DERECHOS FUNDAMENTALES DE LOS TRABAJADORES Y PODERES DE CONTROL DEL EMPLEADOR A TRAVÉS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

CARMEN SÁEZ LARA

Catedrática de Derecho del Trabajo y de la Seguridad Social
Universidad de Córdoba

EXTRACTO **Palabras clave: Derechos fundamentales, TICs, poderes de control, protección de datos, Reglamento UE**

El riesgo que las nuevas tecnologías aplicadas a los poderes de control empresarial determina sobre los derechos de los trabajadores a la privacidad, a la autodeterminación informativa y a la libertad de comunicaciones exige una intervención normativa y una respuesta judicial que, adoptando como perspectiva la garantía de estos derechos fundamentales, tutelen también el interés empresarial de sancionar abusos contractuales de los trabajadores. En la actualidad, la doctrina constitucional y la doctrina judicial creo que no ha conseguido armar unos criterios hermenéuticos que garanticen suficientemente aquellos derechos en los centros de trabajo. Especialmente es criticable, a mi juicio, la aplicación, en muchos supuestos, del canon de control de la expectativa razonable de privacidad y de confidencialidad para excluir la aplicación del art. 18 CE. El Reglamento UE sobre protección de datos, aplicable a partir de 2018, promueve una normativa estatal laboral sobre esta cuestión que impondrá importantes cambios sobre el actual estado de la cuestión. En primer lugar, será preciso aplicar las estrictas exigencias de información a los afectados, léase trabajadores, previstas en el Reglamento, en el marco del reforzamiento del tratamiento de datos leal y transparente que el mismo persigue, y, en segundo lugar, en favor de la tutela de los derechos de los trabajadores se establece un nuevo cuadro de exigencias formales y sustantivas que se imponen al responsable del tratamiento de datos, para la instalación de cualquier sistema de control de la actividad laboral. En definitiva, la transparencia en el desarrollo de la actividad laboral conllevará una mayor transparencia de la facultad de control empresarial.

ABSTRACT **Keywords: Fundamental rights, ICT, powers of control, data protection, EU regulation**

The risk that the new technologies applied to the powers of corporate control determines the rights of workers to privacy, informational self-determination and freedom of communications requires a policy intervention and response judicial.

Regulation EU data protection, applicable from 2018, which promotes a state labor regulations on this issue, will impose important changes on the current status of the issue among us. First, it will be necessary to apply strict reporting requirements to those affected, read workers, provided for in the regulation, within the framework of the reinforcement of fair and transparent data that it pursues, and, secondly, on behalf the protection of the rights of workers sets a new picture of formal and substantive requirements imposed on the person responsible for the processing of data, for the installation of any system of control of work. Ultimately, transparency in the development of the work must involve in the future some greater degree of transparency of the Faculty of business control.

 Recepción del original: 20.07.2017 Aceptación original: 31.08.2017

ÍNDICE

1. CUESTIONES INTRODUCTORIAS

Los derechos fundamentales de los trabajadores deben hacer frente desde hace unos años a la potencialidad invasiva de las nuevas tecnologías aplicadas al ejercicio del poder empresarial, de forma que el derecho a la intimidad, al secreto de las comunicaciones y a la autodeterminación informativa, entre otros, se ven limitados por formas de control empresarial imprevisibles hace tan sólo una década. Como se sabe, en términos generales, el reconocimiento de los derechos fundamentales de los trabajadores en los lugares de trabajo, tardío y paralelo a la entrada del sindicato en las empresas, no tuvo lugar hasta la segunda mitad del siglo pasado. A este dato debemos añadir que, más concretamente entre nosotros, su configuración constitucional en las relaciones laborales los definió como un límite al poder empresarial, a su vez modulado (y debilitado) por el deber de buena fe contractual. Desde este punto de partida, hemos de analizar el fuerte desafío que para la efectividad de los derechos fundamentales de los trabajadores se encuentra conectado con la introducción en la gestión empresarial de las tecnologías de la información y las comunicaciones, las célebres TIC.

Desde hace algunos años asistimos a cambios continuos de los sistemas de control de la actividad laboral para adaptarse a la nueva realidad digital. De un control físico y presencial se ha pasado a un control virtual y permanente de la actividad laboral. La videovigilancia ofrece múltiples medios de tratamiento de los datos y sistemas, que se perfeccionan a un ritmo acelerado frente a otras

técnicas de control precedentes, como circuitos cerrados de televisión, grabación por dispositivos webcam, digitalización de imágenes o instalación de cámaras. Como ha destacado la Agencia Española de Protección de Datos (AEPD), la aplicación de tecnologías de la información se manifiesta de muy diversas formas, así a través de controles biométricos, huella digital, videovigilancia, controles sobre el ordenador, revisiones, monitorización e indexación de la navegación por Internet, monitorización del correo electrónico, o los controles sobre la ubicación física del trabajador, mediante geolocalizadores.

Pues bien, el uso de tecnologías de la información multiplica las posibilidades de control empresarial al mismo tiempo que se multiplican las posibilidades de limitación de los derechos del trabajador.Los derechos de los trabajadores a la intimidad y a la protección de datos, así como el secreto de las comunicaciones, cuando se verifica controles empresariales sobre ordenadores y dispositivos móviles, resultan afectados y pueden ser vulnerados si se someten a limitaciones injustificadas, desproporcionadas o carentes de habilitación legal.

En consecuencia, el uso de tecnologías de la información por el poder empresarial obliga a adoptar medidas de control de los trabajadores que respeten su dignidad, su vida privada y su derecho a la protección de datos, toda vez que existiendo en la mayor parte de estos supuestos tratamientos de datos personales es necesario cumplir con los principios que rigen este derecho. Como se ha puesto de relieve por la AEPD[1], el incremento experimentado en la instalación de sistemas de cámaras y videocámaras con fines de vigilancia ha generado numerosas dudas en lo relativo al tratamiento de las imágenes que ello implica. Sobre esta cuestión, el TC ha afirmado que debe asegurarse que las acciones dirigidas a la seguridad y vigilancia no contravengan aquel derecho fundamental, que tiene pleno protagonismo en los terrenos de la captación y grabación de imágenes personales que permitan la identificación del sujeto. En relación con el contrato de trabajo este protagonismo cobra, si cabe, mayor relevancia habida cuenta la coincidencia existente entre el locus de trabajo, que es donde pueden movilizarse por los trabajadores las garantías fundamentales, y los espacios físicos sujetos a control mediante sistemas tecnológicos (STC 29/2013, de 11 de febrero, FJ 5).

De otra parte, el correo electrónico como medio de comunicación fundamental en las relaciones laborales, el uso de redes sociales por la empresa y la creación de redes sociales corporativas pueden además implicar que los datos personales de los trabajadores sean visibles para terceros, si el almacenamiento

[1] Instrucción 1/2006, de 12 de diciembre, 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

de los mismos pasa del ordenador a la nube. Es precisa pues una aplicación estricta de la normativa sobre protección de datos por parte del empresario como responsable del tratamiento de estos datos.

Pues bien, España se sitúa en ese grupo de países, sin regulación legal específica sobre videovigilancia empresarial y sobre el control empresarial de los instrumentos telemáticos, que ha confiado a los tribunales laborales la garantía del necesario equilibrio entre el interés empresarial y los derechos fundamentales de los trabajadores[2].

En efecto, en este contexto de cambio empresarial y cuando se utilizan sistemas de verificación de la actuación de los trabajadores imprevisibles para el legislador español de 1980, nuestro marco normativo sobre el poder de control empresarial, en cambio, ha permanecido inamovible. Ninguna reforma ha experimentado el art. 20.3 ET, que dispone que el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control, lo que lleva a afirmar generalizadamente que es admisible la videovigilancia. Ahora bien, ésta no es un mero instrumento de control del cumplimiento de los deberes laborales sino que invade la privacidad del trabajador obteniendo información y datos personales relevantes. Las imágenes grabadas son datos personales relevantes para conocer el perfil del trabajador. No es sólo un instrumento de control del trabajo sino de supervisión del propio trabajador. A mi juicio, las características de este medio de vigilancia implican un cambio cualitativo del poder de control empresarial, que resulta así difícilmente incardinable en el citado precepto Estatutario, pensado para una realidad distinta y que nos permitiría cuestionar que la libertad de empresa pueda ser un título legitimador suficiente de estos tipos de video control.

