. 18 CE, fundamentalmente en el contexto del derecho a la intimidad.

424 Art. 15 Constitución República italiana: *"Serán inviolables la libertad y el secreto de la correspondencia y de cualquier otra forma de comunicación. La limitación de los mismos sólo podrá producirse por auto motivado de la autoridad judicial con las garantías establecidas por la ley"*.

425 JIMÉNEZ CAMPO, J., "La garantía constitucional…, *op. cit.*, *Revista Española de Derecho Constitucional*, Año 7, núm. 20, Mayo-Agosto 1987, pág. 59.

426 RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones: tecnología e intimidad*, McGraw Hill, Madrid 1998, pág. 94.

Según el Tribunal Constitucional, razonabilidad significa que la limitación ha de perseguir un fin legítimo y constitucionalmente protegido, debiendo ser, además, indispensable para alcanzar ese fin, de forma que sólo es legítimo imponerla cuando no existieren medios alternativos menos lesivos para el disfrute de los derechos fundamentales.

De igual modo, la envergadura de la limitación debe ser proporcional a la importancia de la finalidad que persigue[427]; y, por último, las limitaciones de derechos deben ser adecuadas para la consecución de su fin, esto es, susceptibles de alcanzarlo. A todo lo anterior se añade la obligación de que las limitaciones de derechos estén legalmente autorizadas y respeten el contenido esencial de éstos. Pues bien, todos y cada uno de estos puntos deben ser debidamente argumentados por las medidas limitadoras de los derechos fundamentales.

La exigencia de motivación de las resoluciones judiciales que autorizan las intervenciones telefónicas forman parte del contenido esencial del art. 18.3 CE[428], siendo el fundamento de esta exigencia cualificada de motivación el respeto del derecho de defensa del sujeto pasivo de la medida[429].

Al referirse al requisito de la motivación y al juicio de razonabilidad en el contexto del art. 18, el TC alude a la jurisprudencia del TEDH. Y es que el art. 18 CE se corresponde en buena medida con el art. 8 CEDH, que reconoce el derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia. El apartado segundo de este artículo establece que toda injerencia en el ejercicio de estos derechos debe ser necesaria en una

427 STC 7/1994, de 17 de enero.

428 SSTC 25/2011, de 14 de marzo; 70/2010, de 18 de octubre 167/2002, de 18 de septiembre; 184/2003, de 23 de octubre; 197/2009, de 28 de septiembre.

429 SSTC 26/201O, de 27 de octubre, 72/201O, de 18 de octubre, 197/2009, de 28 de septiembre, entre otras.

sociedad democrática para alcanzar un determinado fin legítimo, en concreto, para la protección de la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud y de la moral, o la protección de los derechos y las libertades de los demás.

Según interpretación de la Comisión y del TEDH, la expresión "necesaria en una sociedad democrática" se traduce en los requisitos de necesidad y proporcionalidad. De acuerdo con el primero, toda injerencia debe ser el modo de alcanzar el fin deseado que implique la menor intrusión posible en los derechos reconocidos en el Convenio; de acuerdo con el segundo, la injerencia debe guardar adecuada proporción con la importancia del fin que con ella se persigue y que la justifica[430]. La expresión "necesaria en una sociedad democrática" impone, en suma, un juicio de razonabilidad semejante al que ha desarrollado nuestro Tribunal Constitucional.

5. Por otro lado, entender que el juez a cuya resolución remite el art. 18.3 CE es sólo el penal[431] es una tesis errónea, como los son también –y el Tribunal Constitucional se ha encargado de constatarlo[432]- las que pretenden descartar toda afectación a los derechos reconocidos en los arts. 17.1 y 18.2 CE que no provenga de un órgano de aquella jurisdicción. Existen bienes jurídicos (derechos e intereses de terceros) que pueden llevar a la norma que los tutele a prever medidas de intervención sobre las comunicaciones para evitar que, a su través, se cometan ilícitos o se defrauden aquellos derechos o

430 En relación con el respeto de la correspondencia, Silver y otros c. Reino Unido; Margareta y Roger Andersson c. Suecia, sentencia de 25 de febrero de 1992; Pfeifer y Plannkl c. Austria, sentencia de 25 de febrero de 1992; Campbell c. Reino Unido, sentencia de 25 de marzo de 1992.

431 BASILE, S., "La restricción del derecho sólo es posible por exigencias de la justicia penal", en *Los valores superiores, los principios fundamentales y los derechos y libertades públicas en la Constitución de 1978,* GARCÍA DE ENTERRÍA, E. y PREDIERI, A. (eds.), Madrid, 1980, pág. 293.

432 Por lo que al derecho de libertad personal ex art. 17.1 CE se refiere, véase STC 178/1985, de 19 de diciembre. En cuanto al mandamiento por juez civil de entrada en un domicilio, STC 22/1984, de 17 de febrero.

intereses[433]. Este es el sentido que tiene en nuestro ordenamiento la previsión legal de la retención de la correspondencia del concursado, la cual ha de ser dispuesta por el juez mercantil.

6. La interceptación con fines probatorios es, sin duda, la que más dificultades suscita y la que más pone en riesgo el principio constitucional de seguridad y el derecho a la defensa de los propios derechos e intereses. Esta interceptación depende de un acto motivado del juez penal y tiene como finalidad la obtención de datos que puedan contribuir al esclarecimiento de los hechos[434]. Se trata de una medida *post delictum* dictada tras haber llegado al juez la *notitia criminis* y también, generalmente, tras haberse dictado auto de incoación del sumario[435].

No son posibles, pues, sobre la base del art. 18.3 CE, interceptaciones meramente preventivas al margen de la realización de un hecho delictivo y tendente sólo -convirtiendo a cualquiera en sospechoso- a determinar la realización de supuestas conductas criminales. La norma que previese dicha posibilidad –sobre afectar, sin duda, al principio de seguridad jurídica- incurriría en una restricción del derecho que no podría dejar de ser calificada como desproporcionada, pues el interés en la prevención del delito no puede justificar la injerencia en la libertad, forzosamente, indiscriminada, a que daría lugar con este tipo de interceptaciones[436].

7. En definitiva, el requisito de la resolución judicial no puede entenderse cumplido con la mera constatación de su existencia formal, sino que la misma debe cumplir los siguientes requisitos:

433 JIMÉNEZ CAMPO, J., La garantía constitucional del secreto…, *op. cit.*, pág. 68.

434 JIMÉNEZ CAMPO, J., *Idem.*, pág. 69.

435 JIMÉNEZ CAMPO, J., *Idem.*, *Ibidem.*

436 JIMÉNEZ CAMPO, J., *Idem.*, pág. 70.

1) Motivación de la resolución judicial, debiendo ser ésta expresa y atenerse al criterio de proporcionalidad que justifica la intervención y precisar el alcance de la medida, en qué va a consistir la misma, cómo se llevará a cabo y cuáles serán sus límites.

2) Establecimiento de un plazo, que empezará a contar desde la aprobación del auto judicial.

3) La intervención debe referirse a personas concretas y respecto a delitos determinados.

4) Finalizada la intervención, deberá comunicarse a los afectados[437].

Toda interceptación que incumpla estos requisitos será ilegítima por vulnerar el derecho al secreto de las comunicaciones e implicar la nulidad de cualquier prueba que hubiere podido obtenerse como consecuencia de la interceptación ilegítima. Esta consecuencia, que ha sido reiterada por la jurisprudencia[438], deriva, según el TC, de la posición preferente de los derechos fundamentales, de su condición de inviolables, y de la necesidad institucional de no confirmar, reconociéndoles efectividad, sus contravenciones[439]. Lo contrario implicaría, además, la vulneración del derecho a un proceso con todas las garantías y, en su caso, de la presunción de inocencia si se produjera la condena penal basándose en una prueba que es inválida[440].

437 DÍAZ REVORIO, F. J., "El derecho fundamental al secreto de las comunicaciones: una visión…, *op. cit.*, págs. 140-141.

438 SSTC 114/1984, de 29 de noviembre; 81/1998, de 2 de abril; 49/1999, de 5 de abril; 299/2000, de 11 de diciembre; 184/2003, de 23 de octubre.

439 STC 49/1999, de 5 de abril.

440 DÍAZ REVORIO, F. J., "El derecho fundamental al secreto de las comunicaciones: una visión…, *op. cit.*, pág. 142.

De esta forma, el derecho al secreto de las comunicaciones se encuentra más protegido en comparación con el derecho a la intimidad respecto del que no existe en la Constitución reserva absoluta de previa resolución judicial, por lo que en determinados casos se admite que la Policía Judicial lleve a cabo diligencias que supongan una injerencia leve en dicho derecho[441].

8. La resolución judicial legitimadora de la intervención debe ser un auto por ser ésta la forma que han de adoptar las resoluciones judiciales que deciden cuestiones que van más allá de la mera ordenación material del proceso y requieren de una adecuada fundamentación dada la importancia de su contenido, no pudiendo adoptarse la medida limitativa por medio de providencia por carecer la misma de motivación[442]. Así, la STC 181/1995, de 11 de diciembre, declara que la restricción del derecho fundamental debe adoptarse por resolución motivada, siendo ello debido a la estrecha relación que existe entre la motivación judicial y las circunstancias de hecho que justifican dicha restricción dado que sólo mediante aquélla pueden ser conocidas y ponderadas éstas.

No obstante, si la resolución judicial revistiere finalmente la forma de providencia, esta circunstancia aislada no deberá entenderse por sí sola como causante de nulidad.

9. Aplicando la doctrina del TC reseñada al uso correo electrónico, no cabe duda que la intervención del mismo exige que la resolución judicial especifique la concreta cuenta de correo electrónico afectada, no siendo una práctica idónea la de especificar la línea telefónica normalmente utilizada por el

441 Vid. *ad exemplum* STC 70/2002, de 3 de abril. En el mismo sentido, Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado, sobre Pautas en relación con la Diligencia de Intervención de las Comunicaciones Telefónicas.

442 Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado, sobre Pautas en relación con la Diligencia de Intervención de las Comunicaciones Telefónicas.

sujeto pasivo dado que éste puede acceder a su cuenta de correo electrónico a través de otra línea.

A estos efectos habrá de aplicarse el mismo régimen a las diversas modalidades de mensajería instantánea *(v.gr. whatsapp o messenger*) habida cuenta de que la opción de aplicarle al correo electrónico el régimen jurídico de la intervención de la correspondencia resulta de difícil encaje. Baste reparar en que sería necesario citar al interesado para acceder a su contenido, lo que obviamente conduciría al truncamiento de la diligencia.

10. Al margen del correo electrónico, existen otros medios - chats y foros - que permiten la comunicación entre varias personas de forma simultánea y públicamente en tiempo real. En estos casos, cuando las conversaciones sean accesibles para cualquier usuario de Internet, las mismas carecen de la consideración de privadas, de modo que no caen dentro del ámbito de aplicación del secreto de las comunicaciones, no requiriéndose autorización judicial para ser grabadas. Distinto será el tratamiento de los supuestos en los que se use la opción de comunicación bidireccional cerrada entre dos usuarios, pues en estos casos, conforme a la propia naturaleza del acto comunicativo, deben activarse de nuevo las garantías del art. 18.3 CE[443].

11. Por su parte, la apertura de archivos de un disco duro tampoco afecta al derecho al secreto de las comunicaciones, sino que se considera más bien el cuerpo de los delitos informáticos, no siendo imprescindible la autorización judicial, salvo cuando se acceda a correos electrónicos. Los documentos no integrados en un proceso de comunicación y almacenados en archivos informáticos - teléfonos móviles, PDA u ordenadores - tienen la consideración

443 Circular 1/2013, de 11 de enero, de la Fiscalía General del Estado, sobre Pautas en relación con la Diligencia de Intervención de las Comunicaciones Telefónicas.

de simples documentos y, por tanto, sólo resultan protegidos por el derecho a la intimidad[444].

Por eso, los Cuerpos y Fuerzas de Seguridad del Estado pueden, sin necesidad de autorización judicial, intervenir un soporte electrónico (v. gr. la lectura del disco duro de un ordenador) si se apreciaren razones de urgencia y se persiguiere un interés constitucionalmente legítimo en base en la habilitación legal para dicha actuación reconocida en los arts. 282 LECrim., 11.1 L.O. 2/1986 de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y 547 LOPJ, aun cuando su contenido material pudiera afectar al derecho a la intimidad[445]. Esta doctrina sería también aplicable a las unidades de almacenamiento externo, PDA y asimilados.

12. Trasladándonos al ámbito de las relaciones laborales, observamos que el estado del arte de la jurisprudencia relativo a la interpretación y aplicación a las relaciones de trabajo del secreto de las comunicaciones presenta una seria fractura dado que contrastan frontalmente dos normas en el Derecho vigente, a saber: (i) el plus de tutela constitucional que recibe ex art. 18.3 CE (el derecho al secreto de las comunicaciones no tendrá más límite que el de la autorización judicial)[446] con (ii) el vaciamiento práctico de la garantía del contenido esencial del derecho del art. 18.3 CE en la relación laboral operado tanto por el TC como por el TS en el sentido de reformular el mandato constitucional hacia una mutación del siguiente tenor: *"el derecho en cuestión estará limitado por el ámbito que, en cada caso, configure el poder de vigilancia y control del empresario conforme al art. 20.3 ET, bien de manera unilateral*

444 STS 782/2007, de 3 de octubre.

445 En este sentido, vid. STC 173/2011, de 7 de noviembre, en relación con la investigación de un delito de pornografía infantil.

446 Así lo entendió la STS (Sala 2ª) 528/2014, 16 de junio, así como, con más matices, entre otras, la STSJ Galicia 119/2014, de 30 de diciembre.

(Código de Conducta), bien de forma convencional (Convenio colectivo)"[447]. Así lo decidieron las SSTC 241/2012, de 17 de diciembre y 170/2013, de 7 de octubre, y así lo ha reeditado, considerándose no concernido por el "Test Barbulescu de Garantía de la Privacidad", la STS 119/2018, de 8 de febrero, que casa en este punto a la STSJ Galicia 119/2014, de 30 de diciembre.

Y, como se ha dicho, a falta de una regulación expresa en el ámbito laboral, debe ser la garantía constitucional del contenido esencial del derecho al secreto de las comunicaciones el que actúe como técnica de protección también en el trabajo. Es cierto que el secreto de las comunicaciones carece de una elaboración dogmática precisa y acabada. Pero la doble función de los derechos fundamentales - la de servir de límite al ejercicio de acciones (poderes) que pretendan injerirse en él y la de actuar como fuente integradora de obligaciones positivas en todas las relaciones en que se invoca, también entre particulares, sobre todo en las laborales - ha de tener su proyección para el secreto de comunicaciones que, en nuestra Constitución, además, goza de una protección reforzada.

Pero el TC no ha seguido igual lógica en el nuevo entorno laboral digital, sino que, más bien, se ha dirigido en una dirección de desprotección absoluta en línea con la sentencia Barbulescu I de 12 de enero de 2016 (como evidenciara la STC 39/2016, de 3 de marzo, si bien referida a un supuesto de video vigilancia y no de secreto de comunicaciones), si bien la Gran Sala del TEDH ha corregido con posterioridad esa posición liberal de su Sección Cuarta en la sentencia Barbulescu II de 5 de septiembre de 2017, no habiendo hecho lo propio ni el TC ni el TS español pese a su vinculación a esta jurisprudencia europea *ex* arts. 10.2 y 96 CE, manteniéndose de este modo una profunda fosa entre la delimitación del ámbito de cobertura del derecho extra-muros de la empresa (sociedad civil), donde adquiere una importante vitalidad, y dentro de ella (configurada como una ciudad sólo de trabajo y para el trabajo), donde se

447 MOLINA NAVARRETE, C., "El derecho al secreto de las comunicaciones en la relación de trabajo…,*op. cit.*, pág. 3.

debilita, volviéndose un derecho de papel, pese a la solemne —a menudo sólo formal y retórica— proclamación del modelo de "ciudadanos en la ciudad, los trabajadores deben serlo también en la empresa" (STC 88/1985, de 19 de julio)[448], de modo que la visión expansiva en la vida civil del derecho al secreto de comunicaciones muta en estrecha en la vida laboral (STC 170/2013, de 7 de octubre).

Más concretamente: si el secreto de las comunicaciones puede vulnerarse tanto por la interceptación como por el conocimiento antijurídico de lo comunicado, resulta que en el ámbito laboral el hecho de considerar canales de comunicación abiertos a los correos electrónicos no encriptados desactiva el efecto útil de la tutela del art. 18.3 CE, de forma que, teóricamente, los trabajadores tendrían garantizada la impenetrabilidad por parte de terceros (SSTC 114/1984, de 29 de noviembre y 56/2003, de 24 de marzo), así como la identidad subjetiva de los interlocutores – v. gr. listados telefónicos - (STC 230/2007, de 5 de noviembre, en línea con la STEDH de 3 de abril de 2007, caso Copland), pero, en la práctica, el empleador puede interferir tanto en el flujo comunicacional como en su contenido concreto por la sola prohibición general, empresarial o colectiva, de un uso no particular. De hecho, el art. 87.2 de la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, permite al empleador acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

Recuérdese que la STC 241/2012, de 17 de diciembre, supuso legitimar el conocimiento de chats y programas de comunicación específicos entre trabajadores por el sólo hecho de que hubieran inobservado la prohibición de instalarlos, confundiendo el derecho legítimo a sancionar el incumplimiento con

448 OJEDA AVILÉS, A., *Ciudadanía en la empresa y derechos fundamentales inespecíficos*, Laborum, Murcia, 2011, pág. 12.

una -ilegítima, a mi juicio- facultad para penetrar en el canal que las trabajadoras se habían reservado[449].

O que la STC 170/2013, de 7 de octubre, supuso aceptar que la empresa interceptara mensajes SMS obtenidos del teléfono móvil, incluso sorpresivamente, sin norma de trasparencia específica informativa previa, con la simple referencia a una cláusula convencional disciplinaria[450], de modo que estamos ante sentencias constitucionales interpretativas involutivas que reinvierten el orden constitucional ignorando toda vertiente de obligación positiva, exigida para respetar plenamente la libertad de comunicación digital (deber de tolerar cierto uso privado social de las herramientas digitales en la empresa), como el TEDH ha consagrado con la doctrina Barbulescu II[451], de manera que, frente al carácter indisponible del derecho, salvo autorización judicial (modelo de tutela máxima *ex* art. 18.3 CE), el TC autoriza al empleador a una disposición unilateral (convirtiendo en papel mojado la concepción ciudadana del trabajador) permitiendo una facultad omnímoda de acceso a los contenidos del correo electrónico si cuenta con una orden limitativa del uso privado de los dispositivos electrónicos, excluyendo de esta forma el juicio de adecuación (proporcionalidad) de tales órdenes al Derecho, ya desactivado por la existencia de información previa. Y lo mismo cabe decir del referenciado art. 87 de la Ley 3/2018, de 5 de diciembre.

Para ser conscientes de la restricción constitucional de garantías y del error de juicio constitucional baste con recordar que el TEDH tiene una visión opuesta de las cosas. Así, en el caso Barbulescu, pese a que había

449 CARDONA RUBERT, M. B., "Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás", *RDS*, nº 60, 2012, págs. 169 y sigs.

450 Para la Resolución de la AEPD, R/01755/2013, el acceso al contenido de los correos por virtud del art. 20.3 ET no excluye que implique tratamiento de datos personales.

451 MOLINA NAVARRETE, C., "El derecho al secreto de las comunicaciones en la relación de trabajo…",*op. cit.*, pág. 4.

una prohibición expresa de la empresa de intercambiar comunicaciones de carácter personal, la Gran Sala sostiene que, pese a la misma, el trabajador mantiene una expectativa razonable de confidencialidad de su correspondencia, aunque se trate de relaciones comunicativas privado-familiares, afirmando al efecto que las instrucciones de una empresa no pueden anular el respeto a la confidencialidad de las comunicaciones, aunque pueden limitarse dentro de las medidas de necesidad", de modo que la existencia de normas -empresariales o convencionales- vinculantes prohibitivas de un uso social de útiles de comunicación digital en la empresa no autoriza el acceso del empleador sin más, asumiendo de este modo el TEDH una concepción social para las modernas formas de comunicación en las relaciones de trabajo de nuestro tiempo, siempre que se mantengan dentro de un orden de razonabilidad y no perjudique la rentabilidad de la empresa. Y en caso de que se sobrepasen esos límites, el empresario tiene todo el derecho a sancionar al trabajador.

No obstante, aquí se produce, como ya tuvo ocasión de advertir el voto particular a la STC 241/2012, de 17 de diciembre, (caso "Trillian", instalación de programas de mensajería en ordenadores de uso común para chatear dos trabajadoras en contra de la prohibición del empleador), pero extensible a la doctrina constitucional en general sobre el secreto de las comunicaciones digitales de los trabajadores (STC 170/2013, de 7 de octubre), una confusión muy grosera porque supone justificar los medios (sacrificio del secreto de comunicaciones) por los fines (protección del interés empresarial).

En efecto, el TC distingue dos planos diferentes: el propio de la sanción del incumplimiento -del que sospecha- y el del modo para llevar a cabo la fiscalización del mismo a fin de disciplinar al trabajador. Respecto al primero (fin), es claro que la infracción de la orden empresarial prohibitiva permite tanto su sanción como su verificación (art. 20.3 ET). Ahora bien, en relación al segundo (medio), tal potestad no le legitima para injerirse, *per*

se, en el contenido de la comunicación personal efectuada en contra de la prohibición porque, precisamente, la función del derecho fundamental es la de condicionar ese modo de ejercicio de las facultades empresariales, sin impedirlo, por supuesto (STC 41/2006, de 13 de febrero). De otro modo, el fin último legítimo (disciplina) justificaría un medio ilegítimo (quiebra del secreto comunicativo) por la sola razón de facilitar la prueba necesaria para asegurar el buen éxito de aquél (fin medial o procedimental)[452]. Sin embargo, no es ese el modelo diseñado por el art. 18.3 CE, que establece un régimen de protección reforzada (autorización judicial) sin que una norma legal laboral (art. 20.3 ET) tenga la habilitación para desnaturalizarlo, como tampoco es el conformado por el TEDH *ex* art. 8 CEDH.

2.- La aplicabilidad de los arts. 76.4 y 90.2 y 4 LRJS en el acceso a los datos privados del trabajador contenidos en el ordenador de la empresa.

1. Desde el punto de vista procesal, la problemática que genera la acreditación de los hechos imputados por el empresario al trabajador en caso de juicio se basa en que los medios de prueba aportados en juicio por el empresario son considerados, generalmente, por parte del trabajador/actor como obtenidos con vulneración del conglomerado de derechos del art. 18 CE (derecho a la intimidad, derecho al secreto de comunicaciones y derecho a la protección de datos personales), lo cual conlleva una serie de problemas jurídicos de hondo calado procesal, si bien, en cuanto aquí interesa, sólo nos referiremos a la cuestión de si resultan aplicables los arts. 76.4 y 90. 2 y 4 LRJS para acceder a los datos privados del trabajador en el ordenador de la empresa[453].

452 MOLINA NAVARRETE, C., "El derecho al secreto de las comunicaciones en la relación de trabajo…",*op. cit.,* pág. 6.

453 Al respecto, véase BUENO DE MATA, F., "La práctica de la prueba electrónica en sede judicial: ¿vulneración o reforzamiento de principios procesales?", *Diario La Ley* núm. 8332; ABEL LLUCH, X., "Repensando el concepto de documento", *Diario La Ley* núm. 7667.

Es decir, dado que el acceso al ámbito de privacidad del trabajador se enmarca en el secreto de las comunicaciones y el art. 18.3 CE requiere al respecto intervención judicial, cabe preguntarse si este requisito es necesario a efectos de practicar la referida intromisión. No obstante, hay que señalar que la autorización judicial no se observa en forma estricta en el ámbito del derecho a la intimidad (art. 18.1 CE), ni en el de libertad informática (art. 18.4 CE), a lo que cabe añadir que una cosa es la autorización judicial previa para afectar un ámbito de privacidad y otra, muy distinta, la eficacia de la prueba obtenida.

2. El artículo 76.4 LRJS, al regular los actos preparatorios y las diligencias preliminares, contiene la prevención de que si de las mismas se pudiera derivar alguna incidencia a la intimidad personal u otro derecho fundamental, el órgano judicial, si el afectado no consiente, podrá autorizar dicha actuación en la forma y con las garantías establecidas en los apartados 4 a 6 del artículo 90. Y, en concreto, el art. 90.4 LRJS indica que cuando fuere necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que pudieran afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existan medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto, previa ponderación de los intereses afectados a través de juicio de proporcionalidad y con el mínimo sacrificio, determinando las condiciones de acceso, garantías de conservación y aportación al proceso, obtención y entrega de copias e intervención de las partes o de sus representantes y expertos, en su caso.

A lo que hay que añadir que los apartados 2 y 6 del art. 90 LRJS disponen, respectivamente, que no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas (apartado 2) y que si como resultado de las medidas anteriores se obtuvieran datos innecesarios, ajenos a los fines del proceso o que pudieran afectar de manera injustificada o desproporcionada a derechos fundamentales o a libertades públicas, se resolverá lo necesario para preservar y garantizar

adecuada y suficientemente los intereses y derechos que pudieran resultar afectados (apartado 6).

3. Sobre el particular se han ofrecido diferentes opiniones doctrinales que van desde las posiciones que sostienen que, en todos aquellos supuestos en los que la prueba pudiera incidir en el ámbito de la privacidad del trabajador, el empresario deberá forzosamente acudir a ese medio de autorización judicial que se observa en el artículo 76.4 LRJS, hasta aquéllas otras que matizan esa conclusión.

Así, Falguera Baró[454] ofrece una peculiar interpretación de las prescripciones contenidas en los referidos artículos de la norma procesal laboral, sosteniendo que no cabe confundir la autorización del juez para la práctica de la prueba en juicio (art. 90.4 LRJS) con la licencia judicial para acceder al ámbito de privacidad a efectos de obtención de la prueba del art. 76.4 de la ley procesal, entendiendo que de este último precepto parte de la doctrina deriva que si el empresario quiere acceder a los contenidos privados del trabajador ubicados en el ordenador de la empresa debe solicitar la anuencia judicial.

Aunque ese ha sido el criterio sustentado por la Sala de lo Penal del TS[455] hasta la STS de 23 de octubre de 2018 (Sala II), no es, sin embargo, coincidente con la conclusión implícita que se desprende de la doctrina del TEDH, el TC y de la Sala de lo Social del TS en la materia. Y ello porque, sostiene Falguera, en estos casos debe ponderarse el mandato del art. 18.3 CE con el contenido del derecho constitucional a la libre empresa y la capacidad de control de la prestación laboral que del mismo se difiere. De esta forma, aunque en una forma ciertamente atípica, los artículos 18 y 20.3 ET confieren al

454 FALGUERA i BARÓ, M. A., "Nuevas tecnologías y trabajo (III): perspectiva procesal", *Trabajo y Derecho*, núm. 22, octubre 2016, págs. 34-36.

455 STS (Sala 2ª) de 16 de junio de 2014, rec. núm. 2229/2013.

empleador una legitimación suficiente para invadir –con unas ciertas garantías– los ámbitos de privacidad del trabajador, sin que sea precisa la autorización judicial para obtener la prueba. Por tanto, el empleador no tiene porqué reclamar permiso al juez para monitorizar el ordenador o acceder a los contenidos de los correos electrónicos.

A mayor abundamiento de cuanto decimos, el art. 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, bajo la rúbrica "Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral", tras afirmar en su apartado 1 que los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador, determina en su apartado 2 que el empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

No obstante, para poder acceder al contenido del correo electrónico, el empresario habrá de establecer previamente los criterios de utilización de los dispositivos digitales respetando, en todo caso, los estándares mínimos de protección de la intimidad del trabajador de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente, debiendo participar en su elaboración los representantes de los trabajadores (art. 87.3 Ley 3/2018, de 5 de diciembre).

Asimismo, el acceso a los dispositivos respecto de los que hubiere admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad (como la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados), debiendo ser informados los trabajadores de estos criterios de utilización (art. 87.3 *in fine* Ley 3/2018, de 5 de diciembre).

4. En este orden de cosas, la STS de 23 de octubre de 2018 (Sala II) –referida al ámbito penal- establece que, pese a buscarse la fórmula menos invasiva posible para examinar el ordenador, faltaba un *prius* inexcusable, cual es la necesidad de advertencia o instrucción previa por parte del empresario en orden a la necesidad de limitar el uso del ordenador a tareas profesionales y/o, además, alguna cláusula conocida por ambas partes autorizando a la empresa a medidas de vigilancia y control del uso del ordenador o, bien, se hubiese recabado previamente el consentimiento de quien venía usando de forma exclusiva el ordenador.

Añadiéndose que no existiendo advertencia previa acerca de que el ordenador había de ser usado exclusivamente para fines laborales y no constando al empleado que la empresa se reservaba la potestad de su examen, por mucho que se utilizasen métodos informáticos especialmente poco invasivos y selectivos, constituía un cierto atrevimiento (una indiligencia), no recabar antes el consentimiento del titular o, en su defecto, de la autoridad judicial.

Es decir, como pone de manifiesto la propia sentencia, hay un relevante signo diferenciador entre el acceso por el empresario y el acceso por agentes públicos; el primero en virtud de sus facultades de supervisión del trabajo que se presta por una relación laboral; los segundos, en virtud de potestades públicas. En el primer caso nos movemos en el marco de una relación contractual entre particulares. La clave estará en si el trabajador ha consentido anticipadamente reconociendo esa capacidad de supervisión al empresario y, por tanto, cuenta con ello; está advertido; es decir, es una limitación conocida y contractualmente asumida.

En las relaciones con los poderes públicos, sin embargo, no cabe esa cesión anticipada o renuncia previa a ese espacio de intimidad virtual. El reconocimiento previo, explícito o implícito, de esa facultad del empresario

constituye el *punctum dolens*, la clave en el ámbito de las relaciones laborales. En una investigación penal lo será la autorización judicial o el consentimiento actual[456].

Es decir, parece querer decir la sentencia de la Sala II del TS de 23 de octubre de 2018 que cuando se trate de aportar a un proceso penal pruebas contra un trabajador obtenidas de la supervisión del contenido del correo electrónico de éste, las mismas habrán de ser obtenidas mediando autorización judicial o, en su caso, consentimiento expreso del trabajador. Sin embargo, no se pronuncia (por no ser objeto de su jurisdicción) acerca de la necesidad o no de autorización judicial en el marco de un proceso laboral.

5. No obstante, una cosa es la obtención de la prueba y otra la autorización judicial de la práctica de dicha prueba, que es lo que específicamente contempla el art. 90.4 LRJS. Así, si el conocimiento de los hechos por el empleador se deriva del ejercicio de su poder de vigilancia del art. 20.3 ET o de los mecanismos invasivos de la privacidad del art. 18 ET, no será necesaria la solicitud de autorización judicial de la práctica de la prueba[457].

Por el contrario, si por cualquiera de dichas vías apareciera un contenido de privacidad del trabajador (un correo electrónico personal, visita a webs de determinada orientación sexual, etc.) o éste ha establecido un ámbito de privacidad (borrado de archivos, claves de acceso, etc.), sí parecería necesario acudir a dicho trámite, entiende Falguera[458].

456 STS de 23 de octubre de 2018 (Sala II).

457 NORES TORRES, L. E., "Algunas cuestiones sobre la utilización de las redes sociales como medio de prueba en el proceso laboral", *Actualidad Laboral*, núm. 3/2014. Vid. MARTÍNEZ DE CARVAJAL HEDRICH, E., "Valor probatorio de un correo electrónico", *Diario La Ley* núm. 8014; MAGRO SERVET, V., "El uso de la webcam para la práctica de la prueba", *Diario La Ley*, núm. 6132; TIRADO ESTRADA, J. J., "La documentación video gráfica de las vistas orales y su trascendencia procesal. El artículo 147 de la Ley de Enjuiciamiento Civil", *Diario La Ley*, núm. 7674.

458 FALGUERA BARÓ, M. A., "Nuevas tecnologías y trabajo (III): perspectiva procesal", *Trabajo y Derecho*, núm. 22, octubre 2016, pág. 16.

Desde ese punto de vista, si en el legítimo ejercicio de sus capacidades de vigilancia y control el empleador tuviere conocimiento de una determinada comunicación del trabajador a través de una red social abierta, o los interlocutores del correo electrónico, o las webs que consten en el historial del ordenador de uso personal del asalariado, etc., no será precisa ninguna declaración judicial previa sobre la validez de la prueba. Sin embargo, si la prueba consiste en el resultado de una monitorización del ordenador, la aportación de correos de índole personal, documentos o archivos con ámbito de privacidad presunta, grabaciones de cámaras sin notificación previa, etc., el empleador deberá solicitar la autorización judicial de la prueba.

6. Por nuestra parte, entendemos que la prescripción del apartado 3 del art. 18 CE es taxativa al señalar que se garantiza el secreto de las comunicaciones (…), salvo resolución judicial[459], sin que excepcione al respecto supuesto alguno, así como tampoco hace reserva aplicativa, ni expresa ni tácita, para ámbito jurisdiccional alguno, lo que equivale a decir que si el empresario pretendiere monitorizar las comunicaciones mantenidas por el trabajador vía *e-mail* de la empresa accediendo al contenido de los mensajes enviados y/o recibidos por éste, habrá de solicitar del juez la pertinente autorización con especificación de la causa motivadora y teniendo presente que, de no ser así, podría incurrir en el tipo del art. 197 CP[460]. Recuérdese, en

459 Bien es cierto que el legislador del 78 no estaba pensando en el correo electrónico dado que en esos momentos ni existía. La exigencia de resolución judicial estaba prevista originariamente para intervención de teléfonos por parte de la policía.

460 Baste recordar el caso Coapi (vid. Auto dictado por la Audiencia Provincial de Madrid de 23 de enero de 2004, ponente Abad Crespo) una de las escasas resoluciones judiciales en la materia. En dicho caso se estima un recurso de apelación indicando al Juzgado de Instrucción proceder a la continuación de las diligencias previas en un caso en el que se aplica el tipo del art. 197.1 CP a un control del ordenador y del correo electrónico del trabajador mediante la instalación de un programa espía. La Audiencia Provincial estima en su resolución que *"los hechos denunciados (…) revisten provisionalmente caracteres del delito tipificado en el citado art. 197.1 CP, pues tales hechos suponen que la empresa para la que prestaba sus servicios como empleada la denunciante instaló un mecanismo para tener acceso a los correos electrónicos que realizara la denunciante en el ordenador cuyo uso tenía atribuido en el centro de trabajo, y conocer de tal forma el contenido de dichos correos, llegando efectivamente a acceder al contenido de mensajes privados remitidos por la denunciante, y aunque la última finalidad perseguida por la empresa fuera el conseguir pruebas para el despido de la denunciante, es claro que tuvo que conocer que con tal actuar vulneraba la intimidad*

este punto, el principio de jerarquía de fuentes, que determina que la Constitución es la norma suprema del ordenamiento jurídico, de modo que cualquier norma de rango inferior habrá de respetar y seguir sus postulados, entre los que se cuenta el del apartado 3 de su art. 18 (necesidad de resolución judicial para quebrar el derecho al secreto de las comunicaciones).

7. Es por ello que consideramos más acertada con la configuración constitucional del derecho al secreto de las comunicaciones la doctrina de la Sala de lo Penal del TS contenida en la sentencia 528/2014, de 16 de junio[461], que no avala una interpretación que devalúa el modelo constitucional de protección del secreto de las comunicaciones en la empresa privándole de su efecto útil, y en la que hace una diplomática, pero nada disimulada, crítica tanto a la doctrina del TC como a la jurisprudencia social del TS por haber debilitado las garantías constitucionales frente a las injerencias empresariales en el secreto de las comunicaciones de sus empleados.

Y aunque su crítica doctrinal se formulaba *obiter dicta*, pues no afectaba al fallo, abrió sin embargo un importante conflicto, no sólo teórico, entre ambos espacios de control jurisdiccional, el laboral y el penal, en torno al canon específico de control de la licitud de las pruebas electrónicas obtenidas *ex* art. 20.3 ET para fiscalizar el uso por los trabajadores de los dispositivos de comunicación de titularidad de la empresa, entendiendo que el modelo de garantías débiles (naturaleza disponible del derecho para el empleador y/o para el trabajador) no se ajusta al modelo constitucional, por lo que no puede servir para valorar la validez y la eficacia penal de la prueba, articulando su

personal de la denunciante en la variante del derecho al secreto de las comunicaciones, por lo que la conducta objetiva de la empresa estaba intencionadamente destinada como finalidad inmediata a vulnerar la intimidad de la denunciante".

