TRABAJO DE FIN DE GRADO

GRADO EN DERECHO

CURSO ACADÉMICO 2018-2019

DESPIDO Y NUEVAS TECNOLOGÍAS

DISMISSAL AND NEW TECHNOLOGIES

ALUMNA: Teresa Fernández de Lascoiti González Pinto

DIRECTOR: Rubén López-Tamés Iglesias

ÍNDICE

RESUMEN

Actualmente es un hecho indudable que el progreso tecnológico tiene una importancia vital en el ámbito social y laboral. Es el caso de la video vigilancia, de los medios electrónicos, de las redes sociales, etc. Todo esto da lugar a que surjan nuevas cuestiones que deben abordarse también desde varias perspectivas. La más trascendente, y que centrará mi atención, es la incidencia del poder del empresario en determinados derechos fundamentales, en el derecho a la intimidad de los trabajadores, en el secreto de las comunicaciones y en el derecho a la protección de sus datos.

En este trabajo se analiza la principal doctrina de los TSJ y la estricta jurisprudencia surgida por los conflictos entre empleador y empleado a propósito de la utilización de estos medios tecnológicos e informáticos en el ámbito laboral. Tales criterios son imprescindibles para determinar cuando el trabajador o el empleador han incurrido en un grave incumplimiento de sus obligaciones laborales estableciendo las consecuencias de tales infracciones.

ABSTRACT

It is currently an unquestionable fact that technological progress has a vital importance in the social and labor field. This is the case of video surveillance, electronic media, social networks, etc. All this leads to the emergence of new issues that must also be addressed from several perspectives. The most important, and that will focus my attention, is the impact of the employer's power on certain fundamental rights, on the right to privacy of workers, on the secrecy of communications and on the right to the protection of their data.

This paper analyzes the main doctrine of the TSJ and the strict jurisprudence arising from the conflicts between employer and employee regarding the use of these technological and computer resources in the workplace. Such judgements are essential to determine when the worker or employer has incurred a serious breach of their labor obligations by establishing the consequences of such infractions.

1. INTRODUCCIÓN

El objeto de este Trabajo de Fin de Grado se refiere a los conflictos que pueden surgir en la relación laboral con ocasión del empleo de los distintos medios tecnológicos, sometidos a un inevitable y permanente evolución; la video vigilancia, la informática, internet y redes sociales, tan presentes en nuestra sociedad. Con ello se analizan los limites empresariales en el uso de estos medios. El análisis versa sobre la jurisprudencia de diferentes tribunales, tanto a nivel europeo como a nivel nacional, la que permite conocer con precisión los criterios que se siguen cuando están comprometidos los derechos fundamentales.

La elección de este objeto de análisis nace, como no puede ser de otra forma, de la actualidad del tema, cuya vigencia puede presumirse que se mantendrá, ya que se trata de las consecuencias que para el Derecho del Trabajo tienen las nuevas tecnologías. En la última década han evolucionado de forma exponencial y ello ha afectado a las relaciones laborales. Las empresas se han tenido que adaptar a estos avances para permanecer competitivas en el mercado global y esto supone también una nueva realidad para sus trabajadores que se ven obligados a utilizar herramientas tecnológicas que hasta hace escaso tiempo ni se conocían, lo que inevitablemente incide en el ejercicio de los derechos fundamentales.

Empezaré por el análisis del marco normativo sobre los derechos fundamentales y el papel de la LOPD, ya que también está afectado directamente al derecho fundamental de la protección de datos. Inevitable el análisis del poder empresarial y su contrate con los derechos fundamentales del trabajador, si estos quedan modulados en el ámbito laboral, de manera que es necesario precisar cuándo se puede llegar a imponer el poder empresarial sobre ellos. Esta tarea llevará al análisis del juicio de necesidad, ponderación, idoneidad y proporcionalidad.

Se analizan después los distintos métodos con los que el empresario puede vigilar o controlar a los trabajadores, ya que la facultad de control es uno de sus derechos pero, a su vez, estas limitaciones pueden interferir en la relación laboral e incidir en el ejercicio

de los derechos laborales. Son muchas las sentencias, y generan una gran controversia referidas a redes sociales, internet, video vigilancia, etc.

Por último, analizo la calificación del despido, que es la sanción mas grave que puede haber en el ordenamiento laboral, en los supuestos, tan habituales, en los que se presenta una prueba ilícita por vulneración de derechos fundamentales. Más concretamente si el despido ha de calificarse como nulo o, tan solo, improcedente.

2. DERECHOS FUNDAMENTALES Y CONTROL EMPRESARIAL

2.1. LA MODULACIÓN DE LOS DERECHOS FUNDAMENTALES EN EL ÁMBITO LABORAL

Respecto a los derechos fundamentales en el ámbito laboral, se abordan tanto en la CE como en el ET. Dentro de ésta última norma, el Estatuto de los Trabajadores, en el artículo 4.1 ET, recoge los derechos específicos, aquellos derechos básicos de los trabajadores en cuanto tales (trabajo y libre elección de profesión u oficio, libre sindicación, negociación colectiva, huelga, reunión, etc.) pero también los derechos inespecíficos, es decir, aquellos que los asisten como a cualquier ciudadano, con independencia de la misma relación laboral (intimidad, propia imagen, libertad religiosa, derecho a la vida y a la integridad física y moral, igualdad, etc.).

Lo importante es que entre los derechos fundamentales y la relación laboral se produce una relación de mutua limitación, lo que supone la necesidad de proceder a una adecuada ponderación que respete la valoración constitucional del derecho fundamental y de las obligaciones laborales que puedan modularlos. De esta manera cuando un/a trabajador/a firma el contrato de trabajo y se genera con el empleador la relación laboral, estos derechos fundamentales inespecíficos quedarán sujetos al contrato de trabajo.

Se parte de la modulación de los derechos fundamentales en el contrato de trabajo, tal como se recoge en la STC 170/2013 de 7 de octubre, núm. de recurso 2907-2011, de forma que aquí el trabajador no pierde su condición y sus derechos constitucionales “por

insertarse en el ámbito de una organización privada" como es la empresa (STC 88/1985 núm. de recurso 788/1984, sala primera). Pero la "inserción en la organización laboral modula el ejercicio de aquellos derechos constitucionales en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva" (STC 99/1994 de 17 de mayo, núm de recurso 797/90), ya que el desenvolvimiento adecuado de la actividad productiva es "reflejo, a su vez, de derechos que han recibido consagración en el texto de nuestra norma fundamental (arts 33 y 38 CE)", como son el derecho a la propiedad privada y el derecho a la libertad de empresa.

2.2. DERECHO A LA INTIMIDAD, EL SECRETO DE LAS COMUNICACIONES Y EL DERECHO A LA PROTECCIÓN DE DATOS

En cuanto al derecho a la intimidad del demandante, podemos decir que la Constitución Española permite asegurar la plena efectividad de los derechos constitucionales, pero cuando la protección de este derecho colisiona con la libertad de empresa (artículo 38 CE), aparece la dimensión laboral en el derecho fundamental inespecífico y que trata de proteger la intimidad del trabajador.

En el Art 18.1 CE[1] se garantiza el derecho a la intimidad personal. Como se dice en la STC 70/2009 de 23 de marzo, núm. de recurso 2826-2004, sala primera, entre otra, "el secreto sobre la propia esfera de la vida personal y, por tanto, veda a los terceros, particulares o poderes públicos, decidir sobre los contornos de la vida privada (STC 83/2002, de 22 de abril, FJ 5)". En este sentido la STSJ de Baleares de 4 de septiembre de 2009 (AS 2656), donde se analizó un supuesto de instalación de las cámaras de seguridad en un aeropuerto como consecuencia de las sustracciones e incumplimientos sobre registros de consumiciones. Se produjo el archivo de la denuncia ante la Agencia de Protección de Datos, pero se destacó la prevalencia de la perspectiva de la intimidad.

Esta perspectiva es la que ha dominado el debate y las resoluciones del TC, que se basan en lo que llamamos "test de proporcionalidad", y tal doctrina considera que:

[1] Artículo 18.1 CE: "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

A) “El derecho a la intimidad no es absoluto, como no es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes siempre que el recorte que aquel haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, que sea respetuoso con el Derecho” (SSTC 57/1994, F.6 y 143/1994, F.6).

B) El TC ha afirmado que “los hechos referidos a las relaciones sociales y profesionales, en que el trabajador desempeña su actividad no se integran en la esfera privada de la persona (SSTC 98/2000 [RTC 98], 180/1987 [RTC 180], 202/1999 [RTC 202], entre otras). Pero “no puede descartarse que también en aquellos lugares de la Empresa en los que se desarrolla la actividad laboral puedan producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores” como podría ser la grabación de conversaciones entre un trabajador y un cliente o entre los propios trabajadores.

C) La constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. Como sintetizan las SSTC 66/1995 de 8 de Mayo [RTC 66], F.5; 55/1996, de 28 de Marzo [RTC 55], F. 6,7,8 y 9; 207/1996, de 16 de Diciembre, F.4- “para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: juicio de idoneidad, si tal medida es susceptible de conseguir el fin propuesto; juicio de necesidad, si es necesaria, en el sentido en el que no exista otra medida mas moderada para la consecución de tal propósito con igual eficacia y el juicio de proporcionalidad, en sentido estricto, que significa que si la misma 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.

Estas fueron las pautas que permitieron resolver que se declarase, por ejemplo, la constitucionalidad de la medida de instalación de un circuito cerrado de televisión para la vigilancia de la actividad laboral de un trabajador. Como expresaba la STC núm. 186/2000, de 10 de Julio (RTC 186), se cumplían tales pautas: era una medida justificada, ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo, era idónea, ya que trata de verificar si el trabajador cometía las irregularidades sospechadas, era necesaria, ya que la grabación serviría de prueba de tales irregularidades y por último, era equilibrada, ya que la grabación de

imágenes se limitó a la zona de la caja y a una duración de tiempo limitada. Por lo que en este caso debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art 18.1 CE.

Por otra parte en el artículo 18.4 CE[2], se habla sobre la protección de datos de carácter personal, a diferencia del Art 18.1 CE que reconoce de forma directa el Derecho a la intimidad, mientras que el Art 18.4 CE obliga a que una ley limite la aplicación de la informática sobre él. Por tanto, podemos decir que existe una relación directa entre ambos apartados, en la medida que es una protección especial o característica del derecho a la intimidad en el campo de la informática. En este apartado sobre la protección de datos de carácter personal podemos mencionar dos sentencias:

El TC resuelve en su Sentencia núm 26/2013 del 11 de febrero (RTC 26) el caso siguiente: La Universidad de Sevilla contaba con autorizaciones de la AEPD para hacer uso de los soportes informáticos grabados por sus videocámaras, entre ellas una dirigida al control de acceso de las personas de la comunidad universitaria y el personal de empresas externas a los campus y centros. Estas imágenes fueron utilizadas como prueba para la imposición de tres sanciones, de suspensión de empleo y sueldo al subdirector de la unidad técnica de orientación, por faltas reiteradas e injustificadas de puntualidad y transgresión de buena fe contractual y abuso de confianza, así como faltas de asistencia injustificadas al trabajo.

Se considera que las imágenes grabadas constituyen un dato de carácter personal del art 18.4 CE y recogido igualmente en el artículo 3.a) de la LOPD y artículo 2.a) de la Directiva 95/46/CE, esta directiva entiende como “datos personales” a toda información sobre una persona física identificada o identificable. En consecuencia, y según las palabras del Tribunal, en lo supuestos de vídeo-vigilancia nos encontramos dentro del derecho fundamental del art 18.4 CE. Según se expresa en el caso enjuiciado, se vulneró el art 18.4 de la CE, ya que las cámaras de video-vigilancia captaron su imagen, que constituye un dato de carácter personal, y que se emplearon para el seguimiento del

[2] Artículo 18.4 CE “ La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

cumplimento de su contrato, y tampoco se informó al trabajador sobre la utilidad de supervisión laboral asociada a las capturas de su imagen.

Según declaro el TC es necesaria una "información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que la captación podía ser dirigida", información que debe "concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuanto tiempo y con qué propósitos, explicitando que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo".

La Sala 4ª del TS, vino a aplicar la anterior doctrina citada en el caso de los supermercados CHAMPION en su STS de 13 de mayo de 2014. Rec. 1685/2013.

En esta sentencia, el titular del supermercado procede al despido disciplinario de una cajera, basándose en la prueba obtenida por unas imágenes captadas a través de una cámara de seguridad permanente.

Se expresa conforme a la doctrina del TC que por parte de la empresa no se dio una información previa a la trabajadora de la posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras instaladas permanentemente, ni tampoco se informó con carácter previo ni posterior a la instalación de esos dispositivos, a la representación de los trabajadores de las características y el alcance del tratamiento de datos que iba a realizarse; por el contrario, al requerir los representantes de los trabajadores a la empresa, una vez instaladas, se les dijo que su finalidad era la de evitar los robos por terceros y que no era un sistema para controlar su actividad laboral, y que, a pesar de ello, se utilizó con la indicada y distinta finalidad de controlar la actividad de la demandante y luego para sancionar a esta con el despido.

Habría que distinguir en este punto entre una instalación fija, que requiere respetar el artículo 18, apartados 1º y 4º CE, y otra temporal, que requiere respetar el artículo 18.1º CE, ya que el artículo 18.4 CE (la "tutela informática") solo se aplicaría si existe un sistema de captación y tratamiento de imágenes que motivara la protección de datos. No tendría sentido avisar al destinatario de que se va a colocar una instalación temporal para

evitar el delito, ya que, éste, previamente advertido, no podría ser sorprendido. Esta matización se confirma en la STC de 3 de marzo de 2016[3], que posteriormente se desarrollará.