Igualmente, ningún cambio ha experimentado el art. 18 ET que concibe la taquilla como el único espacio de privacidad del trabajador cuando actualmente ésta se ha extendido a otros espacios no físicos, como correos personales o archivos del terminal utilizado por el trabajador para el desarrollo de su actividad laboral. Por su parte, el art. 64 ET, en fin, reconoce los derechos de información y consulta de los representantes de los trabajadores previamente a la adopción y revisión de sistemas de control laboral[3], una regulación que, sin embargo, no ha resultado suficiente para dotar a los representantes de los trabajadores de protagonismo

[2] Para un estudio comparado V. AAVV., Nuevas Tecnologías y gestión de recursos humanos, Proyecto Technos: Impacto de las redes sociales y marco laboral tecnológico (Del Rey Guanter dir.), Wolter Kluwer, 2017, pp. 301-367.

[3] La exigencia de autorización judicial como garantía de la libre comunicación queda referida al ámbito de la prueba en el proceso de conformidad con el art. 90.4 LRJS al señalar que cuando sea necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que pueda afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existan medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto.

en la tutela de los derechos de los trabajadores frente a las decisiones de control empresarial, en el nuevo contexto tecnológico.

La ausencia de una regulación legal específica tampoco se ha visto suplida por la normativa convencional y han sido, de un lado, las políticas de la empresa las "llamadas" a regular una cuestión de relevancia constitucional y, de otro, los tribunales los que finalmente han determinado caso por caso la legitimidad de las medidas empresariales. Como tempranamente señalaría el TC y hoy es plenamente reproducible, no existe normativa específica que regule la instalación y utilización de estos mecanismos de control y vigilancia consistentes en sistemas de captación de imágenes o grabación de sonidos dentro de los centros de trabajo, por lo que son los órganos jurisdiccionales y finalmente el TC, los encargados de ponderar, en caso de conflicto, en qué circunstancias puede considerarse legítimo su uso por parte del empresario, al amparo del poder de dirección que le reconoce el art. 20 ET, atendiendo siempre al respeto de los derechos fundamentales del trabajador, y muy especialmente al derecho a la intimidad personal que protege el art. 18.1 CE, teniendo siempre presente el principio de proporcionalidad (STC 98/2000, de 10 de abril, FJ 8).

En este sentido, es preciso recordar respecto a la posible colisión de intereses que reiteradamente la doctrina constitucional ha puesto de relieve la necesidad de que "los órganos judiciales preserven el necesario equilibrio entre las obligaciones del trabajador dimanantes del contrato de trabajo y el ámbito de sus derechos y libertades constitucionales, pues, dada la posición preeminente de éstos en el Ordenamiento jurídico, en cuanto proyecciones de los núcleos esenciales de la dignidad de la persona (art. 10.1 CE) y fundamentos del propio Estado democrático (art. 1 CE), la modulación que el contrato de trabajo puede producir en su ejercicio ha de ser la estrictamente imprescindible para el logro de los legítimos intereses empresariales, y proporcional y adecuada a la consecución de tal fin"[4].

Son pues los tribunales los que están fijando los criterios sobre el uso de ordenadores fijos o portátiles o del correo electrónico, en base a una doctrina que hunde sus raíces en la doctrina judicial relativa a los criterios establecidos para registro de taquillas, despachos, o el control de llamadas telefónicas y deberán seguir estableciéndolos en relación con el uso de redes sociales y plataformas corporativas. Pero debe tenerse en cuenta que la doctrina judicial en sus análisis no deja de considerar el correo electrónico, internet o el ordenador como instrumentos o herramientas de trabajo. Sin embargo las TIC no son sólo instrumentos de trabajo sino herramientas de comunicación y espacios, eso si no

[4] V. por todas, SSTC 213/2002, de 11 de noviembre, FJ 7; 20/2002, de 28 de enero, FJ 4; y 151/2004, de 20 de septiembre, FJ 7.

físicos sino virtuales, en los que el trabajador puede disponer de una esfera de privacidad legítima.

Las notas características del tema de nuestro estudio ya definidas, es decir la ausencia de normativa laboral específica y el protagonismo judicial han de ser completadas con un marco normativo general de referencia y una serie de documentos relevantes, que han sido aplicados por las resoluciones judiciales para definir las pautas de actuación de los diferentes sujetos protagonistas, operadores jurídicos y agencias de protección de datos.

Así de partida, además de las normas constitucionales (art. 18 apartados 1,3 y 4 CE), las normas internacionales y comunitarias que tienen una incidencia directa sobre nuestro objeto de estudio han sido, fundamentalmente[5], el art. 8 del Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales[6] y la Directiva 95/46/CE, que deroga el Reglamento 2016/679, aplicable a partir del25 de mayo 2018[7], en relación con la tutela del derecho a la protección de datos.

Además del marco normativo de referencia, las decisiones judiciales aplican o en ocasiones simplemente hacen referencia a diversos textos y documentos como son por ejemplo la Instrucción 1/2006, de 12 de diciembre, de la AEPD sobre el tratamiento de datos personales con fines de vigilancia a través de

[5] Además, debe citarse, entre otros, el art. 12 de la Declaración Universal de Derechos Humanos de 1948, el art. 8.1 del Convenio y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966, el Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, conocido habitualmente como Convenio, los artículos de la Carta de derechos fundamentales de la Unión Europea.

[6] El artículo 8 CEDH establece que "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

[7] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). La Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, de fecha 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Según el TJUE, esta norma aspiraba a realizar una armonización completa, es decir, aspira a equiparar los niveles de protección entre todos los Estados miembros, coordinando sus legislaciones, de modo que dispensen una protección equivalente, sin perjuicio de reconocerles un margen de maniobra, pero que han de ejercer de conformidad con el derecho comunitario y dentro de los límites de la propia Directiva (STJCE de 6/11/2003, Lindqvist, ap. 96).

sistemas de cámaras o videocámaras y el Repertorio de Recomendaciones Prácticas sobre Protección de los datos personales de los trabajadores de la OIT. Otros documentos importantes en la materia han sido emitidos por el Grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, que fue establecido por el artículo 29 de la Directiva 95/46/CE, (y cuyas funciones serán asumidas por el Comité Europeo de Protección de Datos)[8] como el dictamen 8/2001, sobre videovigilancia en el contexto laboraly el documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo de 29 de mayo de 2002.

Finalmente, junto con este acervo normativo y documental debemos destacar la existencia también de sentencias de referencia, que han determinado además de la doctrina judicial, las resoluciones de la AEPD, es el caso de las conocidas SSTEDH3/4/2007 Copland c. Reino Unido y de 12/01/2016, Barbulescu c. Rumania, las SSTC 98/2000, de 10 de abril y 186/2000, de 10 de julio, y posteriormente las SSTC 29/2013, de 11 de febrero y 39/2016, de 3 de marzo, en materia de video vigilancia, y, en materia de control de ordenares, la STS de 26/9/2007 y después la STS de 6/10/2011 así como las posteriores SSTC 241/2012, de 17 de diciembre y 170/2013, de octubre[9].

En las páginas siguientes se abordará las soluciones al conflicto entre el interés empresarial y los derechos fundamentales de los trabajadores, planteado por el uso de medios tecnológicos de control de la actividad empresarial, tratando en primer lugar los casos de video vigilancia de la actividad laboral y, en segundo lugar, los de monitorización de dispositivos electrónicos utilizados para el trabajo. Las preguntas que nos plantearemos son si el trabajador tiene garantizada y en qué términos una esfera de intimidad o más correctamente de privacidad en su lugar de trabajo y en el uso de los medios electrónicos de trabajo. De otra parte, la cuestión será determinar si los derechos fundamentales a la protección de datos y a la libertad de comunicación se garantizan en la empresa y en qué términos.

Previamente será preciso realizar algunas consideraciones introductorias sobre la garantía de la "privacidad" de los trabajadores en las empresas como contenido tutelado por el derecho a la "intimidad" (art. 18.1 CE).