461 STS (Sala 2ª) 528/2014, de 16 de junio de 2014, rec. núm. 2229/2013. El caso se refiere a un trabajador de una empresa que, aprovechando su posición en el sistema de pagos a proveedores ideado por aquélla para todo el grupo - sistema de *confirming*- , estableció por su cuenta relaciones con algunos de los proveedores para facilitarles la gestión del cobro - anticipo del vencimiento- a cambio de un precio. De este modo, los proveedores se ahorraban intereses y comisiones de los adelantos negociables directamente con las entidades bancarias pagadoras y el trabajador un ingreso extra.

razonamiento jurídico sobre dos argumentos de estricta hermenéutica constitucional –no penal -, siendo tales que:

a) El texto constitucional no contempla excepción alguna a la necesidad de autorización judicial para la intervención de las comunicaciones, ni por la titularidad dominical del canal elegido para la comunicación (ordenador, teléfono, etc., propiedad de tercero ajeno al comunicante), ni por el carácter del tiempo en el que se utiliza (laboral o personal), ni por la naturaleza del cauce comunicativo (correo corporativo).

b) La eventual tácita renuncia a la expectativa razonable de confidencialidad no convalida la ausencia de intervención judicial, porque ni sería realmente querida por el comunicante que, de saber sus efectos perjudiciales, seguramente se abstendría de realizar la comunicación, ni aunque se formalizara la renuncia-autorización resultaría operativa ya que, a diferencia de lo que ocurre con la protección del derecho a la inviolabilidad del domicilio (art. 18.2 CE), nuestra Constitución no contempla la autorización del propio interesado como argumento habilitante para la injerencia[462].

En suma, la doctrina de la Sala de lo Penal del TS contenida en la sentencia referida no ofrece dudas al respecto: el art. 18.3 CE reconoce un régimen de protección reforzado para el secreto de las comunicaciones al excluir cualquier supuesto que no contemple la intervención del Juez como figura tuteladora del derecho del investigado.

Un plus de protección o tutela reforzada que no sería arbitraria sino lógica y que encuentra su fundamento en la gravedad de esta clase de

462 MOLINA NAVARRETE, C., “El derecho al secreto de las comunicaciones en la relación de trabajo…, *op. cit.*, pág. 11.

injerencias, en tanto que se introducen y revelan toda clase de aspectos referentes a la privacidad del comunicante, tanto los de interés para la investigación como otros por completo ajenos a ese legítimo interés (STS – Sala 2ª – 528/2014, de 16 de junio).

No se puede decir, pues, con mayor claridad ni con más precisión, de modo que en el plano constitucional, no ya sólo en el plano penal, difícilmente puede hallar fisura alguna - más allá, claro está, de querer reservar un ámbito de control privilegiado, devaluado constitucionalmente, para el empleador -, al tiempo que ilustra perfectamente la diferencia entre los límites al control empresarial de las comunicaciones por ordenador en el ámbito laboral y en el penal, dejando en evidencia a la Sala Social del TS y al Tribunal Constitucional, a los que trata de marcar un nuevo camino en la tutela efectiva del derecho fundamental al secreto de las comunicaciones de los trabajadores[463].

En definitiva, la Sala de lo Penal del TS afirma en la sentencia comentada que, para que las comunicaciones de los trabajadores interceptadas por el empresario tengan eficacia probatoria en la jurisdicción

463 MOLINA NAVARRETE, C., "Autotutela empresarial, secreto de las comunicaciones y control judicial: la Sala Social pierde el paso con la Sala Penal, Comentario a la Sentencia del Tribunal Supremo, Sala 2ª, de 16 de junio de 2014, rec. núm. 2229/2013", en *RTSS. CEF*, núm. 381 (diciembre 2014), pág. 158.

Sostiene Molina Navarrete que el legislador español, a diferencia de otros países, apenas ha prestado atención a la regulación del modo y límites en que las empresas pueden fiscalizar el contenido de los ordenadores usados por sus empleados para desarrollar su actividad laboral, así como las comunicaciones telemáticas. Por esta razón abstencionista, las reglas ordenadoras o las hallamos en los escasos convenios colectivos que dedican espacio a ello, o están establecidos, de forma no uniforme, por los diferentes tribunales con competencia en la materia, sean nacionales o internacionales. Por consiguiente, el punto de referencia jurídico fundamental estará en la lectura que cada uno de estos órdenes jurisdiccionales hace de las normas superiores de referencia. En el ámbito nacional, el art. 18.3 CE, que requiere, para el ámbito penal, autorización e intervención judicial como condición ineludible para otorgar eficacia probatoria al resultado de la prueba consistente en la intervención de las comunicaciones protegidas por el derecho consagrado en aquél, así como, para el ámbito internacional europeo, el art. 8 del Convenio Europeo de Derechos Humanos, que prohíbe toda injerencia "pública" en el derecho al respeto de la vida privada y familiar, de su domicilio y de la correspondencia de toda persona, salvo que concurra un interés general suficiente - la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito o la protección de derechos y libertades de los demás-.

penal, resultará siempre necesaria la autorización judicial, según contempla el art. 18.3 CE, con algunas excepciones como son los denominados datos de tráfico, por ejemplo. Pero estos supuestos excepcionales sí quedarían amparados por el derecho a la intimidad, y por lo tanto, les serían aplicables las garantías sobre el juicio de proporcionalidad y las expectativas de derecho[464].

Pero aún más: a nuestro juicio, la Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social, también introduce la exigencia de autorización judicial previa en el orden social. En efecto, el art. 90.4 LRJS, al tratar precisamente la admisibilidad de los medios de prueba en el procedimiento social, no penal, establece que cuando fuere necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que pueda afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existieran medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto, previa ponderación de los intereses afectados a través de juicio de proporcionalidad y con el mínimo sacrificio, determinando las condiciones de acceso, garantías de conservación y aportación al proceso, obtención y entrega de copias e intervención de las partes o de sus representantes y expertos, en su caso.

Este precepto, rememorando la previsión del art. 18.3 CE, llama a la autorización judicial cuando una prueba, que pudiera afectar a la intimidad personal u otro derecho fundamental, resultare necesaria para el buen fin del proceso (a menudo se instrumenta la tecnología del poder digital empresarial al servicio de la constitución de una prueba de garantía para el éxito del poder disciplinario)[465]. Y, como hemos visto, la STS (Sala 2ª) 528/2014, de 16 de junio, con exquisito respeto pero no menor contundencia para quien lo quiera

464 TOSCANI GIMÉNEZ, D. y VALENCIANO SAL, A., *Derechos fundamentales inespecíficos…,*op. cit, pág. 79.

465 TASCÓN LÓPEZ, R., "Tecnovigilancia empresarial y derechos de los trabajadores", *CEF-Revista de Trabajo y Seguridad Social*, nº 415, octubre 2017, págs. 53 y sigs.; PRECIADO DOMENECH, C.H., "La video vigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal", *Revista de Derecho Social*, nº 77, enero-marzo 2017, págs. 85 y sigs.

entender (hasta hoy nadie de la jurisdicción social), evidencia que ese modelo legal es coherente no sólo con la norma penal, ámbito le corresponde delimitar, sino a lo previsto *ex* art. 18.3 CE, sin éste que contenga excepción alguna.

Por tanto, a nuestro entender, actualmente en el orden social, para que se puedan interceptar los correos electrónicos de los trabajadores y tengan valor y eficacia probatoria en la jurisdicción social, es necesario tanto el conocimiento previo por parte del trabajador de esta cuestión como una autorización e intervención judicial previa al efecto, pues se trata de supuestos amparados por el art. 18.3 CE[466].

Es necesario señalar, además, respecto del correo electrónico, que en los supuestos en los que la dirección del correo electrónico pueda dar lugar a ofrecer información sobre la persona que es titular del mismo ya sea a través del nombre y apellidos e incluso cuando dichos datos no estén referenciados como tal, pero pueda desprenderse de la dirección de correo, la Agencia de Protección de Datos determina que dicha información tiene carácter de dato personal, y en consecuencia, la aplicación y protección que la LOPD ofrece en este sentido[467].

8. La Sala de lo Penal[468], en su profunda enmienda hermenéutica al TC y a la Sala de lo Social del TS, no se queda en el plano constitucional, sino que desciende al ordinario para seguir impartiendo doctrina de interpretación jurídica sistemática y finalista, afirmando que el modelo de autorización judicial, frente al modelo de auto-tutela o de policía privada empresarial, es el único

466 En el mismo sentido, TOSCANI GIMÉNEZ, D. y VALENCIANO SAL, A., *Derechos fundamentales inespecíficos…,op. cit,* pág. 80.

467 TÉLLEZ AGUILERA, A., *Nuevas Tecnologías. Intimidad y Protección de datos. Estudio sistemático de la Ley Orgánica 15/1999*, Edisofer, Madrid, 2001, págs. 115 y sigs.

468 STS (Sala 2ª) 528/2014, de 16 de junio.

coherente con la reforma procesal social (art. 90.2 y 4 LRJS) y que, por su especificidad debería desplazar, o cuando menos modular, al art. 20.3 ET.

En definitiva, la Sala de lo Penal propone un modelo de tutela del secreto de las comunicaciones de los trabajadores en la empresa indiferenciada respecto de la vida civil y, por tanto, reforzada y no privilegiada a favor del empleador, si bien la misma da la espalda a la necesidad de una cierta flexibilidad, lo que da idea de lo cuidada de su posición[469].

En efecto, esta regla general de tutela (no cabe más interferencia en las comunicaciones del trabajador que las autorizadas por el juez de lo social, en su caso, o penal, según la causa) encuentra un límite interno relativo a su objeto mismo, dado que para la Sala de lo Penal, que propone una interpretación estricta, la autorización judicial es exigible tan sólo respecto a lo que estrictamente constituye ese secreto de las comunicaciones, es decir, con exclusión de (i) los datos de tráfico de las comunicaciones electrónicas, incluyendo el uso del equipo informático para acceder a otros servicios de la red (páginas web, etc.), y (ii) los mensajes electrónicos recibidos y abiertos por su destinatario, pues estos ya no forman ya parte de la comunicación propiamente dicha.

Y, en estos casos, ¿qué normativa rige para garantizar su protección? -pues no se pueden dejar inermes ante la potestad empresarial -. Al respecto, la Sala de lo Penal precisa que para ellos rigen normas diferentes como las relativas a la protección de datos (art. 18.4 CE) o a la intimidad documental…y sin la exigencia absoluta de la intervención judicial (art. 18.1 CE).

469 MOLINA NAVARRETE, C., "El derecho al secreto de las comunicaciones en la relación de trabajo…, *op. cit.*, pág. 12.

No obstante, conviene poner de relieve que la posición penal no estaba completamente silenciada en sede constitucional, pues la STC 241/2012, de 17 de diciembre, cuenta con un fundado voto particular de dos Magistrados -uno laboralista y de máxima autoridad científica-, en el que se expresó claramente que cualquier intervención empresarial debe producirse con las prevenciones y cánones de la autorización judicial que cita el art. 18.3 CE, en cuya definición la jurisprudencia constitucional incorpora la exigencia de una norma legal que habilite la injerencia (STC 49/1999, de 5 de abril).

Y, asimismo, una posición flexible, pero garantista -ciertamente más transaccional respecto del modelo jurídico fuerte de protección del secreto de comunicaciones digitales del trabajador en el puesto de trabajo (basado en la autorización judicial)-, también está presente en algunos pronunciamientos, minoritarios de la doctrina de suplicación social, tales como el de la STSJ Galicia, de 30 de diciembre de 2014, rec. 3596/14. Aunque esta sentencia asumió que el despido era procedente porque la empresa pudo acreditar la veracidad de la infracción grave imputada al trabajador -aceptar regalos de alta cuantía, prohibidos en el Código de Conducta del Grupo, conocido y consentido por el trabajador expresamente -, en virtud de pruebas basadas en “hallazgos casuales” por un compañero de trabajo (extractos de transferencias a cuentas personales) en una “sala de uso común” para los empleados (sitio de fotocopiadoras), anuló la prueba electrónica consistente en registrar e intervenir el buzón de correo electrónico profesional del trabajador que se aloja en los servidores de la empresa -Grupo Inditex -. Y ello pese a darse por probado que (FJ 5):

1. La empresa contaba con una política relativa a los usos de los dispositivos electrónicos, reservándolos a fines productivos e informando de que tenía la facultad de vigilar su cumplimiento.

2. El trabajador la conoce y la acepta cada vez que entra en el correo, pues se les solicita confirmación de aceptar aquella política de seguridad.

3. El ejercicio del poder de fiscalización de los correos electrónicos ha sido ponderado y limitado a aquello que tenía relación con los documentos hallados y en fechas próximas a las de emisión de las trasferencias.

¿Entonces, por qué llega a la conclusión de la nulidad de la prueba? Pues sencillamente porque asume que no puede haber más intromisión en las comunicaciones electrónicas que las que autorice el juez, habida cuenta de que el control del correo electrónico…queda excluido de las facultades empresariales por estar protegido por los derechos fundamentales relativos a la intimidad personal y al secreto de las comunicaciones.

9. Poco más de 3 años después de ello, la STS 119/2018 (Sala IV), de 8 de febrero, ante los mismos hechos, hará una valoración diferente del estado normativo y jurisprudencial en la materia validando la prueba mediante los siguientes argumentos - además de asumir que existía una política de información previa suficiente (canon de regulación específica y trasparente):

a) Concurre causa legítima del empresario en la monitorización del correo porque había indicios suficientes de infracción por hallazgos “casuales” (justificación).

b) El grado de intromisión del empleador en los contenidos de los mensajes no es desmedido, pues la fiscalización del contenido de tales correos fue selectivo, no indiscriminado (juicio de proporcionalidad).

c) No existían medios menos intrusivos para la consecución del mismo objetivo (juicio de necesidad).

d) En todo caso, el trabajador ha contado con adecuadas garantías judiciales para defender sus derechos e intereses en un juicio justo.

La STS 119/2018 (Sala IV), de 8 de febrero, considera que su razonamiento resulta impecable incluso atendiendo al reciente y más riguroso Test de Conformidad Barbulescu del TEDH, con lo que, de un lado, afirma que el justo equilibrio entre el derecho del trabajador al respeto de su correspondencia y los intereses de la empresa empleadora se habría respetado escrupulosamente en el caso de autos.

10. Sin embargo, frente a lo que afirma el TS, las novedades de la doctrina Barbulescu son más que evidentes, llamando la atención, por un lado, la importancia que a la dimensión social de las relaciones comunicativas en el seno de la empresa se le da, lo cual impide una prohibición de carácter absoluto de un uso no puramente productivo de los dispositivos móviles de titularidad de la empresa, generando una mayor expectativa de reserva de confidencialidad para el trabajador y, de otro, la insuficiencia de la política de información previa empresarial (canon de control basado en la transparencia informativa) para descartar la vulneración de aquélla expectativa[470].

Además, es oportuno introducir un tercer elemento de novedad que ofrece, a mi juicio, el test de conformidad del poder de control de la corrección laboral de las comunicaciones digitales del trabajador durante su tiempo de trabajo, cual es que el juicio sobre el justo equilibrio entre los intereses

470 MOLINA NAVARRETE, C., "El derecho al secreto de las comunicaciones en la relación de trabajo…, op. cit., pág. 15.

contrapuestos en juego (juicio de proporcionalidad) ha de ser concreto, no abstracto, y con efecto útil para el derecho del trabajador, no formal.

En efecto, si se analiza esta jurisprudencia de forma general, sin entrar en la letra pequeña de los detalles –como, a mi juicio, hace la Sala de lo Social del TS -, la conclusión será que existe una sustancial coincidencia entre todos los niveles jurisdiccionales que han intervenido, incluidas las dos Salas del TEDH, así como sus respectivos votos particulares, pues todos ellos asumen que este justo equilibrio necesario entre la legitimidad de control de la empresa y el derecho de protección del trabajador se rige por los principios de justificación suficiente (causa o fin lícitos), trasparencia (información previa adecuada), proporcionalidad (necesidad, idoneidad y ponderación razonable de sacrificios) y de seguridad, en los términos hoy exigibles por el marco jurídico de la protección de datos (Directiva 95/46/CE, en su momento; hoy Reglamento de Protección de Datos).

11. Sin embargo, los tribunales nacionales no han conseguido darles una aplicación adecuada en el plano concreto, tan sólo en el meramente teórico y formal, dado que, de un lado, no basta con informar de que las comunicaciones pueden ser controladas (información previa, potencial y abstracta), sino que ha de hacerse de forma útil y concreta, esto es, en un tiempo cercano al ejercicio del poder de control específico y dando cuenta precisa de la naturaleza y alcance de la vigilancia a que iba a ser sometido, así como del grado de intrusión en su correspondencia[471].

Por otra parte, no basta con informar de que, entre esos medios de control, se encuentra la monitorización de los correos electrónicos y el acceso a su contenido - presumiendo que será profesional, por prohibir el particular -, sino que el empleador está obligado a recurrir a las medidas menos intrusivas

471 MOLINA NAVARRETE, C., “El derecho al secreto de las comunicaciones en la relación de trabajo…, op. cit., pág. 16.

para la correspondencia del demandante –el trabajador-, hasta el punto de exigirle verificar si el acceso al contenido de las comunicaciones hubiera sido posible sin su conocimiento.

Pues bien, si comparamos este riguroso juicio de proporcionalidad – en orden a la medición de la legitimidad de la intrusión empresarial en el secreto de las comunicaciones personales de los trabajadores durante el tiempo de trabajo - con el establecido por el TS, observamos que ni el juicio de trasparencia resulta adecuado (la información era previa; estaba establecida en la política de seguridad de la empresa y no fue próxima al tiempo en que se ejerció el control), ni mucho menos el juicio de necesidad.

12. En efecto, pues si el TS considera suficiente la prueba del "descubrimiento casual", ¿para qué había que entrar en el contenido concreto de los correos, injiriéndose en el secreto de las comunicaciones? La respuesta a este interrogante es obvia: la prueba informática era determinante y, por tanto, daba certeza probatoria al empleador, que de ese modo se aseguraba el éxito judicial de su decisión de despedir.

Pero, como es sabido, el interés protegido del empleador no es el de asegurar su posición probatoria, sino el de disponer de controles útiles para tutelar su interés productivo, siempre respetando los derechos fundamentales del trabajador. Y si quiere asegurarse una prueba basada en injerirse en el secreto de comunicaciones la ley lo prevé, sí, pero por el camino del art. 90.4 LRJS: la autorización judicial.

Y, precisamente, el Juzgado de lo Social nº19 de Madrid, ha dictado la sentencia 453/2017, de 17 de noviembre de 2017 (Autos 737/17), en la que, con aplicación estricta del test Barbulescu, llega a la conclusión de que la empresa ha invadido el derecho fundamental del trabajador al secreto de comunicaciones porque para controlar el incumplimiento del que tenía noticia

por quejas de otros compañeros no tenía necesidad de injerirse en el contenido de los mensajes personales, pues disponía de *"vías menos invasivas, tales como el control de los resultados del trabajo de la demandante…o por medio de la exigencia de una dación de cuenta por parte de la actora de las tareas realizadas…"*. En el supuesto enjuiciado por el Juzgado de lo Social Nº 19 de Madrid, la empresa contaba con una política de uso razonable de los medios electrónicos puestos a disposición de los trabajadores en la que, pese a clarificar el uso prevalentemente profesional, no se excluían los usos personales, siempre que fuesen limitados, esto es, necesarios (mínimos) y no nocivos para la empresa.

13. A todo lo manifestado hay que añadir que el apartado 4 del art. 76 LRJS configura al juez laboral como juez de las garantías y las libertades fundamentales en el ámbito de las relaciones de trabajo y del orden social[472], de modo que cuando la realización de una diligencia preliminar solicitada pudiere afectar a la intimidad personal o a cualquier otro derecho fundamental, el juzgador, de no mediar consentimiento del afectado, podrá autorizar dicha actuación en la forma y con las garantías establecidas en los apartados 4 a 6 del art. 90 LRJS.

Es decir, si existiere riesgo de afectación a derechos fundamentales corresponde al juez de lo social autorizar la actuación y disponer lo necesario en garantía de los derechos fundamentales afectados, a instancia de quien vaya a demandar, bien del trabajador o del empresario y, en general, de quien sea o vaya a ser parte actora en el ulterior proceso, criterio este que, *mutatis mutandis*, puede ser trasladado a los actos preparatorios[473].

472 MARTÍN FLÓREZ, L., "La nueva Ley reguladora de la Jurisdicción Social", en *Actualidad Jurídica Uría Menéndez* 31/2012, pág. 16.

473 FOLGUERA CRESPO, J. A. y otros, *Comentarios a la Ley Reguladora de la Jurisdicción Social*, Lex Nova Thomson Reuters, Valladolid, 2012, págs. 375-376. En idéntico sentido, MERCADER UGUINA, J. R., *Ley Reguladora de la Jurisdicción Social comentada y con jurisprudencia*, La Ley, Madrid, 2015, págs. 645 y sigs.; SEMPERE

A ello se añade por parte de la LRJS, ante la vulneración de derechos fundamentales en la obtención del instrumento probatorio, una novedosa garantía positiva consistente en que no se podrá acceder a documentos o archivos si pudiera verse afectada la intimidad personal o cualquier otro derecho fundamental sin que el juzgador autorice dicha actuación mediante auto, previa ponderación de los intereses que resultaren afectados, determinando las condiciones de acceso, así como las garantías de conservación y aportación al proceso. A lo que hay que unir la prescripción contenida en el apartado 2 del artículo 90 LRJS, que dispone que no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas.

14. Aún más: la STEDH de 30 de mayo de 2017 (caso Trabajo Rueda c. España) señala expresamente que, en lo que respecta al acceso al contenido de un ordenador personal por parte de la policía, la jurisprudencia del TC ha instaurado la regla de la previa autorización judicial, requisito exigido en cualquier caso por el art. 8 del Convenio (que requiere la emisión de una orden por un órgano independiente) cuando se trata de una vulneración de la vida privada de una persona (Dumitru Popescu c. Rumania de 26 de abril de 2007, y Iordachi y otros c. Moldavia de 10 de febrero de 2009), si bien la jurisprudencia constitucional española permite, sin embargo, a título excepcional hacer caso omiso de esta autorización en situaciones de urgencia (“necesidad urgente”) que pueden ser objeto de un control judicial posterior.

En concreto, el TEDH en el caso Trabajo Rueda c. España consideró vulnerado el derecho al secreto de las comunicaciones del demandante en la intervención de su ordenador personal sin orden judicial a pesar de que en dicho registro se comprobó la existencia de archivos de contenido pornográfico de menores, estimando el tribunal que el registro y examen de los archivos del

NAVARRO, A. V., Comentarios a la Ley de la Jurisdicción Social, Thomson Reuters Aranzadi, Pamplona, 2013, págs. 462 y sigs.

ordenador por la policía no fue proporcionado a las finalidades legítimas perseguidas, no existiendo la urgencia necesaria que habría obligado a la policía a registrar los archivos del ordenador personal del demandante y acceder al contenido, sin obtener previamente la autorización judicial requerida, así como tampoco existía ningún riesgo de desaparición de ficheros puesto que el ordenador lo tenía la policía y no estaba conectado a internet. La autorización judicial previa a la intervención sobre el ordenador del demandante podría haber sido obtenida rápidamente, sin haber dificultado la investigación sobre los hechos denunciados[474].

15. ¿Cuál sería, pues, la secuencia lógica para poder solicitar la autorización judicial en orden a la intervención del correo electrónico del trabajador? La respuesta a este interrogante es la siguiente: en caso de que el empresario sospeche de la comisión de algún ilícito por parte del trabajador vía *e-mail* corporativo habrá de proceder al despido de éste previo aseguramiento de sus correos electrónicos y, en caso de que el trabajador demandara, el empresario habrá de solicitar del juez de lo social la pertinente autorización judicial para entrar a conocer del contenido de los correos electrónicos del trabajador asegurados previamente vía notario público, si no quiere vulnerar el derecho al secreto de las comunicaciones, y poder aportarlo al proceso laboral sin riesgo de ser tachado por parte del actor.

3.- Consecuencias de la prueba obtenida con lesión del derecho al secreto de las comunicaciones.

1. Finalmente, conviene exponer, de forma breve, las consecuencias de una prueba obtenida con violación del derecho del secreto de comunicaciones de los trabajadores, pues tan importante cuestión dista de estar clara, así como

474 LARRÁYOZ SOLA, I., "Vulneración del derecho al secreto de las comunicaciones en intervención de ordenador personal", en *Revista Aranzadi Doctrinal num.8/2017 parte Jurisprudencia*, Editorial Aranzadi, S.A.U., Cizur Menor. 2017.

en general las obtenidas con violación de otros derechos fundamentales -vinculados a la protección de la privacidad-, al no existir acuerdo en torno a sus efectos más allá de la sanción de nulidad *ex* art. 90.2 LRJS y 11.1 LOPJ.

De forma sintética, varios serían los aspectos a comentar y precisar: en primer lugar, el alcance de la denominada doctrina del "fruto del árbol envenenado", conforme a la cual deben declararse inválidas todas las pruebas que se deriven, directa o indirectamente, aunque haya sido obtenidas de forma lícita. Para la STS 119/2018, de 8 de febrero, no habiendo prueba ilegítima no hay que plantearse la doctrina del "hallazgo casual", que sí aplico la doctrina de suplicación del TSJ de Galicia, de modo que dejó a salvó todas las pruebas anteriores a la realización de la inspección del correo electrónico -que estimó nula por violación del secreto de comunicaciones-, declarando la procedencia del despido por vulneración del Código Ético o de Conducta del Grupo Inditex (código de prácticas responsables)[475] . Una línea que sí parece tener encaje en la doctrina del TEDH, según se desprende de su sentencia López Ribalda *et alii* c. España (STEDH 9 de enero de 2018).

En segundo lugar, cabe plantearse si, anulada la prueba por violación del derecho fundamental, y no probada la infracción por otro medio de prueba lícito, la calificación del eventual despido basado en la prueba anulada debe ser la de nulidad o de si, en cambio, cabe concluir la improcedencia del despido. Pues bien, al respeto no existe una doctrina de suplicación social (no hay jurisprudencia unificada al respecto), de tal guisa que mientras unas salas asumen que no hay nulidad del despido, pues su móvil es ajeno a la violación del derecho fundamental (STSJ Castilla-La Mancha 25/2018, de 12 de enero y STSJ Canarias de 11 de mayo de 2017), otras entienden que sí por cuanto el art. 55.5 ET asume un modelo objetivo, esto es, la nulidad derivaría tanto si el despido tiene como móvil la vulneración de uno de los derechos fundamentales como si se "produce con violación" de ellos, esto es, si tiene como resultado

475 Una visión expansiva de la responsabilidad de los trabajadores a partir de estos Códigos se encuentra en la STSJ Andalucía (Sevilla) 1736/2017, de 8 de junio. Otra más restrictiva, en la SAN 148/2018, de 16 de febrero.

una violación del mismo, aunque no se busque por el empleador (STSJ País Vasco de 10 de mayo de 2011 y STSJ Extremadura de 30 de julio de 2014)[476], siendo la segunda la solución más acorde con la literalidad del precepto estatutario, e incluso con la mayor efectividad de los derechos fundamentales, aunque la misma expresa un modelo de garantías fuertes que el propio TEDH no ha hecho propio, pues éste ha considerado que ni el despido deviene ilícito por vulnerarse el derecho fundamental, si median otras pruebas lícitas, ni hay violación del derecho a un proceso justo cuando sí concurren otras garantías procesales (asunto López Ribalda *et alii* c. España).

En tercer lugar, y al margen de que la solución más correcta sea la segunda, lo que no sería posible eludir es la indemnización, reparadora y disuasoria, de daños frente a pruebas que se obtengan violando el secreto de comunicaciones. En este sentido, ni la protección del derecho fundamental puede ser puramente simbólica (STC 247/2006, de 24 de julio) - lo que sucedería si, anulada la prueba por violación del secreto de las comunicaciones, el trabajador termina siendo despedido procedentemente por concurrir pruebas lícitas -, ni el daño moral requiere de una prueba específica, presumiéndose de forma automática con la sola infracción (STS 119/2018, 8 de febrero). Otra cosa será su cuantificación (se ha consolidado el criterio de las sanciones del TRLISOS)[477]. De nuevo, el TEDH no parece dar acogida a tal criterio, al entender que la sola declaración de violación del derecho fundamental (como los que se recogen en el art. 8 CEDH) ya constituye una satisfacción suficiente y justa por cualquier daño moral sufrido (apartado 147).

476 Vid. BENITO-BUTRÓN OCHOA, J. C., "¿Cabe reconocer la indemnización de daños cuando se declara nula una prueba con lesión de derechos fundamentales aunque el despido no sea declarado nulo?", *Revista CEF – Trabajo y Seguridad Social*, nº 421, abril 2018, págs. 128 y sigs.

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

CAPÍTULO IV.- EL DEBER DE INFORMACIÓN DEL EMPRESARIO.

1. La legalidad del control empresarial no se subordina únicamente a la superación del triple test de proporcionalidad, sino que se ha de cumplir asimismo con la exigencia de información a los trabajadores acerca del control audiovisual de la actividad laboral[478], de modo que el previo conocimiento de la instalación de cámaras de video vigilancia y de su finalidad deviene requisito imprescindible para la validez de dicho control.

A tal efecto, el art. 89.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, determina que los empresarios habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. Pero conviene señalar que información no equivale a consentimiento, de modo que el empresario puede implantar sistemas de video vigilancia sin contar con la autorización del empleado en virtud del poder de control y vigilancia que le confiere el art. 20.3 ET.

En este sentido, desde la STEDH de 3 de abril de 2007 (caso Copland c. Reino Unido) se entiende que la expectativa de intimidad en el uso de las herramientas informáticas por parte del trabajador sólo desaparece con la previa información que la empresa facilita a éste acerca de la vigilancia que puede ejercitar al respecto, de forma que los empleados habrán de tener conocimiento de la advertencia del empresario acerca del uso estrictamente laboral que haya de darse al correo electrónico y de su posible control,

478 RODRÍGUEZ ESCANCIANO, S., *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015, págs. 70 y 71; FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial de la actividad laboral es España", *Labour & Law Issues*, vol. 2, nº 1, 2016, pág. I-64.

advertencia usualmente incorporada en protocolos internos dado el escaso número de convenios colectivos que incorporan cláusulas al respecto[479].

De este modo, un uso que contravenga las referidas instrucciones habilitaría el control del empresario sin que quepa invocar de contrario una supuesta expectativa de privacidad por parte del trabajador, posición esta que fue ratificada, por lo demás, en las SSTS de 26 de septiembre de 2007 y de 8 de marzo de 2011, entendiendo en ambas el Tribunal Supremo que el trabajador carece de un derecho al uso personal de los medios informáticos que la empresa pone a su disposición para el desarrollo de la prestación laboral, si bien el control ha de efectuarse con garantías, las cuales requieren una previa información a los trabajadores al respecto, así como la existencia de unas reglas de uso que habrán de ser conocidas por los empleados[480].

2. No obstante, la STS de 6 de octubre de 2011 matizó esta posición flexibilizando el control de la legalidad de la actuación empresarial[481] al dejar de exigir estrictos protocolos de uso e información y entender, por el contrario, que bastaría para dejar inoperativa la expectativa de privacidad del trabajador con una mera prohibición absoluta del uso de las herramientas informáticas para fines ajenos a los estrictamente laborales. Es decir, el TS entiende que la mera prohibición del uso personal conlleva implícitamente una advertencia sobre la posible instalación de medidas de control, sin que quepa invocar lesión alguna del derecho a la intimidad del trabajador cuya actividad laboral resulta fiscalizada[482].

479 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.59.

480 FERRANDO GARCÍA, F. M., "Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías", *RTSS. CEF*, núm. 399, 2016, págs. 43 y 44.

481 Al respecto vid. CARRIZOSA PRIETO, E., "El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores", *Temas Laborales*, núm. 116, 2012, págs. 251-267.

482 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.60.

3. Y siguiendo esta visión flexibilizadora del deber de información, la STC 170/2013, de 7 de octubre, también considera suficiente la mera prohibición de una concreta conducta para que el empleador pueda proceder a la fiscalización de la actividad de los trabajadores sin necesidad de facilitarles ningún tipo de información acerca de los posibles medios de control a utilizar. Concretamente, la información previa al empleado se entiende obviada en esta sentencia con la previsión contenida en el convenio colectivo aplicable calificando de falta leve el uso de los instrumentos informáticos para fines distintos de los estrictamente laborales[483].

Ahora bien, si no existiere previsión alguna al respecto, la mera titularidad empresarial del medio de trabajo no se considera justificación suficiente para proceder al control del uso que el trabajador hace del correo electrónico corporativo, sino que, en tales casos éste cuenta con una expectativa general de privacidad dado que la ausencia de instrucciones al respecto es entendida como una suerte de tolerancia empresarial hacia el uso extra laboral de las herramientas informáticas, por lo que cualquier cambio en esta postura exige de una comunicación previa al trabajador por razones de buena fe[484].

4. En definitiva, pesa sobre el empresario el deber de informar adecuadamente del control de la actividad, sin que meros carteles anunciadores de la existencia de dispositivos de vigilancia resulten suficientes. Así lo entendió la STC 29/2013, de 11 de febrero, en la que se consideró que el empleador sólo podía hacer uso de la información así obtenida para los fines que se hubieren comunicado expresamente al trabajador, de forma que la instalación de cámaras de video vigilancia con la finalidad de prevenir la

483 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.61.

484 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., *Idem.*, pág. I.62.

comisión de delitos, así comunicada a éste, no podía ser objeto de invocación para justificar un despido disciplinario en virtud de las imágenes obtenidas.

Esta sentencia es de suma importancia por constituir la misma el primer pronunciamiento que valoró la controversia bajo el tamiz de los principios de la protección de datos, dejando a un lado el derecho de intimidad pese a haber sido este último el invocado por el propio recurrente[485], siendo en virtud del art. 18.4 CE, y no en base al art. 18.1 CE, por el que el TC fundamentó la ilegalidad de unas grabaciones utilizadas para una finalidad diferente a la prevista con su implantación, incumpliéndose de ese modo el deber de información previsto en el art. 5.1 de la entonces vigente LOPD.

5. Fue también la falta de información previa acerca de la finalidad del control la que sustentó la nulidad de la prueba en el caso origen de la STS de 13 de mayo de 2013 referida a la utilización de cámaras de video vigilancia para sancionar a una trabajadora por incumplimiento de sus obligaciones y deberes laborales[486] e insistiéndose en la necesidad de información previa como requisito inexcusable de la legitimidad del control, de modo que el trabajador ha de conocer no sólo que está siendo grabado, sino también que la grabación puede ser utilizada a efectos disciplinarios[487].

6. Por su parte, la STC 39/2016, de 3 de marzo, da una vuelta de tuerca a la cuestión de la información previa en lo que se ha entendido como una evolución de una postura garantista para con los derechos de los trabajadores

485 DE VICENTE PACHÉS, F., "Las facultades empresariales de vigilancia y control en las relaciones de trabajo", *Tribuna Social*, núm. 57, 2004, pág. 30.

486 En esta sentencia se trataba del uso no consentido ni informado de las grabaciones de imágenes para un fin desconocido por la trabajadora afectada y diferente del señalado por la empresa, cual fue la prevención de hurtos por parte de clientes y no para control de la actividad laboral.

487 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.66.

hacia una posición destinada a proteger el interés empresarial[488]. En esta sentencia se aborda el caso de la instalación, por parte de la empresa *Bershka*, de un dispositivo de grabación en la zona de la caja registradora del establecimiento sin comunicárselo a los trabajadores al haberse advertido desde hacía algún tiempo importantes descuadres en la contabilidad, si bien sí había instalado en el escaparate del establecimiento un distintivo informativo en lugar visible, entendiendo el Tribunal Constitucional en esta ocasión que el distintivo informativo colocado en el escaparate era suficiente para entender que los trabajadores tenían un conocimiento preciso de las técnicas de vigilancia, sin necesidad de informar expresamente a aquéllos acerca de la finalidad exacta de ésta, desmarcándose claramente de la postura mantenida en la STC 29/2013, de 11 de febrero.