Y por último en cuanto al apartado del secreto de las comunicaciones podemos decir que partiendo de que según tiene reconocido el TC el derecho al secreto de las comunicaciones que la CE garantiza es un concepto formal, es decir, no por que lo comunicado sea necesariamente íntimo o reservado, se ha delimitado el contenido de este derecho entendiendo que el artículo 18.3 C[4] protege únicamente ciertas comunicaciones: las que se realizan a través de determinados medios o canales cerrados; así pues quedan fuera de la protección constitucional aquellas formas de envío de la correspondencia que se configuran legalmente como comunicación abierta, esto es, no secreta.

De esta forma, en las comunicaciones electrónicas en el ámbito de las relaciones laborales, que entran dentro de las "facultades de autoorganización, dirección y control correspondientes a cada empresario, no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales".

Existe, sin embargo, un cambio de doctrina en la sentencia del pleno del TC de 3 de marzo 2016 acerca del alcance del deber informativo previo.

Lo hechos de este supuesto son: la demandante de amparo venía prestando sus servicios para la empresa Bershka BSK España, S.A. fue despedida por transgresión de la buena fe contractual. El departamento de seguridad de Inditex, a raíz de la instalación de un nuevo sistema de control informático de caja, detectó que en la tienda y caja donde

[3] Así lo entiende, por ejemplo, C. GONZÁLEZ GONZÁLEZ, "control empresarial de la actividad laboral, vídeo vigilancia y deber informativo". A propósito de la STC de 3 de Marzo de 2016. *Revista Aranzadi Doctrinal, nº 5/2006.* BIB 2016/21165.

[4] Artículo 18.3 CE " Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

prestaba sus servicios la demandante existían múltiples irregularidades. La recurrente en amparo considera vulnerado el art. 18.4 CE porque no había sido informada previamente de la instalación de cámaras de video vigilancia en el puesto de trabajo. Las cámaras de video vigilancia instaladas en la tienda donde prestaba sus servicios captaron su imagen apropiándose de dinero y realizando, para ocultar dicha apropiación, operaciones falsas de devoluciones de venta de prendas.

Según consta en los hechos probados de las resoluciones recurridas, la cámara estaba situada en el lugar donde se desarrollaba la prestación laboral, enfocando directamente a la caja, y en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo exigido por la 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 la demanda se reclama por la vulneración tanto del 18.1 CE como del 18.4 CE, el primero de estos dos derechos examinados por tribunal con un menor énfasis al entender que no se vulnera debido al cumplirse en la medida empresarial el principio de proporcionalidad a la hora de considerar el triple test: idónea, necesaria y proporcionada de la video-vigilancia de la caja registradora por parte de los trabajadores ante una justificación fundada en sospechas. Por otro lado, en lo referente al 18.4 CE, donde esta lo más relevante para el tribunal, la instalación de la cámara no se comunicó a los trabajadores, y sí se informó con carácter general, es decir se colocó el distintivo informativo requerido por la normativa vigente, en un lugar visible del escaparate del establecimiento, es decir, la medida adoptada es proporcional para lograr la finalidad deseada.

Textualmente, la sentencia dice que: Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 TRLET, en conexión con los arts. 33 y 38 CE” y en su fundamento jurídico 4º: “En consecuencia, teniendo la trabajadora información previa de la instalación de las cámaras de vídeo-vigilancia a través del correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el art. 18.4 CE.

Finalmente, el tribunal lo valora como una medida justificada, idónea para la finalidad pretendida por la empresa, necesaria y equilibrada. Por tanto, se decidió desestimar el recurso de amparo interpuesto por la demandante.

El primer voto particular fue del magistrado D.Fernando Valdés Dal-Ré que fue ponente en la STC 29/2013 y al que se adhiere la Magistrada D. Adela Asúa Batarritaque manifiestan que la sentencia supone un "retroceso en la protección de los derechos fundamentales" de los trabajadores. Comprenden que se debió declarar nulo el despido porque la instalación de las cámaras se realizó sin informar al empleado de su finalidad concreta y se vulneró su derecho fundamental a la protección de datos personales.

Según su criterio, la sentencia modifica la doctrina olvidando la capacidad dada hasta ahora por el Tribunal al derecho protegido por el artículo 18.4 CE. La diferencia entre este derecho y el artículo 18.1 CE está en el control del uso y destino de los datos personales "está constitucionalizado y en la base de la consagración del derecho fundamental".

Además, consideran que para verificar el cumplimiento de las obligaciones laborales del empleado se exige ofrecer previamente la información necesaria sobre la finalidad de la instalación de las cámaras.

El segundo voto particular, suscrito por el magistrado Xiol Ríos, estaría dispuesto, dentro de ciertos limites a reconsiderar la jurisprudencia sentada en la STC 29/2013 (RTC 2013,29) sobre el hallazgo casual, en paralelo con la evolución de la jurisprudencia penal sobre la materia pero considera la trascendencia toda omisión de información a los trabajadores (sobre la existencia de cámaras enfocadas a posiciones plantea un supuesto enteramente diferente). Incluso este voto hubiera estado dispuesto a considerar la justificación de que la instalación de las cámaras se notificase únicamente al comité de empresa. También el mantenimiento de las sentencias que dieron lugar al recurso de amparo, habida cuenta de que tanto en primera instancia como en suplicación se hace constar por los respectivos tribunales que existen, otros elementos de prueba independientes de la vídeo-vigilancia suficientes para entender probados los hechos que dieron lugar al despido.

Son multitud los comentarios negativos que se han hecho a esta citada sentencia[5]. No sin embargo, desde otros ámbitos en los que la conducta empresarial se llega a calificar de "castigo altruista"[6].

3. CONTROL EMPRESARIAL Y NUEVAS TECNOLOGÍAS

La tecnología constituye hoy una forma de control prácticamente ilimitada. Abarca desde el sistema más convencional, que sería la vídeo-vigilancia, a otros más novedosos como el registro del ordenador, correo electrónico, historiales de navegación y "cookies", ya de forma física o mediante la instalación de programas espía capaces de revelar un amplio espectro de informaciones, hasta las más sofisticadas formas de control que existen (localización dentro de la empresa y fuera de esta, mediante tarjetas de identificación o sistemas de localización vía satélite o GPS).

Además de las ya conocidas intervenciones de las conversaciones telefónicas mantenidas desde terminales de la compañía o grabaciones y escucha en los centros de trabajo.

El artículo 20.3 del ET comprende la facultad de "*adoptar las medidas que estime mas oportunas de vigilancia y control para verificar el cumplimento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana*".

[5] Por ejemplo, entre otros, el inmediato de W. SANGUINETI, "Derechos fundamentales y poderes empresariales: ¿Quo Vadis TC? Escribe Juan Bautista Vivero".

[6] De lo que hay que alegrarse porque, como habíamos dicho en otra entrada en el Almacén de Derecho, si queremos aumentar los niveles de cooperación en nuestra Sociedad, es imprescindible que incentivemos el llamado "castigo altruista", es decir, el castigo a los que incumplen las reglas aunque sea costoso para el que castiga. Dadas las cantidades sustraídas por la dependienta, es evidente que la Empresa incurrió en gastos muy superiores para descubrir la apropiación indebida de las cantidades sustraídas. J. ALFARO "El Constitucional cambia su doctrina sobre la dependienta ladrona", *Almacén de Derecho*, Miércoles, 16 de Marzo de 2016.

Este genérico precepto regulador del poder de vigilancia y control empresarial se completa con la previsión establecida en el artículo 18 del ET a cuyo tenor: "*solo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo"*.

El poder de vigilancia y control empresarial previsto en el art 20.3 del ET va dirigido a comprobar el efectivo cumplimento por el trabajador del sus "*obligaciones y deberes laborales"*. Pero aquí cabría hacer una distinción entre la utilización de los medios tecnológicos de información y comunicación de la empresa como instrumentos de control y vigilancia de la prestación laboral y el control del uso, adecuado o inadecuado, por el trabajador de dichos medios[7].

En este sentido se afirma que mientras el primero persigue un control objetivo o general del cumplimento de la prestación laboral en sentido positivo, el segundo, en cambio, se dirige a la supervisión, aislada y personal del correcto cumplimiento por parte de un trabajador concreto o un grupo de trabajadores de las obligaciones y reglas laborales. Se trata en este último caso de un control más invasivo, mas incisivo respecto de la intimidad personal. Y, por ello, se sostiene que, para analizar la legitimidad de los mecanismos de control empresarial sobre el uso inadecuado de los medios tecnológicos de información y comunicación por parte de los trabajadores, hay que acudir al art 18 del ET[8].

[7] En este sentido, GONZÁLEZ ORTEGA, S., "La informática en el seno de la empresa. Poderes del empresario y condiciones del trabajo", en AA.VV., *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004, págs 38 y ss.

[8] Cfr. STSJ de Andalucía, Málaga, de 25 de Febrero de 2000 (AS/562).

3.1. USO DEL ORDENADOR Y CORREO ELECTRÓNICO

En cuanto al uso del ordenador, podemos decir que la naturaleza o condición otorgada por el empresario a los medios tecnológicos de información y comunicación es, por lo general, la de propiedad de la empresa, por lo que esta tiene pleno poder de disposición a la hora de concretar las condiciones de uso de los mismos. No está obligada a dejar que se empleen para cuestiones personales;[9] es mas, ni siquiera esta obligada a pactar con el trabajador o con sus representantes las condiciones de uso de los mismos[10].

El Tribunal Constitucional, en su sentencia 173/2011 [11] ya indicó que el ordenador es una herramienta para la emisión y recepción de correos electrónicos y con carácter general es imprescindible para el buen funcionamiento de la organización productiva.

Respecto al correo electrónico, la navegación web o la utilización de un dispositivo telefónico, etc., se trata de instrumentos que son necesarios para el desarrollo de la actividad laboral pero el problema surge cuando se produce un uso indebido de estos medios, es decir, con fines no laborales, sino personales. Aquí es cuando el poder del empleador emerge con su capacidad de control y pudiendo llegar a limitar los derechos del trabajador.

Una de las primeras sentencias destacada por su importancia en el ámbito Europeo, y que incidirá en nuestra jurisprudencia, acerca de la monitorización de los equipos de trabajo. es la conocida como "el Caso Copland contra el Reino Unido"[12]. En este caso, el Tribunal Europeo de Derechos Humanos (TEDH) estimó una

[9] THIBAULT ARANDA, J. L., El Derecho español, cit., pág. 61. "Tecnología informativa y privacidad de los trabajadores" 2003, ISBN 84-9767-257-7.

[10] GOÑI SEIN, J. L., "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", en AA.VV., *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Albacete, 2004, pág. 80.

[11] STC 173/2011 de 7 de noviembre [RTC 2011, 173]

[12] STEDH de 3 abril de 2007 (62617/2000).

demanda interpuesta por un trabajador contra la empresa porque esta última tenía la sospechas de un uso inadecuado de los equipos de trabajo de la empresa (navegación web, teléfono, correo electrónico) y decidió hacer una monitorización o seguimiento de los movimientos realizados por el trabajador. La monitorización no controlaba el contenido, pero sí el número de veces que se visitaban las páginas web, el número de llamadas realizadas y tiempo que dedicaba en ellas y a quien las realizaba, etc.

El Tribunal estimó la demanda y llegó a la conclusión de que la recogida y almacenamiento de información personal sin el consentimiento ni el conocimiento constituye una intromisión en su derecho al respeto de su vida privada.

La jurisprudencia matiza después hasta dónde se puede llegar y qué consecuencias puede llegar a tener un incumplimiento por parte del trabajador, o por el contrario, si está suficientemente justificada la actuación del empleador y si las medidas adoptadas son proporcionales y necesarias.

Una sentencia muy reveladora del Tribunal Supremo, dictada, en recurso de casación para unificación de doctrina[13] , da luz a la cuestión clave. Admitida la facultad de control del empresario y la licitud de una prohibición absoluta de los usos personales, consiste en determinar si existe o no un derecho del trabajador a que se respete su intimidad cuando, en contra de la prohibición del empresario o con una advertencia expresa o implícita de control, utiliza el ordenador para fines personales.

La respuesta parece clara: si no hay derecho a utilizar el ordenador para usos personales, no habrá de haber en unas condiciones que impongan un respeto a la intimidad, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad. Si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo.

[13] STS 8876/2011 de 6 de octubre de 2011.

En el caso del uso personal de los medios informáticos de la empresa no puede existir un conflicto de derechos cuando hay una prohibición valida.

La prohibición absoluta podría no ser válida si existe reconocido en el convenio colectivo aplicable el derecho a un uso personal de ese uso. La prohibición determina que ya no exista una situación de tolerancia con el uso personal del ordenador. En estas condiciones el trabajador afectado sabe que su acción de utilizar para fines personales el ordenador no es correcta y sabe también que está utilizando un medio que, al estar lícitamente sometido a la vigilancia de otro, ya no constituye un ámbito protegido para su intimidad.

La Sentencia de la Sala Cuarta, de 8 marzo 2011[14] confirma referido criterio después: Se trata de un despido por uso del ordenador, el caso consiste en: la Empresa Font Salem, perteneciente al grupo Damm, en los meses de enero y febrero del año 2009 realizó una autoría interna en las redes de información con el objetivo de la mera revisión de la seguridad del sistema y también el de detectar posibles problemas o anomalías en los medios que se les dan a los empleados de dicha empresa. En primer lugar en lo que concierne al ordenador utilizado por los jefes del turno, en los meses que se cortan anteriormente, se detecto que se accedió a internet en las horas de trabajo, con un total de 5.566 visitas a paginas web relacionadas con la piratería informática, televisión, anuncios, etc. Gran parte de estas visitas a las paginas web se realizaron en horas laborales, en los turnos de trabajo de uno de los trabajadores de la empresa. Además, la gran mayoría de visitas a dichas paginas web se realizaron en el momento en el que el trabajador se encontraba solo en el despacho.