[8] El artículo 29 de la citada Directiva estableció un Grupo de trabajo sobre la protección de las personas en lo que respecta al tratamiento de datos personales para examinar la cuestión de la vigilancia de comunicaciones electrónicas en el contexto laboral y las implicaciones de la protección de datos para empleados y empleadores. El Reglamento general sobre protección de datos, derogatorio de la misma ha creado el Comité Europeo de Protección de Datos que asume sus funciones

[9] Así como es destacable la existencia de abundantes estudios doctrinales:

2. DERECHO A LA INTIMIDAD Y DERECHO A LA PRIVACIDAD EN LA EMPRESA

Garantiza el art. 18.1 CE el derecho a la intimidad y no el más amplio derecho a la privacidad, lo que podría suscitar en primer lugar la cuestión de la garantía constitucional ex art. 18.1 CE del derecho a la privacidad y, en segundo lugar, si el citado art. 18.1 CE tutela el derecho a la vida privada del trabajador en los centros de trabajo.

En relación con la primera pregunta, es preciso recordar que el TC ha configurado el derecho a la intimidad como un derecho estrictamente vinculado a la propia personalidad y derivado de la dignidad de la persona reconocido en el artículo 10.1 CE, que implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana"[10]. Por lo que respecta a su contenido tutelado, la propia conceptualización de la intimidad, como ha declarado el Tribunal Constitucional, es abierta y evolutiva en función del tema concreto que se esté tratando (STC 110/1984, de 26 de noviembre, FJ 3º) y lo cierto es que, como ya se ha señalado, tras tres décadas de doctrina constitucional continúa existiendo alguna confusión conceptual en la determinación del contenido del derecho a la intimidad, pues se trata de un derecho cuyas fronteras en relación con otros derechos como el derecho a la protección de datos, no siempre resultan bien definidas[11].

Pues bien, reconoce el art. 18.1 CE el derecho a la intimidad cuando ya las declaraciones de derechos posteriores a la segunda guerra mundial reconocían con un alcance más amplio que incluiría el derecho a la intimidad, el derecho a la vida privada[12]. A pesar de esta falta de equivalencia entre ambos derechos, la doctrina constitucional ha realizado en algunas sentencias una interpretación amplia del derecho a la intimidad para hacer frente a intromisiones en la vida

[10] SSTC 170/1997, de 14 de octubre, FJ 4º; 231/1988, de 2 de diciembre, FJ 3º; 197/1991, de 10 de noviembre, FJ 3º; 57/1994, de 28 de febrero, FJ 5º; 143/1994, de 9 de mayo, FJ 6º; 207/1996, de 16 de diciembre, FJ 3º; y 202/1999, de 8 de noviembre, FJ 2º(entre otras muchas).

[11] V. Pardo Falcón, Los derechos al honor a la intimidad personal y familiar y a la propia imagen, en AA.VV. Comentarios a la Constitución Española (Casas Baamonde, Rodriguez Piñero y Bravo Ferrer directores) p. 410.

12 V. art. 12 Declaración Universal de los Derechos Humanos, art. 17 del Pacto Internacional de los Derechos Civiles y Políticos y el art. 8 del Convenio Europeo de Derechos Humanos. Precisamente uno de los primeros debates generados por el art. 18.1 CE fue el de si el honor, la intimidad y la propia imagen se configuraban como tres derechos autónomos o la triple vertiente del derecho a la privacidad, término usado en el ámbito europeo, siendo la primera la opción interpretativa que resultaría avalada por el TC, V. Pardo Falcón, Los derechos al honor a la intimidad personal y familiar y a la propia imagen, cit.,p. 415.

privada frecuentes en la actualidad[13]. Igualmente pueden citarse en este mismo sentido las sentencias constitucionales sobre videovigilancia de los trabajadores o sobre control de ordenadores, en las que también se equipara tutela de la intimidad y tutela de la vida personal del trabajador en los lugares de trabajo.

En segundo lugar, en relación con la garantía de la privacidad a los trabajadores en el desarrollo de su actividad laboral**,** el TEDH dejaría claro desde sus primeras sentencias que los trabajadores tienen reconocido una esfera de privacidad en el desarrollo de su actividad en las empresas.

Debe así recordarse que la doctrina del TEDH ha afirmado que la noción de vida privada es un concepto amplio que abarca, por ejemplo, el derecho a establecer y desarrollar relaciones con otros seres humanos, y más concretamente ha negado, a efectos del control empresarial del trabajador en su puesto de trabajo, la distinción entre vida personal y vida profesional estableciendo que "en definitiva es el curso de la vida profesional que la mayoría de la gente tiene una oportunidad significativa de desarrollar relaciones con el mundo exterior. De esta forma, ha señalado que sería muy restrictivo limitar la noción de vida privada protegida por el art. 8.1 del Convenio Europeo a un "círculo íntimo" en el que el individuo puede conducir su vida personal a su manera y excluir plenamente el mundo exterior no incluido en este círculo. No puede desconocerse que también en otros ámbitos, y en particular en el relacionado con el trabajo o la profesión, se desarrollan relaciones interpersonales, vínculos o actuaciones que pueden constituir manifestación de la vida privada. La protección de la vida privada en el ámbito del Convenio Europeo, en suma, se extiende más allá del círculo familiar privado y puede alcanzar también a otros ámbitos de interacción social[14].

En definitiva, los trabajadores son "los ciudadanos de las empresas" y, de conformidad con esta doctrina, nuestro TC también señalaría que la intimidad protegida por el art. 18.1 CE no se reduce necesariamente a la que se desarrolla en un ámbito doméstico o privado pues en el desarrollo de su actividad profesional los trabajadores desarrollan su vida privada, es decir existe una esfera de privacidad tutelada más allá de las áreas destinadas al vestuarios, aseo o zonas de esparcimiento y descanso dentro de las unidades productivas.

Ahora bien, la afirmación teórica de partida sobre la existencia de los derechos fundamentales de los trabajadores en las empresas puede quedar en la prác-

[13] Como es el caso del ruido, en la SSTC 119/2001, de 29 de mayo y 16/2004, de 23 de febrero.

[14] STEDH de 16/12/1991, Niemietz c. Alemania, ap.29; doctrina reiterada en las SSTEDH de 4/5/2000, Rotaru c. Rumania, ap.43, y de 27/7/2004, Sidabras y Džiautas c. Lituania, ap. 44. V también SSTEDH de 22/2/1994, Burghartz c. Suiza, ap. 24; y de 24/6/2004, Von Hannover c. Alemania, ap. 69.

tica desatendida si el contenido esencial del derecho se supedita al interés del empresario en la obtención de un medio de prueba de las conductas ilícitas. De hecho existiría cierta contradicción argumental si tras admitir la vigencia en la empresa de los derechos de la personalidad y por tanto del derecho a la vida personal en el terreno de las relaciones profesionales, se considerara, por ejemplo, que la videovigilancia es posible pues el trabajador no desarrolla su intimidad/privacidad en el ámbito profesional o se afirmara que el correo electrónico no deja de ser un medio que, perteneciente al patrimonio empresarial, es puesto a disposición del trabajador para ser utilizado en el cumplimiento de la prestación laboral[15].

Por ello, es necesario analizar, más allá de la anterior afirmación de partida sobre la garantía de la vida privada del trabajador en los centros de trabajo, como está se tutela por nuestros tribunales, lo que se abordará a continuaciónde forma separada en los casos de control con videovigilancia y de control de dispositivos electrónicos.

3. LA VIDEOVIGILANCIA Y LOS DERECHOS A LA INTIMIDAD Y A LA AUTODERMINACIÓN INFORMATIVA

El poder de control del empresario integra la facultad de adoptar las medidas que estime más oportunas de vigilancia y control, para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, pero guardando en su adopción y aplicación la consideración debida a la dignidad del trabajador. Ante formas automatizadas de control de la actividad laboral de los trabajadores la cuestión que se plantearía en primer lugar fue la posibilidad de su instalación atendiendo a la afectación a los derechos de los trabajadores y en un primer momento como se sabe, al derecho a la intimidad[16]

Aunque ciertamente, el art. 20.3 ET dispone que el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control, lo que lleva a afirmar generalizadamente que es admisible la videovigilancia, esta no es un mero instrumento de control del cumplimiento de los deberes laborales sino que

[15] Como medio que el empresario pone a disposición del trabajador, la utilización del correo electrónico debe someterse a las instrucciones recibidas al respecto, lo que no puede llevar a pensar que el silencio empresarial implique un permiso para toda suerte de uso desviado, pues ello supondría una transgresión de la buena fe contractual (art. 5.a. ET). FERNÁNDEZ AVILÉS, RODRÍGUEZ-RICO ROLDÁN, Nuevas tecnologías y control empresarial de la actividad laboral en España, Labour and LawIssues, 2016p. 57.