Esta interpretación - que resulta más que cuestionable a la luz del art. 5 de la derogada LOPD y del vigente art. 89.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, que exige información a los trabajadores de forma explícita, previa, clara y concisa - siguió la línea argumental de la STEDH de 12 de enero de 2016 (Barbulescu I), que entendió que no se había producido vulneración alguna del derecho a la intimidad del trabajador como consecuencia de la fiscalización por parte de la empresa del servicio de mensajería *(Yahoo Messenger)* instalado con fines laborales y cuyo uso para propósitos ajenos a los mismos había sido prohibido.

7. Una vez estimado que se ha cumplido el deber de información, el TC entiende, asimismo, que la medida consistente en la instalación de cámaras de seguridad para controlar la zona de caja superaba el test de proporcionalidad dado que (i) se trataba de una medida justificada por existir razonables sospechas de hurto de dinero por parte de alguno de los trabajadores que prestaban servicios en la caja; (ii) idónea para la finalidad pretendida por la

488 FERRANDO GARCÍA, F. M., "Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías", *RTSS. CEF*, núm. 399, 2016, pág. 45.

empresa, ya que su objetivo era comprobar si alguno de los trabajadores hurtaba dinero para, en tal caso, proceder a la adopción de las pertinentes medidas disciplinarias; (iii) necesaria, dado que la grabación constituía la prueba de dichas irregularidades y, finalmente, (iv) equilibrada, toda vez que la grabación de imágenes se limitó exclusivamente a la zona de la caja, por lo que se descartó cualquier lesión del derecho a la intimidad personal.

8. No obstante, la posterior STEDH de 5 de septiembre de 2017 (Barbulescu II) sí estableció la necesidad de información previa al trabajador acerca de la vigilancia de su correspondencia electrónica y otro tipo de comunicaciones, así como de la concreta puesta en marcha de las medidas al respecto, lo que implica la necesidad de que dicha información haya de ser previa a la efectiva implantación de las medidas de vigilancia y habrá de ser, por lo demás, expresa, precisa y concreta, debiendo los jueces nacionales examinar si el trabajador ha sido informado previamente de la posibilidad de que el empresario aplique medidas de control de las comunicaciones[489].

Por ello, entendemos que es positiva la exigencia del deber de información previo, expreso, claro y conciso del art. 89.1 LOPDGDD, que parece neutralizar la involutiva STC 39/2016, de 3 de marzo. De hecho, la sentencia del TSJ de Andalucía (Sevilla) de 28 de marzo de 2019 refuerza la obligación empresarial de cumplir con el deber de informar de forma clara, precisa y concreta a sus trabajadores del uso que puede hacer de los dispositivos tecnológicos puestos a su disposición para la realización de sus actividades productivas.

La sentencia de la Sala de lo Social del TSJ de Andalucía (Sevilla) acoge la doctrina de algunas sentencias del Tribunal Constitucional (núm. 170/2013, de 7 de octubre), del Tribunal Supremo (26 de septiembre de 2007 y

489 *"The notification should normally be clear about the nature of the monitoring and be given in advance"*, dice literalmente la STEDH de 5 de septiembre de 2017 (Barbulescu II).

6 de octubre de 2011) y del TEDH (5 de septiembre de 2017, caso Barbulescu II), y acude también a la nueva regulación legal sobre el uso de los dispositivos informáticos puestos por la empresa a disposición del trabajador (art. 87 Ley Orgánica 3/2018, de 5 de diciembre), si bien con la manifestación de que la norma no es aplicable en razón de las fechas en que ocurrieron los hechos objetos del litigio.

La Sala efectúa una buena síntesis, a mi parecer, de cuál es la doctrina que puede extraerse del conjunto de las sentencias referenciadas, que se plasma en estas tres premisas: i) el trabajador goza de una expectativa razonable de confidencialidad según la cual puede realizar un uso moderado con fines privados de los dispositivos digitales facilitados por la empresa como herramientas de trabajo; ii) esta expectativa razonable de confidencialidad puede neutralizarse por el empresario mediante la prohibición expresa del uso para fines privados de los dispositivos digitales facilitados por la empresa; iii) los trabajadores deben ser debidamente informados de la prohibición, entendiéndose cumplida esta obligación si la prohibición se contempla en el convenio colectivo, en el contrato de trabajo o en la normativa sobre las técnicas de información y comunicación de la empresa[490].

No obstante, la norma contenida en el art. 89.1 LOPDGDD tampoco desconoce la posición de defensa del interés del empleador, pues incluye una medida de flexibilización del deber de información previa para los supuestos de captación de imágenes que revelen "la comisión flagrante de un acto ilícito", en cuyo caso se entiende cumplido el deber con la colocación del dispositivo en lugar visible al que se refiere el artículo 22.4 de la LOPDGDD[491].

490 http://www.eduardorojotorrecilla.es

491 MIÑARRO YANINI, M., "La Carta de derechos digitales de los trabajadores…", *op. cit.*, *Revista de Trabajo y Seguridad Social, CEF*, 430 (enero 2019), pág. 9.

Sin embargo, entendemos que existen bastantes dificultades para conciliar este debilitado deber de información con el más exigente derivado de la doctrina López Ribalda, en el que, aunque las grabaciones captaron apropiaciones indebidas de productos, no se eximió a la empresa del deber de información previa, expresa y precisa.

De hecho, la Sentencia 52/2019 de fecha 18 de febrero de 2019 del Juzgado de lo Social nº 3 de Pamplona, que versa sobre la validez de la video vigilancia para acreditar un despido disciplinario, concluye que la prueba obtenida de la grabación es nula porque la empresa se había limitado a poner un cartel avisando de la presencia de cámaras, pero no había informado a los trabajadores de su instalación ni de la concreta finalidad del sistema instalado[492].

El magistrado declara que la validez de la prueba exige que la empresa cumpla el deber de informar previamente a los trabajadores de la instalación de las cámaras de vigilancia y de la concreta finalidad del sistema instalado, lo cual incluye informar acerca de si las imágenes pueden ser utilizadas por el empresario con una finalidad sancionadora si las mismas captaren incumplimientos laborales de los trabajadores, no siendo posibles y quedando absolutamente prohibidas, señala la sentencia, las grabaciones encubiertas u ocultas, de modo que las sospechas de irregularidades en el desempeño de la prestación laboral no constituyen legitimación alguna para excepcionar del

492 El magistrado plantea si, en un caso de despido disciplinario en el que unas cámaras de vigilancia de la empresa capturan la imagen de dos trabajadores que se agreden mutuamente, la prueba mediante la grabación de la conducta por las cámaras de seguridad era válida conforme a la nueva ley o si vulneró el derecho del trabajador a la protección de datos personales que reconoce el art. 18.4 CE, el art. 8 del CEDH y el artículo 8 de la Carta Europea de Derechos Fundamentales. La sentencia recoge los hitos en la evolución de la jurisprudencia sobre el control empresarial mediante la video vigilancia y la incidencia del Reglamento Europeo de Protección de datos, así como de una Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018, que consideró vulnerado el derecho a la protección de datos personales porque la empresa no informó a los trabajadores sobre la finalidad del sistema de video vigilancia que implantó y cuyas imágenes sirvieron para despedir a varias trabajadoras de un supermercado por incumplimientos laborales.

deber de informar de la grabación, así como tampoco exonera del cumplimiento de las exigencias del Reglamento General de Protección de Datos.

El magistrado considera que el deber informativo sobre el alcance de las medidas de video vigilancia, incluyendo la finalidad sancionadora, es una exigencia que se impone en todo caso, más allá de la mera colocación del cartel informativo, conforme a la jurisprudencia del TEDH y al propio Reglamento General de Protección de Datos. En consecuencia, el juez concluye que la prueba obtenida es nula de pleno derecho por vulnerar un derecho fundamental y no debe ser admitida a trámite.

La interpretación del Juzgado de lo Social nº 3 de Pamplona choca frontalmente, sin embargo, con la que ha dado el Tribunal Superior de Justicia del País Vasco en sentencia de 11 de diciembre de 2018, en la que la Sala de los Social de este Tribunal confirma la suspensión de empleo y sueldo de un conductor de autobús que, merced a una cámara instalada en el vehículo, fue descubierto conduciendo de forma temeraria. En este caso, la empresa advertía de la presencia del dispositivo de grabación, pero no de la concreta finalidad de control laboral para el que podían emplearse las imágenes.

La sentencia subraya que en este caso no se vieron lesionados los derechos a la intimidad y la protección de datos del trabajador dado que en el vídeo no aparece él, sino sólo imágenes de la calle que permiten acreditar su modo de conducir[493]. No obstante (y aquí está el *quid* de la cuestión), los magistrados amplían su razonamiento y expresan que *"aunque la grabación recogiese la imagen del trabajador, tampoco nos encontraríamos ante un uso de datos personales contrario a los derechos fundamentales del recurrente, atendiendo a las circunstancias concurrentes"*. Y ello porque *"ha quedado acreditado que la empresa informó al trabajador de la videovigilancia mediante una pegatina en el vehículo y que ha empleado la grabación para comprobar*

493 *"La grabación se limitó a las circunstancias del tráfico"*, explica el texto, por lo que no hay vulneración de derechos.

datos relativos al desenvolvimiento de la prestación de servicios". Por ello, concluye la resolución, *"no es preciso el consentimiento expreso del trabajador para esta grabación (...), sino simplemente estar informado de ello"*, y tampoco es preciso *"que se informase al trabajador de la finalidad exacta de la videovigilancia"*.

La línea que sigue el TSJ del País Vasco es acorde con la doctrina manifestada por el Tribunal Constitucional y el Tribunal Supremo antes de la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y de la plena vigencia del Reglamento Europeo de Protección de Datos de 27 de abril de 2016. El Alto Tribunal estableció que, ante actos delictivos, bastaba con que la plantilla conociera la instalación de las cámaras.

La sentencia del TSJ del País Vasco cuenta, en todo caso, con un voto particular que afirma que *"el contrato de trabajo determina un ámbito de la persona que, como tal, no está ajeno a la totalidad de los derechos fundamentales que se desarrollan en el ámbito ciudadano"*. El magistrado discrepante considera que el empleado debía conocer la finalidad de la video vigilancia y *"si no conoce este fin del sistema (para el control en su trabajo), ni consiente, ni asiente, no le puede perjudicar. Si no se le ha informado de ello, el elemento de reproducción no es aceptable como instrumento para controlar la relación laboral"*. Eso sí, añade un último inciso que puede sembrar alguna duda (que no se advierte en la sentencia del juzgado de Pamplona): *"salvo que se muestre absolutamente imprescindible para ejercer las funciones de control laboral"*.

El debate, pues, está servido y, dada la gran cantidad de matices que presenta la nueva normativa y la casuística laboral, todo indica que será el Tribunal Constitucional quien, en último término, tenga que zanjar cómo

interpretar el derecho fundamental a la protección de datos con relación al uso de video vigilancia en el entorno del trabajo.

De cualquier modo, es oportuno apuntar que la jurisprudencia del TEDH no ha descartado de forma absoluta la validez de la prueba de video vigilancia, incluso en ausencia de cualquier información previa, siempre que concurran circunstancias especiales -sospecha fundada de incumplimiento, grabación selectiva del trabajador afectado, breve periodo de tiempo-. En ello incide en su Sentencia López Ribalda, con remisión a su Sentencia de 5 de octubre de 2010 (asunto Köpke).

9. En este debate ha sido recurrente la cuestión de si el trabajador ha de saber o no que está siendo controlado y a través de qué medios. De la STC 186/2000, de 10 de julio, parece desprenderse una respuesta negativa. En dicha sentencia se analizaba, como se ha dicho, un supuesto de hecho en el que un trabajador, cajero en un economato, fue despedido bajo la imputación de apropiación indebida tras constatar la empleadora la existencia de determinados descuadres en determinadas secciones, por lo que contrató a una empresa de seguridad la instalación de cámaras de video vigilancia, descartando el TC en su pronunciamiento que hubiera existido una vulneración del derecho a la intimidad de los trabajadores al considerar que la medida estaba justificada, resultaba idónea para la finalidad perseguida y era necesaria y equilibrada. Y en relación a la falta de información al afectado y a sus representantes se señala que el conocimiento de la existencia del sistema de filmación frustraría la finalidad apetecida, sin que se infrinja la previsión del art. 64.5.f) ET, que es además una cuestión de mera legalidad ordinaria.

La evolución que el deber de información ha tenido en la doctrina jurisprudencial del TS y del TC se puede resumir del modo que sigue:

1.- Jurisprudencia del Tribunal Supremo.

En la doctrina jurisprudencial del Tribunal Supremo relativa al deber de información nos encontramos con tres momentos fundamentales, coincidentes con la evolución doctrinal del Tribunal Constitucional vista con anterioridad, que se pueden sintetizar del modo que sigue:

1.1.- Video vigilancia con fines distintos a los estrictamente laborales (STS de 13 de mayo de 2014).

1. Esta sentencia enjuicia el caso de una trabajadora que trabaja como cajera de un supermercado *(Supermercados Champion, S.A.)* y que es sorprendida por las cámaras de seguridad de la empresa - colocadas con el fin de evitar hurtos por parte de los clientes - evitando el escaneo de diversos productos en beneficio de una persona que estaba realizando una compra. La existencia de las cámaras era apreciable a simple vista por los trabajadores.

La cajera fue despedida por incumplimiento de sus deberes laborales, formulando la misma demanda alegando despido nulo dado que la empresa no le informó que las cámaras de seguridad, ubicadas en su zona de trabajo, tenían también la finalidad de controlar sus actividades laborales y que, por tanto, la empresa ha vulnerado su derecho a la intimidad.

2. El Tribunal Supremo, sosteniendo sus argumentos en la STC 29/2013, de 11 de febrero, resuelve señalando que lo que se ha vulnerado es el derecho a la protección de datos de la trabajadora, toda vez que la empresa ha utilizado para sancionarla el sistema de cámaras de video vigilancia colocado con fines de seguridad y no para controlar las actividades laborales de sus empleados. En consecuencia, sostiene el Tribunal Supremo, se trata del uso de un sistema de control no consentido, que tenía un objeto adicional al de seguridad como

era la supervisión del cumplimiento de los deberes de los trabajadores por parte de la empresa, el cual no había sido comunicado o informado adecuadamente ni a los trabajadores ni a sus representantes.

En definitiva, esta sentencia casacional está aplicando las garantías correspondientes a la libertad informática (art. 18.4 CE) y no las del derecho a la intimidad (art. 18.1 CE), aunque en su contenido parecen mezclarse ambos derechos. Y es ésa una cuestión transcendente, en tanto que la previa comunicación del tratamiento de datos por parte de los empresarios es una característica propia del derecho a la libertad informática.

3. Señalar que la sentencia cuenta con un voto particular del Magistrado José Manuel López García de la Serrana, cuya discrepancia del criterio mayoritario de la Sala deriva de entender que se ha violado por la mayoría la doctrina del TC acerca de la video vigilancia como prueba ilícita por violación del derecho a la intimidad y del derecho a la protección de datos en el sentido de que la sentencia es contraria a lo resuelto en la materia tanto por el TC como por el TEDH.

1.2.- Cambio de doctrina. Video vigilancia en zonas restringidas al público (STS de 7 de julio de 2016).

1. Los hechos enjuiciados en esta sentencia cabe resumirlos del modo que sigue: con fecha 19 de febrero de 2014 el Juzgado de lo Social nº 1 de Badajoz dictó sentencia desestimatoria de la petición formulada por la actora, Regina, contra Distribuidora Internacional de Alimentación, S.A. *(DIA, S.A.)* sobre despido, declarando la procedencia del mismo.

En dicha sentencia se declara probado que, tras haberse constatado en dicho centro un alto nivel de pérdidas desconocidas (más de 32.000 euros en el

año 2012), la empresa había instalado varias cámaras de video vigilancia en las zonas de trabajo. Y, entre ellas, en la denominada "reserva" dedicada a almacén. Como consecuencia de dicha instalación se comprueba que el 13 de marzo de 2013 la actora accedió a dicha zona portando un carro lleno de cartones para introducirlos en la máquina compactadora, extrayendo al mismo tiempo un paquete de lomo loncheado que comenzó a consumir inmediatamente, dejando el paquete encima de la mesa de las devoluciones, procediendo a consumirlo del todo un tiempo después. Con posterioridad volvió a realizar la misma operación consumiendo otro paquete del mismo producto, cuyo envase, una vez vacío, al igual que el anterior, tiró a la compactadora.

Es de destacar que todo el personal de la tienda tenía pleno conocimiento de la instalación de las cámaras situadas en distintas zonas pero no en los aseos, vestuarios y oficina, existiendo, además, distintos carteles advirtiendo de los sistemas de video vigilancia.

La citada sentencia fue recurrida en suplicación por la actora ante la Sala de lo Social del TSJ de Extremadura, el cual dicta sentencia estimatoria de la petición de la actora y declarando nulo el despido de la misma.

La representación legal de *DIA S.A.* interpuso recurso de casación para unificación de doctrina ante la Sala de lo Social del TS, la cual estima el recurso dando validez a la prueba video gráfica presentada por la empresa con la argumentación de que la trabajadora tenía pleno conocimiento de la existencia de cámaras de video vigilancia en una zona restringida al público, llamada de "reserva" (zona de almacén) dado que existían carteles anunciadores, no siendo dicha zona un área de privacidad como pueden ser los vestuarios y aseos, a lo que hay que unir el hecho de que la instalación de cámaras de video vigilancia obedecía a una finalidad protectora del patrimonio empresarial toda vez que se habían detectado pérdidas en los últimos tiempos.

2. En definitiva, el TS analiza el caso desde la óptica del derecho a la intimidad del art. 18.1 CE, desentendiéndose por completo del derecho a la protección de datos personales del art. 18.4 CE, entendiendo por un lado que, pese a no existir una comunicación expresa a los trabajadores sobre la instalación de cámaras de video vigilancia y del motivo de las mismas, su existencia era conocida por la trabajadora por ser de común conocimiento por parte de los mismos dado que estaban instaladas en lugares visibles y existían carteles indicadores al respecto. Y, por otro lado, que la presencia de cámaras en la generalidad del centro de trabajo sugiere una finalidad de protección del patrimonio empresarial.

3. Asimismo, sostiene que las cámaras estaban instaladas también en zonas restringidas al público a la que sólo podían acceder los empleados del establecimiento y, por último, entiende que la proporcionalidad en el caso enjuiciado conduce a la apreciación de un uso apropiado de la video vigilancia, estando el objetivo perseguido por ésta ajustado a las exigencias razonables de respeto a la intimidad de la persona.

1.3.- Sistema de video vigilancia. Alcance del deber informativo previo (STS de 31 de enero de 2017).

1. La STS de 31 de enero de 2017 trae su causa originaria de una sentencia del Juzgado de lo Social nº 15 de Barcelona, de fecha 5 de diciembre de 2014, que enjuicia el caso de un despido por transgresión de la buena fe contractual, fraude, deslealtad y abuso de confianza por manipulación de tickets y hurto de diferentes cantidades de dinero en diferentes fechas, debiéndose señalar que el centro de trabajo disponía de un sistema de video vigilancia por razones de seguridad, siendo la actora conocedora de la existencia del mismo y sin que hubiese sido informada del destino que pudieran darse a las imágenes ni que pudieran ser utilizadas en su contra, siendo el objeto del procedimiento la validez de las pruebas videográficas empleadas por

el empleador para probar la causa justificadora del despido de la trabajadora, declarando el Juzgado de lo Social la improcedencia del mismo.

Tras recurrirse en suplicación la sentencia por parte de la empresa ante el TSJ de Cataluña, éste dicta sentencia desestimatoria del recurso en fecha 22.05.2015.

2. Recurrida, por parte de la empresa, la sentencia del TSJ de Cataluña en casación para unificación de doctrina, el TS entra a conocer del caso haciendo recordatorio expreso de la doctrina sentada en la STC 39/2016, de 3 de marzo, en la que el Alto Tribunal estimaba que no se había violado el derecho a la protección de datos porque, dada la existencia de una relación laboral entre las partes, no resultaba necesario el consentimiento de los trabajadores en orden a la adopción de medidas de control de la prestación laboral y que el deber de información previo acerca del dispositivo instalado había quedado salvado con la colocación del correspondiente distintivo informando de su existencia, razón por la que acababa concluyendo que el proceder de la empresa había superado el pertinente juicio de proporcionalidad.

Esa decisión la fundamentaba con el argumento de que, si bien el consentimiento del afectado es el elemento definidor del sistema de protección de datos de carácter personal, la derogada LOPD excepcionaba el mismo si existía una habilitación legal expresa al efecto para que los datos pudieran ser tratados sin dicho consentimiento. Y en este sentido, el art. 6 de la derogada LOPD, en su apartado 2, enumeraba una serie de supuestos en los que resultaba posible tratar y ceder datos sin recabar el consentimiento del afectado, señalando al efecto que no era preciso el consentimiento cuando los datos de carácter personal se referían a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y fuesen necesarios para su mantenimiento o cumplimiento.

3. En el ámbito laboral, pues, el consentimiento del trabajador se sitúa en un segundo plano por entenderse el mismo implícito en la relación contractual, siempre que el tratamiento de datos personales fuere necesario para el cumplimiento del contrato firmado por las partes[494]. Por el contrario, el consentimiento de los trabajadores afectados sí resultará necesario cuando el tratamiento de datos se utilizare con una finalidad ajena al cumplimiento del contrato.

4. No obstante, pese a no ser necesario el consentimiento en los casos señalados, el deber de información sí continúa vigente dado que el mismo permite al afectado el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como conocer la dirección del responsable del tratamiento o, en su caso, del representante (art. 5 derogada LOPD).

Pues bien, el TS aplicando la doctrina señalada al tratamiento de los datos obtenidos por la instalación de cámaras de video vigilancia en el centro de trabajo concluye que el empleador no necesita del consentimiento expreso del trabajador para tratar las imágenes obtenidas con la finalidad de seguridad o control laboral por tratarse de una medida dirigida a controlar el cumplimiento de la prestación laboral, siendo conforme la misma con el art. 20.3 ET.

5. En suma, la exigencia de finalidad legítima en el tratamiento de datos prevista en el art. 4.1 de la derogada LOPD viene dada, en el ámbito laboral, por las facultades de control empresarial que reconoce el art. 20.3 ET, siempre que las mismas no lesionen derechos fundamentales de los trabajadores.

Y, en este sentido, la empresa había colocado el pertinente distintivo en el escaparate de la tienda donde prestaba sus servicios la trabajadora, de

494 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.64.

modo que ésta podía conocer la existencia de las cámaras y la finalidad para la que habían sido instaladas, habiéndose cumplido con la obligación de información previa dado que basta, a tales efectos, con el cumplimiento de los requisitos específicos de información a través del distintivo, de conformidad con lo señalado en la Instrucción 1/2006 AEPD.

El trabajador conocía, pues, que la empresa había instalado un sistema de control por video vigilancia, sin que haya necesidad alguna de especificar la finalidad exacta del mismo, sino que lo determinante es que los datos obtenidos se hubieren usado para la finalidad de control de la prestación laboral, porque sólo en el caso de que el objetivo del tratamiento de datos no guardare relación directa con el mantenimiento, desarrollo o control de la relación laboral el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados.

Es por ello que el TS estima el recurso de casación por entender que la instalación de las cámaras de seguridad fue una medida justificada por razones de seguridad (control de hechos ilícitos imputables a empleados, clientes y terceros y por motivos de seguridad); idónea para la consecución de ese fin; y necesaria y proporcionada al fin perseguido, razón por la que estaba justificada la limitación de los derechos fundamentales en juego, máxime cuando los trabajadores estaban informados expresamente de la instalación del sistema de vigilancia por razones de seguridad, expresión ésta que incluye la vigilancia de actos ilícitos de los empleados y de terceros y, en definitiva, de la seguridad del centro de trabajo, pero que excluye otro tipo de control laboral que sea ajeno a la seguridad, como puede ser el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc.

2.- Jurisprudencia del Tribunal Constitucional.

La doctrina jurisprudencial del Tribunal Constitucional en orden al deber de información viene marcada por dos hitos principales, a saber:

2.1.- El deber de información previo (STC 29/2013, de 11 de febrero).

1. El TC resuelve el conflicto entre el derecho a la intimidad personal (art. 18.1 CE) y las facultades de control empresarial de la actividad laboral con la aplicación estricta del principio de proporcionalidad. Pero la doctrina va a ser corregida en la STC 29/2013, de 11 de febrero, que añade una serie de condicionantes necesarios para la validez de la utilización de las cámaras de vigilancia en los centros de trabajo, exigiendo con rigor el cumplimiento del deber de información previo a los trabajadores para admitir las grabaciones como prueba del comportamiento de éstos.

Hay que tener en cuenta, como hemos advertido con anterioridad, que el TC hasta entonces había establecido los principios en esta materia sobre la base de la colisión de las facultades de control con el derecho a la intimidad de los trabajadores, sin ninguna referencia al derecho de autodeterminación informativa que consagra art. 18.4 CE. En cambio, la STC 29/2013, de 11 de febrero sí que atiende específicamente a las exigencias derivadas del respeto al contenido esencial del derecho en materia de protección de los datos de carácter personal.

2. El caso que accede al amparo en esta ocasión no es un despido disciplinario, sino la imposición de tres sanciones de suspensión de empleo y sueldo por infracciones muy graves a un Director de Servicio de la Universidad de Sevilla por incumplir el horario y la jornada de trabajo. Ante la sospechas de la empleadora procedió a reproducir las grabaciones efectuadas por las

cámaras de seguridad[495] en donde se veía como el trabajador firmaba a unas determinadas horas, aunque entraba al establecimiento a otras horas[496]. Consta también en el relato de los hechos que el convenio colectivo aplicable preveía la posibilidad de que el empresario efectuase control sobre los medios informáticos y audiovisuales. El comité de empresa había sido informado sobre la adopción de estas medidas y existían incluso carteles informativos en donde se avisaba de la existencia de cámaras. Sin embargo, los trabajadores no habían sido informados previa y expresamente de la finalidad para la que podían ser recabados esos datos personales derivados de las grabaciones.

3. La STC 29/2013, de 11 de febrero, estima el recurso de amparo al apreciar que se ha violado el núcleo esencial del derecho fundamental del art. 18.4 de la CE por incumplimiento del deber de informar a los trabajadores de la existencia de las cámaras de seguridad y la finalidad a la que podía destinarse los datos personales[497]. Es necesario destacar que en la determinación del contenido esencial del derecho de autodeterminación informativa sigue aquí la doctrina de la STC 292/2000, de 30 de noviembre[498], que resuelve el recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la derogada Ley

495 Quedó acreditado que la Universidad de Sevilla tenía concedida autorización administrativa de la AEPD para el control de acceso de las personas de la comunidad universitaria y del personal de empresas externas a sus campus y centros. En virtud de dicha autorización tenía instaladas varias cámaras de vídeo-grabación en los accesos al recinto del centro con la debida señalización y advertencia públicas.

496 Se declaró probado en la Sentencia del Juzgado de lo Social que en la mayoría de los días laborables existía una demora en la hora de entrada al trabajo de entre treinta minutos y varias horas.

497 Declara la nulidad de las sanciones porque habiéndose acordado con base en una lesión del art. 18.4 CE no podrían dejar de calificarse como nulas de acuerdo con la calificación nacida de las SSTC 88/1985, de 19 de julio; o 134/1994, de 9 de mayo.

498 La STC 292/2000, de 30 de noviembre, diferencia el contenido del derecho a la intimidad personal y del derecho de protección de los datos de carácter personal. Subraya que la función del derecho a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en dicho ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de intromisiones de terceros en contra de su voluntad. En cambio, el derecho a la protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, añadiendo que *"ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin"*.

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

4. La doctrina que establece la STC 29/2013, de 11 de febrero, cabe resumirla del siguiente modo:

i) La habilitación legal para recabar los datos personales sin necesidad de consentimiento en el ámbito de las relaciones laborales no exime del derecho de información del trabajador, dado que es complemento del derecho fundamental del art. 18.4 CE la facultad de conocer quién dispone de esos datos y para qué. Una cosa es la necesidad o no de autorización del afectado y otra, distinta, el deber de informarle sobre su poseedor y el propósito del tratamiento[499].

ii) El derecho de información solo puede venir limitado por Ley y en el ámbito de las relaciones laborales no existe habilitación legal expresa que permita su omisión ni tampoco puede justificarse la misma en el control de la actividad laboral[500].

499 Previamente destaca la STC 29/2013 que el deber informativo es exigible también cuando el control empresarial incide en el derecho a la intimidad personal (art. 18.1 CE), y no sólo cuando está en juego el derecho a la protección de datos de carácter personal (art. 18.4 CE). Argumenta que, no obstante la doctrina de la STC 186/2000, el art. 18.1 CE impone como regla de principio y, de forma añadida al resto de sus garantías, un deber de información que protege frente a intromisiones ilegítimas en la intimidad.

500 Para la STC 29/2013, de 11 de febrero, tampoco podría situarse el fundamento en la exención del deber informativo al trabajador en el interés empresarial de controlar la actividad laboral a través de sistemas no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. Considera la Sentencia glosada que *"esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial. En efecto, se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que lesiona el art. 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible"*.

iii) El derecho de información no puede ser obviado por la mera existencia de anuncios acerca de la instalación de cámaras o porque se hubiera notificado la creación del fichero a la AEPD.

iv) Supone una lesión del art. 18.4 CE la utilización, para verificar el cumplimiento de las obligaciones laborales, de medios encubiertos que nieguen al empleado la información exigible.

v) Respecto del alcance del deber de información, señala que éste ha de ser previo, expreso, preciso, claro e inequívoco acerca de la finalidad del control de la actividad laboral, debiendo concretar la información tanto las características como el alcance del tratamiento de los datos que se vaya a realizar. Es decir, en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósito y explicitando de modo particular que las mismas pueden ser utilizadas para imponer sanciones disciplinarias por incumplimientos laborales[501].

5. La diferencia entre los pronunciamientos contenido en las SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio y el expresado en la STC 29/2013, de 11 de febrero reside en que en las dos primeras sentencias el Tribunal analiza el deber de preavisar desde la perspectiva del art. 18.1 CE, mientras que esta última lo hace aplicando el art. 18.4 CE, a lo que cabe añadir que la STC 186/2000, de 10 de julio, lo que analiza es un supuesto de instalación de sistemas de grabación con el único fin de perseguir un posible ilícito de autor indeterminado, en tanto que la STC 29/2013, de 11 de febrero, se refiere al uso laboral de un sistema de grabación de carácter general, ajeno a la prestación laboral en cuanto tal[502].

501 LÓPEZ DE LA FUENTE, G., "La doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos…, *op. cit.*, pág. 12.

502 FALGUERA BARÓ, M. A.: "Nuevas tecnologías y trabajo (II): perspectiva constitucional", *Trabajo y Derecho*, núm. 21, septiembre 2016, pág. 36.

6. En definitiva, el Tribunal Constitucional tras estimar que las imágenes grabadas en un soporte físico constituyen datos de carácter personal protegidos por el derecho de protección de datos, sostuvo que la solución del recurso se encontraba en la STC 292/2000, de 30 de noviembre, pronunciamiento referido específicamente al artículo 18.4 CE y, en base a ella, se reafirmó que el derecho de información es parte del núcleo esencial del derecho de autodeterminación informativa dado que es complemento dispensable del mismo la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo[503].

En base al art. 18.4 CE el afectado tiene derecho a ser informado sobre los referidos extremos, incluso en los casos en los que la recogida de datos no requiera consentimiento del titular, pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, distinta, el deber de informarle sobre su poseedor y el propósito del tratamiento[504]. No obstante, el propio TC reconoció que la exigencia informativa no es absoluta, dado que caben limitaciones al derecho de información previa por razones constitucionalmente admisibles y legalmente previstas, las cuales deberán ser necesarias y proporcionadas.

7. En aplicación de dicha doctrina, se concluyó que al no existir habilitación legal expresa para omitir el derecho a la información previa en el ámbito de las relaciones laborales, no cabe que éste sea desconocido. De donde deriva la proscripción de cámaras ocultas así como la utilización de grabaciones para finalidades distintas mientras no exista norma legal que las ampare, no siendo suficiente que el tratamiento de datos esté amparado en la Ley o que pueda resultar en el caso concreto proporcionado. Siguiendo esta doctrina, el derecho de información previa prohibiría emplear la video vigilancia de forma subrepticia aunque pueda estar justificada para detectar

503 STC 292/2000, de 30 de noviembre.

504 STC 29/2013, de 11 de febrero.

incumplimientos contractuales graves, irregularidades en el trabajo o, incluso, actividades fraudulentas o delictivas[505].

En este marco, en el caso concreto, hubiera sido necesario que los trabajadores hubiesen sido informados de manera previa, expresa, clara e inequívocamente sobre la posibilidad de utilizar las grabaciones provenientes de cámaras instaladas en vestíbulos y zonas públicas con finalidad de control de la actividad laboral, debiendo la información concretar las características y el alcance del tratamiento de datos que iba a realizarse[506], no bastando con que existieran distintivos sobre la instalación de cámaras en el centro de trabajo ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos.

8. Resulta importante poner de manifiesto que tras la STC 29/2013, de 11 de febrero, un importante sector de la doctrina entendió que recurriendo al artículo 18.4 CE se habría dejado sin efecto la doctrina de la STC 186/2000, de 10 de julio[507], sosteniéndose que, respecto a la constitucionalidad de las grabaciones ocultas, se habría llegado a una solución por la vía del artículo 18.1 CE y a otra distinta por la del número 4 de dicho artículo, en donde se habría prescindido de la ponderación, bastando comprobar el incumplimiento del deber de información previa para determinar la lesión al derecho de autodeterminación informativa. Además, que mientras el derecho de información se erige como una cuestión de legalidad ordinaria en el caso del derecho a la intimidad, constituye el contenido esencial del derecho a la autodeterminación informativa.

505 GALLARDO MOYA, R.: "El derecho fundamental a la protección de datos y la videovigilancia empresarial", *Revista de Derecho Social*, nº 62, 2013, pags. 169-170.

506 STC 29/2013, de 11 de febrero.

507 DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: "Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia", *Revista General del Derecho del Trabajo y de la Seguridad Social*, nº 39, págs. 7-10.

9. Al respecto, la STC 29/2013, de 11 de febrero, técnicamente no contradice ni deja sin efecto la doctrina constitucional emanada de la STC 186/2000, de 10 de julio. Si bien en ambos casos se encuentran en juego los derechos a la intimidad y a la autodeterminación informativa, la naturaleza de la medida de control es sustancialmente distinta y precisamente en este extremo radicaría el quid de la cuestión, a saber: en el primero se está frente a la utilización de la video vigilancia como medida de control extraordinaria, que busca verificar la comisión por el trabajador de un atentado contra los bienes del empresario; mientras que en el segundo se está frente a una medida de control ordinaria en la que el objetivo es obtener información sobre el comportamiento laboral del trabajador.

En un caso no se le habría informado al trabajador sobre la propia existencia de las cámaras, en atención a que la medida específica de control buscaba comprobar la sustracción de bienes, que incluso configuraría un delito, en tanto que en el otro, al tratarse del control ordinario de la prestación laboral, el trabajador tendría derecho a saber que se le controlaría a través de cámaras y que las que estaban ubicadas en los vestíbulos tendrían dicha finalidad[508].

10. Sobre el derecho de información, señaló la STC 29/2013, de 11 de febrero, que de una recta lectura de la Sentencia 186/2000, de 10 de julio, deriva que la legalidad ordinaria no se predica del derecho de información como garantía nuclear del art. 18.1 CE, sino de sus garantías complementarias, esto es de los derechos de información del comité de empresa[509].

Así, el referido derecho también tendría trascendencia constitucional respecto a la intimidad personal, sucediendo que, en el caso concreto, tras la

508 GUERRA RODRÍGUEZ, L.: "Ejercicio del poder de control a través de cámaras de videovigilancia…", *op. cit.*, *Trabajo y Derecho* 29/2017 (mayo), nº 29 de 1 de mayo de 2017, pag. 4.