Pero sin embargo, en el caso denominado “las Manteletas”, resuelto por STS del 6 de Octrubre del 2011, en la Sala General, se suavizan los requisitos referidos. Este caso trata sobre: la empresa entregó a todos los trabajadores una carta, la cual firmaron, en la cual se comunicaba a estos que quedaba prohibido el uso de los medios que han sido dispuestos por la empresa, tales como, ordenadores, internet, móviles, etc. Se especificó que esta prohibición era únicamente para el uso personal de los mismos, y tanto fuera

[14] RJ 2011\932

como dentro del horario de trabajo. Por consiguiente, la Empresa decidió hacer una comprobación sobre el uso de estos medios, para ver si se seguían las órdenes dadas anteriormente, se realizó a finales de enero de 2009, y consistió en la monitorización de los ordenadores de dos trabajadoras, encargándose de la instalación del software de monotorización, con el objeto de capataz las pantallas a las que se había accedido y para más tarde realizar dicha comprobación. A raíz de esto, se detectó por la empresa que una de las trabajadoras realizadas determinadas visitas a internet por asuntos propios, que nada tenía que ver con su cometido laboral, todo esto en horas de su jornada laboral, por lo tanto, como consecuencia de esto, se procedió a su despido.

Se introduce una matización respecto a lo antes señalado, la cual es novedosa, por la STS de 2007, que trata sobre: la admisión del control oculto, el que se realiza sin la advertencia de la posible motorización por parte de la Empresa, cuando ésta ha prohibido de manera expresa el uso personal de los medios informáticos de su propiedad.

Las prohibiciones de uso personal de las herramientas telemáticas, ya implican una advertencia del posible control por parte de la empresa, y estas por tanto incluyen la instalación de sistemas de control del uso de estos medios por parte de los trabajadores, por lo tanto elimina toda intimidad y secreto de comunicaciones por parte de ellos. Confiera el criterio menos exigente, anteriormente empleado por alguna otra resolución.

Podemos hacer referencia aquí a lo expuesto en la STS del 26 de septiembre de 2007 (RJ 2007, 7514), la cual dice que se exige la información a los trabajares de la posible existencia de control por parte de la empresa, de estos medios informáticos. Esta exigencia no se podría aplicar a los supuestos de una prohibición absoluta de los medios tecnológicos, en los que no concurre ninguna expectativa de una posible intimidad por parte de los trabajadores.

La diferencia que podemos apreciar entre estas sentencias del TS y la sentencia del TC de 170/2013, es que en la primera de ellas se entiende que el trabajador ya está previamente avisado sobre el posible control de los sistemas informáticos que la Empresa pone a su disposición, ya que esto se encuentra recogido en el convenio colectivo al que pertenece la empresa y por consiguiente, los trabajadores.

En este sentido nos parece, también clarificadora la cercana STS de la Sala de lo Social de 20 de Marzo de 2018, rcud 1461/2017, en la que se plantea un despido disciplinario cuya razón se encuentra en el control de la empresa del ordenador portátil y del teléfono móvil entregado a un trabajador.

En este caso[15] la Sala, resuelve, en primer lugar, la alegación de nulidad de actuaciones, por no haberse valorado la prueba de acceso al ordenador y teléfono móvil; y al respecto, tras referir abundante doctrina, concluye que en este caso es obligado determinar si existe una prohibición empresarial de usar tales medios, ordenador y teléfono móvil, mas allá que para cuestiones empresariales, prohibiendo el uso particular. Y entiende que es una cuestión no discutida que no existía una prohibición expresa del empresario al respecto, aunque sí que existía dicha prohibición en los arts 50 y 51 del Convenio Colectivo para las empresas siderometalúrgicas de la región de Tarragona, que es el que regula las relaciones laborales de la empresa. En el art 50.i) del Convenio se cita entre las faltas graves: "la realización sin previo consentimiento de la empresa, de trabajos particulares durante la jornada de trabajo, así como el empleo para usos propios o ajenos de los útiles, herramienta, maquinaria o vehículos de la empresa, incluso fuera de la jornada de trabajo. "Pero a juicio de la sala no puede perderse de vista la especial situación que respecto al uso de ordenadores y teléfonos móviles se produce, con situaciones que

[15] El demandante prestó servicios para la empresa demandada, Unidalque Servicio y Mantenimiento SL, ostentando la categoría profesional de Maestro Industrial. La empresa entregó al inicio de la relación laboral, entre otros útiles, un ordenador portátil y un teléfono móvil, para la ejecución de su trabajo tanto en España como en los distintos viajes al extranjero que ha debido de realizar durante los años 2013-2015; dicho ordenador (y móvil) era utilizado esencial y básicamente para su actividad profesional, si bien residualmente era utilizado por el actor para algunas cuestiones personales, no habiéndosele prohibido desde su entrega que lo utilizara para tareas ajenas al trabajo. El 4-12-2015 el Gerente de la empresa accedió al ordenador entregado por el actor, así como al teléfono móvil, sin autorización del mismo, y sin presencia de ningún otro trabajador de la empresa, comprobando que en él había fotografías personales, vídeos y datos personales del demandante, introduciéndose en su contenido. Como consecuencia, la empresa procedió a expedir la carta de despido el 16- 12-2015; posteriormente, contrató los servicios de un Ingeniero Informático, quien el 23-2-2016 en las oficinas de la empresa junto con el Gerente y una empleada y el propio Letrado de la empresa accedieron al ordenador y al móvil que había entregado el actor, a fin de que dicho perito emitiera un dictamen sobre los datos y su contenido.

no se dan con otros útiles que la empresa pone a disposición de los trabajadores para desarrollar su trabajo, como, por ejemplo, camiones, automóviles, martillos, etc…, respecto de ninguna de las cuales se llega a afirmar la existencia de un "hábito social generalizado de tolerancia con ciertos usos personales moderados", máxime en el caso de autos, en los que el ordenador no está en la empresa, sino que es portátil y por lo tanto el trabajador lo lleva siempre consigo para el desarrollo de su trabajo, algo que por cierto se da siempre con el teléfono móvil. Y siendo así, concluye que la prohibición que se deriva de la calificación como falta grave del empleo para usos propios de los útiles, herramientas, maquinaria o vehículos de la empresa, no puede por lo tanto considerarse como una prohibición absoluta de utilización del ordenador y teléfono movil entregado al actor por la empresa y consiguientemente, no está amparado el ejercicio de control realizado por el gerente de la Empresa el 4/12/2015.

Se denuncia la infracción de los arts. 50 y 51 del Convenio en lo relativo a la imputación consistente en el uso del ordenador y del teléfono móvil. La Sala señala la íntima conexión que tiene con la cuestión planteada de la nulidad. Y señala que ninguna infracción se ha producido ante la inexistencia de prohibición expresa del empresario respecto de la utilización para fines privados del teléfono móvil y del ordenador portátil, pues el examen de ambos por el empresario vulnera el Derecho a la intimidad del trabajador y por lo tanto, no puede darse por válido lo obtenido por este en el examen y consecuentemente no existe elemento fáctico alguno que permita sustentar el incumplimiento denunciado; de donde deriva que no se ha producido ningún incumplimiento grave y culpable del trabajador.

El recurso de casación para la unificación de doctrina se interpone por la Empresa y tiene por objeto determinar la procedencia del despido del acto, por ser válido el examen del ordenador del trabajador, en tanto que herramienta de trabajo facilitada por la Empresa y ser de aplicación correspondiente Convenio Colectivo, que tipifica como falta muy grave el uso para usos propios ajenos a los útiles o herramientas facilitados por la empresa.

En lo que interesa a esta casación unificadora, razona la defensa de la parte recurrente que los documentos relacionados en la carta de despido han sido obtenidos de forma "ilegal" por lo que se debió declarar la nulidad de los mismos ya que en su obtención no se han respetado las garantías que amparan al trabajador afectado, pues, si

bien el ordenador que utilizaba el actor era propiedad de la empresa y es un medio de producción que utilizaba el trabajador, ello no puede suponer que sobre el mismo y sobre su contenido haya un poder omnímodo e indiscriminado por parte del empresario. También se afirma por el recurrente que no se dan los requisitos fijado por el TC para considerar validas las pruebas que alega la empresa en la carta de despido, por lo que las mismas debieron declararse nulas por vulneración de derechos fundamentales del trabajador.

De conformidad con lo establecido en los artículos 219 y 255 de la LRJS, sin que consten escrito de alegaciones de la parte en contestación a la providencia de la sala de 17 de Noviembre de 2017, se procede a a declaración de inadmisión del recurso.

La sala acuerda declarar la inadmisión del recurso de casación para unificación de doctrina interpuesto en nombre de Unidalque Servicio y Mantenimiento S.L, contra la sentencia dictada por la Sala de lo Social del Tribunal Superior de Justicia de Cataluña.

También alguna sentencia de los Tribunales Superiores de Justicia me ha parecido relevante, como la sentencia TSJ nº 2716/2010, de 5 octubre, Rec. núm. 2195/2010, de la Comunidad Valenciana.

El supuesto es claro: la actora había cambiado la dirección IP del ordenador, borraba el historial tras estar navegando por internet viendo cosas ajenas al trabajo (carteleras de cine, dormitorios infantiles, traspaso de negocios o inmuebles de forma continuada), intenta también cambios del número de proveedor, intentó formatear el ordenador, incluso alterar el programa de control, es decir, llevó a cabo conductas inadecuadas en los instrumentos que tenía a su disposición para trabajar. Esta conducta fue calificada de transgresión de la buena fe contractual, pues se quebrantó la confianza y lealtad exigibles en la relación laboral. Por ello, se estimo correcta la decisión empresarial al calificarla como falta muy grave tipificada por el convenio colectivo aplicable.

Pero lo que se analiza, sobre todo, es si la empresa podía acceder al ordenador de la trabajadora a fin de comprobar cuanto era el tiempo que se utilizaba para acceder a páginas de internet ajenas a la empresa, o al correo electrónico. Desde este punto de vista,

se señala que constituye ya jurisprudencia aceptada y reiterada que las medidas empresariales encaminadas a realizar una actuación inspectora o de control de la actividad laboral de sus trabajadores, deben de ir precedidas, de la necesaria información a los concretos destinatarios de los sistemas de control establecidos. Así se ha considerado, que sería contrario a lo que llamamos buena fe contractual que debe presidir las relaciones laborales en la empresa, el establecimiento de mecanismos de supervisión del uso que hacen los trabajadores de los medios informativos que les da la empresa para el ejercicio de su cometido laboral, sobre todo si la implantación de tales medios no obedece a una sospecha previa de actuación fraudulenta por parte del trabajador que ha sido investigado.

La valoración que ha sido efectuada por el TS en la sentencia del 26 de Septiembre de 2007 (RJ 2007,7514), rec. 966/2006, la cual expuso en su aplicación a un supuesto de hecho muy similar que: "el art 18 del ET no es aplicable al control por el empresario de los medios informáticos que se ponen a disposición de los trabajadores para la ejecución de la prestación laboral", o dicho de otra forma "el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del art 18 del ET, una justificación especifica de caso por caso. Por el contrario, su legitimidad deriva directamente del art 20.3 del ET".

La aplicación de tal doctrina implica que en el caso concreto, la empresa procedió a avisar de la instalación de un programa para contabilizar el tiempo que cada trabajador empleaba en internet, en el que se procedía al registro de todas las direcciones que se visitan, y de los correos electrónicos, recordando a los trabajadores de la empresa que se trata de herramientas que se ponen a disposición del trabajador con el fin de desarrollar su tare profesional de forma mas rápida y eficaz, y que todo uso que no sea adecuado de internet o del correo electrónico sería registrado y grabado; esto constituyó un aviso claro y conciso del sistema de control que la empresa iba a efectuar, que se ajustaba a las previsiones legales y doctrinales, ya que fue comunicado tanto a los trabajadores como a los representantes de éstos y esto no implicaba un exceso, ya que no ha afectado al contenido de los mensajes de correo.

En cuanto a la intervención del correo electrónico, es bien conocida la STC (sala 1ª) 170/2013, de 7 de Octubre de 2013[16]. El trabajador fue despedido por transgresión de la buena fe contractual al que se refiere el articulo 54.d) del ET. Los preceptos del convenio colectivo aplicable eran, de acuerdo con el propio relato de STC 170/2013, en, primer lugar, el que lo tipificaba de falta leve: "la utilización de medios informáticos propiedad de la empresa (correo electrónico, internet.) para fines distintos de los relacionados con la propia prestación laboral. El segundo precepto la califica como falta muy grave, y facultaba para sancionar, como tal, la inobservancia del deber de reserva de datos de la empresa. Por ello, considera que si el medio se utilizaba en contra de prohibiciones (de uso) y con conocimiento por parte de los afectados de los controles y medidas aplicables, no podía entenderse que, al realizarse el control por parte de la Empresa, se haya vulnerado una expectativa razonable de intimidad del trabajador.

Se considera que la comunicación no es secreta o realizada en "canal cerrado" sino comunicación abierta porque, establecida la prohibición del uso "extralaboral" del ordenador, a través de la sanción prevista en el convenio, la empresa está habilitada para el registro empresarial del ordenador de trabajo, en el ejercicio del poder de dirección, en su vertiente de "vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales" (art 20.3 ET). También se rechaza la supuesta violación de la intimidad del demandante y la "proporcionalidad en sentido estricto". La medida adoptada de registro del disco duro del ordenador de trabajo del demandante se entiende en el caso "ponderada y equilibrada", ceñida a los "correos electrónicos aportados por la Empresa como prueba en el proceso de despido", y sin abarcar " aspectos específicos de la vida personal y familiar del trabajador".