[16] En el caso resuelto por la 98/2000 la infracción del derecho a la intimidad personal consagrado en el art. 18.1 CE, se afirmaba producida directamente por la instalación y puesta en funcionamiento del sistema de captación y grabación de sonido en diversos lugares del casino (zonas de caja y de ruleta francesa).

invade la privacidad del trabajador obteniendo información y datos personales relevantes. No es solo un instrumento de control del trabajo sino sobre todo una forma de supervisión del propio trabajador. A mi juicio, las características de este medio de vigilancia implican un cambio cualitativo del poder de control empresarial que permiten cuestionar que la libertad de empresa sea un título legitimador suficiente de estos tipos de video control.

La instalación de este medio de vigilancia a través de captación de imágenes se ha condicionado a una serie de exigencias por su afectación al derecho a la intimidad y al derecho a la protección de datos, pues, como antes se afirmó, en el desarrollo de su actividad profesional los trabajadores desarrollan su vida privada y al incorporarse las imágenes a ficheros resulta aplicable el régimen jurídico del derecho a la protección de datos. Por tanto, su admisiblidad debe estar fundamentada, de conformidad con la doctrina constitucional, sobre ambos derechos fundamentales, estando en juego tanto el art. 18.1 como el art. 18.3, que consagran dos derechos autónomos.

3.1. Admisión de los sistemas de videovigilancia y derecho a la privacidad

De acuerdo con la normativa aplicable y la doctrina constitucional, la videovilancia para ser constitucionalmente admisible habrá de ser un medio adecuado necesario y proporcionado.

De conformidad con el citado art. 20.3 ET, sólo será adecuado este medio de control si su finalidad es verificar el cumplimiento de las obligaciones contractuales laborales por parte del trabajador. Igualmente, entre los principios de la protección de datos el artículo 4 LOPDP sobre calidad de los datos establece en su primer apartado que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, en este caso, el control del cumplimiento de la prestación laboral.

De conformidad con la doctrina constitucional, este medio de control ha de ser además necesario y proporcional pues las Sentencias del Tribunal Constitucional 98/2000, de 10 de abril y 186/2000, de 10 de julio, se apartan de aquella interpretación judicial[17] y doctrinal[18]para la que el centro de trabajo

[17] V. STSJ Cataluña, de 25/04/1994, STSJ Galicia, de 25/01/1996.

[18] Tras la referida STC 98/2000 se sigue afirmando que la mera captación de la imagen de una persona cuando cumple con su prestación laboral en un lugar abierto al público no tiene por qué considerarse lesiva –a no ser que concurran otras circunstancias– de aquel derecho fundamental: Desdentado Bonete, A. y Muñoz Ruiz, B., Control Informático, Videovigilancia y Protección de Datos en el Trabajo, Lex Nova, 2012, pág. 25.

no podía constituir, por definición, un espacio en el que se ejerza el derecho a la intimidad por parte de los trabajadores, "ya que el referido derecho se ejercita en el ámbito de la esfera privada del trabajador, que en el centro de trabajo hay que entenderlo limitado a los lugares de descanso o esparcimiento, vestuarios, lavabos o análogos, pero no a aquéllos lugares en los que se desarrolla la actividad laboral"(STC 98/2000, FJ 6)[19].

En definitiva, la importancia de estas dos primeras sentencias constitucionales sobre vigilancia y TIC fue asumir la tesis, ya sostenida por el TEDH, y que afirma que más allá de las zonas o espacios privados de los centros de trabajo y en el desarrollo de su actividad laboral también existen esferas de privacidad del trabajador, lo que, a mi juicio, se deduce directamente de la vigencia de los derechos de la personalidad en los lugares de trabajo, pues como se había dicho ya los trabajadores no dejan aparcados sus derechos en las puertas de la fábricas.

Además de necesario, un mecanismo de control como la videovigilancia debe ser un medio de control proporcional. Según la STC 98/2000, la implantación de tales sistemas de control ha de ser conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial.

Como reiteradamente ha señalado nuestro TC, el principio de proporcionalidad formulado para comprobar la admisibilidad constitucional si una medida restrictiva de un derecho fundamental, exige constatar si cumple tres requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, 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 (juicio de proporcionalidad en sentido estricto).

Un test que no superaría como se recuerda la instalación por la empresa Casino de La Toja, S.A. de micrófonos en determinadas dependencias del centro de trabajo (secciones de caja y ruleta francesa) cuando ya existía un sistema de control de captación de imágenes en el caso resuelto por la STC 98/2000 y si

[19] "*En suma, habrá que atender no solo al lugar del centro del trabajo en que se instalan por la empresa sistemas audiovisuales de control, sino también a otros elementos de juicio (si la instalación se hace o no indiscriminada y masivamente, si los sistemas son visibles o han sido instalados subrepticiamente, la finalidad real perseguida con la instalación de tales sistemas, si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control, etc.) para dilucidar en cada caso concreto si esos medios de vigilancia y control respetan el derecho a la intimidad de los trabajadores*."(STC 98/2000, FJ 6)

la instalación de un circuito cerrado de televisión que enfocase únicamente a las tres cajas registradoras tras un descuadre llamativo en los rendimientos del economato de la empresa ENSIDESA, y de alguna advertencia sobre el irregular proceder de los cajeros[20]. Y un test que también se supera en la STC 39/2016, de 3 de marzo, en el caso de instalación de cámaras de seguridad que controlaban la zona de caja donde se desempeñaba la actividad laboral[21].

La instalación de medios de control de la actividad laboral de los trabajadores que afecten a sus derechos fundamentales sólo son constitucionalmente admisibles pues si constituyen medios adecuados, necesarios y proporcionados. Su adopción y aplicación se rige por los principios de proporcionalidad y de intervención mínima. El principio de intervención mínima ha sido doctrinalmente desarrollado[22], y lo afirma expresamente la STC 98/2000, así como también lo recoge la Instrucción de 1/2016 AEPD[23].

3.2. Admisión de los sistemas de videovigilancia y derecho a la autodeterminación informativa

Junto a las exigencias para su admisibilidad constitucional, desde la perspectiva del derecho a la intimidad, los sistemas de videovigilancia de los trabajadores han de adoptarse y aplicarse, de conformidad con el contenido

[20] En este segundo caso resulta relevante que se tratara de verificar las fundadas sospechas de la empresa sobre la torticera conducta del trabajador, pretensión justificada por la circunstancia de haberse detectado irregularidades en la actuación profesional del trabajador, constitutivas de transgresión a la buena fe contractual. Se trataba, en suma, de tener una prueba fehaciente de la comisión de tales hechos, para el caso de que el trabajador impugnase, como así lo hizo, la sanción de despido disciplinario que la empresa le impuso por tales hechos.

[21] Era, a juicio del TC, una medida justificada (ya que existían razonables sospechas de que alguno de los trabajadores que prestaban servicios en dicha caja se estaba apropiando de dinero); idónea para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.

[22] Cfr., Goñi Sein, La videovigilancia empresarial y la protección de datos personales, Thomson Cívitas, 2007, p. 41. Para este autor estos medios de control a través de la imagen estarían prohibidos como regla general para un control directo sobre la actividad laboral que sólo se admitirían si concurren fines legítimos, como la protección de bienes, seguridad en el trabajo, la comprobación del ilícito y la obtención de pruebas (pp, 109 y ss). Más recientemente sobre este tema del mismo autor, Nuevas Tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016, Revista de Derecho Social, 78/2017, pp. 15 y ss..

[23] El uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia lo que en definitiva supone adoptar otros medios menos intrusivos a la intimidad de las personas: Instrucción 1/2006, de 12 de diciembre, AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

constitucional y el régimen jurídico del derecho de protección de datos personales[24].

El art. 18.4 CE regularía la protección de datos como una garantía normativa, dando así acertadamente relevancia constitucional a un derecho que empezaba a establecerse en Europa y en USA. Por su parte, el TC lo configuró como un derecho fundamental, el derecho a la protección de datos o *habeas data* (STC 254/1993, de 20 de julio[25]), cuyo contenido esencial delimitaría definitivamente en las SSTC 290 y 292/2000 de 30 de noviembre. Sobre todo esta última sentencia confirmaría el carácter autónomo del derecho fundamental a la protección de datos.