509 El art. 64.1 ET establece que *"el comité de empresa tendrá derecho a ser informado y consultado por el empresario sobre aquellas cuestiones que puedan afectar a los trabajadores (…)"*.

aplicación del principio de proporcionalidad, se encontró justificada su limitación. Cabe aquí señalar que la polémica radica en que respecto del derecho a la intimidad se entendería que el derecho de información puede ser modulado tras el correspondiente test de proporcionalidad, pero no respecto del derecho a la protección de datos, pues en este último caso se requeriría ley previa que así lo habilite. De este modo, la sentencia analizada no sitúa su razonamiento en términos de límites de los derechos fundamentales inespecíficos en la relación laboral, sino en el de determinación del ámbito protegido en cada uno de los derechos en cuestión[510].

2.2.- Debilitamiento del deber de información previa (STC 39/2016, de 3 de marzo).

1. En la STC 39/2016, de 3 de marzo, el Pleno del Alto Tribunal analizó por vez primera la instalación de cámaras de video vigilancia de manera integral, esto es desde la perspectiva de ambos derechos involucrados (derecho a la intimidad y derecho a la autodeterminación informativa). El supuesto de hecho analizado por la sentencia versa sobre una trabajadora que prestaba sus servicios como dependienta en un centro comercial de León por cuenta de la empresa *Bershka BSK España, S.A* y es despedida en 21 de junio de 2012 por transgresión de la buena fe contractual.

La empresa, a raíz de instalar un nuevo sistema de control informático de caja, detectó la existencia de múltiples irregularidades en la caja de la tienda en la que prestaba sus servicios la demandante, tras lo cual encargó a una empresa de seguridad la instalación de una cámara de video vigilancia que controlara la caja registradora, siendo instalada la misma sin que se

510 SEPÚLVEDA GÓMEZ, M.: "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contralímites", *Temas Laborales*, nº 122, 2013, pág. 204.

comunicase este hecho a los trabajadores, si bien se colocó un distintivo informativo en el escaparate del establecimiento en un lugar visible.

En la carta de despido se imputaba a la trabajadora la apropiación de efectivo de caja – 186,92 euros - en diferentes fechas mediante diversas operaciones falsas de devolución de venta de prendas tendentes a la ocultación de las mismas.

La trabajadora presentó demanda de despido contra la empleadora en solicitud de la nulidad del mismo por atentar contra su honor, intimidad y dignidad y, subsidiariamente, la declaración de improcedencia. Nótese que no se menciona el art. 18.4 CE. Alegaba que en el centro de trabajo no existían carteles anunciadores de la existencia de cámaras de video vigilancia, así como tampoco había comunicación a la AEPD ni autorización por la Sección de Seguridad Privada de la Comisaría de Policía, ni informe previo del comité de empresa acerca de la instalación de la video vigilancia.

2. En primera instancia la Sentencia del Juzgado de lo Social núm. 2 de León de 11 de marzo de 2013 desestima la demanda y declara procedente el despido.

Interpuesto recurso de suplicación se desestima el mismo por STSJ de Castilla y León de 24 de julio de 2013, por entender la Sala que la decisión de colocar la cámara de video vigilancia superó el juicio de proporcionalidad constitucionalmente exigido para dilucidar los límites de la injerencia del poder de control de la actividad laboral por parte del empresario cuando ese poder afectare a derechos fundamentales del trabajador.

Seguidamente, la trabajadora accede al amparo constitucional invocando como vulnerados los arts. 14, 15, 18.1, 18.4 y 24 CE, siendo el

recurso desestimado por el Alto Tribunal y modifica la doctrina de la STC 29/2013, de 11 de febrero, delimitando el alcance del deber informativo a los trabajadores, el cual considera cumplido cuando la empresa coloca los distintivos informativos en las condiciones que establece la Instrucción 1/2006, de 8 de noviembre, de la AEPD[511].

3. Se puede decir que la STC 39/2016, de 3 de marzo, establece la siguiente doctrina sobre la colisión entre las facultades de control empresarial a través de la video vigilancia y los derechos a la intimidad y a la protección de los datos de carácter personal:

i) El derecho a la protección de datos comprende el derecho del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos[512].

ii) Aunque el consentimiento del afectado es el elemento que define el sistema de protección de datos, la derogada LOPD excepcionaba los supuestos en los que concurría una habilitación legal para que los datos pudieran ser tratados

511 Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. En su art. 3 dispone que *"Los responsables que cuenten con sistemas de video vigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán: a) Colocar, en las zonas video vigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999"*. El contenido y el diseño del distintivo informativo se debe ajustar a lo previsto en el Anexo de la Instrucción, según el cual, el distintivo deberá incluir una referencia a la Ley Orgánica 15/1999, de protección de datos, una mención a la finalidad para la se tratan los datos ("Zona video vigilada") y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los arts. 15 y siguientes de la Ley Orgánica 15/1999.

512 Sigue en esto de forma expresa a lo declarado por la STC 292/2000, de 30 de noviembre.

sin dicho consentimiento, como sucede en el ámbito de las relaciones laborales[513].

iii) La dispensa del consentimiento abarca a los datos que fueren necesarios para el mantenimiento y cumplimiento de la relación laboral, incluyendo a las obligaciones derivadas del contrato de trabajo. Por el contrario, sí se requerirá el consentimiento de los trabajadores afectados cuando el tratamiento de datos se utilizare con finalidad ajena al cumplimiento del contrato.

iv) No obstante no ser necesario el consentimiento en los casos señalados, el deber de información sigue existiendo, ya que el mismo permite al afectado el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como conocer la dirección del responsable del tratamiento o, en su caso, del representante (art. 5 derogada LOPD).

v) El incumplimiento del deber de requerir el consentimiento del afectado para tratar los datos o del deber de información previo sólo supondrá una vulneración del derecho a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada.

513 El art. 6.1 de la derogada LOPD preveía que *"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"*. El propio art. 6 de la derogada LOPD, en su apartado 2, enumeraba una serie de supuestos en los que resulta posible el tratar y ceder datos sin recabar el consentimiento del afectado; en concreto, *"no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento ; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado"*.

vi) El empleador no necesita del consentimiento del trabajador para tratar las imágenes que hubieren sido obtenidas a través de cámaras instaladas en el centro de trabajo con una finalidad de seguridad o de control laboral habida cuenta de que se trata de una medida destinada a controlar el cumplimiento de la prestación laboral, resultando la misma conforme con el art. 20.3 ET.

vii) El deber informativo previo al trabajador se entiende cumplido con la colocación de los distintivos informativos previstos en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos.

viii) Cuando se cumple con la exigencia de la información previa de la instalación de las cámaras de video vigilancia a través del correspondiente distintivo informativo no podrá entenderse vulnerado el art. 18.4 CE, de modo que el control que ha de realizarse consistirá en determinar si la instalación y el empleo de medios de captación y grabación de imágenes por la compañía ha respetado el derecho a la intimidad personal, de conformidad con las exigencias del principio de proporcionalidad[514].

4. A la vista de esta doctrina resuelve el recurso el TC, entendiendo que se cumplió el deber informativo que pesaba sobre la empresa porque la empresa había colocado en el escaparate del establecimiento, en un lugar visible, el distintivo informativo exigido por la Instrucción 1/2006, de 8 de noviembre, de la AEPD, por lo que la trabajadora podía conocer la existencia de las cámaras, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control empresarial.

514 Cita aquí expresamente a las SSTC 186/2000, de 10 de julio y 98/2000, de 10 de abril.

5. Como señala Jesús Lahera[515], esta relajación de la información desmonta la, hasta ahora, consolidada separación jurisprudencial entre cámaras de seguridad y cámaras laborales, con exigencias y reglas jurídicas distintas, que parecen converger en esta mera asunción de un distintivo visible en la empresa sin mayores consideraciones. Esta consecuencia termina arrastrando la aplicación de la doctrina del "hallazgo casual", más propia de la seguridad en espacios públicos que del ámbito laboral, ante hechos cometidos por trabajadores.

En apariencia, el giro consiste en admitir una pegatina visible en la empresa como título informativo de la grabación; pero el cambio es mucho más sustancial porque quiebra las categorías jurídicas admitidas, hasta ahora, en la proyección de la LOPD en este control laboral de la empresa, como ponen de manifiesto los dos votos particulares a la sentencia de Fernando Valdés Dal-Ré y de Juan Antonio Xiol Ríos.

En el viraje que supone la STC 39/2016, de 3 de marzo, se observa la incidencia, con invocación expresa, de la STEDH de 12 de enero de 2016, Sección Cuarta, (caso Barbulescu I). El TC cuida en el discurso teórico de la sentencia, como hizo el TEDH, condicionar la legitimidad final al balance valorativo exigido por las concretas circunstancias del caso, pero en la práctica termina, también como el TEDH, sacrificando para el caso el sentido práctico del derecho, como evidencian los votos particulares, constituyendo un ejemplo de la difusa tendencia a ofrecer soluciones civiles indiferenciadas para problemas netamente laborales, de modo que bastaría con el anuncio genérico hecho al público sobre la existencia de cámaras de seguridad en el local para satisfacer el deber de información previa, suficiente y adecuada en atención a cada colectivo de interesados (art. 5 de la derogada LOPD), ignorando la STC 39/2016, de 3 de marzo, deliberadamente, en el ámbito laboral, ese deber de

515 LAHERA FORTEZA, J.: "Nueva jurisprudencia constitucional en la videovigilancia laboral: valoración crítica (STC 39/2016, de 3 de marzo)", *Derecho de las Relaciones Laborales, Jurisprudencia en detalle*, nº 5, mayo 2016, pág. 495.

información que exige la adaptación a las singularidades del mismo, en línea con la doctrina sentada por la STC 29/2013, de 11 de febrero, la cual es abandonada, sin explicación alguna, para anclarse en otras muchos más antiguas –como le reprocha el voto particular de los Magistrados Valdés Dal-Ré y Xiol Rios, muy razonados y razonables-, como son la STC 186/2000, de 10 de julio, o más ambiguas –STC 170/2013, de 7 de octubre-.

Sorprendentemente, la fuerza prevalente del Derecho se diluirá con la sola constatación de una pegatina informativa que reúna, eso sí, los exigentes requerimientos de formato establecidos en el Anexo de la Instrucción 1/2006, de 8 de noviembre de la AEPD –como, con fina ironía, le reprocha el Magistrado Fernando Valdés Dal-Ré-. Consecuentemente, una vez existente la pegatina con el correspondiente distintivo, y constatada una fundada sospecha, el poder de control quedará plenamente legitimado para adentrarse en la vigilancia directa del trabajador.

6. En suma, la sentencia señala que el consentimiento del afectado se erige en elemento definidor del sistema de protección de datos de carácter personal, entendiéndose implícito el mismo, en el ámbito de las relaciones laborales, en la aceptación del contrato, el cual implica un reconocimiento del poder de dirección del empresario, eso sí, sólo en la medida que el tratamiento de datos personales sea necesario para el mantenimiento y el cumplimiento del contrato de trabajo.

Ahora bien, conforme sostiene la propia sentencia, que no sea necesario el consentimiento no significa que se anule el derecho de información previo de uso y destino de los datos personales que integra el contenido esencial del derecho a la protección de datos, si bien la propia sentencia matiza la referida afirmación al señalar expresamente que a la hora de valorar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información, la dispensa del consentimiento al tratamiento de datos en

determinados supuestos debe ser un elemento a tener en cuenta dada la estrecha vinculación existente entre el deber de información y el principio general de consentimiento.

De este razonamiento se desprende que el TC entiende que, en los casos en los que no se exige consentimiento para la recogida de datos, como sucede en el ámbito de las relaciones laborales, podría modularse el derecho de información dado que no es absolutamente determinante que el trabajador conozca el uso y destino que tendrán sus datos personales si no puede evitar su recogida, lo cual implicaría que la habilitación legal expresa que exime al empresario de la obligación de solicitar el consentimiento de los trabajadores para el tratamiento de datos vinculados al mantenimiento o cumplimiento del contrato, impacta a su vez con la observancia del deber de información previa. A diferencia de la STC 29/2013, de 11 de febrero, no se dispone en este pronunciamiento que el derecho de información pueda ser desconocido exclusivamente en supuestos previstos en norma con rango de ley.

En dicha línea, el TC estima que no siempre el incumplimiento del deber de solicitar el consentimiento o del deber de información previo por parte del empresario implicará una vulneración del artículo 18.4 CE, pues ello dependerá de la superación del test de proporcionalidad. No se debe perder de vista que la STC 29/2013, de 11 de febrero, disponía precisamente lo contrario, a saber: al lesionarse el derecho de información previo, contenido esencial del derecho de protección de datos, no tenía cabida la aplicación del principio de proporcionalidad en ese extremo.

7. La primera gran diferencia entre las sentencias analizadas consiste en que mientras bajo la STC 29/2013, de 11 de febrero, el derecho de información - dada la inexistencia de habilitación legal expresa que justificara su omisión - no podía ser desconocido bajo ningún supuesto, en la STC 39/2016, de 3 de

marzo, ello dependerá de la superación del test de proporcionalidad, en definitiva de las concretas circunstancias del caso.

Esta primera modificación de la doctrina constitucional, que uniformiza los parámetros a ser tomados en cuenta frente a la instalación de cámaras de video vigilancia, es apropiada dada la inexistencia de un motivo objetivo y razonable que justifique la diferencia de tratamiento jurisprudencial. De este modo, a partir de la STC 39/2016, de 3 de marzo, no solo respecto del derecho a la intimidad deberá aplicarse el test de proporcionalidad, sino también respecto del derecho de autodeterminación informativa[516].

Por otro lado, la segunda manifestación del cambio de doctrina operado estriba en la manera de cómo debe cumplirse el deber de información previo. En la STC 39/2016, de 3 de marzo, el Tribunal Constitucional se aleja de lo dispuesto en la sentencia precedente al estimar que basta con colocar el distintivo informativo genérico de "zona videovigilada" exigido por la Instrucción AEPD 1/2006, de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Ello sería suficiente para permitir a los afectados conocer la existencia de las cámaras y la finalidad genérica de vigilancia para la cual fueron instaladas aquéllas, no siendo sería necesario, según el TC, especificar, más allá de la mera vigilancia, la finalidad exacta asignada a ese control, dejándose atrás, de esta manera, el criterio adoptado en la STC 29/2013, de 11 de febrero, que exigía que se proporcionara a los titulares de los datos información específica e individualizada, bastando ahora con la colocación de un distintivo genérico que no especifica la finalidad concreta del medio de vigilancia.

516 GUERRA RODRÍGUEZ, L.: "Ejercicio del poder de control a través de cámaras de videovigilancia…", op. cit., *Trabajo y Derecho* 29/2017 (mayo), nº 29 de 1 de mayo de 2017, pag. 5.

Sobre este punto, en tanto que los titulares de los datos personales son los trabajadores, son éstos quienes deben ser informados. No siendo estos los destinatarios naturales del distintivo genérico "zona videovigilada", siéndolo más bien los clientes de la tienda[517], no debería admitirse como suficiente la información genérica anunciando la instalación de cámaras. En vista de ello, el canal a ser utilizado debería ser uno típicamente laboral, dirigido a informar - no necesariamente de manera individualizada, más sí concreta, expresa, inequívoca y directa - al grupo de trabajadores afectados de la presencia de cámaras en el centro de trabajo y de su finalidad de control de la prestación laboral.

En aplicación de esta doctrina al caso concreto, el Tribunal Constitucional determinó que la obligación de información previa fue cumplida habida cuenta de que la empresa colocó el distintivo informativo exigido por la Instrucción AEPD 1/2006, de 8 de noviembre, no vulnerándose así el derecho a la protección de datos. En atención a lo señalado, el control de constitucionalidad de la medida se realizó en relación con el derecho a la intimidad personal, remitiéndose a tal efecto a la doctrina constitucional desarrollada en las STC 186/2000 y 98/2000.

Por último, señalar que la sentencia cuenta, como se ha dicho, con dos Votos particulares, formulados por los magistrados Fernando Valdés Dal-Ré - al que se adhiere la Magistrada Adela Asúa Batarrita -, y Juan Antonio Xiol Ríos.

517 VIVERO SERRANO, J.: “Las sentencias anotadas. Vigilancia y control de los trabajadores mediante cámaras de video”, *Trabajo y Derecho*, nº 17, 2016.

2.2.1.- Voto particular del Magistrado Fernando Valdés Dal-Ré.

1. Discrepa el Magistrado Fernando Valdés Dal-Ré tanto con la doctrina asentada en esta sentencia sobre los derechos fundamentales afectados, en concreto respecto del art. 18.4 CE, como con el método de enjuiciamiento utilizado, así como con el canon de constitucionalidad aplicado, sosteniendo que el despido debió haber sido calificado como nulo por incumplimiento del deber de información que impone al empresario el art. 18.4 CE.

Se muestra disconforme con la forma con la que esta sentencia se separa de la jurisprudencia del TC sobre el derecho a la protección de datos en los casos de video vigilancia laboral contenida en la STC 29/2013, de 11 de febrero, sosteniendo que el cambio de doctrina se ha operado sin aportarse la necesaria argumentación jurídico-constitucional acerca de los motivos conducentes al abandono de una jurisprudencia que tenía como objetivo fijar los límites del contenido esencial del derecho fundamental que el art. 18.4 CE confiere a los trabajadores.

Señala también que la doctrina defendida en esta sentencia se sitúa en una senda de retroceso en la protección de los derechos fundamentales de los trabajadores, revelando una orientación tendente a vaciar de contenido sustantivo un modelo constitucional de relaciones laborales acorde con el Estado Social y Democrático de Derecho previsto en el art. 1.1 CE.

2. Objeta, asimismo, que la sentencia constituye respuesta a una noción del poder directivo empresarial contraindicada para el modelo de relaciones laborales instaurado por la Constitución de 1978, no siendo el art. 20.3 ET, a juicio del Magistrado Fernando Valdés, un parámetro de constitucionalidad

limitador de los derechos fundamentales en el seno de las organizaciones empresariales, sino que aquél constituye, únicamente, una regla jurídica rectora de la relación contractual.

3. Entiende, asimismo, que los poderes empresariales no son expresiones directas de los arts. 33 y 38 CE que quepa confrontar de manera automática, sin ningún tipo de fundamentación, con los derechos fundamentales de los trabajadores, del mismo modo que las facultades del empresario no pueden restringir estos derechos en el seno de las empresas, incluidos, obviamente, los formulados en el art. 18 CE.

4. Y, por último, sostiene que resulta poco ortodoxo erigir una Instrucción de la AEPD en elemento decisivo para un juicio de constitucionalidad. En el plano de la legalidad, se puede discutir si la proyección de la información del art.5 LOPD en el contrato de trabajo es suficiente o no con esta Instrucción, pero en la dimensión constitucional la conclusión nunca puede sostenerse en esta referencia reguladora de la APD.

2.2.2.- Voto particular del Magistrado Juan Antonio Xiol Ríos.

1. Por su parte, el Magistrado Juan Antonio Xiol Ríos manifiesta su discrepancia tanto con la fundamentación jurídica como con el fallo que, en su opinión, debería haber sido estimatorio de la demanda de la trabajadora.

Compartiendo el contenido del Voto particular formulado por el Magistrado Fernando Valdés a la sentencia, no obstante acompaña su adhesión con algunas matizaciones, a saber:

1.- Argumenta que, si bien la sentencia admite en el ámbito de las relaciones laborales la existencia de una deber de información acerca de la instalación de cámaras de video vigilancia, la cuestión, no obstante, radica en determinar (i) si esa información ha de suministrarse a los trabajadores especificando su finalidad de control del cumplimiento de la prestación laboral; o (ii) si, como entiende la sentencia, ese deber de información se cumple suficientemente con la mera colocación de un anuncio hecho al público sobre la existencia de cámaras de seguridad en el establecimiento.

2.- Discrepa de la opción 'ii' por las siguientes razones:

a) La STC 29/2013, de 11 de febrero, estableció la doctrina de que el deber de información relativo a la instalación de cámaras de vigilancia en las empresas debía ir acompañado de la necesaria información a los trabajadores acerca de su finalidad de control de la prestación laboral y la sentencia a la que se refiere este voto particular no se atiene a esa jurisprudencia.

b) Los precedentes del TC citados como concluyentes (de manera especial la STC 292/2000, de 30 noviembre) carecen de entidad suficiente para justificar la postura de la sentencia dado que aquéllos se refieren a supuestos de hallazgos casuales por videocámaras instaladas por motivos de seguridad, en tanto que en el presente caso se refiere a una cámara dirigida específicamente a lugares ocupados por los trabajadores con el objeto de investigar determinadas circunstancias.

c) Otra razón por la que los precedentes referidos resultan a todas luces insuficientes radica en que los mismos tienen una antigüedad superior a quince años, período en el que se ha producido una notable evolución en el ámbito del derecho a la protección de datos, reflejada la misma, entre otros aspectos, en

el hecho de que los amparos entonces resueltos no se fundamentaban jurídicamente en el derecho a la protección de datos, sino, más primariamente, en el derecho a la intimidad.

d) Sostiene, asimismo, que no resulta aceptable que una mera información dirigida al público en general constituya elemento suficiente para entenderse cumplido el deber de información para con los trabajadores, de modo que la omisión de toda información a éstos acerca de la existencia de cámaras orientadas específicamente hacia sus posiciones supone una lesión del derecho fundamental que afecta a su contenido esencial, cualquiera que sea el método de ponderación utilizado para determinar su contenido.

e) Finalmente, considera que pulveriza el contenido esencial del derecho a la protección de datos admitir que el empresario, ante cualquier sospecha que pudiera albergar, esté autorizado por la Constitución a instalar libremente - siempre que en el entorno haya un aviso al público sobre la existencia de cámaras de seguridad - cámaras para el control del trabajo orientadas a vigilar en primer plano determinadas posiciones ocupadas por los trabajadores.

3.- DE LÓPEZ RIBALDA I A LÓPEZ RIBALDA II.

1. Tras la STEDH (Gran Sala) en el caso Barbulescu c. Rumanía de 5 de Septiembre de 2017, dicho Tribunal volvió a dictar Sentencia el 9 de enero de 2018 en el caso López Ribalda *et alii* c. España, también conocida como López Ribalda I, la cual aborda la video vigilancia en el lugar de trabajo y el necesario equilibrio que debe existir entre el poder de dirección del empresario y el derecho a la protección de datos y a la intimidad.

La sentencia del caso López Ribalda I revisó la actuación empresarial en un supuesto de video vigilancia empresarial que se había considerado ajustada a derecho por los tribunales españoles en el marco de un procedimiento por despido declarado procedente por éstos, y corrige a nuestros tribunales, concluyendo que no hubo proporcionalidad en las medidas adoptadas por el empresario con el objetivo legítimo de proteger sus intereses de propiedad.

2. Los hechos se pueden resumir del modo que sigue: en un supermercado fueron detectados importantes diferencias entre el inventario de productos y lo facturado en las cajas, por lo que se instalaron una serie de cámaras de control de dos tipos: cámaras visibles para grabar posibles robos de clientes (de lo cual fue informada la representación de los trabajadores y los propios empleados) y cámaras ocultas para grabar posibles robos de los empleados, que enfocaban la zona de las cajas. Tras un período de grabación, la compañía citó a los empleados que aparecían implicados en los robos, reconociendo todos ellos su involucración en los hechos. Los despidos disciplinarios fueron impugnados ante la jurisdicción social, siendo el principal argumento de las demandantes que la video vigilancia oculta había vulnerado su derecho a la intimidad.

3. Tanto el Juzgado de lo Social como el Tribunal Superior de Justicia de Cataluña confirmaron la procedencia de los despidos, alegando que el uso de la video vigilancia encubierta en el lugar de trabajo sin una comunicación previa era conforme con el art. 20.3 ET, que permitía a un empresario la utilización de medidas de control y vigilancia que considerara adecuadas, siempre que se cumpliera el test de proporcionalidad, lo que en este caso se producía dado que la medida estuvo justificada debido a las fundadas sospechas de robo; fue apropiada al objetivo legítimo perseguido, necesaria y proporcionada por no existir otros medios igual de eficaces en orden a proteger los derechos del empresario que interfirieran menos con el derecho de las demandantes al respeto de su vida privada.

4. La demanda que se plantea ante el TEDH por cinco de las personas despedidas alega como argumento principal la vulneración del art. 8 del CEDH. El TEDH reconoce que la video vigilancia encubierta se llevó a efecto después de que hubiera fundadas sospechas de la comisión de robos por parte de las demandantes, pero recuerda que los datos visuales obtenidos implican el almacenamiento y procesamiento de datos de carácter personal, estrechamente vinculados a la esfera privada de las personas (lo que va en línea con la doctrina de nuestro Tribunal Constitucional que afirma que las imágenes grabadas en un soporte físico constituyen un dato de carácter personal que queda integrado en la cobertura del art. 18.4 CE)[518].

5. Por ello, continúa el TEDH, conforme al art. 5 de la derogada Ley española de Protección de Datos de Carácter Personal (LOPD), las demandantes tenían derecho a ser informadas "previamente de modo expreso, preciso e inequívoco" de "la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información", así como del resto de la información regulada en dicho artículo. La existencia de la norma implicaba que las demandantes tenían una expectativa razonable de respeto a su privacidad y la empresa no cumplió con los requisitos del citado art. 5 LOPD (lo que llevará al TEDH a considerar que se vulneró el art. 8 del CEDH).

6. Y, asimismo, estableció diferencias con un caso con ciertas similitudes que el TEDH había enjuiciado anteriormente (el caso Köpke c. Alemania), donde sí avaló el proceder de la empresa, dado que en este último caso no existía normativa nacional al respecto, y la video vigilancia encubierta estuvo limitada tanto (i) en el ámbito subjetivo (se restringió a las dos demandantes sobre las que existía sospecha justificada, frente al caso López Ribalda en el

518 GIMÉNEZ-ARNAU, R., "Poder de dirección y derecho a la protección de datos. Algunas reflexiones a raíz del Caso López Ribalda", *https://elderecho.com/poder-de-direccion-y-derecho-a-la-proteccion-de-datos-algunas-reflexiones-a-raiz-del-caso-lopez-ribalda*

que la sospecha era general y afectaba a todo el personal de cajas registradoras) como (ii) en el ámbito temporal (se llevó a cabo durante dos semanas, mientras que en el caso analizado se realizó durante varias semanas, sin límite de tiempo y durante todas las horas del trabajo).

7. Por ello el TEDH concluye que no hubo un justo equilibrio entre el derecho de las demandantes al respeto de su vida privada al amparo del art. 8 CEDH y el interés del empresario en la protección de sus derechos propietarios, y que la actuación empresarial vulneró el citado art. 8 del CEDH.

8. El Reino de España solicitó al TEDH el reexamen del caso, dictando el Tribunal (Gran Sala) sentencia de fecha 17 de Octubre de 2019, también conocida como López Ribalda II. La sentencia analiza el ordenamiento español, (anterior a la LOPDGDD), así como la doctrina de la STC 186/2000, de 10 de julio, y concluye, por catorce votos a favor y tres en contra, que la empresa no vulneró el art. 8 CEDH, entendiendo que son válidos los controles ocultos a los trabajadores mediante el sistema de video vigilancia, pero nunca ante la más mínima sospecha de apropiación indebida o cualquier otro delito por parte de los empleados, sino que se requiere la existencia de sospechas razonables de que se ha cometido una infracción grave con perjuicios importantes para la empresa.

9. Lo primero que hay que destacar de esta sentencia es que la misma incorpora el Test Barbulescu de Garantía de la Privacidad (relativo al control del uso del ordenador) al control por video vigilancia de los trabajadores en su puesto de trabajo, de forma que los tribunales nacionales deberán tener en cuenta los siguientes factores cuando sopesen los diversos intereses en conflicto:

i) Si el trabajador ha sido informado de la posibilidad de que el empleador pudiera adoptar medidas de video vigilancia y de su efectiva

implementación. Si bien en la práctica los trabajadores pueden ser informados de varias maneras, dependiendo de las circunstancias fácticas particulares de cada caso, la notificación normalmente debe ser clara sobre la naturaleza del vídeo vigilancia y debe darse anterior a su aplicación[519].

ii) El alcance de la video vigilancia por parte del empresario y el grado de intrusión en la privacidad del trabajador. En este sentido, se deberá tener en cuenta el nivel de privacidad en el área que se está vigilando, junto con las limitaciones de tiempo y espacio y la cantidad de personas que tienen acceso a los resultados.

iii) Si el empleador ha proporcionado razones legítimas para justificar la video vigilancia y el alcance de la misma. Cuanto más intrusiva sea la video vigilancia, mayor será la justificación que se requerirá.

iv) Si hubiera sido posible establecer un sistema de video vigilancia basado en métodos y medidas menos intrusivos. A este respecto, debe existir una evaluación a la luz de las circunstancias particulares de cada caso en cuanto a si el objetivo perseguido por el empleador podría haberse logrado a través de un menor grado de interferencia con la privacidad del empleado.

v) Las consecuencias de la video vigilancia para el trabajador, debiendo tenerse en cuenta, en particular, el uso que hace el empresario de los resultados de la supervisión y si dichos resultados se han utilizado para lograr el objetivo declarado de la medida.

519 PRECIADO DOMENECH, C. H. “Comentarios de urgencia a la STEDH de 17 de octubre de 2019 caso López Ribalda c. España (Gran Sala), *newsletter laboral de Juezas y Jueces para la democracia*, 21 Octubre 2019.

vi) Si el trabajador ha recibido las garantías apropiadas, de manera especial cuando las operaciones de video vigilancia del empleador son de naturaleza intrusiva. Dichas garantías pueden tomar la forma, entre otras, de proporcionar información a los empleados interesados o a los representantes de los trabajadores en cuanto a la instalación y el alcance de la video vigilancia, o una declaración de tal medida a un organismo independiente o la posibilidad de presentar una queja[520].

En suma, se establece un riguroso control garantista de los derechos a la intimidad y la protección de datos de las personas de los trabajadores.

10. En segundo lugar, un gran avance que ha supuesto la sentencia ha sido que clarifica la cuestión de los controles ocultos y viene a validar y acotar la doctrina del TC, sentada en su STC 186/2000, de 10 de julio, en cuya virtud sólo puede prescindirse de la información previa y la transparencia en la video vigilancia en supuestos excepcionales, cuando consten sospechas razonables de una infracción laboral que afecte gravemente a los intereses de la empresa, y siempre que no haya medios alternativos menos intrusivos.

El TEDH acota dicha doctrina precisando que no son válidos los controles ocultos por el sistema de video vigilancia ante la más mínima sospecha de apropiación indebida o cualquier otro delito por parte de los empleados, sino que se deben existir sospechas razonables de que se ha cometido una infracción grave que atente gravemente contra los intereses de la empresa.

520 PRECIADO DOMENECH, C. H. “Comentarios de urgencia a la STEDH de 17 de octubre de 2019 caso López Ribalda c. España (Gran Sala), *newsletter laboral de Juezas y Jueces para la democracia*, 21 Octubre 2019.

11. En tercer lugar, la sentencia no aprecia vulneración del art. 8 CEDH, en los controles ocultos, porque los mismos fueron proporcionados, pero también porque las demandantes podían denunciar la infracción de su derecho a la información en la protección de datos ante la AEPD y ante los tribunales, tanto en vía civil como administrativa, de modo que la infracción del deber de información de los trabajadores en materia de protección de datos puede recibir su adecuada compensación (AEPD, demanda civil en reclamación de daños y perjuicios).

12. Asimismo, el TEDH considera que la información que se debe suministrar a los trabajadores objeto de video vigilancia constituye solo uno de los criterios a tener en cuenta para evaluar la proporcionalidad de una medida de este tipo en un caso dado. No obstante, si falta dicha información, las garantías derivadas de los otros criterios serán aún más importantes.

Es decir, lo que la Gran Sala del TEDH hace en su sentencia es relativizar el deber de información caracterizándolo como un componente más del juicio de proporcionalidad (apartado 131 de la sentencia).

13. En definitiva, según la sentencia, la privacidad e intimidad de las personas trabajadoras sigue exigiendo que, como norma general, el empresario les notifique previamente las medidas intrusivas contra su intimidad y privacidad, tales como al video vigilancia, informando además sobre su finalidad.

14. Ahora bien, la Gran Sala admite que, en casos muy concretos en los que existan sospechas muy bien fundadas de incumplimientos graves por parte de los trabajadores, se pueda usar, excepcionalmente, cámaras ocultas. Ello significa, según la Gran Sala, que:

a) Cualquier mínima sospecha no justifica el uso de cámaras ocultas.

b) Cualquier incumplimiento tampoco lo justifica, sino que éste ha de ser grave o muy grave. E irregularidades graves o muy graves son delitos. Y no meros actos ilícitos o simples incumplimientos laborales, que pueden ser infracciones menos graves. Y es así, y no de otro modo, como debe interpretarse el segundo párrafo del art. 89.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales[521].

c) La medida debe de ser siempre limitada y proporcionada, no pudiendo ser general e indiscriminada.

15. Por último, señalar que la sentencia cuenta con el voto particular discrepante de tres Magistrados, que manifiestan su desacuerdo general con la interpretación efectuada por los restantes magistrados por la razón de que la sentencia "respalda una respuesta legal a una cuestión particular que surgió sólo después de los hechos y en relación con un caso particular. Si tal aproximación, que da al juez nacional cierto margen de maniobra para elaborar una respuesta jurídica a un conflicto que dé lugar a una controversia particular sobre derechos convencionales concurrentes, puede ser apropiada en algunos casos, creemos que no es apropiado para los casos de video vigilancia electrónica, precisamente por la facilidad con la que se puede utilizar la tecnología para llevar a cabo y difundir la vigilancia y difundir las imágenes por medios electrónicos, con las consecuencias negativas potencialmente amplias e importantes que pueden tener sobre el derecho de cada individuo al respeto de la privacidad. Un régimen jurídico claro y predecible, que ofrezca garantías adecuadas y efectivas, es crucial. En el presente caso, el régimen jurídico en vigor no preveía más que una garantía específica, a saber, la obligación de notificar a los empleados la instalación y el uso de la monitorización, y no

521 Sobre este particular vid. LAHERA FORTEZA, J., "Seguridad jurídica en la videovigilancia laboral", *https://cincodias.elpais.com/cincodias/2019/10/28/opinion/1572280911_312873.html*

contemplaba ninguna excepción a esta garantía. Este elemento, a nuestros ojos, es crucial a efectos de un análisis jurídico adecuado y de las conclusiones a sacar en el caso en juego".

16. En definitiva, el voto particular afirma con claridad que los tribunales españoles no aplicaron el régimen jurídico que garantizara la protección de los datos, ni tampoco tomaron en consideración la situación de las recurrentes de una manera detallada e individualizada[522].

Con aplicación de las tesis recogidas en la sentencia Barbulescu II, y ahora por la de 17 de octubre de 2019 (López Ribalda II), enfatiza que los tribunales españoles deberían "haber considerado las medidas alternativas que el empleador podría haber tomado para alcanzar su objetivo legítimo. Medidas que, al mismo tiempo, habrían violado menos gravemente el derecho a la privacidad de los trabajadores", y que en ningún caso el legítimo ejercicio de acciones por parte empresarial para tratar de encontrar respuesta a los problemas existentes de sustracción de productos, es decir una infracción punible en sede laboral, no justificaba una actuación privada como la que se llevó a cabo mediante la utilización de la video vigilancia, que para la sentencia de Sala, y ahora en tesis reiterada por el voto discrepante, "constituye una medida en exceso intrusiva y un abuso de poder", y habiendo ahora sido aceptada por la Gran Sala el TEDH está "animando a cada una a tomarse la justicia por sí mismo".

522 ROJO TORRECILLA, E., "Medias verdades y fake news en el mundo jurídico. No cabe todo en la videovigilancia de una persona trabajadora. A propósito de la sentencia "López Ribalda" de la Gran Sala del TEDH de 17 de octubre de 2019 (y recordatorio de la sentencia de Sala de 9 de enero de 2018 y del caso Barbulescu II, sentencia de Gran Sala de 5 de septiembre de 2017)", *http://www.eduardorojotorrecilla.es/2019/10/medias-verdades-y-fake-news-en-el-mundo.html*

CAPÍTULO V.- LA PROPORCIONALIDAD DE LAS MEDIDAS DE CONTROL.

1.- El poder de dirección del empresario y el derecho a la intimidad del trabajador: la necesidad de ponderación.