Descendiendo a la doctrina de los Tribunales Superiores, una de las primeras que abordó estas cuestiones, fue la STSJ de Madrid, del 30 de Enero de 2001, recurso de suplicación 3341/01, sobre un despido disciplinario calificado como procedente por el

[16] Referida a un trabajador de la sociedad Alcal, S.A. Ésta se dedica al cultivo de la planta adormidera para la obtención de alcaloides. Alcal tuvo noticias de que su actividad productiva estaba siendo puesta en conocimiento de otra empresa a través de alguno de sus empleados, por ello decidió adoptar medidas de control, y una de ellas fue al ordenador del demandante de amparo.

uso abusivo del correo electrónico por parte de un trabajador[17], se alega en el recurso una violación de la presunción de inocencia. El motivo es desestimado porque, siguiendo la jurisprudencia constitucional, resulta inaplicable en el ámbito de las relaciones laborales. Alegada una violación al derecho a la intimidad, también es desestimado, porque es el empresario el que ha prohibido el uso del ordenador para fines meramente personales y que puede comprobar la utilización de que el mismo hace. Por lo tanto, el despido se califica como procedente.

Más recientemente, todas estas cuestiones han quedado afectadas por la doctrina del TEDH,que consagra importantes límites a la restricción a los derechos fundamentales. Lo hace en el denominado caso "BARBULESCU contra RUMANIA". El demandante era el responsable de ventas de la empresa, advertido del uso de recursos de la empresa para usos personales creó una cuenta de Yahoo Messenger para atender a las solicitudes de los clients. A pesar de negarlo, se comprobó que se había utilizado para tales fines particulares. Lo utilizaba para comunicarse con su novia y sus hermanos. El empleador le informó de que había realizado un control de la actividad de esa cuenta de correo durante la semana anterior. La empresa demostró los hechos con una transcripción de las comunicaciones de dicha cuenta y el tribunal entendió con amparo en la Directiva 95/46/CE[18] que la conducta del empleador había sido razonable y que la vigilancia de las comunicaciones había sido el único método para establecer si se había producido una infracción disciplinaria[19].

El demandante, además de negar los hechos de que se le acusaba, señaló que se había vulnerado su derecho al secreto de la correspondencia al haber sido registrado su correo electrónico.

[17] El actor fue despedido por utilizar para enviar desde el ordenador del puesto de trabajo correos electrónicos con fines personales, algunos de ellos insultantes para miembros de la familia titular la Empresa.

[18] Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta tratamiento de datos personales y a la libre circulación de estos.

[19] STEDH de fecha 12 de enero de 2016.

Ante el TEDH, el trabajador alegó una vulneración del artículo 8 del Convenio para la protección de los derechos y de las libertades fundamentales (Roma, 4 de noviembre de 1950), que dice que “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”.

Los tribunales de Rumanía declararon que el despido era procedente al haberse realizado conforme a la legislación aplicable, y que no se había violado el derecho a la intimidad del trabajador, pues éste había sido informado de la normativa interna de la empresa y el registro de su correo era el único modo para comprobar si se habían cumplido las normas.

El Tribunal señala que el empleador puede comprobar que sus empleados cumplen con sus obligaciones durante el horario de trabajo, y que en este caso había accedido a la cuenta de correo del trabajador suponiendo que solo contenía comunicaciones con los clientes de la empresa. Además, señala el Tribunal que los órganos judiciales internos no desvelaron el contenido de las comunicaciones, sino que éstas se utilizaron únicamente para probar que el trabajador utilizó el ordenador de la empresa con fines distintos a los estrictamente laborales durante la jornada de trabajo.

El TEDH concluye por tanto, que no se ha producido una vulneración del artículo 8 del Convenio, puesto que los tribunales rumanos mantuvieron un equilibrio adecuado entre el derecho del trabajador al respeto de su vida privada y su correspondencia y los intereses del empleador.

Pero, sin embargo, en la reciente sentencia de 5 de septiembre de 2017 la Gran Sala del TEDH anula la anterior, dictada el 12 de enero de 2016, por el propio Tribunal, se establecen determinadas pautas que fueron incumplidas en este supuesto, las más importantes son:

- Que se exige Información previa al trabajador, de la posibilidad de que el empresario adopte medidas de vigilancia de su correspondencia y de sus otras comunicaciones, así como de la puesta en práctica de tales medidas. El carácter previo supone que la información ha de ser recibida con carácter anterior al inicio de la vigilancia.

- El empresario ha de proporcionar los motivos que justifiquen la vigilancia de las comunicaciones del trabajador, más allá del art. 20.3 ET. El TEDH se refiere a motivos concretos.

- La vigilancia ha de ser proporcionada: hay que determinar si hubiera sido posible emplear un sistema de vigilancia conforme a medios y medidas que fuesen menos intrusivas que el acceso directo al contenido de las comunicaciones del empleado.

3.2. PÁGINAS WEB Y REDES SOCIALES

Sobre el control de la navegación por internet, cabría distinguir dos supuestos de hecho[20]. Por un lado, cuando la identificación del itinerario de navegación se obtiene del registro efectuado por el servidor externo a la empresa, no se considera que pueda quedar comprometida ni la intimidad ni ningún otro derecho fundamental del trabajador. Sin embargo, en los supuestos en los que el control de la navegación por internet se realiza accediendo a los datos registrados en la memoria del ordenador del trabajador (cookies), se considera que tal actividad empresarial de verificación puede afectar a la intimidad del trabajador. Por ello se deberán extender las garantías contenidas en el art 18 del ET a los registros de la memoria del ordenador, ya que en tal ámbito existe una expectativa de intimidad del trabajador merecedora de tutela.

La sentencia más transcendente, en cuanto a páginas web y derechos fundamentales, es la del 26 de Septiembre de 2007. Según el relato de los hechos probados, el actor, Director General de la empresa demandada, prestaba servicios en un despacho sin seguridad, sin llave, en el que disponía de un ordenador, que carecía también de clave de acceso y conectado a la red de la empresa que dispone de ADSL. Costaba también que había sido requerido un técnico informático para comprobar los fallos del ordenador y en él se detectaron la existencia de virus informáticos, como consecuencia de la navegación por páginas poco seguras de internet. Y en presencia del administrador de la empresa se comprobó que existían archivos temporales de unos antiguos accesos a páginas pornográficas, las cuales se entregaron a un notario en una memoria USB.

Las operaciones que se llevaron a cabo en el ordenador se habían realizaron sin la presencia del actor, ni de algún trabajador de la empresa ni de los representantes de los trabajadores.

[20] MARTÍNEZ FONS, D., El Poder de Control del empresario en la relación laboral, cit., págs 305-306. Consejo Económico y Social (España), 2002, Madrid. ISBN 9788481881585.

La sentencia recurrida confirmó la decisión de instancia, que aprecia la falta de validez de la prueba obtenida por parte de la empresa, ya que había sido obtenida mediante un registro que no cumplía con lo dispuesto en el art 18 del ET.

Establece la sentencia varios criterios:

- En cuanto al control del uso del ordenador facilitado al trabajador, que no se regula por el art 18 del ET, sino por el art 20.3 del ET.

- La garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentren en el ordenado. Lo que en este caso podría ser mas discutible, ya que se trataba de archivos temporales, que son copias que se guardan automáticamente en el disco duro del ordenador de los lugares que han sido visitados a través de internet. Se trata por lo tanto de rastros de la navegación de internet y no de informaciones personales de carácter reservado, pero en principio entran dentro de la protección de la intimidad.

- No es obstáculo para la protección a la intimidad que el ordenador careciera de clave de acceso, en su despacho sin llave tampoco, lo que no supone por parte del trabajador la aceptación del acceso empresarial a la información contenida en su ordenador.

- Lo que debe hacer la empresa es establecer previamente las reglas de uso de estos medios e informar a los trabajadores de que va a existir un control sobre los medios informáticos con el fin de comprobar que se hace un correcto uso de ellos. Por lo tanto, si estos medios se utilizan con carácter privado, en contra de estas prohibiciones y con un previo conocimiento de estos eventuales controles, no se puede entender que al realizarse el control se esté vulnerando el derecho a la intimidad.

- Y por ultimo, no cabe entender que estemos ante un "hallazgo casual" (sentencias 20 de Septiembre (RJ 2006,6402)) y 1 de Diciembre de 2006 (RJ 2006, 9564), pues se ha ido más allá de la entrega para la reparación justificada.

La sentencia de 8 de Marzo de 2011 confirma referido criterio[21]. Podemos decir quizás que se introduce en esta última una matización novedosa respecto a la sentencia del TS de 2007: se admite el control oculto cuando la empresa ha prohibido expresamente el uso personal de los medios telemáticos de su propiedad.

[21] RJ 2011/932.

Las prohibiciones absolutas de uso personal ya implican una advertencia de posible control por parte del empresario e incluyen la instalación de sistemas de control del uso del ordenador por parte de los trabajadores, lo que elimina la expectativa de intimidad y del secreto de las comunicaciones de aquellos.

Según se expone, en la STS del 26 de Septiembre de 2007, se exigía informar previamente a los trabajadores de la existencia de control empresarial y los medios utilizados, pero esto no es posible en los supuestos de prohibición absoluta del uso de los medios tecnológicos con una finalidad privada.

Ya respecto a las redes sociales, cada vez tienen una presencia mayor, y los problemas a que pueden dar lugar son muy prolijos (publicar fotos, colgar videos, publicar estados y comentarios personales, etc.) y como ello puede a su vez crear un conflicto y afectar directamente a la relación laboral.

Durante la relación laboral las redes sociales pueden dejar huella y que el trabajador sea sancionado hasta el punto incluso de que se llegue a extinguir el contrato, siempre y cuando se produzca un mal uso. Veremos como la doctrina constitucional y la jurisprudencia trata este tipo de situaciones.

En la STC 241/2012, de 17-12-(RTC 2012,241), se aborda los siguientes hechos: Dos trabajadoras instalan en un ordenador de uso común un programa llamado “Trillian” de mensajería instantánea. La empresa tiene conocimiento de esta situación y durante tres meses fiscaliza las conversaciones que mantienen las trabajadoras. Después se les convoca una reunión a la que asisten y en ella se abordan las conversaciones mantenidas, en las que existían todo tipo de comentarios despectivos en relación con sus compañeros de trabajo, superiores y clientes. La empresa decide amonestar verbalmente a las trabajadoras.

Considera el voto mayoritario que no ha habido vulneración del derecho a la intimidad y el secreto de las comunicaciones por una serie de razones y, entre ellas, que e ordenador era de uso común para los trabajadores y cualquier persona podía acceder a ellos.

Sin embargo, el voto particular, del magistrado Fernando Valdés Dal-Ré y al que se adhiere la Magistrada Adela Asunta Batarrita, entiende que tales circunstancias no deben limitar el derecho al secreto de las comunicaciones y que el acceso era en cualquier caso, complejo.

Además, como consideran, el incumplimiento de las órdenes empresariales no legitima al empleador para que vulnere directamente derechos fundamentales, criterio que no se ve afectado por el hecho de que sea en ámbito de las relaciones laborales en donde se mueve el Derecho a la intimidad y el secreto de las comunicaciones y pese a que se justifique con dicha intervención que los hechos sancionados eran ciertos.

Respecto al uso de una red social muy conocida, Facebook, me ha resultado interesante la sentencia de mi región, del TSJ de Cantabria de 10-11-2015. Rec. Núm. 765/2015. El actor prestaba servicios en una empresa como ayudante de camarero, obtuvo una baja por incapacidad temporal, situación en la que pertenece cuando es despedido, ya que la empresa había tenido conocimiento mediante publicaciones efectuadas en las redes sociales y, en concreto, en Facebook, de conductas incompatibles con su situación de incapacidad.

En el primero de los motivos se solicita la nulidad de las actuaciones porque se consideraba que existía una violación del art 18.3 de la CE, en relación con el art 90 de la LRJS, al haberse admitido como prueba, las fotos que se encontraban en el muro de Facebook.

La Sala considera que tal alegación carecía de sentido, ya que a dichos datos se podían acceder, ya que eran públicos, además de haber sido tomadas las fotografías en lugares públicos y en presencia de más personas, de forma que no se había vulnerado derecho alguno.

Además, según el art 20.3 del ET, el empresario está facultado para adoptar las medidas que estime oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones y deberes laborales. Y aquí tampoco se puede hablar de vulneración del derecho a la intimidad, ya que no solo por el lugar donde se tomaron las fotos, sino dada la eventualidad de su proyección pública a través de Facebook, que se

presume admitida por el actor y que tampoco existió reparo por parte de éste, a tomarse fotos en lugares públicos.

3.3. SISTEMAS DE SONIDO Y VIDEOVIGILANDIA

Otro de los medios del control empresarial mas utilizado es el de los sistemas de sonido y de videovigilancia. Existe una infinidad de sentencias. En primer lugar, se ha plantado el debate respeto de la intimidad y de la protección de datos en la utilización de tales medios (art 18.1 y 18.4 CE). La STSJ de Baleares de 4 de Septiembre de 2009, nº 333/2009, rec. 265/2009 analiza, por ejemplo, un supuesto de instalación de cámaras de seguridad en un aeropuerto como consecuencia de una serie de sustracciones e incumplimientos sobre consumiciones. Y considera que prevalece la perspectiva de la intimidad sobre la protección de datos. Esta perspectiva se basa en el llamado "test de proporcionalidad".

Se afirma que el derecho a la intimidad no es absoluto partiendo de que el Tribunal Constitucional también afirma que "los hechos referidos a las relaciones profesionales no se integran en la esfera privada de la persona". Pero también se destaca que "no puede descartarse que en aquellos lugares en los que se desarrolla la actividad laboral pueden producirse intromisiones ilegitimas del empresario en el Derecho a la intimidad de los trabajadores", como podría serlo la grabación de conversaciones entre un trabajador y un cliente o entre los propios trabajadores.

Como sintetizan las SSTC 66/1995, de 8 de Mayo [RTC 66], F.5; 55/1996, de 28 de Marzo [RTC 55], F. 6,7,8 Y 9; 207/1996 de 16 de Diciembre, F.4, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario comprobar si cumple los tres requisitos siguientes: si tal medida es susceptible de conseguir el fin propuesto (juicio de idoneidad), si es necesaria, en la medida en que no exista otra medida mas moderada para la consecución de tal propósito (juicio de necesidad) y, si la misma es ponderada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes (juicio de proporcionalidad en el sentido estricto),

Estas fueron, por ejemplo, las pautas que permitieron resolver que se declarase la constitucionalidad de la medida de instalación de un circuito cerrado de televisión para la vigilancia de la actividad laboral de un trabajador. Según la STC núm. 186/2000, de 10 de Julio (RTC 186) se cumplían tales pautas.