Como señalara la STC 29/2013, de 11 de febrero, está fuera de toda duda 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, ya que el derecho fundamental amplía la garantía constitucional a todos aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil (ideológico, racial, sexual, económico o de cualquier otra índole) o para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo, lo cual, como es evidente, incluye también aquellos que facilitan la identidad de una persona física por medios que, a través de imágenes, permitan su representación física e identificación visual u ofrezcan una información gráfica o fotográfica sobre su identidad[26].

Estamos, en definitiva, dentro del núcleo esencial del derecho fundamental del art. 18.4 CE[27].De conformidad con la Directiva 95/46/CE, la Ley Orgánica

[24] El Dictamen 8/2011, de 13 de septiembre sobre el tratamiento de datos personales en el contexto laboral, del Grupo de Trabajo del Art. 29, afirmaba que los principios de protección de datos son plenamente aplicables al conjunto de operaciones de recogida de los extremos personales del trabajador y a todas las formas de vigilancia y control empresarial, incluida la utilización del correo electrónico y acceso a internet.Los datos que se obtengan y almacenen deberán ser exactos y puestos al día y no podrán conservarse más tiempo del necesario. Se recomienda a los empleadores fijar un plazo de conservación

[25] Cuyo punto de partida fue el citado Convenio Europeo para la protección de datos de 1981 y ratificado por España en 1984.

[26] SSTC 292/2000, de 30 de noviembre, FJ 6 y 29/2013 FJ 5. V. art. 6 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, art. 3 Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y art. 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

[27] La Universidad de Sevilla es la responsable del tratamiento de las imágenes obtenidas por cámaras de vídeo-grabación instaladas en los accesos y en los recintos universitarios, y que sin poner en conocimiento del trabajador su posible uso para controlar las horas de entrada y de salida, posteriormente fueron medio de prueba para sancionarle con suspensión de empleo y sueldo por incumplimiento reiterado e injustificado de la jornada laboral.

15/1999, de 13 de diciembre, de protección de datos de carácter personal(LOPD) establece un sistema de protección de datos personales que, por lo que aquí interesa, se fundamenta en la calidad de los datos (art. 4), el derecho de información y el consentimiento del afectado (arts. 5 y 6) y exige a la empresa notificar previamente a la Agencia de Protección de Datos la creación de ficheros de datos de carácter personal y la finalidad de los mismos,a los efectos de su necesario registro (art. 26).

Como señalaría el TC, al definir inicialmente este derecho, los elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales son "los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele" (STC 292/2000, de 30 de noviembre, FJ 7).

Sobre estos derechos del afectado en el ámbito del control empresarial del cumplimiento de las obligaciones laborales se han pronunciado las SSTC 29/2013,de 11 de febrero, sobre videovigilancia en un recinto universitario yla STC 39/2016,de 3 de marzo, relativa a la grabación de imágenes al haberse advertido desde tiempo atrás sustanciales descuadres en la contabilidad de un establecimiento comercial.

3.3. Vigilancia empresarial y consentimiento del trabajador

El consentimiento del afectado es como ya se ha visto el elemento definidor del sistema de protección de datos de carácter personal. La LOPD establece el principio general de que el tratamiento de los datos personales solamente será posible con el consentimiento de sus titulares, salvo que exista habilitación legal para que los datos puedan ser tratados sin dicho consentimiento. En este sentido, no podemos olvidar que conforme señalara la STC 292/2000, de 30 de noviembre, "es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es el quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias" (FJ 16).

El art. 6.1 LOPD prevé que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga

otra cosa". El art. 6.2 LOPD enumera una serie de supuestos en los que resulta posible el tratar y ceder datos sin recabar el consentimiento del afectado, entre ellos, cuando los datos de carácter personal cuando se refieran a las partes de un contrato laboral y sean necesarios para su mantenimiento o cumplimiento.

Como se sabe, la interpretación realizada del art. 6.2 LOPD afirma 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[28].

La dispensa del consentimiento se refiere, así, a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, lo que abarca, se afirma, 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 (STC 39/2016 FJ 4).

Aplicando la doctrina expuesta al tratamiento de datos obtenidos por la instalación de cámaras de videovigilancia en el lugar de trabajo, el TC ha afirmado 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 control laboral, y que el consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario.

Ahora bien, aunque no sea necesario el consentimiento del trabajador, 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 (derechos ARCO) (art. 5 LOPD).

3.4. Vigilancia empresarial y derecho de información de los trabajadores

La facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo es el complemento indispensable del derecho fundamental del art. 18.4 CE. Por consiguiente, el Pleno del Tribunal en la STC 292/2000, de 30 de noviembre, señalaría como elemento caracterizador

[28] Esta excepción a la exigencia de consentimiento aparece también recogida en el art. 10.3 b) del Reglamento de desarrollo de la LOPD.

de la definición constitucional del art. 18.4 CE, de su núcleo esencial, el derecho del afectado a ser informado de quién posee los datos personales y con qué fin.

La STC 29/2013 estableció con rotundidad en relación con el derecho de información los siguientes criterios: a) no es admisible una interpretación restrictiva del mismo; b) el derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, (pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento); c) no hay una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales[29], y d) la omisión del tratamiento tampoco podría fundamentarse en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia, pues esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial[30].

Sin embargo, la STC 39/2016, partiendo de la misma doctrina, considera cumplido este derecho de información a través de la colocación por la empresa del distintivo informativo exigido por la Instrucción 1/2006 AEPD[31]. A estos efectos, la argumentación de esta sentencia había partido de considerar que, dada la estrecha vinculación entre las exigencias de consentimiento e información, la

[29] Es verdad que esa exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles y legalmente previstas, pero no debe olvidarse que la Constitución ha querido que la ley, y sólo la ley, pueda fijar los límites a un derecho fundamental, exigiendo además que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero, FJ 2, y en relación con el derecho a la protección de datos personales, STC 292/2000, FFJJ 11 y 16).

[30] En efecto, argumenta el TC, "*se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que lesiona el art. 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible*".

[31] La instrucción 1/2006, de 8 de noviembre, AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, en su art. 3, exige a los responsables que cuenten con sistemas de videovigilancia cumplir con el deber de información previsto en el art. 5 de la LOPD, y a tal fin deberán "colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados" y "tener a disposición de los/las interesados impresos en los que se detalle la información prevista en el art. 5.1 LOPD".

dispensa del consentimiento del trabajador debía ser un dato a tener en cuenta, a la hora de valorar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información.

En el caso resuelto por la STC 29/2013 la ausencia de información determina la violación del art. 18.4 CE en un supuesto en el que las cámaras de video-vigilancia instaladas en un recinto universitario reprodujeron la imagen del empleado y permitieron el control de su jornada de trabajo, sin haber informado al trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen[32].De otra parte, en el caso resuelto por la 39/2016 se declaró que, teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia 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.

Lo anterior explica el voto particular formulado por el Magistrado Valdés Dal-Ré a la STC 39/2016, en el que afirma la correcta doctrina de la anterior STC 29/2013 sobre la inexistencia de una habilitación legal expresa para la omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales. Tampoco es dable situar, se afirma, su fundamento en el mero interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. A su juicio, la lógica de la STC39/2016 quebranta la efectividad del derecho fundamental del art. 18.4 CE, en su núcleo esencial[33].

[32] No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la AEPD; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía 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 cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo (STC 29/2013, FJ 8).

[33] Confunde, afirma el voto particular, la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD). Y lo cierto es, sin embargo, que cabe proclamar la legitimidad de aquel objetivo (incluso sin consentimiento del trabajador, art. 6.2 LOPD, como señala la Sentencia aprobada) y, al mismo tiempo, hacer constar que lesiona el art. 18.4 CE la utilización, para ejecutar el acto, de medios encubiertos que niegan al trabajador la información exigible.

3.5. La aplicación de la doctrina constitucional

El cambio doctrinal del TC, en relación con las exigencias informativas al trabajador sobre los sistemas de videocontrol, se ha trasladado también a la doctrina judicial y a la jurisprudencia. En la aplicación de la doctrina constitucional por la jurisdicción ordinaria, tras la STC 29/2013, se exigirá la necesaria información previa del trabajador[34]y, tras la STC 39/2016, este requisito se entenderá cumplido con el distintivo informativo, cualquiera que sea el supuesto de hecho.