1. Si bien la celebración del contrato de trabajo no supone en ningún caso la anulación de los derechos fundamentales que asisten al trabajador, lo cierto es que sí modula en cierta medida el alcance de los mismos[523]. En este sentido, el TC viene sosteniendo que el contrato de trabajo genera un conjunto de derechos y obligaciones recíprocas entre trabajador y empresario que condiciona el ejercicio de los derechos cuya titularidad corresponde a los trabajadores, de forma que expresiones de los mismos que, en otro contexto, pueden resultar legítimas no tienen por qué serlo necesariamente en el marco de la relación laboral[524].

No hay que olvidar que en el ámbito de las relaciones laborales están en juego, asimismo, intereses constitucionales. Así, la libertad de empresa supone poderes empresariales entre los que la potestad de control de las obligaciones laborales del trabajador por parte del empresario es una muestra de ello, quedando limitado de ese modo el alcance de los derechos de los trabajadores[525], si bien hay que recordar que esa limitación no equivale, en modo alguno, a anulación, siendo necesario articular fórmulas jurídicas que

523 SEMPERE NAVARRO, A. V. y MATEOS Y DE CABO, O., "Uso y control de herramientas informáticas en el trabajo (marco legal, pautas judiciales y convencionales)", en AA. VV.: *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, SAN MARTÍN MAZZUCCONI, C. (Dir.), Eolas, 2014, págs. 110-114.

524 SSTC 120/1983, de 15 de diciembre; 6/1988, de 21 de enero; 4/1996, de 16 de enero; 106/1996, de 12 de junio; 1/1998, de 12 de enero; 20/2002, de 28 de enero; 126/2003, de 30 de junio; o 151/2004, de 20 de septiembre.

525 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.54.

permitan conciliar las exigencias de dignidad y privacidad del trabajador con los intereses empresariales[526].

2. Expuesto el conflicto entre los derechos de ambas partes, la solución al mismo viene dado a través de la técnica de la ponderación habida cuenta de que la consagración de los derechos fundamentales en el seno de la empresa presenta, como efecto, la modulación de los poderes de vigilancia y control del empresario, de modo que aquéllos suponen un decidido límite en la operatividad de éstos[527].

Es por ello que el derecho a la intimidad, lejos de ser un derecho absoluto, es susceptible de limitación o modulación, la cual sólo está justificada por la necesidad de proteger otro valor también considerado digno de protección en el ordenamiento jurídico[528]. No obstante, a pesar de la posibilidad de limitar o modular los derechos fundamentales de los trabajadores en el seno de la relación laboral, tales límites resultan acotados por "la noción de imprescindibilidad"[529], la cual es consecuencia de la posición de prevalencia que, en nuestro ordenamiento jurídico, tienen los derechos fundamentales[530].

A tal efecto, el TC ha entendido que el ejercicio de los derechos fundamentales del trabajador sólo admite sacrificios en la medida en que se desenvuelven en el seno de una organización que refleja otros derechos

526 PÉREZ DE LOS COBOS ORIHUEL, F., *Nuevas tecnologías y relación de trabajo*, Tirant lo Blanch, Valencia, 1990, pág. 90.

527 GUTIÉRREZ PÉREZ, M., *Ciudadanía en la empresa y derechos fundamentales inespecíficos*, Ed. Laborum, Murcia, 2011, págs. 165-167 y 185.

528 TOSCANI GIMÉNEZ, D. y VALENCIANO SAL, A., *Derechos fundamentales inespecíficos de los trabajadores*, Bomarzo, Albacete, 2016, pág. 210.

529 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.54.

530 SSTC 90/1999, de 26 de mayo, y 213/2002, de 11 de noviembre.

también reconocidos constitucionalmente, como el derecho a la libertad de empresa del art. 38 CE[531].

No obstante, sin perjuicio de que el derecho a la intimidad no sea un derecho de carácter absoluto, tampoco es posible atribuir dicho carácter a los límites a los que puede someterse su ejercicio[532], de modo que cabe modular aquel derecho a la luz del interés empresarial, si bien éste no puede adquirir en ningún momento una importancia[533], correspondiendo a los órganos judiciales la preservación del necesario equilibrio entre las obligaciones del trabajador dimanantes del contrato de trabajo y el ámbito de sus derechos y libertades constitucionales.

2.- El juicio de proporcionalidad: su articulación y presupuestos.

1. Las relaciones entre los derechos fundamentales y los poderes empresariales constituye uno de los temas que más número de aristas presenta, hasta el punto de constituir uno de los problemas centrales de la dogmática actual de los derechos fundamentales[534]. Como ponía de relieve el voto particular formulado por el Magistrado Vicente Gimeno Sendra que acompañaba a la STC 215/1994, de 17 de abril, *"la proporcionalidad no es más que un método que nos indica en qué condiciones puede una norma, que incide en un derecho fundamental, obtener una aplicación conforme con la Constitución y no un examen de la norma que permita, en cualquier caso, predicar su constitucionalidad o la aplicación constitucional de la misma"*.

531 SSTC 98/2000, de 10 de abril; 99/1994, de 11 de abril; 6/1995, de 10 de enero; 106/1996 de 12 de junio; y 136/1996, de 23 de julio.

532 STC 20/1990, de 15 de febrero.

533 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.55.

534 GÓMEZ MONTORO, A., "La titularidad de derechos fundamentales por personas jurídicas: un intento de fundamentación", *REDC*, 2002, nº 65, pág. 50.

Por ello, como principio general, cabe señalar que la constitucionalidad de cualquier medida restrictiva de los derechos fundamentales vendrá siempre determinada por la estricta observancia del principio de proporcionalidad[535]. Y a los efectos que aquí importan, baste señalar que, como exponen las SSTC 66/1995, de 8 de mayo; 55/1996, de 28 de marzo, y 207/1996, de 16 de diciembre, en orden a la comprobación de si una determinada medida restrictiva de un derecho fundamental supera el pertinente juicio de proporcionalidad, resultará necesario constatar si aquélla cumple los tres requisitos siguientes, a saber: i) que la medida sea susceptible de alcanzar el objetivo propuesto (juicio de idoneidad); ii) si, además, es necesaria, en el sentido de que no exista otra más moderada para la consecución de tal propósito con idéntica o similar eficacia (juicio de indispensabilidad o de estricta necesidad); y, finalmente, iii) si aquélla es ponderada o 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)[536].

La triple secuencia expuesta ha sido resumida contestando a la siguiente pregunta: ¿pueden los trabajadores ejercer sus derechos constitucionales en el seno de la relación laboral?, siendo la respuesta de índole positiva. En este sentido, el TC entiende que el empleador no se encuentra facultado para llevar a cabo intromisiones ilegítimas en la intimidad de los trabajadores sobre la base de sus facultades de vigilancia y control *ex* art. 20.3 ET, sino que también las facultades organizativas de aquél encuentran límites derivados de los derechos fundamentales que asisten al trabajador, estando el empresario obligado a respetar éstos (STC 186/2000, de 10 de julio), de modo que el ejercicio de las facultades organizativas de éste no puede conducir en ningún

535 Sobre el juego del principio de proporcionalidad como límite al ejercicio de los derechos fundamentales, *vid.* MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales*, Madrid, McGraw Hill, 1996, págs. 117 y sigs.

536 GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, JESÚS R., "Conflicto y ponderación de los derechos fundamentales de contenido laboral", en *El modelo social en la Constitución Española de 1978*, Dir. SEMPERE NAVARRO, A. V., Coord., MRTÍN JIMÉNEZ, R., MTASS, Madrid, 2003, pág. 257.

caso a la producción de resultados inconstitucionales en los derechos fundamentales del trabajador[537].

2. Es por ello que, para determinar si son legítimas o no, habrá que estar al juicio de proporcionalidad[538], el cual, aplicado en el ámbito laboral desde la STC 99/1994, de 11 de abril, supone que la doctrina constitucional no concede el mismo valor a los derechos de los trabajadores y a los intereses del empresario, de modo que el equilibrio entre ambos no se halla en el punto medio entre los mismos, pues uno y otro no coinciden en el mismo plano de relevancia constitucional[539]. Sólo cuando se supere el referido test de proporcionalidad cabrá imponer límites a los derechos de los trabajadores[540]. Es decir, sólo en los casos en que dichos límites se revelaren absolutamente necesarios para la consecución de un fin constitucionalmente legítimo; resultaren proporcionados para alcanzarlo y, en todo caso, fueren respetuosos con el contenido esencial del derecho[541].

De este modo, el juicio de proporcionalidad emerge en este contexto como parámetro necesario para la determinación de la validez de las potenciales acciones restrictivas de derechos fundamentales, verificando su adecuación en función de una finalidad que debe resultar legítima y proporcionada[542]. Se trata, en definitiva, de determinar la idoneidad, la

537 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.55.

538 GARCÍA-PERROTE ESCARTÍN y MERCADER UGUINA, J. R., "Conflicto y ponderación de los derechos fundamentales de contenido laboral", en *El modelo social en la Constitución Española de 1978*, Dir. SEMPERE NAVARRO, A. V., Coord., MRTÍN JIMÉNEZ, R.), MTASS, Madrid, 2003, pág. 257.

539 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., *Idem.*, pág. I.55.

540 SEMPERE NAVARRO, A. V. Y MATEOS Y DE CABO, O., "Uso y control de herramientas informáticas…, *op. cit*., págs. 121 y 122.

541 SSTC 57/1994, de 28 de febrero; 143/1994, de 9 de mayo; 98/2000, de 10 de abril; 186/2000, de 10 de julio; y 156/2001, de 2 de julio.

542 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., *Idem.*,pág. I.56.

necesidad y la proporcionalidad de la medida en orden a la consecución de un fin legítimo[543]. Es decir, en el terreno de las obligaciones recíprocas de empresario y trabajador se admiten, pues, ciertas modulaciones al ejercicio del derecho fundamental a la intimidad, pero siempre a la luz del principio de proporcionalidad[544].

3. De cualquier modo, no resulta suficiente la mera alegación de la conveniencia de introducir una concreta medida restrictiva de los derechos fundamentales, dado que se han de invocar motivos objetivos. Así lo entiende el TC, que afirma que, desde la posición prevalente de los derechos fundamentales del trabajador, la limitación de éstos por las facultades del empresario sólo puede derivar, bien del hecho de que la propia naturaleza del trabajo contratado implicare la restricción del derecho de que se trate[545], bien de una acreditada necesidad o interés empresarial, sin que resulte suficiente a estos efectos su mera invocación para sacrificar el derecho fundamental del trabajador[546]. De ahí que la constitucionalidad de cualquier medida restrictiva de derechos fundamentales haya de venir siempre determinada por la estricta observancia del principio de proporcionalidad.

3.- La proporcionalidad en la instalación de cámaras de video vigilancia.

1. Siendo la video vigilancia de los trabajadores la modalidad más común de control tecnológico de la actividad laboral, una de las principales cuestiones a dilucidar consiste en la determinación del concreto lugar de instalación de los

543 BARAK, A., *Proporcionalidad. Los derechos fundamentales y sus restricciones*, Palestra, Perú, 2017, pág. 197.

544 GUTIÉRREZ PÉREZ, M., *Ciudadanía en la empresa y derechos fundamentales inespecíficos*, Laborum, Murcia, 2011, pág. 198.

545 SSTC 99/1994, de 11 de abril y 106/1996, de 12 de junio.

546 SSTC 99/1994, de 11 de abril; 6/1995, de 10 de enero; 136/1996, de 23 de julio; y 98/2000, de 10 de abril.

medios audiovisuales de control. Según el TC[547], resulta lesiva, en todo caso, para el derecho a la intimidad del trabajador la instalación de cámaras de video vigilancia en zonas de descanso o esparcimiento, vestuarios, aseos, comedores y análogos - pero no si se graba solamente el acceso a tales espacios -[548] por resultar ajenas a la prestación laboral. Asimismo, enfocar directamente una cámara de seguridad en una trabajadora y su ordenador vulnera el derecho a su intimidad y propia imagen y no está justificado por razones de seguridad y no es proporcional[549]

En consonancia con ello, a nivel legislativo, el art. 89.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, prescribe que en ningún caso será admisible la instalación de sistemas de grabación de sonidos ni de video vigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

Como ha puesto de relieve el Tribunal Constitucional, la expectativa razonable de privacidad se identifica con el derecho de la persona a mantener una "barrera de reserva"[550] en sus diversos ámbitos de relación, incluido – obviamente - el ámbito laboral, formando parte integrante de este ámbito privado las zonas de esparcimiento, el comedor, los lavabos o los vestuarios, sin obviarse otras zonas en las que el derecho a la intimidad también despliega toda su eficacia aunque en las mismas se desarrolle una actividad laboral, siendo así que el Tribunal Constitucional rechaza de plano la premisa según la cual el centro de trabajo no constituye, por definición, un espacio en el que se ejerza o pueda ejercerse el derecho a la intimidad por parte de los trabajadores.

547 STC 98/2000, de 10 de abril.

548 STS de 7 de julio de 1998.

549 Sentencia 104/2019, de 9 de abril, del Juzgado de lo Social nº 2 de Badajoz.

550 SSTC 99/1994, de 11 de abril; 156/2001, de 2 de julio; 72/2007, de 16 de abril y 77/2009, de 23 de marzo.

De este modo, para la determinación de la procedencia de la instalación de sistemas audiovisuales será preciso atender no sólo a las características concretas del centro de trabajo, sino también a otros elementos de juicio, tales como el hecho de si la instalación ha sido o no indiscriminada[551] o si han sido instalados de forma subrepticia[552] o cuál es la finalidad realmente perseguida, si existen razones objetivas de seguridad, etc. En definitiva, habrá que responder a la cuestión de si la instalación de tales sistemas de control audiovisual ha respondido o no a estrictos criterios de proporcionalidad.

2. En definitiva, la concreta ubicación espacial o física de las cámaras de video vigilancia ha dejado de ser el elemento primordial para la apreciación de la posible vulneración o no del derecho a la intimidad de los trabajadores, como se había considerado tradicionalmente[553], habiendo sido desplazado ese criterio por el juicio de las circunstancias del caso concreto a la luz ponderativa del juicio de proporcionalidad[554].

A tal efecto, el art. 89.3 de la referida Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, señala que la utilización de sistemas para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resultaren relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de

551 Vid. STEDH de 9 de enero de 2018 (caso López Ribalda *et alii* c. España).

552 En este sentido cabe citar la STS (Sala Social, Sección 1ª) de 13 de mayo de 2014, que entiende vulnerado el derecho a la intimidad de una trabajadora por la utilización de cámaras de video vigilancia instaladas como elemento disuasorio de hurtos de clientes por causa de la falta de información sobre la utilidad de supervisión laboral asociada a las capturas de imágenes de los trabajadores.

553 Recuérdese que la STSJ de Andalucía (Sevilla), de 17 de enero de 1994, estimó que la actuación del empresario no vulneró el derecho a la intimidad del trabajador por el mero hecho de quedar reducido el control sólo a las concretas dependencias de trabajo, sin afectar aquél a los espacios personales, de manera que la actividad de vigilancia a través de cámaras de video había resultado lícita.

554 FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial…, *op. cit.*, pág. I.63.

la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad y el de intervención mínima.

3. Por su parte, las pautas jurídico-prácticas en la materia ofrecidas por el Dictamen 2/2017 del Grupo de Trabajo del art. 29 (GT29), de 8 de junio de 2017, sobre el tratamiento de datos en el trabajo (complementario del Dictamen 8/2001 sobre el tratamiento de los datos personales en el contexto del empleo y del documento de trabajo de 2002 sobre la vigilancia de las comunicaciones electrónicas en el lugar de trabajo) cabe sintetizarlas del modo siguiente:

a) Debería exigirse una causa específica que legitime el dispositivo de vigilancia, sin que resulte suficiente el mero interés genérico al control de la prestación o la mera mejora de la productividad (ejemplo: el cumplimiento de una obligación legal por parte del empleador, como mejorar la seguridad del empleado –Informe AEPD 90/2009, en relación al personal de escolta-).

b) Obligación de evaluación previa de la necesidad específica de introducir este tipo de dispositivos, así como garantía de que, en todo caso, siempre resulte estrictamente adecuado a la finalidad y ponderado.

c) Obligación de información de calidad reforzada, intensificando el deber de información general, una vez aceptado que el consentimiento del trabajador aparece debilitado en el ámbito laboral (Informe AEPD 193/2008), centrándose la garantía en la información (Informe AEPD 613/2009). Así, no sólo debe ser previa, sino que habrá de formularse nítidamente a los empleados sobre los dispositivos de vigilancia instalados y sus finalidades, siempre específicas, no genéricas.

d) Limitación de datos susceptibles de ser recabados por este medio (Resolución AEPD E/742/2008).

e) Se recomienda la información a los representantes de los trabajadores, incluso el papel de la negociación colectiva, en relación a la información y demás garantías de este tipo de dispositivos de vigilancia.

3.1.- Jurisprudencia europea (TEDH).

1. La jurisprudencia europea en materia de video vigilancia viene constituida fundamentalmente por las SSTEDH (sección quinta) de 5 de octubre de 2010 (caso Köpke c. Alemania); la de 28 de noviembre de 2017 (caso Antovic y Mirkovic c. Montenegro) y las más recientes de 9 de enero de 2018 (caso López Ribalda *et alii* c. España I) y de 17 de octubre de 2019 (López Ribalda II), pudiendo extraerse de las mismas que para el TEDH la video vigilancia encubierta de un empleado en su lugar de trabajo sin motivo alguno constituye una intrusión en la vida privada del empleado, si bien la misma estaría justificada siempre que fuese una respuesta a una situación ilícita, previamente detectada, al objeto de lograr su comprobación y que la misma no se efectúe de manera indiscriminada, sino que deberá circunscribirse a un momento temporal y espacial concreto.

2. Asimismo, señala el TEDH en su sentencia de 28 de noviembre de 2017 (caso Antovic y Mirkovic c. Montenegro) que la video vigilancia de un empleado en el lugar de trabajo, sea encubierta o no, debe considerarse una intrusión considerable en la vida privada del empleado y, por consiguiente, considera que constituye una injerencia en el sentido del art. 8 CEDH dado que el profesor puede tener una expectativa de privacidad en el sentido de que normalmente puede esperar que lo que está sucediendo en el aula pueda ser seguido sólo por aquellos que tienen derecho a asistir a la clase y quien

realmente lo atiende. No hay "atención no deseada" de los demás, que no tienen nada que ver con la clase. Puede haber excepciones, por ejemplo, cuando una conferencia se graba con fines educativos, incluso para uso de estudiantes que no pudieron asistir físicamente a la clase.

Ahora bien, lo anterior no significa que la video vigilancia en un auditorio no sea posible, sino que pueden existir razones para poner un auditorio bajo video vigilancia. Pero, dado que el art. 8 CEDH es aplicable, tal medida deberá cumplir con las condiciones establecidas en el art. 8.2, lo que significa, entre otras cosas, que debe existir una base legal adecuada, que el alcance de la vigilancia debe ser limitado y que deben existir garantías contra el abuso (ver Vukota-Bojić c. Suiza, § 60, de 18 de octubre de 2016).

3.2.- Jurisprudencia constitucional.

3.2.1.- Primera etapa: admisión generalizada de mecanismos de control tecnológico (STC 142/1993, de 22 de abril).

1. Durante mucho tiempo, los tribunales admitieron la utilización de medidas de control empresarial de índole tecnológico con muy pocas reservas, bajo el entendido que el centro de trabajo constituía un lugar público en el que no cabía el ejercicio del derecho de intimidad, salvo en los espacios destinados al descanso o aseo personal[555].

A tal efecto, el Tribunal Constitucional en Sentencia 142/1993, de 22 de abril, llegó a señalar que la conexión de la intimidad con la libertad y la dignidad personal implica que la esfera de la inviolabilidad de la persona frente a

555 GUERRA RODRÍGUEZ, L., "Ejercicio del poder de control a través de cámaras de videovigilancia: análisis de la doctrina constitucional", *Trabajo y Derecho* 29/2017 (mayo), nº 29 de 1 de mayo de 2017, pag. 2.

injerencias externas - el ámbito personal y familiar - sólo en ocasiones tenga proyección hacia el exterior, por lo que no comprende, en principio, los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, las cuales están más allá del ámbito del espacio de intimidad personal y familiar sustraído al conocimiento e intromisiones de terceros[556].

La protección del derecho a la intimidad quedaba, pues, sujeta a un criterio meramente espacial, rigiendo una teoría contractualista según la cual los derechos fundamentales del trabajador debían ceder frente al poder de dirección del empresario en tanto que la formalización del contrato de trabajo mitigaba la posibilidad de su aplicación en el tiempo y en el lugar de trabajo[557].

3.2.2.- Segunda etapa: admisión del principio de proporcionalidad (SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio).

1. La doctrina reseñada en el punto anterior fue desautorizada por el Tribunal Constitucional a través de dos importantes sentencias: la 98/2000, de 10 de abril y la 186/2000, de 10 de julio. Estas dos sentencias establecieron los principales criterios interpretativos en la materia, viniendo a introducir posteriormente importantes correcciones, respecto de sus conclusiones, la sentencia 29/2013, de 11 de febrero y, más recientemente, la sentencia

556 En línea con lo establecido en la STC142/1993, de 22 de abril , la STSJ de Cataluña de 25 de abril de 1994 admitió la instalación de un circuito cerrado de televisión con sistema de grabación de imagen y sonido en múltiples espacios del centro de trabajo tras considerar que entender que la medida vulnera el derecho a la intimidad *"(...) supondría extender la protección de tales derechos a instalaciones que suponen la práctica totalidad de espacios públicos del hotel en el que éste presta sus servicios a los clientes y, en consecuencia, donde los trabajadores desarrollan su actividad. La intimidad de éstos no resulta agredida por el solo hecho de que ésta sea objeto de filmación, pues no se trata de divulgar su conducta, sino de obtener un conocimiento de cuál es su comportamiento laboral".*

En la misma línea, la STSJ de Galicia de 25 de enero de 1996 señaló que *"(...) ha de partirse de una premisa básica, cual es que el centro de trabajo no constituye, por definición, un espacio en el que se ejerza el derecho a la intimidad por parte de los trabajadores".*

557 FABREGAT MONFORT, G., "El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave", *Trabajo y Derecho*, nº 5, 2015, pág. 2.

39/2016, de 3 de marzo. No obstante, debe tenerse en cuenta que en las dos primeras el conflicto se plantea exclusivamente desde la perspectiva del derecho a la intimidad (art. 18.1 CE), quedando al margen del debate el derecho a la autodeterminación informativa que se integra en el derecho a la protección de los datos personales, que es, justamente, el que tuvo en cuenta la sentencia 29/2013, de 11 de febrero.

2. La STC 98/2000, de 10 de abril resuelve el supuesto de la utilización en un casino - Casino de la Toja - de micrófonos en determinadas zonas del centro de trabajo (secciones de caja y ruleta francesa) donde eran grabadas las conversaciones de los trabajadores. La sentencia estimó el recurso de amparo, reconociendo la vulneración del derecho a la intimidad del trabajador recurrente, sin admitir que la actuación de la empresa tuviera en el caso concreto amparo en las facultades de vigilancia y control reconocidas al empresario en el art. 20.3 ET.

Aunque el caso se refiere a la grabación de sonido (no de imágenes), sin embargo, la doctrina que establece tiene alcance general en la fijación de criterios en la resolución de los conflictos que puedan producirse entre los medios de control utilizados por los empresarios y los derechos fundamentales de los trabajadores. De hecho, la STC 186/2000, de 10 de julio - que sí resuelve el caso de un despido disciplinario en el que se utiliza como prueba de cargo las grabaciones de video vigilancia[558]- se funda precisamente en esos criterios aplicativos y en la doctrina establecida por la STC 98/2000, de 10 de abril[559].

558 Sobre videovigilancia, véase BAUZA MARTORELL, F. J., *Régimen jurídico de la videovigilancia*, Marcial Pons, Madrid, 2004; FERNÁNDEZ DIEZ, A.: "Control de la actividad laboral a través de un circuito cerrado de televisión", *Información Laboral*, nº 7, 2000; LÓPEZ PARADA, R., "Análisis jurisprudencial acerca de la instalación por el empresario de sistemas de videovigilancia en lugares de trabajo", *Información Laboral*, nº 9, 1999; THIBAULT ARANDA, J., *Control multimedia de la actividad laboral*, Tirant lo Blanch, Valencia, 2006.

559 ESCRIBANO GUTIÉRREZ, J., "El derecho a la intimidad del trabajador. A propósito de la Sentencia del Tribunal Constitucional 186/2000, de 10 de julio", *Relaciones Laborales*, t. I, 2001.

Los criterios establecidos por esta sentencia en orden a la resolución de los conflictos entre el derecho a la intimidad y las medidas de control de la actividad laboral adoptadas por los empresarios son los siguientes:

i) Las facultades empresariales de control que incidan en el derecho fundamental sólo pueden derivar bien de la circunstancia de que la naturaleza del trabajo convenido implicare la restricción del derecho, bien de un acreditado interés o necesidad empresarial, sin que resulte suficiente a estos efectos su mera invocación para poder sacrificar el derecho fundamental del trabajador.

ii) El ejercicio de las facultades de organización y control del empresario no puede conducir, en ningún caso, a la producción de resultados inconstitucionales lesivos para los derechos fundamentales de los trabajadores.

iii) La necesidad de preservar el adecuado equilibrio entre las obligaciones derivadas del contrato del contrato de trabajo y el ámbito de la libertad constitucional del trabajador.

iv) Las limitaciones o modulaciones de los derechos fundamentales del trabajador habrán de ser las estrictamente indispensables en orden a la satisfacción de un interés empresarial que fuere merecedor, asimismo, de tutela y protección, de manera que si existieren otras posibilidades de satisfacción de dicho interés que fueren menos gravosas para el derecho en cuestión, habrá que emplear estas últimas.

En el caso enjuiciado se estimó el amparo, anulándose las sentencias dictadas en el orden social, bajo el entendimiento de que la instalación de los micrófonos que permitían la grabación de conversaciones de trabajadores y clientes en determinadas zonas del casino no se ajustaba a las necesarias

exigencias de respeto a la intimidad ni a los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales.

Aunque la instalación de aparatos de grabación del sonido en dos zonas concretas del casino -la caja y la ruleta francesa- fuesen de utilidad para la empresa, la mera conveniencia para ésta no legitima sin más su instalación toda vez que el casino ya disponía de otros sistemas de seguridad, no habiendo quedado acreditado que la instalación del sistema de grabación de sonidos fuese indispensable para la seguridad y el buen funcionamiento de aquél.

Concluye el Tribunal señalando que el uso de un sistema de audición indiscriminado de todo tipo de conversaciones, incluidas las de carácter privado - ajenas por completo al interés empresarial - tanto de los trabajadores como de los clientes, constituye una actuación que rebasa notablemente las facultades de control que el art. 20.3 ET otorga al empresario, suponiendo aquél una intromisión ilegítima en el derecho a la intimidad.

3. En definitiva, en la STC 98/2000, de 10 de abril, el Tribunal descartó que el ejercicio del derecho a la intimidad en el ámbito de las relaciones laborales se limite solamente a ciertos espacios físicos donde no se desarrollan tareas profesionales, reconociéndose su aplicación de manera genérica en el lugar de trabajo.

Así, tras reconocer que la instalación de tales medios en lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos resulta lesiva para el derecho a la intimidad de los trabajadores, señaló que ello no significa que esa lesión no pueda producirse también en aquellos lugares donde se realiza la actividad laboral, debiéndose atender a las circunstancias del caso concreto en orden a la determinación de esta posibilidad, siendo, entre otros, los elementos de juicio a tomar en consideración el carácter masivo e

indiscriminado de la instalación de los mecanismos tecnológicos de control, la comunicación sobre la existencia de los mismos a los afectados, la presencia de razones de seguridad vinculadas al tipo de actividad desarrollada, descartándose como tal la mera utilidad o conveniencia.

De este modo, la STC 98/2000, de 10 de abril, reafirmó la vigencia de los derechos laborales inespecíficos, sosteniendo que la celebración de un contrato de trabajo no priva al trabajador en ningún caso de los derechos fundamentales que le corresponden como ciudadano, por más que en ocasiones su ejercicio pueda sufrir justificadas modulaciones, si bien éstas tienen que ser, como ha quedado dicho, las estrictamente indispensables para satisfacer un interés empresarial merecedor de tutela y protección, de forma que si existen otras posibilidades de satisfacer dicho interés menos agresivas para el derecho en cuestión, habrá que emplear estas últimas.

4. Por su parte, la segunda Sentencia a tener en cuenta - STC 186/2000, de 10 de julio - sí se enfrenta a un despido disciplinario en el que se imputa al trabajador la sustracción de dinero de la caja de un economato, habiendo utilizado la empresa para acreditar la conducta las grabaciones del sistema de video vigilancia que instaló para comprobar sus sospechas.

En concreto, el trabajador afectado prestaba servicios como cajero del economato de su empresa (ENSIDESA) y, como consecuencia de un descuadre importante en la caja de dicho economato, la empresa contrató con una empresa de seguridad la instalación de un circuito cerrado de televisión enfocando únicamente a las cajas registradoras y al mostrador de paso de las mercancías. Como consecuencia de la vigilancia realizada en diferentes fechas entre los meses de abril y mayo de 1995 se acordó el despido del trabajador recurrente en amparo dado que las grabaciones efectuadas revelaron que éste efectuó reiteradamente diferentes maniobras en el cobro de diversos artículos a los clientes del economato sustrayendo varias cantidades de la caja de éste.

Los Tribunales declararon procedente el despido no apreciando vulneración alguna del derecho a la intimidad del trabajador derivada de la instalación de las cámaras de vigilancia. Por su parte, el TC desestimó el recurso de amparo considerando que en este caso se respetó por la empresa el derecho fundamental del trabajador y que las pruebas video gráficas eran válidas. Reitera la doctrina de la STC 98/2000, de 10 de julio y fija como principios esenciales a tener en cuenta los siguientes:

i) El derecho a la intimidad resulta de aplicación al ámbito de las relaciones laborales, si bien no es un derecho ilimitado o absoluto, sino que el mismo puede ceder ante intereses constitucionalmente relevantes siempre que la limitación que aquél hubiere de experimentar se revelare como necesaria para lograr el fin legítimo previsto, fuere proporcionada para alcanzarlo y, en todo caso, sea respetuosa con el contenido esencial del derecho[560].

ii) El poder directivo empresarial, reconocido en el art. 20.3 ET, atribuye al empresario la facultad de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por parte del trabajador de sus obligaciones y deberes laborales, respetando, en todo caso, la dignidad de éste (arts. 4.2.c) y 20.3 ET).

iii) El empresario no está facultado para llevar a cabo, so pretexto de las facultades de vigilancia y control del art. 20.3 ET, intromisiones ilegítimas en la intimidad de sus trabajadores.

iv) La constitucionalidad de cualesquiera medidas restrictivas de derechos fundamentales vendrá siempre determinada por la estricta observancia del principio de proporcionalidad.

560 SSTC 57/1994, de 28 de febrero y 143/1994, de 9 de mayo.

v) En orden a la comprobación de si una concreta medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, resulta necesario constatar si cumple los tres requisitos siguientes: i) que la medida sea susceptible de alcanzar el objetivo propuesto (juicio de idoneidad); ii) que, además, sea necesaria, en el sentido de que no exista otra medida menos gravosa, de igual o similar eficacia, para la consecución de tal propósito (juicio de necesidad); y, finalmente, iii) que la misma sea ponderada o 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)[561].

Para la STC 186/2000, de 10 de julio, se cumplieron las condiciones para la validez de la prueba video gráfica, descartando que se hubiera producido lesión alguna del derecho a la intimidad personal y a la propia imagen, afirmando que la instalación del circuito cerrado de televisión fue una medida justificada por existir razonables sospechas de la comisión de graves irregularidades por parte del trabajador; idónea para la finalidad perseguida por la empresa, cual era la de verificar si aquél cometía efectivamente las irregularidades sospechadas para, en tal caso, proceder a la adopción de las medidas disciplinarias pertinentes; necesaria, ya que la grabación serviría de prueba de dichas irregularidades; y, finalmente, equilibrada, dado que la grabación de imágenes se limitó a la zona de caja, teniendo la misma una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada en el tiempo.

Destaca, además, de forma especial que en este caso la medida no obedeció al propósito de vigilar y controlar genéricamente el cumplimiento por parte de los trabajadores de sus obligaciones laborales, a diferencia del caso resuelto en la STC 98/2000, de 10 de abril, en el que la empresa, existiendo un

561 SSTC 66/1995, de 8 de mayo; 55/1996, de 28 de marzo; 207/1996, de 16 de diciembre y 37/1998, de 17 de febrero.

sistema de grabación de imágenes, decidió instalar un sistema de grabación de sonido adicional para mayor seguridad, sin que quedase acreditado ni que el nuevo sistema se instalase tras haberse detectado una quiebra en los sistemas de seguridad ya existentes ni que el mismo resultase indispensable para la seguridad del casino. Por el contrario, en el caso que resuelve la STC 186/2000, de 10 de julio, previamente se había detectado un importante descuadre contable, y se adoptó la medida de vigilancia de modo que las cámaras únicamente grabaran las cajas registradoras.

5. En resumen, cabe señalar que de la doctrina que se establece en las SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio, se infiere que la capacidad de control del empresario no es ilimitada y que, en aquellos casos en los que exista una posible colisión con el derecho a la intimidad, deben ponderarse los intereses en juego en función de los siguientes principios: a) justificación, b) idoneidad; c) necesidad; d) proporcionalidad y e) mínima intervención respecto a las garantías reconocidas en el art. 18.1 CE.

4.- La utilización del correo electrónico para fines extra laborales y la proporcionalidad en su control.

1. Como es sabido, el correo electrónico es una herramienta de trabajo que permite notables ventajas en orden a la mejora de la productividad, al tiempo que facilita la comunicación entre los trabajadores entre sí y con terceros ajenos a la empresa. Ahora bien, un uso desviado de dicha herramienta puede ser causa de perjuicios de índole económica para la empresa, de modo que el control de cualquier extralimitación en el uso de aquélla resulta de suma utilidad en el marco del poder de vigilancia y control del empresario.

2. No obstante, la cuestión radica en determinar hasta qué punto esa injerencia colisiona frontalmente con el derecho a la intimidad del trabajador o

con el derecho al secreto de las comunicaciones[562], dado que junto al uso laboral se suele producir un uso personal de las herramientas informáticas, sin perjuicio de que llegue a producirse dicho control incluso sobre terceros ajenos – clientes o proveedores - a la relación laboral que entran, a través de dichos medios, en contacto o comunicación con los trabajadores[563].

Y es que como afirmó el TEDH en su Sentencia de 3 de abril de 2007, (caso Copland c. Reino Unido), *"los correos electrónicos enviados desde el lugar del trabajo están incluidos en el ámbito de protección del art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las libertades fundamentales, por cuanto pueden contener datos sensibles que afecten a la intimidad y al respeto de la vida privada del trabajador"*.

3. Llegados a este punto, se ha de señalar que no sólo la información juega un papel fundamental como se ha visto en el capítulo anterior, sino que el juicio de proporcionalidad se convierte en factor determinante en la valoración de hipotéticas vulneraciones de los derechos fundamentales de los trabajadores, en cuya virtud el control ha de ejecutarse siempre de modo proporcional a la finalidad perseguida para que pueda superarse el triple test de proporcionalidad aludido en el epígrafe anterior[564].

Es por ello que resulta conveniente emplear medios que no se centren en el análisis del contenido del correo electrónico, prefiriéndose, por el contrario, el control de elementos adyacentes o circunstanciales del mismo,

562 Véase ALGAR JIMÉNEZ, C., "El Derecho laboral ante el reto de las nuevas tecnologías", *Difusión jurídica y temas de actualidad*, Madrid, 2007, págs. 45-49.

563 DESDENTADO BONETE, A. Y MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, pág. 139.

564 SEGOVIANO ASTABURUAGA, M. L., "El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores", *Revista jurídica de Castilla y León*, núm. 2, 2004, págs. 159-161.

tales como el destinatario del mensaje, su asunto o el número y frecuencia de mensajes enviados[565].

En este sentido, se ha de señalar que entre los sistemas de control existentes hoy día en el mercado se pueden encontrar programas de monitorización que permiten saber en tiempo real las páginas web visitadas, la duración de la conexión y la frecuencia de las visitas; cortafuegos que impiden el acceso a determinadas páginas y *sniffers* que, instalados en el servidor, alertan sobre lo que el trabajador realiza en la jornada laboral[566], sin necesidad de tener que penetrar en el contenido del correo electrónico, de modo que la regla de la proporcionalidad –con sus tres premisas de adecuación, necesidad y proporcionalidad en sentido estricto -, exige que se haya de optar por un control indirecto referido a la frecuencia y al tiempo de conexión a sitios web no autorizados, por ser ajenos a los intereses profesionales, antes que el control del contenido de las páginas visitadas[567].