A diferencia del caso resuelto en la STC 98/2000 (RTC 2000,98), en el que la empresa, existiendo ya un sistema de grabación de imágenes, decidió instalar un sistema de grabación de sonido para un mayor seguridad, sin quedar acreditado que este nuevo sistema se instalase como consecuencia de la detección de una quiebra en los sistemas de seguridad ya existentes y sin que quedara acreditado que este nuevo sistema, que permitiría la audición continuada de todo tipo de conversaciones, resultase indispensable para la seguridad y el buen funcionamiento del centro de trabajo.

Respecto a la incidencia de tales medios de la protección de datos de carácter personal hago referencia a dos sentencias más recientes: la STC núm 26/2013 de 11 de Febrero (RTC 26) Y STS de 13 de Mayo de 2014 (RJ 3307), que plantean el mismo problema desde una perspectiva distinta.

El TC resuelve en su Sentencia de 11 de febrero de 2013, con voto particular, un caso concreto: la Universidad Pablo Olavide de Sevilla contaba con autorizaciones de la AEPD para hacer uso de soportes informáticos grabados por sus videocámaras, entre ellas una dirigida al control de acceso de los universitarios y el personal de empresas externas a los campus. Tales imágenes fueron utilizadas como prueba para la imposición de tres sanciones de suspensión de empleo y sueldo al subdirector de la unidad técnica de orientación, por faltas reiteradas e injustificadas de puntualidad y transgresión de buena fe contractual y abuso de confianza, así como faltas injustificadas al trabajo.

Considera el Tribunal Constitucional que las imágenes grabadas constituían un dato de carácter personal del art 18.4 CE y recogido igualmente en el art 3.a) de la LOPD y art 2.a) de la Directiva 95/46/CE. En palabras del tribunal, en estos supuestos de videovigilancia nos encontramos dentro del derecho fundamental del art 18.4º CE.

Como se expresa "*En el caso enjuiciado, las cámaras de videovigilancia instaladas en el recinto reprodujeron la imagen del recurrente y permitieron el control*

de su jornada de trabajo; captaron, por lo tanto, su imagen, que constituye un dato de carácter personal y se emplearon para el seguimiento del cumplimento de su contrato. La persona jurídica titular del establecimiento donde se instalaron las cámaras, y que fue quien utilizó al fin descrito las grabaciones, es la responsable del tratamiento de los datos, ya que no se informó al trabajador sobre la utilidad de supervisión laboral asociada a las capturas de su imagen, por lo tanto aquí decimos que se vulnera el art 18.4 CE". El comité de empresa había sido informado sobre la adopción de esas medidas e incluso existían carteles informativos donde se avisaba de la existencia de cámaras. Pero sin embargo, los trabajadores no habían sido informados previa y expresamente de esto, y según lo que declaro el TC es necesaria una "información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que la captación podría ser dirigida", información que debe "concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podrían ser examinadas, durante cuanto tiempo y con qué propósitos, y explicitando que podrían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo".

En cuanto a la Sentencia del 13 de mayo de 2014, rec 1685/2013, que también cuenta con voto particular, la Sala 4ª de TS vino a aplicar la anterior doctrina, pero en este caso en un marco distinto, en los supermercados CHAMPION. El titular del supermercado procede al despido disciplinario de una cajera, basándose en las pruebas obtenidas en imágenes grabadas por una cámara de seguridad permanente.

En este caso se expresa , conforme a la doctrina del Tribunal Constitucional que no se dio información previa a la trabajadora dela posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras instaladas permanentemente, ni tampoco se informó con carácter previo ni posterior a la instalación, a la representación de los trabajadores de las características y el alcance del tratamiento de datos que iba a realizarse, ni explicitando que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos de contrato de trabajo. Sin embargo, se les indico a los trabajadores, una vez instaladas las cámaras, que su finalidad era la de evitar robos por terceros y que no se trataba de un sistema para el control de la actividad laboral, pero en este caso se utilizó justamente para eso, con el posterior despido de la trabajadora.

Habría que distinguir en estos casos entre una instalación fija, que requiere respetar el art 18, apartados 1º y 4º de la CE, y otra temporal que requiere respetar el art 18.1º CE, ya que el 18.4º (la "tutela informativa") solo se aplicaría si existe un sistema de captación y tratamiento de las imágenes, que motivara la protección de datos, esto se confirma en la STC de 3-3-2016[22]

Sin embargo, creo que nos encontramos con un cambio de doctrina en la sentencia del pleno del TC, 39/2016, de 3 de marzo y acerca del alcance del deber informativo previo: los hechos de este supuesto son los siguientes

La Empresa detectó a raíz de instalar un sistema de control informativo de caja, que en la tienda donde prestaba sus servicios la demandante existían múltiples irregularidades. Por ello se encargo a una empresa de seguridad, Prosegur, la instalación de una de cámara vídeo vigilancia que controlara dicha caja. La cámara se instalo sin comunicación a los trabajadores, pero se colocó en el escaparate del establecimiento un distintivo informativo de la existencia de

En la carta de despido se imputaba a la trabajadora la apropiación de efectivo de la caja, en diferentes fechas y de forma continuada. La trabajadora presentó demanda de despido contra la empleadora, solicitando la nulidad del despido por atentar contra su honor, intimidad y dignidad, y la declaración de improcedencia de este. Alegaba que en el centro de trabajo no existían carteles informativos de la existencia de dichas cámaras de vídeo grabación, ni tampoco comunicación a la AEPD, ni tampoco informe previo al comité de empresa de la instalación de estas.

En primera instancia se desestima la demanda y se declara procedente el despido, por el juzgado de lo Social núm. 2 de León de 11 de Marzo de 2013, la empresa manifestó que la propia trabajadora reconoció los hechos. Interpuesto un recurso de suplicación, se desestima por la sentencia dictada por el TSJ de Castilla y León de 24 de julio de 2013.

[22] Así lo entiende, C. GONZÁLEZ GONZÁLEZ, "Control empresarial de la actividad laboral, Video vigilancia y deber informativo". A propósito de la STC de 3 de Marzo de 2016. *Revista Aranzadi Doctrinal, nº 5/2016.* BIB 2016/21165.

Aplicando la doctrina que expone, la Sala expresa que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la Empresa con la finalidad de seguridad o de control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral conforme con el art. 20.3 TRLET, que establece que "*el empresario podrá adoptar las medidas que estime mas oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales*". El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario. Pero, aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de información del art 5 LOPD.

Según consta en los hechos probados, y como hemos expresado, en el escaparate del establecimiento se coloco un distintivo informativo exigido por la instrucción 1/2006, de 8 de Noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Lo importante es que el trabajador conocía que en la empresa ase había instalado un sistema de control de vídeo vigilancia, sin que hubiera que especificar la finalidad exacta de esa vigilancia. Lo importante era determinar si el dato obtenido para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimento del contrato, porque si la finalidad no guarda relación directa con el control de la relación laboral, el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados.

Por lo tanto, teniendo dicha trabajadora información previa de la instalación de esas cámaras con su correspondiente distintivo, se entiende aquí que no se ve vulnerado el art 18.4 CE.

También ha de descartarse la vulneración del derecho a la intimidad personal del art 18.1 de la CE, si se justifica que la medida de instalación de cámaras de seguridad que controlaban la zona de la caja donde el demandante desempeñaba la actividad laboral era una medida justificada, idónea para la finalidad pretendida de la empresa, necesaria y equilibrada.

El primer voto particular, que formula el Magistrado don Fernando Valdés Dal-Ré a la Sentencia dictada en el recurso de amparo núm. 7222-2013, expresa su "intensa y extensa" discrepancia. Considera que el despido debió de considerarse como nulo, y ademas considera que no se ha cumplido el deber de información que impone al empresario el art 18.4 de la CE.

El segundo voto particular, por el Magistrado Xiol Ríos, estaría dispuesto a reconsiderar la jurisprudencia de la STC 29/2013 (RTC 2013, 29) sobre el hallazgo casual, en paralelo con la evolución de la jurisprudencia penal sobre esta materia, pero considera que toda omisión de información a los trabajadores, sobre la existencia de cámaras específicamente orientadas a sus posiciones plantea un supuesto diferente. Incluso este voto hubiera estado dispuesto a considerar, al margen de mas tecnicismos, la justificación de que la instalación de cámaras se notificase únicamente al comité de dicha empresa. También el mantenimiento de las sentencias que dieron lugar al recurso de amparo, habida cuenta de que tanto en primera instancia como en suplicación se hace constar por los respectivos tribunales que existen otros elementos de prueba independientes de la de la video vigilancia, suficientes para que se entiendan probados los hechos que dieron lugar a este despido.

Son muchos los comentarios negativos que se han hecho a esta sentencia[23] desde el ámbito laboral.

También haré alguna referencia a alguna sentencia reciente de los Tribunales Superiores de Justicia que aborda esta problemática. Por ejemplo, la del TSJ de Valencia 347/2017 del 8 de Febrero de 20, recurso 3428/2016, que la aborda desde la perspectiva de un despido disciplinario.

Se alega la vulneración de derechos fundamentales por grabación de una cámara de videovigilancia. La actora prestaba servicios en un supermercado, MERCADONA SA,

[23] Por ejemplo, entre tantos otros, el de W. SANGUINETTI, "Derechos fundamentales de la persona del trabajador y poderes empresariales, relaciones laborales: revista crítica de teoría y práctica, ISSN 0213-0556, nº 21-22, 2012, págs 15-30 : ¿Quo vadis TC? (II) escribe Juan Bautista Vivero".

en cuya división de facturas y cobros se detecta alarma respecto al numero de "consulta artículos", realizados por la actora, y ante la sospecha de hurto se procede a realizar controles, percatándose que faltan los productos consultados, por lo que se investigan los hechos, mediante la instalación de cámaras de video-vigilancia especificas para el control de la caja donde la trabajadora realizaba sus funciones, durante ocho días a través de la empresa de instalación de sistemas de seguridad, habiéndose comunicado con anterioridad tal medida al Comité de intercentros.

La trabajadora es despedida por transgresión de la buena fe contractual y hurto de productos y dinero de la empresa. Tras lo cual, la actora presentó denuncia a la Guardia Civil por posible delito de coacciones y amenazas por el método en que fue despedida y vulneración del derecho a la intimidad y propia imagen y la ley de protección de datos. La sentencia del juzgado de lo social desestima la demanda y declara el despido procedente, pero la actora interpone recurso y la Sala lo desestima también. Se analiza el cumplimento del requisito formal de la carta de despido conforme al art 55.1 ET. Sin embargo, la carta especifica los hechos y las fechas en que se cometieron, de manera que la actora conoce los hechos que se le imputaban consistentes en apropiarse del dinero a través de un sistema por el que en lugar de facturar el articulo que adquiría el cliente, accionaba la fecha “consulta del articulo” y se apropiaba del importe de la venta.

Respecto al canon de la proporcionalidad de la instalación de cámaras de vídeo-vigilancia, se recuerda la doctrina de la STS 39/2016, de 3 de Marzo, antes referida, respecto al juicio de idoneidad, de necesidad y de proporcionalidad, y se concluye que la medida está justificada pues existían razonables sospechas de que la trabajadora se apropiaba del dinero dado el elevado número de “consultas de artículos” que se correspondían con el descuadre de productos en el stock-, es idónea para verificar los hechos, necesaria para probar dichas irregularidades y equilibrada, ya que la cámara se instaló durante un breve periodo de tiempo y enfocando a la caja en que trabajaba la actora, además se puso en conocimiento de la representación legal de los trabajadores.

Podríamos hacer referencia a otras sentencias más recientes, también sobre el tema en cuestión de despidos provocados por la utilización de cámaras de seguridad, como la STS del 18 de Octubre de 2016, núm recurso 2645/2015.

Este caso trata sobre un despido disciplinario en la que se denuncia la vulneración de derechos fundamentales, en concreto[24].

Iniciado procedimiento sancionador frente a Serviseg, el 18 de diciembre de 2013 el instructor propuso su archivo, al considerar que la citada empresa no ha utilizado el sistema de videovigilancia para el control laboral de sus empleados.

La Inspección de Trabajo ha emitido informe en el que indica que la instalación de las cámaras no vulnera ningún derecho de los trabajadores.[25]

La Sala de suplicación, tras rechazar la denuncia de vulneración del derecho a la tutela judicial efectiva, considera que los hechos acreditados son subsumibles en la falta muy grave que se contempla en el art. 55.10 del Convenio aplicable.

En definitiva los datos personales grabados han sido utilizados para una finalidad compatible con aquella que justifica su recogida, esto es, la seguridad de las instalaciones y personas que se encuentran en el polígono.

[24] El actor venía prestando servicios para la empresa Serviseg Levante S.A., con la categoría de Vigilante de seguridad desde el 8 de septiembre de 2007. El centro de trabajo en el que presta servicios se encuentra situado en el Polígono Industrial de Los Camachos en Cartagena. La empresa demandada suscribió contrato con la empresa principal, para la prestación del servicio de vigilancia en el citado centro. La contratista tiene instaladas en el interior de la caseta de vigilancia cámaras de grabación con la finalidad de vigilar el equipo que es de su propiedad y que está valorado en 15.000 €. El equipo de grabación controla el perímetro y las instalaciones a vigilar, para la seguridad del propio vigilante y también para el control de sus obligaciones. El actor denunció el 31 de octubre de 2013 a la Agencia Estatal de Protección de datos la instalación de las citadas cámaras de seguridad.