Atendiendo a las diversos supuestos de hecho resueltos por las SSTC 29/2013 y 39/2016, podría realizarse una interpretación de las exigencias para la adopción y aplicación de estos medios de control que distinguiera entre las facultades empresariales de control general del cumplimiento de las obligaciones laborales y las de control específico de concretos trabajadores, ante sospechas fundadas de la infracciones laborales o penales de los trabajadores. De esta forma, sólo en este último caso, sería admisible la instalación de un mecanismo de control de captación de imágenes sin información previa al concreto trabajador afectado, es decir, el secreto en materia de vigilancia[35]. Cuando se trata de sistemas generales para el control de la actividad de los trabajadores no podría eludirse la necesaria información previa a los afectados, como presupuesto del ejercicio de sus derechos ARCO.

Sin embargo, lo cierto es que tal interpretación aun contenida en alguna Sentencia del TS[36], no se deduce de la doctrina constitucional por lo que,

[34] Un buen ejemplo fue la STS 13/5/2014 RJ 2014\330 que declara vulnerado el derecho a la intimidad en un supuesto de utilización de las cámaras de video-vigilancia instaladas como sistema disuasorio de hurtos de clientes, para sancionar a una trabajadora, existiendo falta de información sobre la utilidad de supervisión laboral asociada a las capturas de imágenes de los trabajadores, sin que contrarreste esa conclusión que existieran dispositivos anunciando su instalación y la captación de imágenes, así como la notificación de la creación de ficheros a la AEPD. STSJ Andalucía (Sevilla) 4/11/2015 AS 2015\2685 supuesto donde no se vulnera el derecho a la intimidad pues la trabajadora fue informada expresamente de la colocación de cámaras de videovigilancia. STSJ Castilla-La Mancha de 4/05/2016, que considera ilícita la obtención de pruebas mediante la colocación de cámaras de grabación, sin haber informado ni al trabajador ni al comité de empresa aunque ponen de manifiesto la perpetración de faltas muy graves, tales como la sustracción de materiales destinados a su reciclaje o fumar en lugares peligrosos e inflamables.

[35] El Repertorio de Recomendaciones Prácticas sobre Protección de los datos personales de los trabajadores de la OIT, tras disponer el apartado 6.14.1 que "Cuando los trabajadores sean objeto de medidas de vigilancia, éstos deberían ser informados de antemano de las razones que las motivan, de las horas en que se aplican, de los métodos y técnicas utilizados y de los datos que serán acopiados, y el empleador deberá reducir al mínimo su injerencia en la vida privada de aquéllos" se añade que " El secreto en materia de vigilancia sólo debería permitirse cuando a) se realice de conformidad con la legislación nacional; o b) existan sospechas suficientes de actividad delictiva u otras infracciones graves".

[36] En este sentido, la STS de 7/07/2016 (RJ 2016\4434) acepta como válida la prueba de video

transcendiendo las circunstancias de los casos resueltos, a la vista de los términos generales en los que se formula la doctrina constitucional de la STC 39/2016, ésta sería aplicable en otros casos sobre vigilancia empresarial[37].

Ilustrativas a este respecto son las SSTS de 31/1/2017de 1/2/2017 y de 2/2/2017[38], en las que se declara la válida utilización por la empresa de cámaras de videovigilancia, al conocer el trabajador su existencia en el centro de trabajo, aun cuando no hubiera sido informado expresamente sobre el uso y destino de las cámaras instaladas.

Además, en las SSTS de 31/1/2017 y de 1/2/2017, la Sala declara que se trata de una medida justificada por razones de seguridad, expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo, Y frente a los defectos informativos, se afirma, que pudieron reclamar a la empresa más información o denunciarla ante la Agencia Española de Protección de Datos, para que la sancionara por las infracciones que hubiese podido cometer. De esta forma, el TS mantiene la doctrina sobre no vulneración del derecho a la autodeterminación informativa aun reconociendo que la empresa no ha cumplido con sus obligaciones en materia de información con los afectados por las grabaciones de imágenes.

vigilancia que capta un hurto en una tienda cuando las cámaras se colocan como una reacción a una situación de pérdidas importantes de material en el interior del centro de trabajo y con carteles que advertían de su presencia, lo que hace que los trabajadores conozcan su existencia y finalidad. Para esta Sentencia, las STC 29/2013 y 39/2016 "valoran situaciones distintas a la vez de un derecho fundamental, el de su intimidad, dando como resultado distintas soluciones". "En la primera sentencia citada la empleadora impone una sanción sirviéndose de datos obtenidos en el exterior del lugar de trabajo lo que no cumple ni siquiera una función de advertencia implícita y que tampoco va unida a la comunicación específica dirigida a los trabajadores. En la segunda sentencia, una cámara es situada exactamente sobre la caja una vez producidos hechos irregulares sirviendo en definitiva para comprobar lo que era objeto de sospecha y se deniega el amparo que la trabajadora solicita por las razones antes expuestas." Para esta sentencia que se viniera observando irregularidades con anterioridad y la colocación allí donde tienen lugar las irregularidades, es lo que diferencia la STC 39/2016 de la STC 29/2013.

[37] STSJ Castilla y León (Burgos) de 9/02/2017 AS 2017\183 declara la inexistente vulneración del derecho a la intimidad y la válida utilización por la empresa de cámaras de videovigilancia al conocer el trabajador de su existencia dado el cumplimiento por la empresa de los requisitos específicos de información a través del distintivo, de acuerdo con la Instrucción 1/2006.

Por el contrario v. STSJ Cataluña, de 9/03/2017 (JUR 2017\124182) que declara la vulneración del derecho a la intimidad, por la utilización de cámaras de vídeo-vigilancia en un caso de falta de información previa a los trabajadores de las características y el alcance del tratamiento de los datos obtenidos, así como por no ser una medida idónea para la finalidad pretendida, necesaria y equilibrada. La empresa, a través de una agencia de detectives, instaló dos cámaras ocultas de vigilancia durante 3 semanas en el turno de noche de esterilización.

[38] V. respectivamente, RJ 2017\1429, RJ 2017\1105 y RJ 2017\1628.

Esta doctrina tiene que ser analizada a la luz del nuevo Reglamento UE sobre protección de datos que será de aplicación en 2018.

3.6. Consentimiento e información de los trabajadores a la luz del Reglamento general de protección de datos

En primer lugar, en relación con el consentimiento de los trabajadores, el TC ha realizado una "generosa" interpretación de la excepción prevista en el art. 6.2 LOPD, sobre la posibilidad de tratar y ceder datos de carácter personal sin recabar el consentimiento del afectado, cuando se refieran a las partes de un contrato o precontrato de una relación negocial laboral y sean "necesarios para su mantenimiento o cumplimiento", considerando la captación de imágenes del trabajador "necesaria" para el "cumplimiento" de la relación laboral. Y sobre esta premisa, que no se encuentra discutida doctrinalmente, en la STC 39/2016 se ha desconocido el derecho a la información previa establecido por el art. 5LOPD y contenido esencial del derecho a la autodeterminación informativa.

Ambos temas, el consentimiento implícito en el contrato de trabajo y la falta de información al trabajador afectado tendrán que ser objeto de mayor motivación en el futuro, desde la perspectiva de los derechos fundamentales afectados. A mi juicio, tras el Reglamento de la UE 2016 sobre protección de datos, deberá formularse una mayor motivación para mantener esa interpretación sobre el consentimiento implícito en el contrato de trabajo para el tratamiento y cesión de datos personales, como las imágenes del trabajador con el fin de controlar el cumplimiento de la prestación laboral. Aunque el art 6 del citado Reglamento formula la exigencia de consentimiento del afectado y las excepciones al mismo en iguales términos que el art. 7 de la Directiva, el art. 7 del Reglamento incorpora una nueva regulación relativa a las previsiones sobre las condiciones para el consentimiento, que habrá de ser atendida.[39]

Por lo que se refiere a las exigencias de información de los trabajadores, las mismas se verán reforzadas en la nueva y relevante dimensión que la transparencia adquiere en el Reglamento general de protección de datos, cuyo Capítulo III reconoce derechos del interesado, estableciendo en los arts. 12 y 13 expresamente concretas obligaciones de información por escrito[40].