4. En este sentido, la STEDH de 5 de septiembre de 2017 (Barbulescu II) recupera en sus verdaderos términos el principio de proporcionalidad en orden a la evaluación de la licitud del control empresarial y, con ello, un canon de enjuiciamiento más equilibrado al objeto de ponderar el conflicto entre los derechos fundamentales del trabajador y las facultades del poder empresarial.

Así, en orden a la valoración de la posible restricción del ejercicio del derecho fundamental del trabajador por la vigilancia del empresario exige que éste proporcione previamente un motivo legítimo que justifique la vigilancia de las comunicaciones y el control de su contenido, esto es, que exista una

565 THIBAULT ARANDA, J., *Control multimedia de la actividad laboral*, Tirant lo Blanch, Valencia, 2006.

566 Véase RODRÍGUEZ ESCANCIANO, S., Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores, Tirant lo Blanch, Valencia, 2015, pág. 86.

567 ROIG BATALLA, A., *Derechos Fundamentales y Tecnologías de la Información y de las Comunicaciones (TICs)*, Bosch, 2011, págs. 22-24.

verdadera adecuación entre el motivo del control y la limitación que sufra el derecho a la vida privada o a la correspondencia del trabajador. Condición ésta que choca frontalmente con la tesis del Tribunal Constitucional según la cual *"los grados de intensidad o de rigidez con que deben ser valoradas y aplicadas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario para tal fin"*.

Por otro lado, requiere que la vigilancia haya de ser idónea, es decir, obliga a determinar si hubiera sido posible utilizar un sistema de control menos invasivo para el derecho fundamental de que se trate, de modo que habrá de valorarse si es necesario e idóneo acceder al contenido de las comunicaciones o bastará con un mero informe de la frecuencia de las mismas, obviamente menos intrusivo.

En todo caso, como insiste el TEDH, teniendo en cuenta que el acceso al contenido de las comunicaciones es siempre el acto más invasivo de los derechos de vida privada y correspondencia, se necesita una justificación más fuerte o más fundamentada, de donde cabe interpretar que la intensidad de la vigilancia permitida dependerá del carácter defensivo o preventivo de la misma. En suma, deberá tenerse en consideración cuáles han sido las consecuencias de la vigilancia para el trabajador a efectos de valorar los sacrificios innecesarios o excesivos de los derechos fundamentales y descartar las conductas de vigilancia o control empresarial más agresivas a los derechos de vida privada y correspondencia.

De conformidad, pues, con la doctrina sentada por la Gran Sala en la sentencia Barbulescu II, la expectativa del derecho a la intimidad y a la confidencialidad en las comunicaciones deja de depender exclusivamente de las órdenes impartidas por el empresario y de su prohibición para usos

extralaborales para situar el centro de atención y valoración en la previa información al trabajador, que requiere de un aviso suficiente y claro en relación con las políticas de uso , así como sobre los controles que se vayan a realizar y de los posibles medios que se emplearán en los mismos.

Con ello, la sentencia referida enmarca la forma de enfocar el conflicto desde una metodología más equilibrada y racional en la valoración de los derechos fundamentales del trabajador que se aleja de la perspectiva contractual que ha venido utilizando hasta ahora el Tribunal Constitucional.

Asimismo, en consonancia con lo anterior, marca las pautas a la hora de ponderar los intereses en conflicto que descansa en el test de proporcionalidad y que comporta un análisis detallado desde la perspectiva de la idoneidad, necesidad y proporcionalidad en sentido estricto en relación con el objetivo perseguido con la vigilancia.

5. Volviendo al contexto de confrontación de derechos en sede internacional, que versa sobre la aplicación del art. 8 CEDH, el TEDH nos proporciona un protocolo de actuación a modo de preguntas *check-list* o lista de comprobaciones denominado por la doctrina *test Barbulescu*. En este sentido, Eduardo Rojo[568] sintetiza el manual de instrucción que todo tribunal deberá seguir para comprobar que no se ha vulnerado el derecho a la vida privada - incluida la privacidad de la correspondencia - del trabajador en el ámbito de su relación laboral del siguiente modo:

- ¿Se ha informado al trabajador acerca de la posibilidad de que el empresario tome medidas para controlar su correspondencia y otras

568 ROJO TORRECILLA, E., "De Barbulescu I a Barbulescu II. La Gran Sala del TEDH refuerza la protección del trabajador frente al control y vigilancia de las comunicaciones electrónicas en el ámbito laboral por parte empresarial", http://www.eduardorojotorrecilla.es/2017/09/de-barbulescu-i-barbulescu-ii-la-gran.html Notas a la importante sentencia de 5 de septiembre de 2017, y amplio recordatorio de la sentencia de la Sala Cuarta de 12 de enero de 2016.

comunicaciones? En este sentido hay que aclarar que para respetar el art. 8 del CEDH la información *"debe, en principio, ser clara en cuanto a la naturaleza de la vigilancia y anterior a su puesta en práctica"*.

- ¿Cuál fue el alcance de la vigilancia llevada a cabo por el empresario y el grado de intromisión en la vida privada del trabajador? No es lo mismo que el control se haga del número de comunicaciones que hacerla de sus contenidos; o que se hayan controlado todos o sólo una parte de los correos, así como durante cuánto tiempo se llevó a cabo el control y el número de personas han podido acceder al contenido de tales informaciones.

- ¿Han existido motivos legítimos, debidamente acreditados por el empleador, para justificar la vigilancia y el acceso a los contenidos de las comunicaciones? Razona el Tribunal la proporcionalidad de la medida recordando que, *"dado que la vigilancia del contenido de las comunicaciones es por su naturaleza un método mucho más invasivo, el Tribunal exige justificaciones más fundamentadas"*.

- ¿Habría sido posible establecer un sistema de control y vigilancia basado en medios menos intrusivos que el acceso directo al contenido de las comunicaciones? A este respecto, recuerda la sentencia que *"es necesario evaluar, en función de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario puede alcanzarse sin que éste tenga pleno y directo acceso al contenido de las comunicaciones del empleado"*.

- ¿Qué consecuencias ha tenido para el trabajador la vigilancia llevada a cabo por el empresario? Es decir, cómo se ha utilizado por éste la

información obtenida y si ha sido útil para alcanzar el objetivo perseguido.

- ¿Cuáles son las garantías de que ha dispuesto el trabajador en los casos en que la vigilancia tiene un evidente carácter de intromisión? Nuevamente la doctrina de la Gran Sala del TEDH es nítida al respecto con la finalidad de proteger la privacidad del trabajador: las garantías habrán de ser de tal calibre que impidan que el empresario pueda tener acceso al contenido de las comunicaciones cuya litigiosidad está en juego antes de que el trabajador haya sido advertido de tal posibilidad.

Es, pues, conveniente, si en algún momento se pretende acceder, justificadamente, a alguno de los medios telemáticos puestos a disposición de los trabajadores por parte de la empresa, aplicar este test y saber que un análisis interno previo a la intromisión es de vital importancia para asegurar el buen fin del procedimiento[569].

569 SÁNCHEZ DEL OLMO, V., "El impacto (divergente) de la doctrina Barbulescu en las resoluciones de instancia. Comentarios a las sentencias 341/2017 y 737/2017 de los Juzgados de lo Social de Madrid nº 19 y nº 33", *Trabajo y Derecho,* nº 45, 1 de septiembre de 2018, pág. 2.

VI.- CONCLUSIONES.

PRIMERA.- Tanto la jurisprudencia del TEDH como del TC y del TS delimitan los casos en los que el acceso a datos privados constituye una injerencia en el derecho al respeto de la vida privada y familiar atendiendo a la existencia o no en el caso concreto de una expectativa razonable de privacidad por parte del trabajador, pudiendo el empresario limitar dicha expectativa de confidencialidad mediante el establecimiento de reglas de uso de los equipos informáticos de la empresa que determinen si está permitido o no el uso privado y las medidas de control que aplicará.

SEGUNDA.- En caso de que el trabajador prestare su consentimiento para que el empresario pudiera acceder a los contenidos relacionados con su actividad informática que tuviesen carácter personal y reservado, el derecho a la intimidad del trabajador no resultaría afectado siempre que se cumplieran los siguientes requisitos: i) el trabajador estuviera informado previamente del alcance y la finalidad de la investigación que el empresario pretendiese realizar; ii) que el trabajador prestare su consentimiento de modo expreso a la investigación con los referidos alcance y finalidad; y iii) que la investigación no exceda del alcance indicado ni los resultados se usen para una finalidad distinta de aquella para la que el trabajador prestó su consentimiento.

TERCERA.- No obstante, el TEDH no excluye la posibilidad de que puedan realizarse determinados controles “necesarios en una sociedad democrática” y, por tanto, lícitos, sobre el uso que hacen los trabajadores del teléfono, del correo electrónico o de Internet en la empresa, si bien, será necesario para ello que la empresa haya establecido previamente reglas de utilización de los medios tecnológicos en orden a poder eliminar cualquier expectativa de intimidad, secreto o confidencialidad que pudiera tener el trabajador y hubiere informado expresamente de las mismas a los trabajadores.

CUARTA.- El TEDH entiende que, incluso cuando las normas del empleador con respecto a la vida social privada de los empleados en el lugar de trabajo sean restrictivas, éste no puede reducirse en ningún caso a cero, teniendo el Estado la obligación positiva (obligación de hacer) de procurar que se respete la vida privada de los empleados en el seno de la empresa (caso Bărbulescu c. Rumanía), recordando el TEDH que sea el legislador quien cumpla con esa obligación positiva mediante la fijación del marco normativo que determine la protección de los diversos intereses en juego y, en defecto de regulación legal, corresponde a los órganos judiciales nacionales asegurar que la adopción empresarial de medidas de vigilancia de la correspondencia y de otras comunicaciones se efectúe con las garantías adecuadas y suficientes contra los abusos y las arbitrariedades.

QUINTA.- La última jurisprudencia del Tribunal Constitucional referida al secreto de las comunicaciones en el seno de la empresa se adentra por una senda en la que la ponderación de derechos se desvanece a favor de un criterio maximalista que exacerba el poder de dirección del empresario.

Las SSTC 241/2012, de 17 de diciembre y 170/2013, de 7 de octubre (casos Trillian y Alcaliber, respectivamente), sitúan la intervención empresarial en las comunicaciones electrónicas en el marco de las facultades de auto-organización, dirección y control empresariales *ex* art. 20.3 ET, de modo que para el TC la expectativa de confidencialidad del trabajador respecto de sus comunicaciones se determina en función de las instrucciones que hayan podido ser impartidas por el empresario a tal fin, de forma que si no existe una situación de tolerancia al uso personal del ordenador no puede existir una expectativa razonable de confidencialidad. O, dicho de otro modo, si existiere prohibición expresa al respecto, la empresa podría vigilar el correo electrónico corporativo de sus trabajadores.

SEXTA.- El acceso a un correo electrónico que no haya sido leído por su destinatario, con independencia del concreto momento del proceso comunicativo en que se encuentre - ya estuviere escrito y almacenado en el ordenador personal o en el terminal telefónico pendiente de ser enviado a su destinatario final o enviado y recibido, hubiere sido o no leído por el destinatario -, pero siempre durante dicho proceso, supone una injerencia en el secreto de las comunicaciones. Y lo mismo sucede con los mensajes almacenados en la carpeta de "enviados" una vez remitidos a su destinatario, respecto de los cuales se predica que los mismos forman parte de un proceso de comunicación ya iniciado, de modo que el acceso a los mismos compromete el derecho al secreto de las comunicaciones.

SÉPTIMA.- El Tribunal Constitucional ha llegado a sostener en diferentes sentencias que, finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza a través de las normas que tutelan el derecho a la intimidad u otros derechos y no a través del secreto de las comunicaciones. No obstante, cabe señalar la existencia de demasiadas contradicciones en la jurisprudencia del Tribunal Constitucional referente al tema en cuestión como para sostener que el derecho al secreto de las comunicaciones protege a éstas de su interceptación única y exclusivamente mientras exista un proceso de comunicación en curso, de modo que el hecho de que el acceso al mensaje protegido haya tenido lugar una vez concluso el proceso comunicativo no excluye de por sí que la fuente de conocimiento del contenido del mismo se haya obtenido mediante la interceptación de la comunicación en su discurrir a través del servicio que la conduce a su destino. Si así fuere hay que entender violado el derecho al secreto de las comunicaciones pese a que el acceso a lo comunicado tuviere lugar tras la recepción del mensaje por el destinatario.

OCTAVA.- La exigencia de previsión legal de las medidas de injerencia en la privacidad del trabajador prevista en el art. 8 del Convenio de Roma ha sido detallada por la jurisprudencia del TEDH, pudiendo deducirse que la misma

encierra tres requisitos: i) la existencia de una base en el derecho interno; ii) la accesibilidad de la ley para la persona implicada y iii) la previsibilidad de la ley en cuanto al sentido y la naturaleza de las medidas aplicables (calidad de la ley).

NOVENA.- En punto a la normativa laboral, lo primero que se advierte en clave jurídica es que, a falta de regulación en convenio colectivo o en normativa interna, el ordenamiento jurídico español carece de una norma que expresamente contemple y regule el conflicto de intereses entre trabajador y empresario subyacente a las situaciones que nos ocupan, como sucede, sin embargo, con el registro operado en la persona del trabajador, su taquilla y efectos particulares, el cual está pormenorizadamente regulado en el art. 18 ET. La regulación contenida en el art. 20.3 ET se revela, por sí sola, insuficiente para evitar arbitrariedades, quedando sometido el trabajador a la incertidumbre de desconocer qué aspectos de su vida privada son conocidos, grabados y conservados o cedidos y tratados, considerándose la misma como un instituto jurídico muy limitado para dar respuesta satisfactoria a los nuevos retos planteados por las TIC.

DÉCIMA.- Las garantías del art. 18 ET no resultan aplicables a los supuestos de control de los medios informáticos facilitados a los trabajadores para la ejecución de su prestación laboral por mor de lo establecido en la STS de 26 de septiembre de 2007, que entiende que el supuesto regulado por el art. 18 ET es completamente distinto del que se produce con ocasión del control de los medios informáticos en el trabajo, considerando éstos de propiedad de la empresa, la cual los facilita al trabajador para el cumplimiento de la prestación laboral, por lo que su uso queda dentro del ámbito del poder de vigilancia del empresario contemplado en el art. 20.3 ET y no por el art. 18 del mismo cuerpo legal.

DECIMOPRIMERA.- Un análisis de la normativa paccionada nos permite la identificación de cuatro grandes contenidos de convenios: i) un primer grupo de convenios incluyen una regulación de la materia, si bien referida principalmente a la utilización de las TIC con fines sindicales; ii) un segundo grupo norma el uso de las TIC en el seno de la empresa para uso personal, si bien lo hace utilizando fórmulas abiertas, carentes de seguridad jurídica al objeto de evitar posibles conflictos; iii) un tercer grupo, minoritario, destaca por ofrecer un modelo de regulación detallada del uso de las TIC en el seno de la empresa. Se trata, generalmente, de convenios de empresa; iv) y, por último, un cuarto conjunto que regula el fenómeno solamente desde un plano meramente sancionador mediante su inclusión en el catálogo de faltas laborales.

DECIMOSEGUNDA.- El estado del arte de la jurisprudencia relativo a la interpretación y aplicación a las relaciones de trabajo del secreto de las comunicaciones presenta una seria fractura, contrastando de manera frontal dos normas en el Derecho vigente, a saber: (i) el plus de tutela constitucional que recibe ex art. 18.3 CE (el derecho al secreto de las comunicaciones no tendrá más límite que el de la autorización judicial) con (ii) el vaciamiento práctico de la garantía del contenido esencial del derecho del art. 18.3 CE en la relación laboral operado tanto por el TC como por el TS en el sentido de reformular el mandato constitucional hacia una mutación del siguiente tenor: el derecho en cuestión estará limitado por el ámbito que, en cada caso, configure el poder de vigilancia y control del empresario conforme al art. 20.3 ET, bien de manera unilateral (Código de Conducta), bien de forma convencional (Convenio colectivo).

DECIMOTERCERA.- La sentencia de la Sala II del TS de 23 de octubre de 2018 parece sostener que cuando se trate de aportar a un proceso penal pruebas contra un trabajador obtenidas de la supervisión del contenido del correo electrónico de éste, las mismas habrán de ser obtenidas mediando autorización judicial o, en su caso, consentimiento expreso del trabajador. Sin

embargo, no se pronuncia (por no ser objeto de su jurisdicción) acerca de la necesidad o no de autorización judicial en el marco de un proceso laboral.

DECIMOCUARTA.- Pesa sobre el empresario el deber de información previo al trabajador acerca de la vigilancia de su correspondencia electrónica y otro tipo de comunicaciones, así como de la concreta puesta en marcha de las medidas al respecto, información que, por lo demás, habrá de ser expresa, precisa y concreta, debiendo los jueces nacionales examinar si el trabajador ha sido informado previamente de la posibilidad de que el empresario aplique medidas de control de las comunicaciones.

No obstante, la STEDH de 17 de octubre de 2019 (López Ribalda II) relativiza el deber de información del empresario caracterizándolo como un componente más del juicio de proporcionalidad, señalando que son válidos los controles ocultos a los trabajadores mediante video vigilancia, pero nunca ante la más mínima sospecha de apropiación indebida o de cualquier otro delito por parte de los empleados, sino sólo en supuestos en que hubiere sospechas razonables de que se hubiere cometido una infracción grave con perjuicio importante para la empresa.

DECIMOQUINTA.- No obstante, la concreta ubicación física de las cámaras ha dejado de ser el elemento determinante para apreciar vulneración o no del derecho a la intimidad de los trabajadores, como se había considerado tradicionalmente. Ese criterio ha sido desplazado por la valoración de las circunstancias del caso concreto llevado a cabo a través del pertinente juicio de proporcionalidad. A tal efecto, la utilización de sistemas para la grabación de sonidos en el lugar de trabajo será admitida únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad y el de intervención mínima.

No obstante, bajo ningún concepto se podrá admitir la instalación de sistemas de grabación de sonidos ni de video vigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos por ser ajenos a la prestación laboral.

DECIMOSEXTA.- El principio de proporcionalidad viene sufriendo en la práctica judicial un proceso de erosión importante motivado por el hecho de que los tribunales adoptan un sentido bastante laxo del término idoneidad, independiente del juicio previo sobre la legitimidad del interés empresarial de control, lo que pone de manifiesto que el juicio de proporcionalidad resulta insuficiente para delimitar el poder de control del empresario ejercido a través de los medios tecnológicos, pasando a ser el derecho a la protección de datos, o el derecho a ser informado de quién posee sus datos personales y con qué finalidad, el derecho clave en el poder de control del empresario derivado de las nuevas tecnologías de la información.

DECIMOSÈPTIMA.- La STEDH de 5 de septiembre de 2017 (Barbulescu II) señala a los tribunales la necesidad de hacer un ejercicio riguroso del control de la proporcionalidad, que deberá modularse en función de la intensidad del control empresarial, para lo cual resultará determinante valorar si se accede al contenido de los mensajes, así como determinar la amplitud de las comunicaciones sometidas a vigilancia, la duración del control o el número de personas que tienen acceso a los resultados. Asimismo, los controles que supongan un acceso por parte del empresario al contenido de las comunicaciones deberán ser sometidos a un control de proporcionalidad más intenso, así como también habrá de someterse a ponderación la severidad de las medidas disciplinarias adoptadas por el empresario.

Por otro lado, se impone también la obligación de ponderar la necesidad y el alcance efectivo de la vigilancia realizada por el empresario poniendo en

relación la finalidad pretendida con los medios utilizados para alcanzarlos, de forma que será necesario determinar si hubiera sido posible el empleo de medidas menos intrusivas al efecto. De igual modo, se habrá de tener en cuenta cuáles han sido las consecuencias de la vigilancia para el trabajador.

BIBLIOGRAFIA.

ABEL LLUCH, X., "Repensando el concepto de documento", *Diario La Ley* núm. 7667, 2011.

ABERASTURI GORRIÑO, U., "Control empresarial del correo electrónico del empleado y relevancia de la información previa a los trabajadores como garantía mínima para ejercer ese control a la luz de la STC de 7 de octubre de 2013", *Nueva revista española de Derecho del Trabajo*, nº 180, 2015.

AGUT GARCÍA, C., "Las facultades empresariales de vigilancia y control sobre útiles y herramientas de trabajo y otros efectos de la empresa", *Tribuna Social*, nº 163, 2004.

ALARCÓN CARACUEL, M. R., "La informatización y las nuevas formas de trabajo", en Alarcón Caracuel, M. R. y Esteban Legarreta, R. (Coords.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004.

ALEXY, R., *Teoría de los derechos fundamentales* (trad.: E. Garzón Valdés), Centro de Estudios Constitucionales, Madrid, 1993.

ALGAR JIMÉNEZ, C., "El Derecho laboral ante el reto de las nuevas tecnologías", *Difusión jurídica y temas de actualidad*, Madrid, 2007.

ALONSO GARCÍA, E., *La interpretación de la Constitución*, CEC, Madrid 1984.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. Mª, "La libertad informática, un nuevo derecho fundamental en nuestra Constitución", *La Ley*, núm. 5230, 22 enero 2001.

- *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona, 1999.

APARICIO ALDANA, R. K., *Derecho a la intimidad y a la propia imagen en las relaciones jurídico laborales*, Thomson Reuters Aranzadi, Cizur Menor, Pamplona, 2016.

- "Las nuevas tecnologías en las relaciones laborales: análisis de la STC 241/2012, de 17 de diciembre", *Revista general de Derecho del Trabajo y de la Seguridad Social,* nº 36, febrero 2014.

APARICIO TOVAR, J., "Los derechos fundamentales y el juicio de proporcionalidad degradados a mera retórica: a propósito de la STC 170/2013, de 17 de octubre", *Revista de Derecho social*, nº 64, 2013.

APILLUELO MARTÍN, M., "Contornos de control empresarial de la intimidad del trabajador ante las nuevas tecnologías y a la luz de la doctrina judicial", *AS*, núm. 4/2003.

ARAGÓN REYES, M., *Estudios de Derecho Constitucional*, Madrid, Centro de Estudios Constitucionales, Madrid, 1998.

- "La interpretación de la Constitución y el carácter objetivado del control jurisdiccional", Revista Española de Derecho Constitucional, núm. 17, 1986.

ARBONÉS LAPENA, H. I., "El acceso por el empresario al ordenador y correo electrónico del trabajador: ¿un tema resuelto?", *Revista de Información Laboral*, nº 8, agosto 2013.

- "Grabación de imagen o sonido y control del correo electrónico por el empresario", *Nueva revista española de Derecho del Trabajo*, nº 178, 2015.

ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F., El derecho de los trabajadores a la intimidad, Thomson-Aranzadi, Pamplona, 2006.

AROLD LORENZ, N.-L; GROUSSOT, X. y PETURSSON, G. T.: *The European Human Rights Culture - A Paradox of Human Rights Protection in Europe?*, Martinus Nijhoff Publishers, Leiden, 2013

ARZOZ SANTISTEBAN, X., "Derecho al respeto de la vida privada y familiar", en LASAGABASTER HERRARTE, I., *Convenio Europeo de Derechos Humanos. Comentario sistemático*, Thomson Civitas, Madrid, 2009.

- *Videovigilancia, seguridad ciudadana y derechos fundamentales*, Civitas, Madrid, 2010.
- *La concretización y actualización de los derechos fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014.

BAETHGE, M. y OBERBECK, H., *Nuevas tecnologías y perspectivas profesionales de la gerencia empresarial*, MTSS, Madrid, 1995.

BALAGUER CALLEJÓN, M.L., Interpretación de la Constitución y ordenamiento jurídico, vol. I, Tecnos, 2ª reimpr., Madrid, 1997.

- "Capacidad creativa y límites del legislador en relación con los derechos fundamentales. La garantía del contenido esencial de los derechos", en APARICIO PÉREZ, M. A. (Coord.), *Derechos constitucionales y pluralidad de ordenamientos*, CEDECS, Barcelona, 2001.

BARAK, A., *Proporcionalidad.Los derechos fundamentales y sus restricciones*, Palestra, Perú, 2017.

BASILE, S., "La restricción del derecho sólo es posible por exigencias de la justicia penal". "Los valores superiores, los principios fundamentales y los derechos y libertades públicas en la Constitución de 1978", GARCÍA DE ENTERRÍA, E. y PREDIERI, A. (eds.), Madrid, 1980.

BASTIDA FREIJEDO, F.J. et al., *Teoría general de los derechos fundamentales en la Constitución de 1978*, Tecnos, Madrid, 2004

BAUZA MARTORELL, F. J., *Régimen jurídico de la video vigilancia*, Marcial Pons, Madrid, 2004.

BAVIERA PUIG, I., "Sobre la calificación del despido basado en pruebas ilícitas", *Revista Doctrinal Aranzadi Social* num.12/2008 parte Estudio, Aranzadi, Cizur Minor, Pamplona, 2008.

BAYLOS GRAU, A., "La protección de los derechos fundamentales por el Tribunal Constitucional español: auge y declive de la función de tutela", *RDS*, núm. 69.

BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *Trabajo y Derecho*, nº 54/2019.

BEANEY, W., "The right to privacy and American Law", en *Law and contemporary problems*, núm. 31,1966.

BERNAL PULIDO, C., *El principio de proporcionalidad y los derechos fundamentales: el principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculante para el legislador*, CEPC, Madrid, 2003.

BLÁZQUEZ AGUDO, E. Mª, "Novedades laborales en la nueva Ley Orgánica de Protección de Datos", en *Trabajo y Derecho* 50/2019 (febrero).

BORK, R., *The tempting of America. The political seduction of the Law*, New York, Touchstone, 1990.

BOROWSKI, M., "La restricción de los derechos fundamentales", *Revista Española de Derecho Constitucional*, núm. 59, 2000.

BORRAJO DACRUZ, E., "Privacidad e informática", *Actualidad Laboral,* núm. 33, 1998.

- "El impacto de las nuevas tecnologías y medio informáticos en la relación de trabajo", *AEDIPE*, 1984.
- "Derechos fundamentales y relación de trabajo: casos judiciales significativos", *AL*, núm. 3, 2004.

BOSSU, B. y BAREGE, A., "Preuve et surveillance des salariés: regard français", *Les cahiers de Droit*, vol. 54, nº 2-3, juin-septembre 2013.

BROWN, C. y CAMPBELL, B. A., "The impact of Technological change on work and wages", *Industrial Relations*, vol. 41, núm. 1, 2002.

BUENO DE MATA, F., "La práctica de la prueba electrónica en sede judicial: ¿vulneración o reforzamiento de principios procesales?", *Diario La Ley* núm. 8332.

CABEZA PEREIRO. J., "La protección jurisdiccional de los derechos humanos y libertades fundamentales de los trabajadores ante el TEDH", en *Revista de Derecho Social*, núm. 69, 2015.

CALVO GALLEGO, F. J., "TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales", *Revista Doctrinal Aranzadi Social* paraf.num.71/20129/2012 parte Presentación, Aranzadi, Cizur Minor, Pamplona, 2012.

- *Códigos Éticos y Derecho de los Trabajadores*, Bomarzo, Albacete, 2008.

CANTWELL, J. y ARULA, R., *International business and the eclectic paradigm*, Londres/Nueva York, 2003.

CARDONA RUBERT, Mª. B., "Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás. Comentario a la STC 241/2012, de 17 de septiembre", *Revista de Derecho social*, nº 60, 2012.

- "Control del correo electrónico de los empleados. Transgresión de la buena fe contractual", *Aranzadi Social*, nº 17, 2001.
- "Relaciones laborales y tecnologías de la información y de la comunicación", *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 9, 2004.
- "La utilización de las redes sociales en el ámbito de la empresa", *Revista de Derecho Social*, núm. 52, 2010.
- *Informática y contrato de trabajo*, Tirant lo Blanch, Valencia, 1999.
- "Las relaciones laborales y el uso de las tecnologías informáticas", *Lan Harremanak. Revista de Relaciones Laborales*, núm. extra, 2003.

CARRASCO DURÁN, M., "El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa", *Revista Aranzadi Doctrinal,* nº 9, 2014.

CARRILLO LÓPEZ, M., *La tutela de los derechos fundamentales en los Tribunales ordinarios (aplicación jurisdiccional de la Ley 62/1978, de 26 de diciembre de Protección Jurisdiccional de los Derechos Fundamentales de la Persona)*, Centro de Estudios Constitucionales, Madrid, 1995

- "El uso de Internet en la empresa: a propósito de la STEDH de 12 de enero de 2016, caso Barbulescu c. Rumanía", *IUSLabor,* nº 1, 2016.
- "Los ámbitos del derecho a la intimidad en la sociedad", en *El derecho a la privacidad en un nuevo entorno tecnológico*, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, Centro de Estudios Políticos y Constitucionales, Madrid, 2016.

CARRIZOSA PRIETO, E., "El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores", *Temas Laborales*, núm. 116, 2012.

CASAS BAAMONDE, Mª E., "La plena efectividad de los derechos fundamentales: juicio de ponderación (¿o de proporcionalidad?) y principio de buena fe", *Relaciones Laborales*, núm. 12, 2004.

- "Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral, *Derecho de las Relaciones Laborales*, I2, 2018.
- "Anotaciones sobre las obligaciones del Estado de garantizar la vida privada en el trabajo en la era digital", *Actum Social*, nº 136, junio 2018.

CASAS BAAMONDE, Mª. E.; BAYLOS GRAU, A. y ESCUDERO RODRÍGUEZ, R., "El Estatuto de los Trabajadores. Diez años después: pervivencias, insuficiencias desviaciones y reformas", *Relaciones Laborales*, núms. 6- 7, 1990.

CASTELLS OLIVÁN, M., "Vigilancia de la salud y tutela de la intimidad del trabajador", en *Aranzadi Social,* núm. 19, 2004.

CAVAS MARTÍNEZ, F., "Reflexiones sobre el trabajo y su papel en la actual sociedad de la información", *Aranzadi Social*, núm. 10, 2004.

CHLAPOWSKI, F., "Note: The Constitutional Right to informational privacy", en *Boston University Law Review*, vol. 71, 1991.

CIDONCHA, A., *La libertad de empresa*, Madrid, Instituto de Estudios Económicos-Thomson Civitas, 2006.

COLÁS NEILA, E., *Derechos fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia*, Bomarzo, Albacete, 2012.

CONDE-PUMPIDO TOURON, M. T., "El nuevo poder de dirección del empresario", en Bodas Martín, R. (Coord.), *El Poder de Dirección del Empresario*, Madrid, 1997.

COOLEY, T. M., *A treatise on the Lw of Torts or the Wrongs which arise independent of contract*, Callaghan, Chicago, 1888.

CÓRDOBA CASTROVERDE, D., "Las cámaras de videovigilancia en la jurisprudencia. Respuesta de los tribunales", *El Derecho Editores / Revista de Jurisprudencia El Derecho*, nº 2, Junio 2015.

CÓRDOBA CASTROVERDE, D. y DÍEZ-PICAZO GIMÉNEZ, I., "Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico", en *El derecho a la privacidad en un*

nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, Centro de Estudios Políticos y Constitucionales, Madrid, 2016.

CORRY, D. J., "Employee e-mail and Internet use: Canadian legal use", *Journal of labor research*, vol. 24, nº 2, 2003.

COTINO HUESO, L., *Libertad en Internet. La red y las libertades de expresión e información*, Tirant lo Blanch, Valencia, 2007.

CRUZ VILLALÓN, J., "Poder de dirección y nuevas estructuras empresariales", *Relaciones Laborales*, núm. 19-20, octubre 2005.

- "Control de la calidad de la ley y calidad del control de la ley", *Derecho Privado y Constitución*, núm. 17, Enero-Diciembre 2003.

CUEVA CALABIA, J. C., "La LORTAD y la seguridad de los sistemas automatizados de datos personales", *Actualidad Informática Aranzadi,* núm. 13, 1994.

CUEVA PUENTE, Mª. C., "Contrato de trabajo, derechos fundamentales y uso de las tecnologías de la información y de la comunicación en los lugares de trabajo", *Documentación Laboral*, nº 76, 2006.

CUBERO MARCOS, J. I., "Protección de los datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007, sobre conservación de datos", en *Revista española de derecho constitucional*, n. 83 (mayo-agosto 2008), 175-197.

DAVARA RODRÍGUEZ, M. A., "La nueva Ley Orgánica de Protección de Datos de Carácter Personal", en AA.VV. (DAVARA RODRÍGUEZ, M. A., Coord.): *XIII Encuentro sobre Informática y Derecho*, Aranzadi, Pamplona, 2000.

DE LA IGLESIA CHAMORRO, A., "Video surveillance, public space and fundamental rights", *Int. J. Human Rights and Constitutional Studies*, Vol. 5, Nos. 3/4, 2017.

DE LA QUADRA-SALCEDO JANINI, T. y SUÁREZ CORUJO, B., "¿Trabajadores incomunicados?: la deriva de la doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones", en Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social (Actas del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social), Varios, Madrid 2014.

DE LLERA SUÁREZ-BÁRCENA, E., *La observación o escucha de las comunicaciones telefónicas*. Estudios Jurídicos del Ministerio Fiscal. Tomo VI. Centro de Estudios Jurídicos de la Administración de Justicia, Madrid, 1997.

DEL REY GUANTER, S., "Nuevas perspectivas de la Libertad de expresión e información en las relaciones laborales: contrato de trabajo y redes sociales", en AA. VV., Borrajo Dacruz, E. (dir.): *Controversias vivas del nuevo Derecho del Trabajo*, La Ley, Madrid, 2015.

DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012.

- "Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia", *Revista General del Derecho del Trabajo y de la Seguridad Social*, nº 39.
- "El control de la prestación de trabajo a través de las nuevas tecnologías: un estudio sobre la video vigilancia en la doctrina judicial", *Justicia Laboral*, núm. 44, 2010

DÍAZ REVORIO, F. J., "El derecho fundamental al secreto de las comunicaciones", *Revista Derecho PUCP*, núm. 59, 2006.

- *Los derechos humanos ante los nuevos avances científicos y tecnológicos. Genética e Internet ante la Constitución*, Tirant lo Blanch, Valencia, 2009.
- "El derecho fundamental al secreto de las comunicaciones: una visión desde la jurisprudencia europea y su influencia en el Tribunal Constitucional español", Instituto de Investigaciones Jurídicas UNAM, www.juridicas.unam.mx, 2006.

DÍAZ RODRÍGUEZ, J. M., "Las grabaciones ocultas realizadas entre empresarios y trabajadores y su utilización como prueba en juicio", *Trabajo y Derecho* núm. 6/2015.

DÍEZ PICAZO, L. M., Sistema de derechos fundamentales, Aranzadi, Pamplona, 2013.

DOCTOR SÁNCHEZ-MIGALLÓN, R., "La vigilancia de la actividad del trabajador mediante videocámaras y circuitos cerrados de televisión", *IUSLabor*, núm. 3, 2014.

DRUMMOND, V., *Internet, privacidad y datos personales*, Reus, Madrid, 2004.

DUANE, E. L. y GIFFORD, K. D., "Workplace transformation and worker up killing: the perspective of individual workers", *Industrial Relations*, vol. 38, núm. 2, 1999.

DURÁN LÓPEZ, F., "Artículo 18. Inviolabilidad de la persona del trabajador", en Borrajo Dacruz, E. (Dir.), *Comentarios a las Leyes Laborales*, Edersa, Madrid, 1983.

DWORKIN, T. M., "Protecting private ernployees frorn enchaced rnonitoring: legislative aproche", *American Bussiness Law Journal*, vol. 28, 1990.

ELVIRA PERALES, A., *Derecho al secreto de las comunicaciones*, Iustel, Madrid, 2007.

ESCOBAR ROCA, G., "Derechos fundamentales e intervención administrativa (A propósito de la sentencia del Tribunal Constitucional 37/1998)", La Ley, D-141, Madrid, 1999.