[25] Por carta de 20 de diciembre de 2012 y con la misma fecha de efectos el actor es despedido disciplinariamente, por ofensas verbales y físicas al representante de la empresa, por transgresión de la buena fe contractual, al haberse dormido durante el servicio en determinadas fechas y por amenazas, al haberse puesto ante las cámaras de seguridad exhibiendo una navaja, en actitud desafiante y agresiva.

Por otra parte, el actor conocía la existencia del sistema de video-vigilancia ya que era precisamente el encargado de controlar su correcto funcionamiento. Sin que fuera necesario en el caso el permiso del actor para la obtención de las imágenes, puesto que la misma era una consecuencia de la relación laboral del actor, una de cuyas funciones era la de estar en el puesto de trabajo frente a las pantallas que emiten las imágenes grabadas, por lo que a su vez su imagen era grabada por las cámaras instaladas dentro de la caseta de vigilancia.

Recurre en casación unificadora el actor alegando infracción del art. 4 de la Ley 15/1999 en relación con el art. 18.4 de la Constitución Española e invocando como sentencia de contraste la del Tribunal Supremo de 13 de mayo de 2014 (R. 1685/2013). Dicha resolución aborda un supuesto en el que la actora prestaba servicios en Supermercados Champion S.A, supuesto ya mencionado anteriormente.

De lo expuesto se desprende que las sentencias comparadas no son contradictorias al resolver sobre supuestos que no son iguales. En particular, en la recurrida las cámaras de vigilancia no son instaladas por la empleadora, sino por la empresa principal que la contrató para la prestación del servicio de vigilancia y seguridad. Y es dicha empresa principal la que accede a las grabaciones y pone en conocimiento de Serviseg los hechos en los que luego se basa el despido. Consta además, que el trabajo del actor era precisamente estar pendiente del correcto funcionamiento de las cámaras de seguridad, por lo que no podía desconocer la existencia de un sistema de videovigilancia. Finalmente, también consta que por el instructor del expediente instado por el actor ante la Agencia estatal de protección de datos se ha propuesto el archivo al considerar que la citada empresa no ha utilizado el sistema de videovigilancia para el control laboral de sus empleados.

Asimismo, la Inspección de Trabajo ha emitido informe en el que indica que la instalación de las cámaras no vulnera ningún derecho de los trabajadores.

No es ocioso advertir que la tradicional doctrina constitucional relativa a la vulneración de los derechos a la intimidad, honor, propia imagen y a la protección de datos ha sido matizada por la reciente sentencia del Pleno del Tribunal Constitucional de 3 de marzo de 2016 (recurso de amparo 7222/2013) en la que se analiza un supuesto de

despido de la dependienta de una tienda de ropa que fue grabada por las cámaras instaladas por la empresa en la zona de cajas apropiándose de 186,92. La sentencia, en cuanto a la vulneración del derecho a la protección de datos, considera que: 1. Para el acceso a los datos de carácter personal -grabación de imágenes- es necesario el consentimiento del afectado.

Declarar la inadmisión del recurso de casación para la unificación de doctrina.

Por ultimo cabe mencionar la STS 21/2019 del 15 de Enero de 2019, núm de recurso 341/2017. La trabajadora, Dª Natalia trabajó para la Empresa TRANSPORTES BOYACAS S.L desde el 14/12/2000, mediante contrato indefinido a tiempo completo, con la categoría profesional de oficial 1ª administrativo Tras haberse constatado la apertura de varias cajas a lo largo de la semana se procedió a revisar su contenido por parte del responsable del almacén, quien comprobó la falta de tres unidades. Tras haber procedido al visionado de las grabaciones de todas las fechas, se había podido comprobar que dicha señora ha sido uno de los trabajadores que ha sustraído dicho material.

Se centra el objeto del recurso de casación para la unificación de doctrina en determinar si debe admite como prueba de los hechos imputados en la carta de despido la grabación obtenida por cámaras de vídeo vigilancia que la empresa había instalado, con conocimiento de los trabajadores, pero sin que estos fueran informados del destino que le iba a dar al control obtenido por medio de la grabación.

A tal fin, la empresa demandada ha formulado el recurso señalando como sentencia de contraste la dictada por el TC, núm 39/2016, de 3 de Marzo de 2016, dictada en el recurso 7222/2013 y denunciando como precepto normativo infringido el art 24 de la CE, en relación con el art 90.1 y 2 de la LRJS y arts. 4.2 e), 18.4 y 20.3 del ET. Se procede a un largo debate entre admitir o no el recurso de casación para la unificación de doctrina, analizando la sentencia de contraste propuesta por la parte demandada.

En la sentencia de contraste la grabación se limitó a la zona en la que se estaban produciendo los hechos sospechados mientras que en la sentencia recurrida la instalación de cámaras era general, prolongada y sin conocerse su objetivo. Es cierto, como expresa la sentencia de la Sala Cuarta que en la sentencia de contraste se dice que "*En el ámbito*

laboral el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes. Esta excepción a la exigencia de consentimiento aparece también recogida en el art. 10.3 b) del Real Decreto 1720/2007, de 21 de diciembre , por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, según el cual los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando "se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento".

La dispensa del consentimiento se refiere así a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, lo que abarca, sin duda, las obligaciones derivadas del contrato de trabajo. Por ello un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato", pero tal afirmación va seguida de otra vinculada a aquélla, según la cual " aunque no sea necesario el consentimiento en los casos señalados, el deber de información sigue existiendo, pues este deber permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o, en su caso, del representante (art. 5 LOP).

Como expone entonces la Sala Cuarta, el deber de información previa forma parte del contenido esencial del derecho a la protección de datos, pues resulta un complemento indispensable de la necesidad de consentimiento del afectado. El deber de información sobre el uso y destino de los datos personales que exige la Ley Orgánica de Protección de Datos de Carácter personal está íntimamente vinculado con el principio general de consentimiento para el tratamiento de los datos, pues si no se conoce su finalidad y destinatarios, difícilmente puede prestarse el consentimiento.

Y sigue diciendo "*Sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad. Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores, en conexión con los arts. 33 y 38 CE* ".

Y que "*el sometimiento de la falta o insuficiencia de información al reiterado juicio de proporcionalidad requerirá determinar en cada supuesto, con carácter previo, si se ha producido o no la indicada omisión de la información debida*".

A la hora de valorar si la sentencia recurrida se aparta de la doctrina constitucional no puede reducirse tal examen a la mera valoración de existencia del consentimiento, con base en que la instalación de las cámaras era conocida por todos los trabajadores, ya que la doctrina constitucional no se limita a ese extremo a la hora de justificar si hay vulneración de derechos fundamentales sino que atiende a la concurrencia de la información legalmente exigible en la materia y al juicio de ponderación.

La reciente sentencia del Caso López Ribalda y otros contra ESPAÑA (Demandas nº 1874/13 y 8567/13) de 9 de enero de 2018, revisa la actuación empresarial de videovigilancia, que se había considerado ajustada a derecho por los tribunales españoles, el procedimiento por despido declarado procedente, y corrige a nuestros tribunales, concluyendo que no hubo proporcionalidad en las medidas que fueron adoptadas por el empresario con el objetivo legítimo de proteger sus intereses de propiedad.

Los hechos eran los siguientes: en un supermercado se detectaron diferencias entre el inventario de productos y lo facturado en las cajas, por lo que se instalaron 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, y todos ellos reconocieron su involucración en los hechos. Los despidos

disciplinarios fueron impugnados ante la jurisdicción social, siendo el principal argumento de las demandantes que la videovigilancia oculta había vulnerado el derecho a la protección de su intimidad**.**

Tanto el juzgado de lo social, como el TSJ de Cataluña confirmaron la procedencia de los despidos, alegando que el uso de la videovigilancia encubierta en el lugar de trabajo sin una comunicación previa era conforme al artículo 20 ET, que permitía a un empresario la utilización de medidas de control y vigilancia que considerara adecuadas, siempre que se cumpla el test de proporcionalidad, lo que en este caso se producía este cumplimento: la medida estuvo justificada (debido a que había sospechas de robo), apropiada al objetivo legítimo perseguido, necesaria y proporcionada, dado que no existían otros medios igual de eficaces de proteger los derechos del empresario que interfirieran menos con el derecho de las demandantes al respeto de su vida privada.

La demanda, que se plantea ante el TEDH por cinco de las personas despedidas alega como argumento principal la vulneración del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales ("el Convenio"), en concreto en su artículo 8, que habla sobre el derecho al respeto a la vida privada y familiar.

El TEDH reconoce que la videovigilancia 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 iría en línea con la doctrina de nuestro Tribunal Constitucional que dice 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).

Por ello, continúa diciendo el TEDH, conforme al artículo 5 de la Ley española de Protección de Datos de Carácter Personal (LOPD), que 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"; y 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 en este caso no cumplió

con los requisitos del citado art. 5 LOPD (lo que como luego veremos llevará al TEDH a considerar que se vulneró el art. 8 del Convenio).

3.4. UTILIZACIÓN DEL GPS

Entre las nuevas tecnologías se encuentra el uso de sistemas de geolocalización GPS (Global Positioning System) instalados en vehículos de la empresa y acoplados a una red digital de comunicaciones móviles GSM (Global System for Mobile Communications). Dichos dispositivos, además de facilitar la conducción, permiten localizar en todo momento al vehículo con un margen de error de unos pocos metros y son de utilidad en empresas de transporte, taxis, viajantes, etc. Esta capacidad de localización permite organizar con mayor eficacia las rutas, entregas, y en general el control del trabajo y del uso que se ha hecho del vehículo fuera del centro de trabajo (horas de arranque, paradas, kilómetros recorridos, cantidad de combustible consumido, etc).

Llegados a este punto no debemos olvidar que cuando la prestación de servicios del trabajador se realiza fuera del centro de trabajo las facultades de control del mismo por el empresario siguen siendo legítimas en virtud del art.20.3 , siempre que la vigilancia se circunscriba exclusivamente a las "obligaciones y deberes laborales" tal y como indica el precepto legal[26]. Para comprobar que la prestación se cumple de forma efectiva se han utilizado diversos métodos, como por ejemplo, la confección de partes de trabajo firmados por cliente y trabajador, la emisión de partes de actividades al seguimiento por otro personal de la empresa, el uso de teléfonos móviles para permitir el contacto constante entre trabajador y empresario, e incluso el seguimiento por parte de detectives privados, en caso de fundadas sospechas sobre la conducta irregular de un trabajador[27]. En el caso de que el trabajador deba utilizar un vehículo de la empresa para el desempeño

[26] La facultad de control, por lo tanto, «no puede alcanzar más que a los extremos que guarden directa relación con el trabajo, prestación básica de aquella relación contractual, y cualquier extralimitación de tal potestad deviene ilegítima y como tal no sólo fuera del amparo jurisdiccional, sino de su inmediata coercitiva exigencia» (STC de 23 de enero de 1982).

[27] FERNÁNDEZ VILLAZÓN, L. A.: Las facultades empresariales... , op. cit., pg. 174.

de la actividad laboral, debe entenderse que se trata de una herramienta propiedad del empresario por lo que también cabe un control sobre el uso del mismo.

La Agencia Española de Protección de Datos (en adelante, AEPD) ha dictaminado en su Informe núm. 193/2008 que los datos obtenidos a través del sistema de geolocalización (rutas seguidas, tiempos de parada, velocidad y consumo de combustible del vehículo, etc.) están asociados a información concerniente a una persona física identificada o identificable, por lo que según el art. 3 a) de la Ley Orgánica de Protección de Datos) (en adelante, LOPD) se consideran datos de carácter personal que deben generar un fichero debidamente inscrito en el Registro General de Protección de Datos.

Entra así en el tema el derecho fundamental a la protección de datos de carácter personal consagrado en el art. 18.4 CERCL 1978, 2836) que implica «el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama la informática» (STC 254/1993, de 20 de julio). Su objeto de protección «no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal», y así, «los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier utilidad que en determinadas circunstancias constituya una amenaza para el individuo» (STC 292/2000, de 30 de noviembre).

Respecto al tema que nos ocupa, es trascendente la STS 5259/2012 del 21/06, núm de recurso 2194/2011. Se abordaba el despido por actividad en la incapacidad temporal y se plantea el problema de la violación del derecho a la intimidad, dado el medio de control empleado (instalación de localizador GPS en el vehículo del actor). Pese a que no entra en el fondo, dada la falta de contradicción, resalta la importancia de los datos distintivos.

En el burofax que se le envía al actor se detallaba exhaustivamente todos los desplazamientos que realiza, con sus fechas correspondientes, todo ello controlado a

través del GPS de su vehículo, mientras se encontraba en la situación de incapacidad temporal derivada de enfermedad común.

Para acreditar esa actividad, se instaló, por un detective privado, en el vehículo particular del actor un aparato localizador GPS, con el que se procedió a complementar el seguimiento. La sentencia de instancia declaró nulo el despido, porque los datos en que se fundaba la carta de despido se habían obtenido con vulneración del derecho fundamental a la intimidad en relación con los derechos a la libertad de circulación y a la tutela judicial efectiva.

Como sentencia contradictoria se aportaba la de la Sala de lo Social de Galicia de 27 de noviembre de 2003. Se decide en ella sobre el despido de un trabajador, al que se le imputaba también una trasgresión de la buena fe contractual durante la incapacidad temporal. El trabajador fue sometido a un control por investigador privado, "siendo seguido y grabado en lugares públicos", actuación que fue encargada por la empresa "a raíz de ser publicada en el diario La Región del día 21/10/02 una fotografía en la que aparecía el actor y de la que era deducible la posibilidad de que estuviera realizando actividades de caza incompatibles con la situación de IT en que se encontraba". El trabajador pretendía la nulidad radical del despido, invocando la lesión del derecho a la intimidad, pretensión que se rechaza por entender que la empresa está legitimada para vigilar y comprobar el cumplimiento de los deberes laborales de sus empleados, utilizando los adelantos técnicos y los servicios de agencias de investigación privada, pues, por una parte, existía un indicio de incumplimiento (la fotografía publicada en un medio informativo), el control tenía que realizarse, dado su objeto, fuera de la empresa y se desarrolló en lugares y espacios públicos "en días y en momentos concretos y en el exclusivo contexto de la investigación laboral".