[39] V. Art. 7. Relativo a las condiciones para el consentimiento que dispone en su apartado 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

[40] En el art. 13.1 indica toda la información que el responsable del tratamiento debe suministrarse al interesado, cuando se obtengan datos personales relativos a él, en el momento en que

En términos generales, creo que puede afirmarse que las exigencias formales y sustantivas establecidas para la instalación por las empresas de estos medios de control de la actividad laboral se van a ver reforzada por el Reglamento general de protección de datos que en aplicación, entre otros, del principio de transparencia, establece nuevas obligaciones para el responsable del tratamiento de datos (art. 35), además de la figura del delegado de prevención de datos (art. 37) y promueve los Códigos de Conducta (art. 40). Todo ello en el marco dirigido a garantizar un tratamiento de datos leal y transparente.

En efecto, el citado Reglamento general impone al responsable del tratamiento la obligación de realizar, antes del tratamiento, una evaluación de impacto relativa a la protección de datos, cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas (Art. 35.1)[41]. Para lo cual el responsable del tratamiento recabará el asesoramiento del delegado de protección de datos[42], si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos (Art. 35. 2).Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento (Art. 35.9). Además, el art. 35. 8 establece que el cumplimiento de los códigos de conducta aprobados por los responsables o encargados correspondientes[43] se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular, a efectos de la evaluación de impacto relativa a la protección de datos.

estos se obtengan. Además, para garantizar un tratamiento de datos leal y transparente, el art. 13.2 dispone que el responsable debe informar si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos.

[41] Téngase en cuenta que de conformidad con el art. 35.3 esta evaluación de impacto relativa a la protección de los datos se requerirá en particular, entre otros, en caso de evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

[42] V. art. 37 relativo a la designación del delegado de protección de datos dispone en su apartado 2 que un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

[43] El art.40, relativo a los Códigos de conducta, establece en su apartado núm. 1 que los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

Todo un conjunto en suma de obligaciones y procedimientos que determinarán mayores dosis de transparencia empresarial en la instalación de sistemas de vigilancia de la actividad laboral de los trabajadores.

Finalmente, debe igualmente destacarse que el Reglamento promueve regulaciones legales o convencionales "específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral". Normas que, se afirma, "incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, (…)y a los sistemas de supervisión en el lugar de trabajo", debiendo ser notificadas por los Estados a la Comisión las disposiciones legales que adopten a más tardar el 25 de mayo de 2018 (art.88).

En definitiva, la aplicación del Reglamento determinará la necesidad de asumir un marco normativo nuevo que determine una mayor transparencia empresarial en el uso de medios de control de la actividad profesional de los trabajadores así como mayores exigencias formales y sustantivas para la instalación de los mismos.

4. MONITORIZACIÓN Y CONTROL DE DISPOSITIVOS ELECTRÓNICOS Y DE LAS REDES CORPORATIVAS

En el caso del uso por el trabajador de los medios informáticos facilitados por la empresa pueden producirse conflictos que afectan a la intimidad de los trabajadores, tanto en el correo electrónico, en el que la implicación se extiende también, al secreto de las comunicaciones, como en la navegación por Internet y en el acceso a determinados archivos personales del ordenador. Como pondría de relieve el Tribunal Supremo, estos conflictos surgen porque existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa. Esa utilización personalizada se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador –como sucede también con las conversaciones telefónicas en la empresa– y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa. Pero, al mismo tiempo, hay que tener en cuenta que se trata de medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario, que, como precisa el artículo 20.3 ET[44].

[44] V. STS 26/09/2007, FJ 2 (RJ 2007, 7514).

Entre nosotros, el estudio del poder de control y los derechos de los trabajadores, cuando se verifican monitorizaciones de los dispositivos electrónicos empleados en el desarrollo de la actividad laboral, tiene como necesario punto de partida la antes citada STS de 26/9/2007. Y ello es así, en primer lugar, porque esta sentencia señala una nueva etapa en relación con las interpretaciones judiciales precedentes que o bien negaban una esfera de privacidad de los trabajadores o bien postulaban la aplicación analógica de la normativa estatutaria del art. 18, relativa a registros de los efectos particulares de los trabajadores. En segundo lugar, esta sentencia asume, en un cierto sentido, la doctrina del TEDH sobre control de ordenadores y navegación por internet, que ha sido determinante en la posterior doctrina constitucional y en la doctrina judicial .Y en tercer lugar, su aplicación promocionaría el desarrollo de políticas empresariales reguladoras del uso de dispositivos electrónicos en las empresas, unas políticas que han sido también doctrinalmente muy valoradas[45].

Pues bien, la doctrina del Tribunal Supremo que en este ámbito, fundada en una interpretación de la doctrina del TEDH, se basa en la aplicación de la "expectativa razonable de intimidad" ha recibido aval constitucional en las SSTC 241/2012, de 17 de diciembre y 170/2013, de 7 de octubre, que se analizarán después, y es seguida también por la doctrina judicial.

Abordaremos primero su estudio para, seguidamente, hacer referencia a la doctrina del TEDH, que le sirve de fundamento en su aplicación de la expectativa razonable de privacidad, a los efectos de delimitar el ámbito de aplicación de la protección de la privacidad y la libertad de comunicación en la empresa.

4.1. La doctrina del Tribunal Supremo

Hasta la citada STS de 26/9/2007, la doctrina judicial se debatió sobre la aplicación del art. 18.3 ET a los controles empresariales sobre el ordenador, el correo electrónico o la navegación por internet por parte de los trabajadores. La aplicación por analogía determinaría la exigencia de garantías para el trabajador, entre otras, la presencia del trabajador y de su representante en el momento del control cuya omisión privaba de valor probatorio al resultado del mismo[46].

El TS en la referida Sentencia de 26/9/2007 declararía, como se sabe, que no cabe la aplicación directa ni analógica del artículo 18 ET al control del uso del ordenador por los trabajadores, fundamentalmente, porque la legitimidad de ese

[45] A favor de políticas empresariales negociada con los representantes legales de los trabajadores: RODRÍGUEZ ESCANCIANO Internet en el trabajo, en Diario La Ley, Nº 8926, Sección Dossier, 21 de Febrero de 2017, Editorial Wolters Kluwer, p. 14

[46] SSTSJ Cantabria de 23/2/2004, Cataluña de 21/9/2004, Madrid de 31/3/2005 y País Vasco de 21/12/ 2004 y de 12/9/ 2006.

control deriva del carácter de instrumento de producción del objeto sobre el que recae. El control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 ET, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 ET.

Esta sentencia tiene la importancia de fijar los límites al ejercicio del poder de control empresarial sobre el uso de los medios informáticos en la empresa. En primer lugar, establecer previamente las reglas de uso de esos medios -los proporcionados por la empresa-, con aplicación de prohibiciones absolutas o parciales. En segundo lugar, informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse, en su caso, para garantizar la efectiva utilización laboral del medio, cuando sea preciso. Así como finalmente la posibilidad de aplicar otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

La referida sentencia contenía finalmente una previsión que ha sido determinante para la resolución doctrinal de estas cuestiones, pues se afirmaba que de esta manera, "si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las SSTEDH, de 25/6/1997 (Halford) y 3/4/2007 (Copland) para valorar la existencia de una lesión del artículo 8 CEDH(FJ 2).

La doctrina de esta STS de 26/9/ 2007 se reproduce por la sentencia de 8/3/ 2011 y se matiza, reforzando el poder de control empresaria, por la STS de 6/10/ de 2011[47].

La STS 6/10/2011 reitera con rotundidad los criterios ya avanzados para la solución de estos supuestos, como la licitud de una prohibición empresarial absoluta de los usos personales y la inexistencia, en el caso del uso personal de los medios informáticos de la empresa por parte del trabajador, de un conflicto de derechos cuando hay una prohibición válida. Al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad. La prohibición absoluta lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador, no siendo posible admitir que surja un derecho del trabajador a que se respete su intimidad en el uso del medio informático puesto a su disposición.

[47] V.RJ 2011, 932 y RJ 2011, 7699, respectivamente.