ESCRIBANO GUTIÉRREZ, J., "El derecho a la intimidad del trabajador. A propósito de la Sentencia del Tribunal Constitucional 186/2000, de 10 de julio", *Relaciones Laborales*, t. I, 2001.

ESCUDERO RODRÍGUEZ, R., "Teletrabajo", en AA. VV., *El empleador en el Derecho del Trabajo*, Tecnos, Madrid, 1999.

EZQUIAGA GANUZAS, F.J., La producción jurídica y su control por el Tribunal Constitucional, Tirant lo Blanch, Valencia, 1999.

FABREGAT MONFORT, G., "El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave", Observatorio temático de jurisprudencia, *Trabajo y Derecho*, núm. 5 – Mayo 2015.

FALGUERA BARÓ, M. A., "Derecho a la intimidad y contrato de trabajo. Reflexiones sobre el tema a partir de la Sentencia del Tribunal Constitucional 98/2000", *Crónica Laboral*, núm. 32, 2000.

- "Uso por el trabajador del correo electrónico de la empresa para fines extra productivos y competencia de control del empleador", *Relaciones Laborales*, núm. 22, 2000.
- *Trabajadores, empresas y nuevas tecnologías*, en AA. VV., Derecho a la intimidad y nuevas tecnologías, CGPJ, Madrid, 2004.
- Nuevas tecnologías y trabajo (I): perspectiva contractual", *Trabajo y Derecho*, núm. 19-20, julio-agosto 2016.
- "Nuevas tecnologías y trabajo (II): perspectiva constitucional", *Trabajo y Derecho*, núm. 21, septiembre 2016.
- "Nuevas tecnologías y trabajo (III): perspectiva procesal", *Trabajo y Derecho*, núm. 22, octubre 2016.

FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial de la actividad laboral en España", *Labour & Law Issues*, vol. 2, nº 1, 2016.

FERNÁNDEZ DIEZ, A., "Control de la actividad laboral a través de un circuito cerrado de televisión", *Información Laboral*, núm. 7, 2000.

FERNÁNDEZ DOMÍNGUEZ, J. J. y RODRÍGUEZ ESCANCIANO, S., *Utilización y control de datos laborales automatizados*, APD, Madrid, 1997.

FERNÁNDEZ ESTEBAN, Mª L., "Estudio de la jurisprudencia constitucional y ordinaria sobre el secreto de las telecomunicaciones entre particulares, en especial en el ámbito de la empresa", *Revista Aranzadi Doctrinal Civil-Mercantil*, nº 3, 2000.

FERNÁNDEZ MÁRQUEZ, O., "La utilización por los trabajadores de los bienes de la empresa: un enfoque desde el derecho de propiedad", *Revista española de Derecho del Trabajo* num.148/2010 parte Estudios, Civitas, Pamplona, 2010.

FERNÁNDEZ LÓPEZ, Mª. F., "Libertad ideológica y prestación de servicios", *Relaciones Laborales*, núm. 7, 1985.

FERNÁNDEZ RODRÍGUEZ, J. J., "Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente", *Revista Española de Derecho Constitucional*, 108, septiembre-diciembre 2016.

- *Secreto e intervención de las comunicaciones en Internet*, Thomson Civitas, Madrid, 2004.

FERNÁNDEZ VILLAZÓN, L. A., *Las facultades empresariales de control de la actividad laboral*, Elcano, Aranzadi, 2003.

- "Tratamiento automatizado de los datos personales en los procesos de selección de los trabajadores", *Relaciones Laborales*, núm. 11, 1994.

FERRANDO GARCÍA, F., "Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías", *Revista de Trabajo y Seguridad Social*, *CEF*, nº 399, junio 2006.

FERRARI, V., "El incierto futuro de los derechos en el trabajo humano", *Trabajo y Derecho*, núm. 52/2019.

FINDLAY, P. y McKINLAY, A., "Surveillance, electronic communications technologies and regulation", *Industrial Relations Journal*, vol. 34, núm. 4, 2003.

FLAHERTHY, D. H., "The emergence of surveillance societies in the Western World", *Government Information Quarterly*, vol. 5, 1998.

FLANAGAN, J. A., "Restricting electronic monitoring in the private workplace", *Duke Law Journal*, vol. 43, 1994.

FOLGUERA CRESPO, J. A. y otros, *Comentarios a la Ley Reguladora de la Jurisdicción Social*, Lex Nova, Valladolid, 2012.

FREIXES SANJUAN, Mª. T., "Las principales construcciones jurisprudenciales del Tribunal Europeo de Derechos Humanos", en *Los derechos en Europa* (Cood., GÓMEZ, SÁNCHEZ, Y.), UNED, Madrid, 1998

FRIGOLS BRINES, E., "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", en BOIX REIG, J. (Dir.) y JAREÑO LEAL, A. (Coord.), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010.

FROSINI, T. E., "Il diritto costituzionale di acceso ad Internet" en Prietrangelo, M. (a cura di), 2010, *Il Dirito di acceso ad Internet*. Atti della Tavola Rotonda, Roma, Edizioni Scientifiche Italiane.

FROSINI, V., "L´orizonte giuridico del l´Internet", in *Il diritto dell´informazione e dell´informatica* nº 2, 2000.

GAETA, L., "La dignidad del trabajador y las perturbaciones de la innovación", en AA. VV., Aparicio Tovar, J. y Baylos Grau, A. (dirs.): *Autoridad y democracia en la empresa*, Trotta, Madrid,1992.

GALLARDO MOYA, R., "El derecho fundamental a la protección de datos y la videovigilancia empresarial", *Revista de Derecho Social*, nº 62, 2013.

- "Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Barbulescu II c. Rumanía", en *Revista de Derecho Social*, Análisis Jurisprudencia, núm. 79, 2017.

GAMPER, A., *Regeln der Verfassungsinterpretation*, Springer, Viena-New York, 2012.

GARCÍA ALBERO, R., "TC y PC", *Actualidad Jurídica Aranzadi* num.834/2012, Cizur Minor, Pamplona, 2012.

GARCÍA COCA, O., "Algunas cuestiones sobre las posibilidades y limitaciones de supervisión del ordenador del trabajador por parte del empresario", *Revista Aranzadi de Derecho y Nuevas Tecnologías* num.34/2014 parte Estudios jurídicos, Aranzadi, Cizur Minor, Pamplona, 2014.

GARCÍA GONZÁLEZ, R. y PASTOR MERCHANTE, J., "Límites a la necesaria flexibilización de los derechos a la intimidad y al secreto de las comunicaciones en el ámbito laboral: una reflexión tras la sentencia del TEDH de 12 de enero de 2016 en el caso Barbulescu", *Diario La Ley*, Nº 8715, Sección Tribuna, 4 de Marzo de 2016, Ref. D-95, Editorial LA LEY.

GARCÍA MACHO, R., De los derechos sociales a los principios rectores en la Declaración Universal de los Derechos Humanos, Bosch, Barcelona, 1998.

GARCÍA MURCIA, J., "Los derechos de la persona en el ámbito del trabajo asalariado", en *Derechos del trabajador y libertad de empresa. 20 casos de Jurisprudencia Constitucional*, Dir. GARCÍA MURCIA, J., Thomson Reuters Aranzadi, Pamplona, 2013.

GARCÍA NINET, J. I., *El control empresarial en el ámbito laboral*, CISS, Bilbao, 2005.

GARCIA NINET, J. I. y VICENTE PALACIO, A., "Los derechos fundamentales como límite a las facultades organizativas del empresario (libertad sindical y movilidad funcional)", *Aranzadi Social*, tomo IV, 1999.

GARCÍA-NUÑEZ SERRANO, F., "La regulación sobre protección de datos personales y su incidencia en el ámbito laboral", *Aranzadi Social*, núm. 21/2000.

GARCÍA-PERROTE ESCARTÍN, I., "Ley, convenio colectivo, contrato de trabajo y derechos fundamentales del trabajador", *Revista de Derecho Social*, núm. 4, 1998.

- "El control empresarial del uso por el trabajador del ordenador (Nota sobre la Sentencia del Tribunal Supremo de 26 de septiembre de 2007)", *Información Laboral Jurisprudencia*, núm. 11, 2008.

- "Convenio Colectivo y contrato de trabajo. Y sobre los derechos constitucionales inespecíficos del trabajador", en E. Rojo Torrecilla (edit.), *Las reformas laborales de 1994 y 1997*, Marcial Pons, Madrid, 1998.

GARCÍA-PERROTE ESCARTÍN y MERCADER UGUINA, J. R., "Conflicto y ponderación de los derechos fundamentales de contenido laboral", en *El modelo social en la Constitución Española de 1978*, Dir. SEMPERE NAVARRO, A. V., Coord., MRTÍN JIMÉNEZ, R., MTASS, Madrid, 2003.

GARCÍA TORRES, J. y JIMÉNEZ-BLANCO, A., *Derechos fundamentales y relaciones entre particulares. La Drittwirkung en la jurisprudencia del Tribunal Constitucional*, Civitas, Madrid, 1986.

GARCÍA VITORIA, I., *La libertad de empresa: ¿un terrible derecho?*, CEPC, Madrid, 2008.

- "La protección de datos como eje de la jurisprudencia del Tribunal de Estrasburgo sobre la privacidad del trabajador y el control empresarial", en http://eapc-rcdp.blog.gencat.cat

GARRORENA MORALES, A., El Estado español como Estado social y democrático de Derecho, Ed. Tecnos, Madrid, 1984.

GAVARA DE CARA, J. C., "El principio de proporcionalidad como elemento de control de la constitucionalidad de las restricciones de los derechos fundamentales", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 16/2003.

GIL y GIL, J. L., "El deber del empresario de salvaguardar los derechos fundamentales del trabajador", *Aranzadi Social*, núm. 12/2003.

GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos de trabajo", *Revista Española de Derecho del Trabajo* num.164/2014 parte Comentario de Jurisprudencia, Ed. Aranzadi, Cizur Minor, Pamplona, 2014.

- "El uso particular de los trabajadores de las nuevas tecnologías empresariales en los códigos de conducta", *Revista española de Derecho del Trabajo* num.155/2012 parte Estudios, Civitas, 2012.

GIMÉNEZ-ARNAU, R., "Poder de dirección y derecho a la protección de datos. Algunas reflexiones a raíz del Caso López Ribalda", https://elderecho.com/poder-de-direccion-y-derecho-a-la-proteccion-de-datos-algunas-reflexiones-a-raiz-del-caso-lopez-ribalda

GOERLICH PESET, J. Mª., "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas", en *El derecho a la privacidad en un nuevo*

entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, Centro de Estudios Políticos y Constitucionales, Madrid, 2016.

GÓMEZ MONTORO, A., "La titularidad de derechos fundamentales por personas jurídicas: un intento de fundamentación", *REDC*, 2002, nº 65.

GONZÁLEZ BEILFUSS, M., *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional*, Aranzadi, Pamplona, 2003.

GONZÁLEZ BIEDMA, E., "Derecho a la información y consentimiento del trabajador en materia de protección de daros", en *Temas Laborales*, núm. 138/2017.

GONZÁLEZ COBALEDA, E*.,* "Dimisión laboral en la red: un "whatsapp" sin guasa: comentario a la sentencia de Tribunal Superior de Justicia de Madrid de 10 de junio de 2015", *Revista de Trabajo y Seguridad Social*, nº 393, 2015.

GONZÁLEZ GONZÁLEZ, C., "Control empresarial de la actividad laboral y uso de las nuevas tecnologías", *Revista Aranzadi Doctrinal* 11/2015.

- "Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016", *Revista Aranzadi Doctrinal* núm. 5/2016.

GONZÁLEZ ORTEGA, S., "La informática en el seno de la empresa. Poderes del empresario y condiciones de trabajo", en M. R. Alarcón Caracuel y R. Esteban Legarreta (edits.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004.

GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador*, Civitas, Madrid, 1988.

- "Controles empresariales: geolocalización, correo electrónico, Internet, video vigilancia y controles biométricos", en *Justicia Laboral*, núm. 39, 2009.

- "La vigilancia empresarial de las conversaciones electrónicas de los trabajadores: a propósito de la Sentencia del TEDH de 12 de enero de 2016, Barbulescu c. Rumanía", *Trabajo y Derecho*, nº 18, junio 2016.

- *La videovigilancia empresarial y la protección de datos personales*, Civitas, Madrid, 2006.

- "El poder de control empresarial en la doctrina del Tribunal Supremo", en: García Murcia, Joaquín (Coord.), *El Estatuto de los Trabajadores en la jurisprudencia del Tribunal Supremo*, Tecnos, Madrid, 2015.

- "Los límites de las potestades empresariales vs. Derecho a la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral de las redes sociales (1)", *Actum Social*, nº 95, enero 2015.

- "Nuevas tecnologías digitales, poderes empresariales y derecho de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016", en *Revista de Derecho Social*, núm. 78, 2017.

GRAU PINEDA, C., "La transgresión de la buena fe contractual en el uso personal del ordenador de la empresa: la legitimidad del control empresarial", *Revista Doctrinal Aranzadi Social* num.11/2008 parte Estudio, Aranzadi, Cizur Minor, Pamplona, 2008.

GUDE FERNÁNDEZ, A., "La video vigilancia laboral y el derecho a la protección de datos de carácter personal", *Revista de Derecho Político*, núm. 91, 2014.

GUERRA RODRÍGUEZ, L., "Ejercicio del poder de control a través de cámaras de videovigilancia: análisis de la doctrina constitucional", *Trabajo y Derecho* 29/2017 (mayo), nº 29 de 1 de mayo de 2017.

GUFFEY, C. J. y WEST, J. F., "Employee privacy: legal implications for managers", *Labor Law Journal*, vol. 47, núm. 11, 1996.

GUTIÉRREZ PÉREZ, M., "Prohibición expresa del uso privado del ordenador como fundamento para su control", *Revista Española de Derecho del Trabajo,* núm. 165/2014 parte Comentario de Jurisprudencia, Aranzadi, Cizur Minor, Pamplona, 2014.

- *Ciudadanía en la empresa y derechos fundamentales inespecíficos*, Ed. Laborum, Murcia, 2011.

HERRERO Y RODRÍGUEZ DE MIÑÓN, M. (1991A), *Idea de los derechos históricos*, Espasa Calpe, Madrid, 1991.

- "La posición constitucional de la Corona" (1991B), Estudios sobre la Constitución Española, Homenaje al profesor Eduardo García de Enterría, t. III, Civitas, Madrid, 1991.

- *Derechos históricos y Constitución*, Taurus, Madrid, 1998.

HERRERO-TEJEDOR, F., *Honor, intimidad y propia imagen*, Colex, Madrid, 1994.

- *La intimidad como derecho fundamental*, Madrid, Colex, 1998.

HESSE, K., Escritos de Derecho Constitucional, 2ª ed., CEC, Madrid, selección, traducción e interpretación de P. Cruz Villalón, 1992.

HIERRO HIERRO, F. J., "Registros sobre la persona del trabajador", *Libertad de empresa y poder de dirección del empresario en las relaciones laborales*, Aranzadi, Pamplona, 2011.

JIMÉNEZ CAMPO, J., "La garantía constitucional del secreto a las comunicaciones", *Revista Española de Derecho Constitucional*, nº 20, 1987.

- "Interpretación de la Constitución", en Enciclopedia Jurídica Básica, vol. III, Civitas, Madrid, 1995.

JIMÉNEZ PÉREZ, A., "El derecho a la intimidad en la jurisprudencia constitucional y convencional: el Tribunal Constitucional Español, el Tribunal Europeo de Derechos Humanos y la Corte Interamericana de Derechos Humanos", en *El derecho a la intimidad. Nuevos y viejos debates*, Dykinson, Madrid, 2017.

KING, D. N., "Privacy issues in the private-sector workplace: protection from electronic surveillance and emerging privacy gap", *California Law Review*, vol. 67, 1994.

KRIELE, M., "Grundrechte und demokratischer Gestaltungsspielraum", en J. Isensee y P. Kirchhof (dirs.), Handbuch des Staatsrechts,vol. 5, 2ª ed., 2000, C.F. Müller, Heidelberg.

LAHERA FORTEZA, J.: "Nueva jurisprudencia constitucional en la videovigilancia laboral: valoración crítica (STC 39/2016, de 3 de marzo)", Derecho de las Relaciones Laborales, Jurisprudencia en detalle, nº 5, mayo 2016, pág. 495.

- "Seguridad jurídica en la videovigilancia laboral", https://cincodias.elpais.com/cincodias/2019/10/28/opinion/1572280911_312873.html

LAPAGE, A., *Libertès e droits fundamentaux à l'epreuve de l'Internet*, Paris, 2002, Litec.

LARENZ, K., *Methodenlehre der Rechtswissenschaft*, Berlín, 2ª ed. 1992

LEZERTUA, M., "El derecho a la vida privada y familiar en la jurisprudencia del Tribunal Europeo de Derechos Humanos", en *Perfiles del derecho constitucional a la vida privada y familiar*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 1996.

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

LLUCH CORELL, F. J., "El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador", 2017, pág. 3, en: http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control- correo-electronico-trabajador_11_1045180003.html

LÓPEZ ANIORTE, Mª. C., "Límites constitucionales al ejercicio del poder directivo empresarial mediante el uso de las TIC y otros medios de vigilancia y seguridad privada en el ordenamiento jurídico español", *Revista Policía y Seguridad Pública*, noviembre 2013-junio 2014.

LÓPEZ DE LA FUENTE, G., "La doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos sobre el control de las comunicaciones electrónicas en el trabajo: ¿el fin de una eterna cuestión?", *Revista de Estudios Europeos*, nº 69, enero-junio 2017.

LÓPEZ GUERRA, L. y otros, Derecho Constitucional. Volumen I. El ordenamiento constitucional. Derechos y deberes de los ciudadanos, Tirant lo Blanch, 8ª ed. Valencia, 2010.

LÓPEZ JIMÉNEZ, D., "Los Códigos Tipo como instrumento para la protección de la privacidad en el ámbito digital: apreciaciones desde el Derecho español", en *Estudios Constitucionales*, año 11, nº 2, Centro de Estudios Constitucionales de Chile Universidad de Talca, 2013.

LÓPEZ-MUÑIZ GOÑI, M., "La ley de regulación del tratamiento automatizado de datos de carácter personal", en *Informática y Derecho*, núm. 6-7, 1994.

LÓPEZ PARADA, R., "Análisis jurisprudencial acerca de la instalación por el empresario de sistemas de video vigilancia en lugares de trabajo", *IL*, núm. 9, 1999.

LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/192, de regulación del tratamiento automatizado de los datos de carácter personal)*, Centro de Estudios Constitucionales, Madrid, 1993.

- "La construcción del derecho a la autodeterminación informativa", en *Revista de Estudios Políticos – Nueva época*, nº 104, abril-junio 1999.
- "Las vicisitudes del derecho de la protección de datos personales", en *Revista vasca de Administración Pública*, nº 58-2, septiembre-diciembre 2000.

LUCAS VERDÚ, P., Teoría de la Constitución como ciencia cultural, Dykinson, Madrid, 1997.

LUGARESI, N., "Electronic privacy in the workplace: transparency and responsibility", *International Review of Law, Computers and Technology*, vol. 24, nº 2, July 2010.

LUJÁN ALCARAZ, J., "Uso y control en la empresa de los medios informáticos de comunicación", en *Aranzadi Social*, núm. 3, 2001.

- "Protección de datos de carácter personal y contrato de trabajo", *Aranzadi Social*, núm. 5/2013.
- "La vigilancia empresarial sobre el uso de los medios informáticos puestos a disposición de los trabajadores", *en Libertad de empresa y poder de dirección del empresario en las relaciones laborales*, Estudios ofrecidos al profesor Alfredo Montoya Melgar, Aranzadi, Thomson Reuters, Cizur Menor, Pamplona, 2011.

LUQUE PARRA, M., Los límites jurídicos de los poderes empresariales, Bosch, Barcelona, 1999.

Ma, F., "Copland v. United Kingdom: What is privacy and how can transnational corporations account for differing interpretations", Loyola of Los Angeles International and comparative Law review, 3-1-2009, available at: http://digitalcommoms.lmu,edu/ilr/vol31/iss2/5

MACAVILCA ROMÁN, Z., "El derecho a la intimidad y las nuevas tecnologías. El derecho a la intimidad en el contexto de las nuevas tecnologías de comunicación e información", en *El derecho a la intimidad. Nuevos y viejos debates,* Dykinson, Madrid, 2017.

MAGRO SERVET, V., "El uso de la webcam para la práctica de la prueba", *Diario La Ley,* núm. 6132.

MANTECA VALDELANDE, V., "Control del empresario sobre el uso del ordenador por los trabajadores: alcance, contenido y límites", *Actualidad Jurídica Aranzadi* num.749/2008 parte Comentario, Aranzadi, Cizur Minor, Pamplona, 2008.

MARCO URGELL, A., *La intervención de las comunicaciones telefónicas: grabación de las conversaciones propias, hallazgos casuales y consecuencias jurídicas derivadas de la ilicitud de la injerencia*, Universidad Autónoma de Barcelona, https://ddd.uab.cat/record/99200.

MARÍN ALONSO, I., *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Tirant lo Blanch, Valencia, 2005.

- "La mensajería electrónica en la empresa: un paso atrás en la protección constitucional del derecho al secreto de las comunicaciones: a propósito de la STC 241/2012, de 17 de diciembre", *Relaciones Laborales: revista crítica de teoría y práctica*, nº 3, 2013.

- "La facultad fiscalizadora del empresario sobre el uso de correo electrónico en la empresa: su limitación en base al derecho fundamental al secreto de las comunicaciones", Temas Laborales, núm. 75/2004.

MARTÍN AGUADO, A., "Actuaciones irregulares que afectan a la libertad, dignidad o vida privada del trabajador. Límites constitucionales al poder de dirección empresarial", en A. Baylos Gru y J. Aparicio Tovar (edits.), *Autoridad y democracia en la empresa*, Trotta, Madrid,1992.

MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones*, Civitas, Madrid, 1995.

- "El derecho a la intimidad. Grabaciones con videocámaras y microfonía oculta", *La Ley*, nº 4, 2004.

MARTÍN-RETORTILLO BAQUER, L., "La calidad de la Ley según la jurisprudencia del Tribunal Europeo de Derechos Humanos (Especial referencia a los casos "Valenzuela Contreras" y "Prado Bugallo", ambos contra España)", *Derecho Privado y Constitución*, núm. 17, Enero-Diciembre 2003.

MARTÍN RETORTILLO, L. y DE OTTO PARDO, I., *Derechos fundamentales y Constitución*, Ed. Civitas, Madrid, 1988.

MARTÍN VALVERDE, A., "El ordenamiento laboral en la jurisprudencia del Tribunal Constitucional", en *RPS*, núm. 147, 1983.

- "Uso extralaboral del correo electrónico empleando medios informáticos de la empresa: control empresarial, requisitos. Comentario a la STC 170/2013, de 7 de octubre", *Actualidad Laboral,* nº 2, febrero 2014.
- "La Constitución como fuente del Derecho del Trabajo", *REDT*, núm. 33, 1988.

MARTÍNEZ DE CARVAJAL HEDRICH, E., "Valor probatorio de un correo electrónico", *Diario La Ley* núm. 8014.

MARTÍNEZ DE PISÓN, J., *El derecho a la intimidad en la jurisprudencia constitucional*, Civitas, Madrid, 1993.

MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, CES, Madrid, 2002.

- "El control de la correspondencia electrónica personal en el lugar de trabajo (Comentario a la SJS núm. 32 de Barcelona, de 16 de septiembre de 2002)", *Relaciones Laborales*, t. I, 2003.
- "Nuevas tecnologías y poder de control empresarial", *Revista Gallega de Empleo*, núm. 1/2000.
- "La doctrina del Tribunal Constitucional sobre el uso y control del correo electrónico en la relación de trabajo", *La ley*, Madrid, 2015.
- "El poder de control empresarial ejercido a través de medios audiovisuales en la relación de trabajo", *Relaciones Laborales*, núm. 4, 2002.

MARTINEZ LÓPEZ, F. J.; LUNA HUERTAS, P.; INFANTE MORO, A. y MARTÍNEZ LÓPEZ, L., "Los sistemas de control de la actividad laboral mediante las nuevas tecnologías de la información y las comunicaciones", *Relaciones Laborales*, núm. 12, 2003.

MARTÍNEZ MARTÍNEZ, R., ¿Minusvaloramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales?, *La Ley*, nº 9329, Sección Tribuna, 3 de enero de 2019.

MARTINOTTI, G., "La difesa della privacy", *Politica del diritto*, núm. 6, 1971.

MCINTOSH, D., "E-monitoring@workplace.com: the future of communication privacy in the Minnesota Private-Sector Workplace". *Hamline Law Review*, núm. 23, 2000.

MEDINA GUERRERO, M., *La vinculación negativa del legislador a los derechos fundamentales,* Madrid, McGraw Hill, 1996.

MERCADER UGUINA, J. R., *Derecho del Trabajo, nuevas tecnologías y sociedad de la información*, Lex Nova, Valladolid, 2002.

- "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?", *Relaciones Laborales*, núm. 20, 2001.

- "Límites del control empresarial sobre el uso por el trabajador del ordenador facilitado por la empresa como instrumento de trabajo: STS de 26.09.2007 como *leading case*", en AA. VV. (coord. SAGARDOY DE SIMÓN, I. y GIL SUÁREZ, L.), *Jurisprudencia y grandes cuestiones laborales*, Francis Lefebvre, Madrid, 2010.

- "Nota informativa sobre derecho a la intimidad y secreto de las comunicaciones en la relación de trabajo: dos casos en las jurisdicciones civil y penal", *Trabajo y Derecho*, núm. 2/2015.

- *Ley Reguladora de la Jurisdicción Social comentada y con jurisprudencia*, La Ley, Madrid, 2015.

- "Aspectos laborales de la Ley Orgánica 3/2018 de 5 de diciembre: una aproximación desde la protección de datos", *Trabajo y Derecho*, núm. 52/2019.

MIERES MIERES, L. J., *Intimidad personal y familiar. Prontuario de jurisprudencia constitucional*, Aranzadi, Navarra, 2002.

- "La protección constitucional de los derechos a la intimidad y a la propia imagen en las relaciones laborales: una visión desde la jurisprudencia constitucional", *RVAP*, núm. 99-100 (Especial "Demetrio Loperena Rota, *In memoriam*), Mayo-Diciembre.

MIÑARRO YANINI, M., "Impacto del reglamento comunitario de protección de datos en las relaciones laborales: un – pretendido – cambio cultural", *Revista de Trabajo y Seguridad Social, CEF*, núm. 423, junio 2018.

- "La Carta de derechos digitales de los trabajadores ya es ley: menos claros que oscuros en la nueva regulación", *Revista de Trabajo y Seguridad Social, CEF*, núm. 430, enero 2019.

MIRANDA BOTO, J. Mª, "Derecho a la intimidad de los trabajadores y uso del messenger corporativo ante el Tribunal Europeo de Derechos Humanos", *Derecho de las relaciones laborales*, nº 2, 2016.

MOLINA NAVARRETE, C., "Expectativa razonable de privacidad y poder de vigilancia empresarial: ¿quo vais justicia laboral?: comentario a la Sentencia del TEDH de 12 de enero de

2016, asunto Barbulescu c. Rumanía", *Revista de Trabajo y Seguridad Social, CEF*, nº 399, junio 2016.

- "Celebrando los 40 años de Constitución (social). Tres temas sociolaborales de hoy, sendos retos de modernización promovidos por la Constitución de 1978", *Revista de Trabajo y Seguridad Social, CEF*, diciembre 2018.

- "De Barbulescu II a López Ribalda: ¿qué hay de nuevo en la protección de datos de los trabajadores? Comentario a la sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018, caso López Ribalda *et alii* vs. España (Demandas acumuladas 1874/13 y 8567/13", *Revista de Trabajo y Seguridad Social, CEF,* febrero 2018.

- "El trabajador transparente, entre metáfora y realidad, y el efecto útil de los derechos de la personalidad en la empresa del siglo XXI", *Revista de Trabajo y Seguridad Social, CEF*, febrero 2018.

- "La Constitución social del trabajo (decente): ¿un divorcio entre el ideal normativo y la cruda realidad en busca de nuevo convenio regulador o de reconciliación?, *Revista de Trabajo y Seguridad Social, CEF,* nº 429, diciembre 2018.

- "Poder de geolocalización, intimidad y autodeterminación digital en las relaciones de trabajo: ¿un nuevo orden eficaz de garantías y límites?", *Diario La Ley*, Nº 9319, Sección Tribuna, diciembre 2018.

- "Ahora que el TC recela de la cámara oculta, el TEDH la respalda en las empresas: la insoportable liquidez de la jurisprudencia", *CEF Laboral Social*, Octubre 2019.

MOLINA NAVARRETE, C. y MONEREO PÉREZ, J. L., "El derecho al trabajo, la libertad de elección de profesión u oficio: principios institucionales del mercado de trabajo", en *Comentarios a la Constitución socio-económica de España*, Comares, Granada, 2002.

- "Bases jurídicas y presupuestos políticos para la eficacia social inmediata de los derechos fundamentales", *RTSS*, julio-septiembre, 1991.

MONEREO PÉREZ, J. L., "El control empresarial del correo electrónico tras la STC 170/2013", *Aranzadi Social*, nº 11, marzo 2014.

- *Algunas reflexiones cobre la caracterización técnico-jurídica del derecho al trabajo*, Civitas, Madrid, 1996

MONTAÑÉS PARDO, M. A., *La intervención de las comunicaciones. Doctrina jurisprudencial*, Aranzadi, Pamplona 1999.

MONTOYA MELGAR, A., "El poder de dirección del empresario", en AA. VV.: *El Estatuto de los Trabajadores. Veinte años después*. Civitas, Madrid, 2000.

- "Derechos del trabajador e informática", *Revista de la Facultad de Derecho de la UCM*, nº 25, 2002.

- "Nuevas tecnologías y buena fe contractual (Buenos y malos usos del ordenador en la empresa)", *Relaciones Laborales*, núm. 5 y 6/2009.

- "Buenos y malos usos del ordenador en la empresa", *Anales de la Real Academia de Jurisprudencia y Legislación*, Madrid, 2009.

- *El poder de dirección del empresario*, IES, Madrid, 1965.

MORALES VÁLLEZ, C.E., "El control de los medios tecnológicos por el empresario a la luz de la STEDH de 12 de enero de 2016", *CEF Laboral-Social,* Febrero 2016.

MORATO GARCÍA, R. Mª., "El control sobre Internet y correo electrónico en la negociación colectiva", *Relaciones Laborales*, vol. 21, nº 24, 2005.

MUHL, C. J., "Workplace e-mail and Internet use: employees and employers beware", *Monthly labor review,* vol. 126, nº 2, 2003.

MÜLLER, F. y CHRISTENSEN, R., *Juristische Methodik*, Berlín, 2002, 8ª ed.

MUÑOZ RUIZ, A. B., "Instrumentos informáticos de utilización generalizada en la empresa o medios de uso personal y secreto de las comunicaciones: comentario a la STC 241/2012, de 17 de diciembre", *Justicia Laboral*, nº 55, 2013.

NARVÁEZ RODRÍGUEZ, A., "Tutela de la privacidad e interceptación de las comunicaciones", en *Cuadernos Penales Jose María Lidón*, núm. 4, Delito e informática: algunos aspectos, Bilbao, Universidad de Deusto, 2007.

NAVARRO MARCHANTE, V.J., *El derecho a la información audiovisual de los juicios*, CEPC, 2011.

- "El recurso a cámaras ocultas en los reportajes periodísticos: el caso Haldimann ante el TEDH" en *REDC* 105, 2015.

NIETO, A., "Peculiaridades jurídicas de la norma constitucional", *Revista de Administración Pública*, núm. 100-102, 1983.

NORES TORRES, L. E., "Algunas cuestiones sobre la utilización de las redes sociales como medio de prueba en el proceso laboral", *Actualidad Laboral*, núm. 3/2014.

O'BRIEN, C., "The impact of employer e-mail policies on employee rights to engage in concerted activities protected by the National Labor Relations Act", *Labor Law Journal*, vol. 53, núm. 2, 2002.

O´CALLAGHAN MUÑOZ, X., Libertad de expresión y sus límites: honor, intimidad e imagen, Editoriales de Derecho Reunidas, Madrid, 1991.

OCÓN, J. (2018), "Derecho a la intimidad y registro de dispositivos informáticos: a propósito del asunto Trabajo Rueda c. España", *REDC*, 113, 327-343.

OLIVER, H., "Email and Internet monitoring in the workplace: information privacy and contracting-out", *Industrial Law Journal,* vol. 31, núm. 4, 2002.

OLLERO TASSARA, A., "¿Son jurídicos los derechos humanos?, *Revista SCIO,* nº 4, 2009.

ORTEGA GIMÉNEZ, A., "Protección de datos, secreto de las comunicaciones, utilización del correo electrónico por los trabajadores y control empresarial" en *La Ley* - 7188 (3 de junio de 2009).

ORTIZ LALLANA, M. C., "Derechos fundamentales y relación laboral", *RMTAS*, núm. 13, 1998.

ORZA LINARES, R. M., "Derechos fundamentales e Internet: nuevos problemas, nuevos retos", *Revista Española de Derecho Constitucional*, núm. 18, julio-diciembre 2012.

OSSENBÜHL, F., "Grundsätze der Grundrechtsinterpretation", en D. Merten y H. J. Papier (eds.), Handbuch der Grundrechte in Deutschland und Europa, vol. I, C.F. Müller, Heidelberg, 2004.

OTTO, M., "The right to privacy in employment. In search of the european model of protection", *European Labour Law Journal*, Vol. 6, 2015, Nº 4.

- *The right to privacy in employment. A comparative analysis*, Hart Publishing, Bloomsbury, 2016

PACHECO ZERGA, L., La dignidad humana en el Derecho del Trabajo, Thomson-Civitas, Pamplona, 2007.

PALOMEQUE LÓPEZ, M. C., "Derechos fundamentales generales y relación laboral: los derechos laborales inespecíficos", en AA. VV. (Dir. Sempere Navarro, A. V. y Coord. Martín Jiménez, R.): *El modelo social en la Constitución Española de 1978*, *MTAS*, Madrid, 2003.

- *Los derechos laborales en la Constitución Española*, CEC, Madrid, 1991.

PARDO FALCÓN, J., "Los derechos del artículo 18 de la Constitución española en la jurisprudencia del Tribunal Constitucional", *Revista Española de Derecho Constitucional*, Año 12, núm. 34, Enero-Abril 1992.

PÉREZ ÁLVAREZ, M. A., *Interpretación y jurisprudencia. Estudio del artículo 3.1 del Código Civil*, Aranzadi, Pamplona, 1994.

PÉREZ DE LOS COBOS ORIHUEL, F., *Nuevas tecnologías y relación de trabajo*, Tirant lo Blanch, Valencia, 1990.

PÉREZ LUÑO, A. E., *Derechos humanos, Estado de Derecho y Constitución*, 7ª ed. Tecnos, Madrid, 2001.

- "La protección de la intimidad frente a la informática en la Constitución española de 1978", en *Revista de Estudios Políticos*, núm. 9.

- "La protección de los datos personales del menor en Internet", en *Anuario de la Facultad de Derecho de la Universidad de Alcalá de Henares*, vol. 2, 2009.

PIÑAR MAÑAS, J. L., "Consideraciones introductorias sobre el derecho fundamental a la protección de datos de carácter personal", en *Boletín del Ilustre Colegios de Abogados de Madrid*, núm. 35, 2007.

- "¿Existe la privacidad? Inauguración del curso académico 2008/2009", Madrid, *Publicaciones de la Fundación Universitaria San Pablo CEU*, 2008.

POQUET CATALÁ, R., *El actual poder de dirección y control del empresario*, Cuadernos de Aranzadi Social, Thomson Reuters Aranzadi, Pamplona, 2013.

POWELL, C. D., "You already have zero privacy. Get over it¡", Would Warren and Brandeis Argue for Privacy for Social Networking, en *Pace Law Review*, vol. 31, núm. 1, 2011.

PRADAS MONTILLA, R., "Organización del trabajo y nuevas tecnologías", *Documentación Laboral*, núm. 53, 1997.

PRECIADO DOMENECH, C. H., *El derecho a la protección de datos en el contrato de trabajo*, Thomson Reuters Aranzadi, Pamplona, 2017.