En este sentido la sentencia recurrida, al igual que la de instancia, valora el carácter permanente del dispositivo de control (GPS) aplicado, su incorporación a un bien propiedad del trabajador, el exceso sobre las exigencias objetivas de control y falta de proporcionalidad resultante. Pese a que el Tribunal Supremo no entra en el fondo, destila la importancia de tales elementos diferenciales.

Podemos hacer referencia a otro tipo de sentencias, como por ejemplo la STSJ núm 3058/2017 de 27 de Diciembre (Sala de lo Social, sección 1ª), rec 2241/2017. Este caso trata sobre una vulneración del derecho a la intimidad por parte del empresario, al adoptar medidas de vigilancia y control: colocación de de dispositivos de localización GPS en los vehículos puestos a disposición de los trabajadores para uso profesional[28].

El propósito de la empresa ZENER COMUNICACIONES SA (en adelante ZENER) de instalar en los vehículos usados por sus trabajadores dispositivos del sistema de posicionamiento global (GPS), provocó la reacción del sindicato CCOO que interpuso demanda de conflicto colectivo para impedir la medida. La sentencia del Juzgado de lo Social núm. 4 de Gijón desestimó las pretensiones del sindicato que, disconforme con el pronunciamiento judicial recurre en suplicación y, manteniendo las dos pretensiones ejercitadas en la demanda, pide: la declaración de nulidad de la sentencia de instancia por omisión de un pronunciamiento; subsidiariamente, la declaración de nulidad de la "orden de geolocalización de las vehículos que utilizan los trabajadores de la empresa demandada, anulando asimismo cualquier decisión amparada en dicha geolocalización y los ficheros de datos obtenidos hasta la fecha y adoptando las medidas que sean precisas para la efectividad de lo acordado"; subsidiariamente, que la empresa "garantice de forma fehaciente a los representantes de los trabajadores que el dispositivo de geolocalización no estará operativo a partir del momento en que finalice la jornada laboral y con cuanto más proceda en derecho".

Al recurso se opuso la empresa, que impugna los motivos de recursos y defiende el acierto de la decisión judicial pues, según afirma, el sistema de geolocalización implantado no vulnera derechos fundamentales de los trabajadores y es eficaz y proporcionado para los fines lícitos pretendidos con su adopción.

[28] La empresa demandada que se dedica al mantenimiento de instalación de telecomunicaciones, dispone en Gijón de un centro de trabajo donde ocupa una plantilla de 58 trabajadores que desarrollan su actividad por toda la comunicad asturiana y que están sujetos al Convenio Colectivo del Metal, estando representador por un comité de empresa de cinco personas cuatro de ellos del Sindicato CCOO y uno mas por USO. El 23 de Noviembre de 2016 la empresa comunica al comité de empresa que se va a proceder a a la instalación de sistemas de geolocalización en los vehículos que se dedican al desarrollo de la actividad profesional.

El recurso de CCOO se divide en tres motivos y el primero, bajo la cobertura formal del art. 193 a) LJS , tiene por objeto fundar la petición de nulidad de la sentencia de instancia por infracción de normas o garantías del procedimiento causantes de indefensión.

Otro de los motivos de recurso, por el cauce procesal del art. 193 c) LJS, está dedicado al examen jurídico de las dos pretensiones formuladas. Comienza denunciando la infracción de los arts. 18.1 , 3 y 4 CE y 4.1 y 2 ET , así como de la doctrina sentada por el Tribunal Constitucional en la sentencia 70/2002 ; después, al iniciar el tratamiento de la reclamación subsidiaria invoca la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), de la que cita los arts. 2 c) y 9.

Alega que la sentencia sacrifica injustificadamente el derecho de intimidad de los trabajadores al derecho de la empresa al control de sus trabajadores durante la prestación de servicios laborales. La instalación y uso de los dispositivos GPS es una medida restrictiva de aquel derecho fundamental que no es idónea, necesaria ni proporcionada por lo cual incumple las exigencias mínimas para su licitud. Para sustentar la petición subsidiaria, esto es, que el dispositivo de geolocalización instalado en los vehículos no esté operativo a partir del momento de finalización de la jornada laboral, destaca la falta de consentimiento de los trabajadores que impide al empresario recoger datos de localización fuera del tiempo de trabajo.

Los datos de los trabajadores así obtenidos y su tratamiento están protegidos por el art. 18.4 CE (la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos), pero también por el art. 18.1 CE que garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Lo explica adecuadamente, con abundante cita de jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos, la sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid de fecha 21 de marzo de 2014 (rec. 1952/2013) en un caso asimismo de colocación de un dispositivo GPS en un vehículo para el control del trabajador que lo conduce: "(...) cuantos datos se conecten a su manejo y, por ende, a su localización y desplazamientos

fuera del centro de trabajo, se proyectan refleja, pero ineluctablemente, sobre la forma de proceder del usuario, que no es otro que el conductor, permitiendo de este modo conocer en todo momento durante su uso parcelas de la vida del trabajador que por muy imbricadas que estén en el desarrollo de la relación laboral con la empresa inciden potencialmente en la esfera de su derecho a la intimidad personal y, de ser objeto de tratamiento como aquí sucede, del que igualmente le asiste a la protección de datos de tal carácter". En parecidos términos, la sentencia del Tribunal Superior de Justicia de Castilla-La Mancha de 28 de abril de 2015 (rec. 134/2015).

Uno de los pilares fundamentales para la licitud del control de los desplazamientos por medio de dispositivos GPSy del tratamiento de los datos personales obtenidos por su medio es que la existencia de relación laboral faculta a la empresa ZENER para, en el ejercicio de sus facultades directivas y supervisoras, establecer algunos límites a derechos fundamentales de los trabajadores.

Cuando finaliza la jornada laboral o acaba el tiempo de trabajo, dichas facultades empresariales desaparecen y el contrato de trabajo deja de constituir el vínculo entre las partes que ampara el poder de la demandada para imponer las medidas implantadas de captación y tratamiento de datos. A partir de ese momento, es imprescindible el consentimiento de los trabajadores para mantener en funcionamiento los dispositivos GPS y para el análisis automatizado de los datos personales conseguidos por ese medio pues el supuesto deja de estar comprendido en la excepción prevista en el art. 6.2 LOPD y se rige por la regla general del art. 6.1 LOPD .

Los trabajadores de la demandada no han prestado el consentimiento, por lo que la empresa ZENER está obligada a contar con un procedimiento que le permita desactivar el sistema de posicionamiento global instalado de forma que no capte datos. Debe adoptar las medidas indispensables para garantizar, es decir dar seguridad y certeza, que el sistema no esté operativo a partir del momento en que finalice la jornada laboral. Por lo expuesto dice que debe estimarse la pretensión subsidiaria.

El fallo de la sentencia dice: que se estima en parte el recurso de suplicación interpuesto por el sindicato CCOO de Asturias, y que se debe revocar y revoca parcialmente la sentencia dictada el 25 de abril de 2017 en el proceso de conflicto

colectivo sustanciado a instancias de aquella parte contra la empresa ZENER COMUNICACIONES SA. Se condena a la empresa demandada a que garantice a los representantes de los trabajadores que el dispositivo de geolocalización implantado en los vehículos de motor utilizados por los trabajadores no estará operativo a partir del momento en que finalice la jornada laboral.

Podemos hacer también referencia a otra sentencia sobre el mismo tema de la sentencia anterior, la sentencia del TSJ de Madrid, (sala de lo social, sección 5ª), núm. 739/2014 de 29 de septiembre, rec 1993/2013, esta sentencia trata sobre una vulneración del derecho a la intimidad, en concreto por la colocación de un dispositivo de un dispositivo de localización GPS en el vehículo cedido a la trabajadora para su uso exclusivamente profesional.

El caso trata sobre[29], la actora permaneció en situación de IT desde el 11/07/12 con el diagnóstico de "embarazo confirmado deseado"; fue alta médica el 27/07/12. Mas tarde por carta de fecha 03/08/12 la empresa comunicó a la actora su despido disciplinario de conformidad con lo previsto en el art 52.2.d) ET. Por lo tanto Dª Tomasa interpuso demanda frente a la empresa REDES INTERMEDIACIÓN FINANCIERA, S.L, alegando la improcedencia del despido y condenando a la Empresa a que en el plazo de cinco días desde la notificación de esta sentencia opte entre la readmisión de la trabajadora o la extinción del contrato con abono de una indemnización.

Contra esta sentencia se interpuso recurso de suplicación por la empresa REDES INTERMEDIACIÓN FINANCIERA, siendo impugnado de contrario.

[29] La actora Dª Tomasa, ha venido prestando servicios por cuanta de la empresa REDES INTERMEDIACIÓN FINANCIERA, S.L. con la antigüedad de 22/04/2010, categoría profesional de Promotor y con un salario de 1.672,11€ con prorrata pagas extraordinarias. Las funciones que desempeñó la actora fue la de visitar estaciones de servicios con el motivo de promocionar la venta de tarjetas VISA; cuando visitaba las estaciones de servicio le daban un justificante. Para el desempeño de sus funciones la empresa puso a su disposición un vehículo modelo Volkswagen Golf. Este vehículo llevaba instalado un sistema de Gestión de Flotas de la compañía DETECTOR, S.A. Este sistema permite la localización y seguimiento continuo del vehículo mediante un dispositivo GPS. La empresa comunico a la actora un "documento de uso del vehículo".

La sentencia de instancia ha declarado la improcedencia del despido practicado por la demandada condenando a ésta a que en el plazo de cinco días desde la notificación de la sentencia opte entre la readmisión de la trabajadora o la extinción del contrato con abono de una indemnización de 5.861,79 € y a que en caso de readmisión abone a la actora los salarios dejados de percibir desde la fecha del despido hasta la notificación de la sentencia de instancia.

Frente a la misma se alza en suplicación la mercantil REDES DE INTERMEDIACIÓN FINANCIERA SA, formulando cinco motivos de recurso con destino a la nulidad de actuaciones, revisión fáctica y censura jurídica. El recurso ha sido impugnado.

El primer motivo con amparo en el apartado a) del artículo 193 de la LRJS solicita la nulidad de las actuaciones con retroacción de las mismas al momento del dictado de sentencia, al sostener que se ha cometido infracción de normas y garantías de procedimiento basada en que ni en la demanda ni en el acto de la vista se planteó la supuesta violación de derechos fundamentales, lo que le ha producido indefensión.

Aduce el recurrente que si la vulneración de la intimidad personal de la actora se hubiese concretado en la demanda (o se hubiese planteado de conformidad con el artículo 97.2 de la Ley procesal durante la fase de admisión de prueba) la empresa habría articulado la prueba de alegaciones necesarias para acreditar la inexistencia de tal vulneración y la licitud de la prueba de seguimiento del vehículo puesto a disposición de la actora.

En el fundamento quinto de la sentencia se argumenta: "Con la anterior práctica la empresa demandada vulneró el art. 6.1 de la Ley Orgánica de protección de datos de carácter personal, ya que la parte actora no prestó su consentimiento inequívoco para al tratamiento de sus datos de carácter personal. Esta vulneración produjo, consiguientemente, una vulneración del derecho a la intimidad personal que garantiza el art. 18.1 C.E . Por ello, de conformidad con el art. 90.2 L.J .S. no debe admitirse la prueba practicada al respecto por la empresa ya que se ha obtenido mediante procedimientos que suponen violación de derechos fundamentales ".

Siendo posible alcanzar esta conclusión tras valorar todos los medios de prueba practicados tras su admisión y declaración de pertinencia por quien es competente para ello, o sea, el Juzgador (artículo 87.4 de la Ley Reguladora de la Jurisdicción Social), momento del juicio que no tiene por objeto exclusivo ponderar el alcance y virtualidad de la actividad probatoria desplegada, sino también la validez de los medios empleados, sobre todo cuando se tacha de ilícito el procedimiento seguido para el logro de alguno de ellos, por lo que la incongruencia invocada es inexistente.

Denuncia infracción del artículo 20.3 del Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 1/1.995, de 24 de marzo, y del artículo 6.2 de la Ley Orgánica 15/1.999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Cita como infringida la doctrina contenida en la sentencias de la Sala de lo Social del Tribunal Supremo de 6 de octubre de 2.011, rec. 4053/2010.

En esencia aduce que la actora tenía conocimiento que el uso del vehículo cedido lo era exclusivamente para uso profesional, por lo que implícitamente existía una prohibición absoluta que válidamente impuso el empresario (artículo 20ET) sobre el uso del vehículo para fines propios. Entendiendo que no se trata de una cámara de video o de un sistema de grabación del sonido instalado en el interior del vehículo como manifestó en conclusiones en el acto de la vista oral, sino que es un sistema pasivo no agresivo, puesto que lo único que determina el sistema es la localización exacta del vehículo, indicando los puntos de arranque y de parada así como los puntos intermedios de trayecto y la hora exacta de todo ello.

La Sala en torno al poder de vigilancia y control que el empresario sustenta ya ha declarado en sentencia de 21/03/2014, recurso 1952/2013 , que " Mas, obviamente, su ejercicio, de igual modo que, incluso, el de los derechos fundamentales no es absoluto, sino que tiene límites que no pueden traspasarse so pena de resultar abusivo e ilícito. En este sentido, traer a colación la sentencia del Tribunal Constitucional 29/2.013, de 11 de febrero , aunque se refiera a supuesto de captación de imágenes de un trabajador en el exterior del recinto donde presta servicios, por cuanto los avances tecnológicos son constantes y cada día más sofisticados, de suerte que pueden llegar a incidir en mayor medida en la vida privada de las personas, esfera que no pierde su carácter por el hecho de que la actuación se enmarque en el ámbito de una relación de trabajo por cuenta ajena.

El Juzgador de instancia concluyó que la utilización en este caso del sistema GPS para obtener datos sobre la forma de desempeñarse profesionalmente la actora con categoría profesional de promotor, infringió la Ley Orgánica de Protección de Datos de Carácter Personal y, a su vez, su derecho fundamental a la intimidad personal que consagra el artículo 18.1 de la Constitución, criterios que la Sala comparte.

La recurrente argumenta como ya hemos dicho que los datos en que la empresa se funda para el despido disciplinario efectuado tienen un carácter exclusivamente profesional.

La Sala no comparte este criterio, pues aunque la recurrente cedió a la trabajadora para uso exclusivamente profesional el vehículo de referencia que, además debía permanecer siempre bajo su custodia, mantenimiento y cuidado, todos los datos que se refieren a su utilización, localización y desplazamientos fuera del centro de trabajo, que son tratados por una empresa externa DETECTOR SA, planean sobre la forma de actuar de la trabajadora, sin haber recibido por parte de la recurrente información alguna al respecto, permitiendo de este modo conocer en todo momento durante su uso determinadas parcelas de la vida de la misma por muy relacionadas que estén en el desarrollo de la relación laboral y que inciden en la esfera de su derecho a la intimidad personal, asistiéndole el derecho de protección de datos de tal carácter. Así lo tiene entendido la doctrina constitucional (Tribunal Constitucional 29/2.013, de 11 de febrero, Recurso 10522/2009) y la jurisprudencia unificadora en su reciente sentencia de 13/05/2014 , rcud 1685/2013.

El fallo de la sentencia es: se desestima el recurso de suplicación interpuesto por la representación letrada de la empresa REDES INTERMEDIACIÓN FINANCIERA, S.L., contra la sentencia dictada el 20 de junio de 2.013 por el Juzgado de lo Social núm. 13 de los de Madrid en el procedimiento núm. 1.062/12, seguido a instancia de Dª Tomasa, contra la empresa recurrente, sobre despido y, en su consecuencia, debemos confirmar, como confirmamos, la resolución judicial recurrida.

4. CALIFICACIÓN DEL DESPIDO, BASADO EN PRUEBA ILÍCITA, POR VULNERACIÓN DE DERECHOS FUNDAMENTALES

La cuestión resulta compleja. Desde una posición se defiende que el despido efectuado con sustento en una prueba ilícita debería declararse improcedente. En cambio, otra postura considera adecuada la declaración de la nulidad del despido, al emplear la doctrina de los frutos del "árbol envenenado". Este efecto de la prueba prohibida ha supuesto una protección más garantista de los Derechos fundamentales.

Tal controversia se plantea en la sentencia de la sala cuarta del 21/06/2012 núm de recurso 2194/2011, pero que no se resuelve por razones formales.

Dentro de la categoría de despidos nulos han de estar aquellos que se sustentan principalmente en pruebas obtenidas con vulneración de derechos fundamentales de los trabajadores. Este carácter ilícito de la prueba debe de comunicarse a la calificación del despido. La declaración de nulidad por lo tanto vendrá motivada por la ilicitud de la fuente de prueba que se trasladará a la calificación del despido disciplinario.

Pero también puede considerarse que en estos casos puede considerarse que lo que ha tenido lugar "con violación de derechos fundamentales" no es el mismo despido (art 55 ET) sino el soporte de la prueba de los incumplimientos imputados y que lo único indudable es que tales pruebas no pueden formar un material idóneo para que el juez llegue a un convencimiento de la procedencia del despido. Así, por ejemplo, tal como lo considera la sentencia del TSJ de Cataluña núm 7109/2000 con recurso 2890/2000: "la calificación del despido debe vincularse al móvil que lo determina, o la violación de derechos y libertades a que se refiere el art 55.5 ET, y no a la ilegalidad de alguna de las pruebas que se incorporó al proceso".

La improcedencia puede defenderse a través de la interpretación del art 11.1 LOPJ cuando sólo establece que una prueba obtenida por violación de derechos fundamentales no será tenida en consideración, y por lo tanto, será nula. Igual criterio el del art 90.2 LRJS dice que las partes podrán valerse de cualquiera de los medios de prueba (…) salvo

que se hubiesen obtenido mediante procedimientos con violación de derechos o libertades públicas.

En los supuestos en los que se busca obtener una prueba ilícita con la finalidad clara de despedir, la nulidad no fuerza las previsiones del art 55.5 ET, al decir que el despido será nulo cuando éste tenga a por "móvil" una de las causas prohibidas por la constitución, o en la ley, o bien que. Se produzca con violación de derechos fundamentales y libertades publicas del trabajador.

La doctrina de suplicación cuando defiende la opción del despido nulo, remite a otras decisiones judiciales, sobre todo del TC. Como por ejemplo, la sentencia del TSJ del País Vasco de 10 de mayo de 2011 con núm de recurso 644/2011: "dado que la única prueba que sirvió de base al acto extintivo fue obtenida violando el derecho fundamental a la intimidad del demandante y que, por lo tanto, el conocimiento de los hechos motivadores de su cese se debió en exclusiva a una prueba ilícitamente obtenida, con vulneración de esa garantía constitucional, la consecuencia que se deriva de ello es la nulidad del despido".

Defienden también esta postura las SSTSJ del País Vasco de 12-9-2006, Galicia, de 3/03/2008 con núm de recurso 6219/2007, y Cataluña, de 3/06/2008 con núm de recurso 2818/2008.

Pero, la doctrina del TC ampara tal nulidad del despido. La sentencia 194/2004 del 15/11/2004, considero que se atentaba contra la intimidad por un reconocimiento médico al que se sometió un trabajador porque no fue previamente informado sobre algunas de las analíticas que se comprendían. El TC entendió que la decisión extintiva debía de compartir la misma calificación que los antecedentes que la produjeron.

En el último fundamento jurídico de esta sentencia se expresa: "la reparación de la lesión de un derecho fundamental, que hubiese sido causado por el despido laboral, debe de determinar la eliminación absoluta de sus efectos, es decir, la nulidad del mismo, lo que implica la anulación de la sentencia impugnada (…)". Es decir, con la aplicación de la anterior doctrina mencionada de los frutos del árbol envenenado.

Podemos también mencionar la mas reciente sentencia del TC 29/2013, de 11/02/2013, por la que se declara nula la sanción de suspensión de empleo y sueldo, al haberse obtenido una grabación de imágenes con vulneración del derecho fundamental a la protección de datos, dice que: " las sanciones impuestas con base en una única prueba, lesiva de aquel derecho fundamental, deben declararse nulas (…), por lo que procederá anular las resoluciones judiciales impugnadas y la resolución rectoral que impuso las sanciones de suspensión de empleo y sueldo al recurrente de amparo".

También podemos decir que reafirma esta postura la jurisprudencia de unificación más reciente, en la sentencia 13/05/2014 con núm de recurso 1685/2013. La cuestión que se plantea aquí es, determinar si existía una vulneración empresarial de los Derechos fundamentales del art 18.4 CE (derecho a la protección de datos de carácter personal) que se provocó por la utilización de cámaras de video-vigilancia para sancionar a una trabajadora por el incumplimiento de sus obligaciones laborales; la vulneración resultaba de la utilización, no consentida ni informada previamente, de las grabaciones de imagen para un fin que era desconocido para la trabajadora afectada en este caso y que fue distinto del señalado por la empresa, al instalar el sistema, de manera permanente, para el control de su actividad laboral.

Y la consecuencia, conforme a la jurisprudencia constitucional, por haberse producido tal vulneración, y acordando la medida impugnada con fundamento en una lesión del art 18.4 CE, es que el despido debe de calificarse como nulo (entre otras SSTC 88/1985 de 19 de julio (RTC 1985,88), 134/1994 de 9 de mayo (RTC 1994,134), 29/2013 de 11 de febrero (RTC 2013,29).

Se acuerda por lo tanto, la nulidad del despido actuado con sustento en el uso ilegitimo de medios de control de la actividad de la trabajadora y del derecho fundamental mencionado referido a los datos personales de la trabajadora demandante, como hicieron antes el Juzgado de instancia y la sentencia del TSJ del País Vasco, núm 609/2013, de 9/04/2013.

Pero por otro lado podemos decir que, desde posturas doctrinales recientes se sigue manteniendo que si la prueba se ha obtenido ilícitamente ello debería determinar la inadmisibilidad de la misma, pero esa ilicitud no se debería trasladar necesariamente a la

calificación del despido convirtiéndolo en nulo, sino que éste debería ser valorado, prescindiendo de la prueba en cuestión y declarado como procedente, improcedente o nulo a tenor de las restantes pruebas. Si no es así, dado el art 90.2 LRJS, se entiende que carecería de sentido. Se aprecia esta posibilidad en el voto particular del magistrado Xiol Ríos en la STC 39/2016 de 3 de Marzo[30] .

5. CONCLUSIONES

I. La inserción en la organización laboral modula el ejercicio de los derechos constitucionales en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva. Entre los derechos fundamentales y la relación laboral se produce una relación de mutua limitación, lo que supone la necesidad de proceder a una adecuada ponderación que respete la valoración constitucional del derecho fundamental y de las obligaciones laborales que puedan modularlos. De esta manera cuando un/a trabajador/a firma el contrato de trabajo y se genera con el empleador la relación laboral, estos derechos fundamentales inespecíficos quedarán sujetos al contrato de trabajo.

II. Es necesario constatar si se cumplen los tres requisitos o condiciones siguientes: juicio de idoneidad, si tal medida es susceptible de conseguir el fin propuesto; juicio de necesidad, si es necesaria, en el sentido en el que no exista otra medida mas moderada para la consecución de tal propósito con igual eficacia y el juicio de proporcionalidad, en sentido estricto, que significa preguntar acerca de si la misma 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.

III. Dentro de las "facultades de autoorganización, dirección y control correspondientes a cada empresario, no cabe duda de que es admisible la ordenación y

[30] L. E. NORES TORRES, "Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales: aspectos individuales, colectivos y procesales", Revista de Información Laboral, nº 7/2016, Parte doctrinal.

regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales.

IV. El poder de vigilancia y control empresarial previsto en el art 20.3 del ET va dirigido a comprobar el efectivo cumplimento por el trabajador del sus *"obligaciones y deberes laborales"*. Pero aquí cabría hacer una distinción entre la utilización de los medios tecnológicos de información y comunicación de la empresa como instrumentos de control y vigilancia de la prestación laboral y el control del uso, adecuado o inadecuado, por el trabajador, de dichos medios. Mientras el primero persigue un control objetivo o general del cumplimento de la prestación laboral en sentido positivo, el segundo, en cambio, se dirige a la supervisión, aislada y personal del correcto cumplimiento por parte de un trabajador concreto o un grupo de trabajadores de las obligaciones y reglas laborales. Se trata en este último caso de un control más invasivo, mas incisivo respecto de la intimidad personal.

V. La reciente sentencia de 5 de septiembre de 2017 de la Gran Sala del TEDH anula la anterior, dictada el 12 de enero de 2016, por el propio Tribunal, establece determinadas pautas que fueron incumplidas en este supuesto y que condicionarán el devenir de la jurisprudencia. Las más importantes son:

- Que se exige Información previa al trabajador, de la posibilidad de que el empresario adopte medidas de vigilancia de su correspondencia y de sus otras comunicaciones, así como de la puesta en práctica de tales medidas. El carácter previo supone que la información ha de ser recibida con carácter anterior al inicio de la vigilancia.

- El empresario ha de proporcionar los motivos que justifiquen la vigilancia de las comunicaciones del trabajador, más allá del art. 20.3 ET. El TEDH se refiere a motivos concretos.

- La vigilancia ha de ser proporcionada: hay que determinar si hubiera sido posible emplear un sistema de vigilancia conforme a medios y medidas que fuesen menos intrusivas que el acceso directo al contenido de las comunicaciones del empleado.

VI. Deben prevalecer los medios de control menos intrusivos, en la esfera privada del trabajo por parte del empresario, frente a los más invasivos. Varios pronunciamientos judiciales defienden la legitimidad de algunos medios empresariales sumamente intrusivos, como la video-vigilancia, cuando, en cambio, existen otros medios menos intrusivos para proteger la intimidad de los trabajadores, de forma que tal doctrina ha de replantearse.

VII. Podemos observar una confrontación en la doctrina, y en las decisiones judiciales, sobre el problema de la calificación del despido basado en prueba ilícita por vulneración de derechos fundamentales: improcedencia o nulidad, que la Sala Cuarta ha de despejar definitivamente.

6. BIBLIOGRAFÍA

ALFARO J., "El Constitucional cambia su doctrina sobre la dependienta ladron", en *Almacén de Derecho*, www.almacendederecho.org. Miércoles, 16 de marzo de 2016.

FERNÁNDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, Aranzadi, 2003.

GONZÁLEZ ORTEGA, S., "La informática en el seno de la empresa. Poderes del empresario y condiciones del trabajo", en AA.VV., *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004.

GOÑI SEIN, J. L., "*Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos*", en AA.VV., Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo, Albacete, 2004,

MARTÍNEZ FONS, D., *El Poder de Control del empresario en la relación laboral*, Consejo Económico y Social (España), 2002, Madrid. ISBN 9788481881585.

NORES TORRES, L.E. "Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales: aspectos individuales, colectivos y procesales", *Revista de Información Laboral*, nº 7/2016, Parte doctrinal.

THIBAULT ARANDA, J. L.. "Tecnología informativa y privacidad de los trabajadores", *Revista Aranzadi de Derecho y Nuevas Tecnologí*as. ISBN 84-9767-257-7, Aranzadi, 2003.

SANGUINETI, W. "Derechos fundamentales de la persona del trabajador y poderes empresariales", *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, ISSN 0213-0556, nº 21-22, 2012, págs 15-30.