- "El nuevo Reglamento 679/2016, de 27 de abril sobre Tratamiento de Datos Personales y su incidencia en las relaciones laborales", *Actum Social*, nº 121, marzo 2017.

- "Nuevas formas de prueba basadas en las tecnologías de la información y la comunicación (TIC). Documento electrónico y prueba digital: Proposición y práctica. Ilicitud de estas pruebas por vulneración de derechos fundamentales", *Actum Social*, nº 131, monográfico 2018.

- "Comentario de urgencia a la Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017. Caso Barbulescu contra Rumanía (Gran Sala). Recuperando la dignidad en el Trabajo". *Blog de la Comisión delo Social de juezas y jueces para la democracia.*

- "Comentarios de urgencia a la STEDH de 17 de octubre de 2019 caso López Ribalda c. España (Gran Sala)*", newsletter laboral de Juezas y Jueces para la democracia, 21 Octubre 2019.*

PURCALLA BONILLA, M. A., "Control de las nuevas tecnologías (y algunas reflexiones sobre la protección de datos) en la relación laboral", *Actum Social*, nº 121, marzo 2017.

QUERALT JIMÉNEZ, A., *El Tribunal de Estrasburgo: una jurisdicción internacional para la protección de los derechos fundamentales*, Tirant lo Blanch, Valencia, 2003.

RALLO LOMBARTE, A., "El nuevo derecho a la protección de datos", *Revista Española de Derecho Constitucional*, núm. 116, Mayo-Agosto 2019.

RAMOS LUJÁN, H. V.: "La intimidad de los trabajadores y las nuevas tecnologías", *Relaciones Laborales*, núm. 17, 2003.

RAY, J-E. y BOUCHET, J-P, "Vie Profesionnelle, vie personnelle et TIC", *Droit Social,* nº 1 Janvier 2010.

RAY, J. E., "Geolocalisation, donness personnelles et droit du travail", *Droil Social*, núm. 12, 2004.

REBOLLO DELGADO, L., *El derecho fundamental a la intimidad*, Dykinson, Madrid, 2005.

REQUENA LÓPEZ, T., *Sobre la función, los medios y los límites de la interpretación constitucional*, Comares, Granada, 2001.

RIFKIN, J., *L'era dell'accesso*, Milano, Mondadori, 2000.

RIBAS, X., "Matizaciones sobre la sentencia del Caso Barbulescu", en https://xribas.com/2017/09/06/matizaciones-sentencia-caso-barbulescu/

RIVERO LAMAS, J., "Derechos fundamentales y contrato de trabajo: eficacia horizontal y control constitucional", AAVV, *El trabajo en la Constitución. Estudios homenaje al Profesor Alonso Olea*, MTSS, Madrid, 2003.

RODOTA, S., "Tecnología y derechos fundamentales", *Datos personales.org. Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 8, 2004.

RODRÍGUEZ CANO, I. A., *Poder de dirección empresarial y esfera personal del trabajador*, CES, Oviedo, 2009.

RODRÍGUEZ ESCANCIANO, S., *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Bomarzo, Albacete, 2009.

- *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015.
- "El control empresarial del correo electrónico de los trabajadores: posibilidades y límites (a propósito de la STC de 7 de octubre de 2013)", *Relaciones Laborales: revista crítica de teoría y práctica*, nº 10, 2014.
- "El control empresarial de la mensajería electrónica como prueba de la transgresión de la buena fe contractual. A propósito de la STC 170/2013, de 7 de octubre", *Diario La Ley*, Nº 8195, Sección Tribuna, 20 noviembre 2013.

- "Innovación tecnológica y productividad empresarial", *La Ley*, núm. 8, 2013.

RODRÍGUEZ LAINZ, J. L., *El secreto de las comunicaciones y su interceptación legal*, Sepin, Madrid, 2016.

RODRÍGUEZ MAGARIÑOS, F. G., "El derecho al respeto a la intimidad telemática versus la sentencia "Barbulescu", del Tribunal Europeo de Derechos Humanos: consecuencias en el orbe penal", *La Ley Penal*, Nº 118, Sección Jurisprudencia aplicada a la práctica, Enero-Febrero 2016, Editorial Wolters Kluwer.

RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., "Derecho a la intimidad del trabajador y contrato de trabajo", en *Diario La Ley*, núm. 6033, de 4 de junio de 2004.

RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones: tecnología e intimidad*, McGrawHill, Madrid, 1998.

ROEL, R. E., "Injured by big brother? Study shows monitored workers get hurt more", *Newsday*, 5 de octubre, 1990.

ROIG BATALLA, A., "El uso de Internet en la empresa: aspectos constitucionales", en A. Roig Batalla (edit.), *El uso laboral y sindical del correo electrónico e Internet en la empresa. Aspectos constitucionales, penales y laborales*, Tirant lo Blanch, Valencia, 2007.

- "Algunas notas sobre los derechos fundamentales de la empresa", *Revista de la Facultad de Derecho de la Universidad Complutense*, núm. 25, 2002.
- *Derechos Fundamentales y Tecnologías de la Información y de las Comunicaciones (TICs)*, Bosch, 2011.

ROJAS RIVERO, G.P., *La libertad de expresión del trabajador*, Universidad de La Laguna, 1990.

ROJO TORRECILLA, E., "De Barbulescu I a Barbulescu II. La Gran Sala del TEDH refuerza la protección del trabajador frente al control y vigilancia de las comunicaciones electrónicas en el ámbito laboral por parte empresarial", Notas a la importante sentencia de 5 de septiembre de 2017, y amplio recordatorio de la sentencia de la Sala Cuarta de 12 de enero de 2016, en www.Eduardorojotorrecilla.es

- "Medias verdades y fake news en el mundo jurídico. No cabe todo en la videovigilancia de una persona trabajadora. A propósito de la sentencia "López Ribalda" de la Gran Sala del TEDH de 17 de octubre de 2019 (y recordatorio de la sentencia de Sala de 9 de enero de 2018 y del caso Barbulescu II, sentencia de Gran Sala de 5 de septiembre de 2017)", *http://www.eduardorojotorrecilla.es/2019/10/medias-verdades-y-fake-news-en-el-mundo.html*

ROMÁN DE LA TORRE, M.ª D., *Poder de dirección y contrato de trabajo*, Grapheus, Valladolid, 1992.

ROMERO COLOMA, A. Mª., *Honor, intimidad e imagen de las personas famosas*, Civitas, Madrid, 2001.

ROQUETA BUJ, R., *Uso y control de los medios tecnológicos de información y comunicación en la empresa*, Tirant lo Blanch, Valencia, 2005.

RÚA RODRÍGUEZ, M., "La revolución tecnológica y sus efectos en el mercado de trabajo: un reto del siglo XXI", *Trabajo y Derecho*, nº 53, 2019.

RUANO ALBERTO, S., "Facultades de control por medios informático", *Tribuna Social*, núm. 162, 2004.

RUBIO LLORENTE, F., "Prólogo" a La interpretación de la Constitución de ALONSO GARCÍA, E., CEC, Madrid 1984.

RUBIO TORRANO, E., "El trabajador infiel", *Revista Doctrinal Aranzadi Civil-Mercantil* num.8/2013 parte Comentario, Aranzadi, Cizur Minor, Pamplona, 2013.
RUIZ MIGUEL, C., *La configuración constitucional del derecho a la intimidad*, Tecnos, Madrid, 1995.

SAGARDOY BENGOECHEA, J. A., *Los derechos fundamentales y el contrato de trabajo,* Civitas, Pamplona, 2005.

SAIZ ARNAIZ, A.: "TC y PC", *Actualidad Jurídica Aranzadi* num.834/2012 parte Cara, Ed. Aranzadi, Cizur Minor, Pamplona, 2012.

SAMPEDRO GULLÓ, V., "Facultades empresariales de vigilancia y control en el centro de trabajo", *Tribuna Social*, núm. 160, 2004.

SAN MARTÍN MAZZUCONI, C., "¿Cómo se mide el uso moderado de Internet para fines personales? ¿Transgrede la buena fe contractual tener abierto un programa para chatear?, *Aranzadi Social,* núm. 7/2004.

- "El uso y el control empresarial de las nuevas tecnologías en el ámbito laboral. Algunas pautas recurrentes en la doctrina judicial para tener en cuenta", *Aranzadi Social* núm. 2/2007.
- "¿Navegar por Internet en horas de trabajo…¿Quién? ¿Yo?", Revista Doctrinal Aranzadi Social num.70/201019/2010 parte Presentación, Aranzadi, Cizur Minor, 2010.

SÁNCHEZ DEL OLMO, V., "El impacto (divergente) de la doctrina Barbulescu en las resoluciones de instancia. Comentarios a las sentencias 341/2017 y 737/2017 de los Juzgados de lo Social de Madrid nº 19 y nº 33", *Trabajo y Derecho*, nº 45, 1 de septiembre de 2018.

SÁNCHEZ-RODAS NAVARRO, C., "Videocámaras y poder de vigilancia", en *Aranzadi Social*, núm. 19, 2000.

SANFULGENCIO GUTIÉRREZ, J. A., "¿Es privado el email? Reflexiones prácticas sobre el uso del correo electrónico en el trabajo y la utilización del ordenador con fines particulares", *El Graduado,* núm. 37, enero 2002.

SANTAMARÍA PASTOR, J. A., *Principios de Derecho Administrativo*, vol. I, 3ª ed., Madrid, 2000.

SANTIAGO REDONDO, K. M., "Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE", *Relaciones Laborales*, Nº 1, Tomo I, 2014.

SANTOLAYA MACHETTI, P., "Derecho a la vida privada y familiar: un contenido notablemente ampliado del derecho a la intimidad (art. 8 CEDH)", en García Roca, J. y Santolaya Machetti, P. (coords.), *La Europa de los derechos. El Convenio Europeo de Derechos Humanos*, Centro de Estudios Políticos y Constitucionales, Madrid 2005.

SCARBROUG, H. y CORBETT, J. M., *Technology and organization (power; meaning and desing)*, Routledge, Londres,1992.

SEGOVIANO ASTABURUAGA, M. L., "El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores", *Revista jurídica de Castilla y León*, núm. 2, 2004.

SELMA PENALVA, A., "Los límites de la tolerancia en la utilización del ordenador de la empresa para fines personales", *Revista Doctrinal Aranzadi Social* num.83/201211/2012 parte Presentación, Aranzadi, Cizur Minor, Pamplona, 2012.

SEMPERE NAVARRO, A. V., "Tras el pronunciamiento del Tribunal Supremo, ¿cabe controlar el ordenador de los trabajadores?", *Actualidad Jurídica Aranzadi* nº 741/2007 parte Tribuna, Aranzadi, Cizur Minor, Pamplona, 2007.

- "¿Puede la empresa controlar el ordenador usado por su trabajador?", *Repertorio de Jurisprudencia* num.21/2007 parte Comentario, Aranzadi, Cizur Minor, Pamplona, 2007.
- *Comentarios a la Ley de la Jurisdicción Social*, Thomson Reuters Aranzadi, Pamplona, 2013.

SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCONI, C., *Nuevas tecnologías y relaciones laborales*, Aranzadi, Pamplona, 2002.

- "Los derechos laborales (inespecíficos) en la negociación colectiva", en AA. VV. (Dir. Sempere Navarro, A. V. y Coord. Martín Jiménez, R.): *El modelo social en la Constitución Española de 1978*, MTAS, Madrid, 2003.

- "Escuchas telefónicas a tele operadoras", Repertorio de Jurisprudencia, núm. 14/2004.

- *Las TICs en el ámbito laboral*, Francis Lefebvre, Madrid, 2015.
- *Derechos fundamentales inespecíficos y negociación colectiva,* Thomson Reuters, Navarra, 2011.

SEMPERE NAVARRO, A. y MATEOS Y DE CABO, O., "Uso y control de herramientas informáticas en el trabajo (marco legal, pautas judiciales y convencionales)", en Carolina San Martín Mazzucconi, *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, Eolas, Madrid, 2014.

SEPÚLVEDA GÓMEZ, M., "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contralímites", *Temas Laborales*, nº 122, 2013.

SERNA BERMÚDEZ, P., "Derechos fundamentales: el mito de los conflictos. Reflexiones teóricas en torno de un supuesto jurisprudencial sobre intimidad e información", Humana Iura, nº 4, 1994.

SERNA BERMÚDEZ, P. y TOLLER, F., La interpretación constitucional de los derechos fundamentales. Una alternativa a los conflictos de derechos, La Ley, Buenos Aires, 2000.

SUÁREZ ESPINO, M. L., "La intimidad de los trabajadores en el centro de trabajo y el poder de vigilancia del empresario", *Diario La Ley,* 2015, núm. 7906.

TALENS VISCONTI, E. E., "La expectativa razonable de confidencialidad como presupuesto de vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario", *Revista Doctrinal Aranzadi Social* paraf.num.51/20138/2013 parte Presentación, Aranzadi, Cizur Minor, Pamplona, 2013.

- "Videovigilancia mediante cámaras fijas y protección de datos en el ámbito laboral. Comentario a la sentencia del Tribunal Constitucional 29/2013, de 11 de febrero de 2013", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, num.33/2013 parte Jurisprudencia.

TASCÓN LÓPEZ, R*., El tratamiento por la empresa de los datos personales de los trabajadores. (Análisis del estado de la cuestión)*, Civitas, Madrid, 2005.

- "El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica", en *Aranzadi Social*, núm. 17, 2007.
- "Los ficheros empresariales sobre trabajadores y los derechos de los mismos en el marco de la relación contractual con el empleador", en AA.VV. (TRONCOSO REIGADA, A., Dir.): *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010.
- "Principios de la protección de datos: consentimiento del afectado. Los ficheros empresariales sobre trabajadores y los derechos de los mismos en el marco de la

relación contractual con el empleador (2ª parte)", Estudios y Comentarios Legislativos (Civitas). Comentario a la ley Orgánica de Protección de Datos de Carácter Personal, Aranzadi, Junio 2010.

- "El poder de control empresarial en la era tecnológica: visión panorámica de una cuestión inacabada", *RTSS. CEF*, núm. 267, 2005.
- "El trabajo humano (y su Derecho) ante el imparable fenómeno de las redes sociales", *RTSS. CEF*, núm. 340, 2011.

TÉLLEZ AGUILERA, A., *Nuevas tecnologías. Intimidad y protección de datos*, Edisofer, Madrid, 2001.

THIBAULT ARANDA, J., *Control multimedia de la actividad laboral*, Tirant lo Blanch, Valencia, 2006.

TIRADO ESTRADA, J. J., "La documentación video gráfica de las vistas orales y su trascendencia procesal. El artículo 147 de la Ley de Enjuiciamiento Civil", *Diario La Ley*, núm. 7674.

TODOLÍ SIGNES, A., "El registro informático como base para el despido. Cuestiones fundamentales", *Revista Aranzadi de Derecho y Nuevas Tecnologías* num.25/2011 parte Doctrina, Aranzadi, Cizur Minor, 2011.

TOSCANI GIMÉNEZ, D., "El uso de Internet y el correo electrónico en la empresa: límites y garantías", *Nueva revista española de Derecho del Trabajo*, nº 165, 2014.

TOSCANI GIMÉNEZ, D. y VALENCIANO SAL, A., *Derechos fundamentales inespecíficos de los trabajadores*, Bomarzo, Albacete, 2016.

TRUJILLO PONS, F.: "Revelación de secretos empresariales a terceros por medio del correo electrónico: posición del Tribunal Constitucional ante una supuesta vulneración a los derechos a la intimidad y al secreto de las comunicaciones: STC 170/2013, de 7 de octubre", *Revista general de Derecho del Trabajo y de la Seguridad Social*, nº 36, febrero 2014.

TULLINI, P., "Comunicazione elettronica, potere di controllo e tutela del lavoratore", *Rivista italiana di diritto del lavoro,* vol. 28, nº 3, 2009.

URBANO CASTRILLO, E., "El derecho al secreto de las comunicaciones", *La Ley,* Madrid, 2011.

VALASTRO, A., "Le garanzie di effettività del diritto di accesso ad Internet e la timidezza del legislatore italiano" en Prietrangelo, M. (a cura di), 2010, *Il Diritto di acceso ad Internet*. Atti della Tavola Rotonda.

VALDÉS DAL RÉ, F., "Poderes del empresario y derechos de la persona del trabajador", *Relaciones Laborales*, 1990-I.

- "Los derechos fundamentales de la persona del trabajador: un ensayo de noción jurídico-formal", *Relaciones Laborales*, núm. 18, 2003.

VALLE VILLAR, J. M., "El derecho a la intimidad del trabajador durante la relación de trabajo", *Actualidad Laboral*, t. III, 1991.

VELOT, F., "Cybersuveillance", *Lamy Social. Bulletin D´Actualité*, nº 156, 2002.

VEGAS TORRES, J., Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa, Universidad Rey Juan Carlos, Madrid, 2011.

VICENTE PACHÉS, F., *El derecho del trabajador al respeto de su intimidad,* CES, Madrid, 1998.

- "El control empresarial del ordenador. A propósito de la Sentencia del Tribunal Supremo –unificación de doctrina- de 26 de septiembre de 2007", en *Tribuna Social,* núm. 214, 2008.

- "Las facultades empresariales de vigilancia y control en las relaciones de trabajo", *Tribuna Social*, núm. 57, 2004

VIVERO SERRANO, J., "Las sentencias anotadas. Vigilancia y control de los trabajadores mediante cámaras de video", *Trabajo y Derecho*, nº 17, 2016.

WARREN, S. D. y BRANDEIS, L. D., "The Right to Privacy", *Harvard Law Review*, Vol. IV, December 15, 1890.

WHITFIELD, K., "High-performance workplaces, training and the distribution of skills", *Industrial Relations*, vol. 39, núm. 1, 2000.

ZEKOS, G., "Cyberspace and globalization", *Law, Social Justice and Global Development Journal*, núm. l, 2002.

ANEXO I.- REPERTORIO DE JURISPRUDENCIA MÁS REFERENCIADA.

A) TRIBUNAL EUROPEO DE DERECHOS HUMANOS

- STEDH de 10 de marzo de 1972 (caso De Wilde y otros c. Bélgica). - STEDH de 6 de noviembre de 1980 (caso Van Oosterwijck c. Bélgica). - STEDH de 22 de octubre de 1981 (caso Dudgeon c. Reino Unido). - STEDH de 28 de junio de 1984 (caso Campbell y Fell c. Reino Unido). - STEDH de 2 de agosto de 1984 (caso Malone c. Reino Unido). - STEDH de 26 de marzo de 1985 (caso X e Y c. Países Bajos). - STEDH de 24 de abril de 1990 (casos Kruslin y Huvig c. Francia). - STEDH de 23 de mayo de 1991 (caso Oberschlick c. Austria). - STEDH de 29 de agosto de 1991 (caso FCB c. Italia). - STEDH de 16 de diciembre de 1992 (caso Niemietz c. Alemania).	- STEDH de 23 de noviembre de 1993 (caso Poitrimol). - STEDH de 25 de junio de 1997 (caso Halford c. Reino Unido). - STEDH de 30 de julio de 1998 (caso Valenzuela Contreras c. España). - STEDH de 25 de marzo de 1998 (caso Kopp c. Suiza). - STEDH de 6 de diciembre de 1998 (caso Barberá, Messegué y Jabardo). - STEDH de 4 de mayo de 2000 (caso Rotaru c. Rumanía). - STEDH de 18 de febrero de 2003 (caso Prado Bugallo c. España). - STEDH de 3 de abril de 2007 (caso Copland c. Reino Unido). - STEDH de 27 de mayo de 2014 (caso La Flor Cabrera c. España). - STEDH de 30 de mayo de 2017 (caso Trabajo Rueda c. España).	- STEDH de 5 de septiembre de 2017 (caso Barbulescu c. Rumanía). - STEDH de 28 de noviembre de 2017 (caso Antovic y Mirkovic c. Montenegro). - STED de 9 de enero de 2018 (caso López Ribalda *et alii* c. España). - STEDH de 22 de febrero de 2018 (caso Libert c. Francia). -STEDH de 17 de octubre de 2019, Gran Sala (caso López Ribalda *et alii* c. España).

B) TRIBUNAL CONSTITUCIONAL

- STC 101/1983, de 18 de noviembre. - STC 120/1983, de 15 de diciembre. - STC 114/1984, de 29 de noviembre. - STC 19/1985, de 13 de febrero. - STC 88/1985, de 19 de julio. - 170/1987, de 30 de octubre. - STC 6/1988, de 21 de enero. - STC 231/1988, de 2 de diciembre. - STC 37/1989, de 15 de febrero. - STC 129/1989, de 17 de julio. - STC 120/1990, de 27 de junio. - STC 197/1991, de 17 de octubre. - STC 20/1992, de 14 de febrero. - STC 142/1993, de 6 de mayo. - STC 254/1993, de 20 de julio. - STC 57/1994, de 28 de febrero. - STC 99/1994, de 11 de abril.	- STC 134/1994, de 9 de mayo. - STC 6/1995, de 10 de enero. - STC 34/1996, de 11 de marzo. - STC 106/1996, de 12 de junio. - STC 136/1996, de 23 de julio. - STC 90/1997, de 6 de mayo. - STC 151/1997, de 29 de septiembre. - STC 11/1998, de 13 de enero. - STC 134/1999, de 15 de julio. - STC 144/1999, de 22 de julio. - STC 202/1999, de 8 de noviembre. - STC 98/2000, de 10 de abril. - STC 186/2000, de 10 de julio. - STC 292/2000, de 30 de noviembre. - STC 156/2001, de 2 de julio. - STC 70/2002, de 3 de abril. - STC 121/2002, de 20 de mayo. - STC 218/2002, de 25 de noviembre.	- STC 127/2003, de 30 de junio. - STC 196/2004, de 15 de noviembre. - STC 281/2005, de 7 de noviembre. - STC 281/2006, de 9 de octubre. - STC 72/2007, de 16 de abril. - Auto TC 29/2008, de 28 de enero. - 77/2009, de 23 de marzo. - STC 173/2011, de 7 de noviembre. - STC 96/2012, de 7 de mayo. - STC 241/2012, de 17 de diciembre. - STC 29/2013, de 11 de febrero. - STC 115/2013, de 9 de mayo. - STC 170/2013, de 7 de octubre. - STC 212/2013, de 16 de diciembre. - STC 39/2016, de 3 de marzo. -STC 26/2018, de 5 de marzo. -STC 24/2019, de 25 de febrero.

C) TRIBUNAL SUPREMO

- STS 9213/2001 de 26 de noviembre (Sala IV). - STS 7798/2003 de 5 de diciembre (Sala IV). - STS 2086/2007 de 7 de marzo (Sala IV). - STS 6128/2007 de 26 de septiembre (Sala IV). - STS 1323/2011 de 8 de marzo (Sala IV). - STS 8876/2011 de 6 de octubre (Sala IV). -STS 342/2013, de 17 de abril.	- STS 2618/2014 de 13 de mayo (Sala IV). - STS 528/2014 de 16 de junio (Sala II). - STS de 20 de noviembre de 2014 (Sala I). - STS 5507/2014 de 20 de noviembre (Sala IV). - STS 630/2016 de 7 de julio (Sala IV). - STS 646/2016 de 12 de julio (Sala IV). - STS 715/2016 de 21 de julio (Sala IV).	- STS 77/2017, de 31 de enero de 2017 (Sala IV). - STS 86/2017, de 1 de febrero (Sala IV). - STS 96/2017, de 2 de febrero (Sala IV). -STS 119/2018, de 8 de febrero (Sala IV). -STS 489/2018, de 23 de octubre (Sala II).

D) AUDIENCIA NACIONAL

- SAN de 24 de enero de 2003 (Sala de lo Cont.-Admvo.). - SAN de 29 de octubre de 2008. - SAN de 27 de mayo de 2010. - SAN de 30 de noviembre de 2011.		

E) TRIBUNALES SUPERIORES DE JUSTICIA

- STSJ Madrid de 24 de febrero de 1993.	- STSJ de Canarias de 22 de marzo de 2002.	- STSJ de Cantabria de 20 de febrero de 2004.
- STSJ Murcia de 20 de julio de 1993.	- STSJ País Vasco, de 1 de julio de 2002.	STSJ de Cantabria de 23 de febrero de 2004.
- STSJ Madrid de 2 de noviembre de 1994.	- STSJ Castilla y León, de 22 de julio de 2002.	- STSJ Comunidad Valenciana, de 27 de abril de 2004.
-STSJ Galicia de 21 de abril de 1995.	-STSJ Madrid de 18 de septiembre de 2002.	- STSJ Asturias de 30 de abril de 2004.
- STSJ de Cataluña de 11 de marzo de 1999.	-STSJ Las Palmas de 25 de octubre de 2002.	- STSJ Cataluña de 21 de septiembre de 2004.
- STSJ de Murcia de 15 de junio de 1999.	-STSJ de Madrid de 13 de noviembre de 2002.	- STSJ Castilla-La Mancha de 28 de febrero de 2005.
- STSJ Madrid de 26 de octubre de 1999.	-STSJ Murcia de 3 de febrero de 2003.	- STSJ Madrid de 28 de junio de 2005.
- STSJ Andalucía (Málaga) de 25 de febrero de 2000.	-STSJ de Cataluña de 11 de febrero de 2003.	- STSJ Cataluña, de 19 de julio de 2005.
- STSJ Cataluña de 19 de mayo de 2000.	-STSJ Madrid de 11 de febrero de 2003.	- STSJ Navarra, de 18 de abril de 2006.
- STSJ de Cataluña de 5 de julio de 2000.	-STSJ Madrid de 10 de abril de 2003.	- STSJ de Andalucía (Sevilla) de 10 de febrero de 2006.
- STSJ Madrid de 14 de septiembre de 2000.	-STSJ Andalucía, de 22 de abril de 2003.	- STSJ Madrid de 14 de junio de 2006.
- STSJ Cataluña, de 23 de octubre de 2000.	-STSJ Madrid de 13 de mayo de 2003.	- STSJ País Vasco de 12 de septiembre de 2006.
- STSJ de Madrid de 16 de enero de 2001.	-STSJ, (Cont-Admvo.) Cantabria de 16 de mayo 2003.	- STSJ Cataluña de 10 de diciembre de 2006.
- STSJ Cataluña, de 29 de junio de 2001.	-STSJ de Galicia de 30 de mayo de 2003.	- STSJ Madrid de 20 de diciembre de 2006.
- STSJ Madrid, de 17 de octubre de 2001.	-STSJ Cataluña de 11 de junio de 2003.	- STSJ Cantabria de 18 de enero de 2007.
- STSJ de Madrid de 21 de noviembre de 2001.	-STSJ Cataluña, de 11 de julio de 2003.	- STSJ País Vasco de 19 de junio de 2007.
- STSJ Galicia de 30 de noviembre de 2001.	-STSJ Madrid, de 23 de julio de 2003.	- STSJ País Vasco de 6 de noviembre de 2007.
- STSJ Galicia de 20 de marzo de 2002. - STSJ Cataluña de 4 de diciembre de 2007.	-STSJ Comunidad Valenciana, de 14 de enero de 2004. - STSJ Comunidad	- STSJ Castilla y León, Burgos (Sala de lo Social, Sección 1ª) Sentencia núm. 59/2017 de 9 febrero.

- STSJ Madrid, de 16 de enero de 2008. - STSJ Cataluña de 3 de junio de 2008. - STSJ Comunidad Valenciana de 11 de julio de 2008. - STSJ Madrid de 28 de septiembre de 2008. - STSJ Madrid de 5 de noviembre de 2008. - STSJ Galicia, de 6 de noviembre de 2008. - STSJ Cataluña, de 14 de enero de 2009. - STSJ Baleares de 28 de febrero de 2009. -STSJ Asturias de 13 de marzo de 2009. -STSJ Madrid de 17 de abril de 2009. -STSJ Burgos de 11 de junio de 2009. -STSJ Murcia de 3 de julio de 2009. -STSJ de Madrid de 5 de noviembre de 2009. -STSJ Extremadura de 1 de diciembre de 2009. -STSJ Comunidad Valenciana de 5 de enero de 2010. -STSJ Madrid de 15 de enero de 2010. -STSJ Murcia de 25 de enero de 2010. -STSJ Comunidad Valenciana, de 16 de febrero de 2010.	Valenciana, de 5 de octubre de 2010. - STSJ Galicia de 25 de enero de 2011. - STSJ País Vasco de 10 de mayo de 2011. - STSJ Madrid de 15 de septiembre de 2011. -STSJ Cataluña de 5 de marzo de 2012. -STSJ de Cataluña de 11 de octubre de 2013. -STSJ Madrid de 21 de marzo de 2014. -STSJ Galicia/A Coruña, de 25 de abril de 2014. -STSJ Castilla-La Mancha de 10 de junio de 2014. -STSJ de Cataluña de 8 de julio de 2014. -STSJ Andalucía (Sevilla) de 13 de octubre de 2014. -STSJ Andalucía (Sevilla) de 23 de octubre de 2014. -STSJ Madrid de 9 de febrero de 2015. -STSJ Castilla-La Mancha de 23 de marzo de 2015. -STSJ Andalucía (Sevilla) de 24 de septiembre de 2015. -STSJ País Vasco de 29 de septiembre de 2015. -STSJ Madrid de 6 de mayo de 2016. -STSJ Madrid de 13 de mayo de 2016.	- STSJ Madrid, (Sala de lo Social, Sección 6ª) Sentencia núm. 467/2017 de 22 mayo. -STSJ Andalucía (Sevilla, Sala de lo Social, Sección 1ª) 2029/2017, de 29 de junio. -STSJ País Vasco, Sala de lo Social, 2469/2018, de 11 de diciembre. -STSJ Andalucía (Sevilla, Sala de lo Social, Sección 1ª) 905/2019, de 28 de marzo.

F) AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

- Resolución AEPD 30/2000, de 27 de diciembre. - Informe AEPD sobre "Videovigilancia en el lugar de trabajo" (2001). -Resolución AEPD 00681/2004. -Instrucción AEPD 1/2006, de 8 de noviembre. -Informe Jurídico AEPD 0391/2007. -Informe AEPD 193/2008. -Resolución AEPD E/742/2008.	- Informe AEPD 101/2008. -Resolución de la AEPD 01823/2008. -Informe Jurídico AEPD 0247/2008: Acceso por el empresario al correo electrónico de los trabajadores. -Informe 402/2009 AEPD de 1 de enero de 2009. -Informe AEPD 613/2009. -Resolución AEPD de 1 de junio de 2009 (Expediente 489/2008).	- Resolución de la AEPD 00500/2009. -Informe Jurídico AEPD 0529/2009: Comunicaciones de la productividad de los trabajadores. -Informe del Gabinete Jurídico de la AEPD nº 0630/2009. -Informe AEPD 6/2009. -Informe AEPD 90/2009.

ANEXO II.- CONVENIOS COLECTIVOS.

CONVENIOS QUE REGULAN LAS CONDICIONES DE USO DE LAS TIC FIJANDO CRITERIOS CONCRETOS

- V Convenio colectivo para el sector de pompas fúnebres de Galicia (DO de Galicia de 16 de junio de 2015).

- I Convenio Colectivo de empresas vinculadas a Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones, SAU (BOE de 21 de enero de 2016).

- Convenio colectivo de “Mapfre, Grupo Asegurador” (BOE de 21 de agosto de 2014).

- Convenio colectivo para el sector de oficinas y despachos de Cataluña para los años 2012-2014 (DOGC de 6 de agosto de 2015).

- Convenio colectivo de seguros, reaseguros y mutuas de accidentes de trabajo (BOE de 16 de julio de 2013).

- BARCLAYS (2002): Acuerdo sobre canales de comunicación electrónica sindical en Barclays Bank, S.A. (firmado el 31 de mayo de 2002 por la compañía y la Sección Sindical Estatal de CC.OO. en la misma).

- LA CAIXA (2003): Código de conducta telemático para los empleados de La Caixa, Barcelona.

- XVIII Convenio Colectivo de la industria química (BOE de 19 de agosto de 2015).

- IV Convenio colectivo de Iberdrola Inmobiliaria, SAU, (BOE de 23 de febrero de 2016).

- Convenio colectivo estatal para el sector de ortopedias y ayudas técnicas, (BOE de 15 de marzo de 2016).

CONVENIOS QUE REGULAN LA UTILIZACIÓN DE LAS TIC MEDIANTE FÓRMULAS ABIERTAS

- Convenio colectivo de ámbito estatal para las industrias extractivas, industrias del vidrio, industrias cerámicas y para las del comercio exclusivista de los mismos materiales (BOE de 5 de junio de 2014).

- V Convenio colectivo estatal de despachos técnicos tributarios y asesores fiscales (BOE de 31 de octubre de 2013).

- XVIII Convenio Colectivo de trabajo para el sector de la industria metalgráfica de Catalunya para los años 2010-2013 (DOGC de 19 de agosto de 2011).

- Convenio Colectivo de Oficinas y Despachos de Huesca para los años 2013-2015 (BOP de

Huesca de 18 de diciembre de 2014).

- Convenio Colectivo de trabajo para el grupo de distribuidores de gases licuados del petróleo de la provincia de Barcelona para los años 2009-2011 (BOP de Barcelona de 25 de julio de 2011).

- Convenio Colectivo del sector de Industrias Transformadoras de Plásticos de Madrid (BO de la Comunidad de Madrid de 1 de noviembre de 2013).

- IV Convenio colectivo regional de empresas de televisión local y regional de Castilla y León (BO de Castilla y León de 11 de abril de 2011).

- Convenio colectivo del sector de transitarios de Madrid (BO de la Comunidad de Madrid de 23 de febrero de 2009).

- V Convenio colectivo para el personal laboral de la Xunta de Galicia (DO de Galicia de 3 de noviembre de 2008).

- XVIII Convenio colectivo general de la industria química (BOE de 19 agosto de 2015).
- Convenio Colectivo para la Industria de Azulejos, Pavimentos y Baldosas Cerámicas de la Comunidad Valenciana (DO de la Comunitat Valenciana de 12 de abril de 2013).

- Convenio Colectivo de trabajo de la industria de la construcción y obras públicas de la provincia de Barcelona para los años 2012-2015 (DOGC de 27 de agosto de 2013).

CONVENIOS QUE REGULAN LAS TIC DESDE UNA PERSPECTIVA ESTRICTAMENTE DISCIPLINARIA

- Convenio colectivo del sector de la madera de Almería (BOP de Almería de 3 de febrero de 2009).

- Convenio Colectivo de “Consum, Sociedad Cooperativa Valenciana” (BOE de 15 de diciembre de 2014).

- Convenio Colectivo del sector del comercio en general, de las comarcas de Lleida para los años 2015-2016 (BO de Lleida de 26 de noviembre de 2015).

- Convenio colectivo del sector de Industrias Transformadoras de Plásticos de Madrid (BO de la Comunidad de Madrid de 1 de noviembre de 2013).

- Convenio colectivo del sector del comercio textil de Valencia (BOP de Valencia de 6 de julio de 2013).

- Convenio Colectivo de la empresa “European Air Transport Leipzig GMBH, sucursal en España” (BOE de 13 de febrero de 2015).

- XIX Convenio colectivo de la ONCE y su personal (BOE de 14 de agosto de 2009).

- Convenio colectivo estatal de Grandes Almacenes (BOE de 22 de abril de 2013).

- Convenio Colectivo de fabricantes de muebles, carpintería, tapicería y ebanistería de Ourense (BOP de Ourense de 11 de diciembre de 2013).

- Convenio Colectivo del sector de industrias de carpintería y ebanistería de Ávila (BOP de Ávila de 28 de febrero de 2014).

- Convenio Colectivo de Actividades de Carpintería y Molduras, Cestería y Artículos de mimbre y junco, ebanistería y tapicería, carrocerías y carreterías, chapa y tableros y aglomerados y almacenistas de madera de Guadalajara (BOP de Guadalajara de 14 de agosto de 2013).

- Convenio Colectivo para industrias de la madera de Salamanca (BOP de Salamanca de 16 de agosto de 2013).

- Convenio Colectivo del sector de industrias y almacenes de la madera de Cádiz (BOP de Cádiz de 29 de agosto de 2013).

- Convenio Colectivo del sector de aserraderos y almacenistas de la madera de Cantabria (BO de Cantabria de 28 de abril de 2011).

- Convenio Colectivo provincial para las industrias de la madera de Toledo (BOP de Toledo de 28 de enero de 2008).

- IV Convenio Colectivo estatal de la madera (BOE de 27 de noviembre de 2012).