Esta sentencia considera además que las obligaciones, sobre reglas uso de los medios informáticos y de informar a los trabajadores, establecidas en la citada STS de 28/9/2007, son "matizaciones que operan ya fuera del marco estricto de la protección del derecho fundamental, como obligaciones complementarias de transparencia" Lo decisivo a efectos de considerar la vulneración del derecho fundamental, es que, "la tolerancia" de la empresa es la que "crea una expectativa de confidencialidad" y por ende, la posibilidad de un exceso en el control llevado a cabo por el empleador que vulnere el derecho fundamental de la intimidad del trabajador.

Avalando la doctrina de la STS 6/10/2011 pueden citarse también la STS de 13/9/2016[48] y la STS de 13/9/2016[49].

Esta doctrina del Tribunal Supremo pivota sobre la inexistencia de una expectativa razonable de intimidad o de confidencialidad en los casos de prohibición empresarial del uso privado de dispositivos informáticos propiedad de la empresa, lo que determina que la actividad del trabajador quede fuera del ámbito tutelado por el art. 18 CE sin que pueda considerarse afectada su privacidad por decisiones de control por parte de la empresa. Esta doctrina laboral, al margen de otras valoraciones posteriores, hemos de señalar que se aparta de la tutela general que el art. 18 CE garantiza a los ciudadanos en relación con la obtención lícita de medios de pruebas en el ámbito penal, tal y como ha destacado la Sala Segunda del Tribunal Supremo[50].

[48] V. RJ 2016\4843. Se impugna la Resolución de 15 julio 2014, de la Televisión de Galicia, S.A., por la que se establece la normativa del uso de los sistemas de información de la compañía no lesiona el derecho a la libertad sindical pues no limita el derecho de información, ni el establecimiento de sistemas de control aleatorio de las páginas de internet visitadas y de los correos electrónicos vulnera el derecho a la intimidad personal ni el secreto de la comunicaciones, salvo en el aspecto referido al control para prevenir fines ilícitos

[49] V. RJ 2016\4843. La Sala afirma en el FJ 5 que la empresa puede monitorizar y comprobar, de forma aleatoria, cualquier sesión de acceso a Internet, y revisar los mensajes de correo electrónico de los usuarios/as de la red corporativa y los archivos LOG de los servidores, con el fin de comprobar el cumplimiento de esta y otras normativas, sin ningún tipo de limitación ni cortapisas, sin ningún tipo de criterio o parámetro limitativo.

[50] La Sala de lo Penal del TS, en Sentencia de 16/6/ 2014,ha afirmado que en la empresa, de un lado, en relación con los correos electrónicos que estén sin abrir por el destinatario rige la protección constitucional que otorga el art. 18.3 CE al secreto de las comunicaciones, siendo necesario contar con autorización judicial; de otro, las comunicaciones ya abiertas por el destinatario que únicamente permanecen en las bandejas de entrada y salida, así como otros aspectos adyacentes (historial de navegación web, acceso al disco duro del ordenador, direcciones, frecuencias…), están tutelados por el art. 18.1 CE, referido al derecho a la intimidad, y por el art. 18.4 CE, relativo a la protección de datos personales, debiendo estar a la conocida teoría de la proporcionalidad en el acceso; en fin, para el registro de medios electrónicos, propiedad del trabajador, utilizados en el tiempo y lugar de trabajo, es necesario contar con autorización judicial. En definitiva, aunque la jurisprudencia laboral sigue admitiendo la licitud de la prueba obtenidas mediante control de

Como se sabe, se trata de una doctrina apuntada ya desde la STS de 2007 con fundamento en la doctrina del TEDH pues este Tribunal había afirmado la existencia de una expectativa razonable de privacidad, en casos en los que no existía tal prohibición empresarial expresa.

Ahora bien, lo que a mi juicio no se deduce directamente de la doctrina europea es la consecuencia contraria, es decir que una prohibición expresa de uso privado implique la inexistencia de una expectativa razonable de intimidad y por tanto la exclusión del ámbito de aplicación del art. 8.1 CEDH o del art. 18CE. Será preciso ver con más detalle la doctrina del TEDH, y ello porque el recogimiento teórico de partida de una esfera legítima de privacidad o del derecho a la protección de datos o a la libertad de comunicaciones en la empresa se concilia mal con la admisión de que la prohibición absoluta de los mismos es suficiente para excluir su aplicación en los lugares de trabajo.

4.2. La doctrina del TEDH sobre afectación del art. 8.1 CEDH en relación con el control de ordenadores, correo electrónico y navegación por Internet

La doctrina del TEDH sobre aplicación del art. 8 del Convenio en las relaciones privadas, en defensa de la vida privada del trabajador en los lugares de trabajo se ha formulado en repetidas ocasiones[51]. El TEDH ha conocido diversos supuestos sobre control empresarial del uso de ordenadores y navegación por internet de trabajadores desde la perspectiva de la afectación del art. 8 del Convenio, afirmando la violación del derecho a la vida privada, en casos en los que el trabajador desconocía que era controlado[52]y negándola en un caso de prohibición empresarial de uso personal[53].

comunicaciones en los casos de prohibición de uso privado, a la vista de lo anterior y en aras de la seguridad jurídica la empresa deberá solicitar la intervención judicial en la obtención de los mensajes cerrados y privados del trabajador para la validez probatoria de los controles sobre el correo electrónico en vía penal, (art, 539 LECR).

[51] Aunque, en esencia, el artículo 8 tiene como objetivo la protección de los individuos ante posibles injerencias arbitrarias por parte de las autoridades públicas, este artículo no se limita a prohibir a los Estados que cometan tales injerencias. Además de esta obligación negativa primordial, el respeto efectivo de la vida privada de los individuos puede conllevar obligaciones positivas. Estas obligaciones pueden implicar la adopción de medidas destinadas a garantizar el respeto de la vida privada incluso en el ámbito de las relaciones inter-personales (STEDH de 16/1/2016, Barbulescu c. Rumanía, Sentencia Barbulescu, en adelante, ap.52)

[52] STEDH de 3/4/2007, Copland c. Reino Unido, Sentencia Copland, en adelante, siguiendo STEDH de 25/6/1997, Halford c. Reino Unido, Sentencia Halford en adelante, sobre llamadas telefónicas.

[53] Sentencia Barbulescu.

Así hemos de recordar que las llamadas telefónicas desde las oficinas de la empresa quedan prima facie abarcadas en las nociones de "vida privada" y "correspondencia" a efectos del artículo 8, apartado 1 (Sentencia Halford, ap. 44) y que también deberían recibir la protección del artículo 8 los correos electrónicos enviados desde el puesto de trabajo, así como toda información recogida a través de una vigilancia del uso personal de internet (Sentencia Copland, ap. 41, y Sentencia Barbulescu, ap.36).Como señala la Sentencia Barbulescu (ap.37) en ausencia de un aviso que le indicara que las llamadas podían ser vigiladas, el trabajador podía razonablemente esperar que las llamadas realizadas desde un teléfono profesional serían privadas (Sentencia Halford, ap. 45) y estas mismas expectativas deberían ser aplicables también en cuanto al uso del correo electrónico e internet por parte del demandante (Sentencia Copland, ap. 45)[54].

Pues bien analizando más concretamente esta doctrina hemos de señalar que en la Sentencia Copland[55], el Tribunal considera que la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la trabajadora, sin conocimiento de la empleada, constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia, en el sentido del artículo 8 del Convenio Europeo (ap. 44), una injerencia que no puede resultar admisible, de conformidad con el art. 8.2 del Convenio, pues no se trata de un injerencia "prevista por la Ley".[56]

[54] En un caso en el que se registró el lugar de trabajo del demandante en una oficina de la fiscalía y se embargaron algunas de sus pertenencias (STEDH de 26/7/2007, Peev contra Bulgaria,), el Tribunal estimó que el registro representaba una injerencia en la "vida privada" del demandante y consideró que el demandante podía razonablemente tener expectativas de privacidad con respecto a las pertenencias personales que guardaba en su despacho (ap. 49).

[55] Sobre un caso de seguimiento del teléfono, correo electrónico y uso de Internet de la empleada. Según el Gobierno, se llevó a cabo este seguimiento al objeto de averiguar si la empleada hacía un uso excesivo de las instalaciones del College para asuntos personales. No existía, a la sazón, ninguna política vigente en el College referente al seguimiento del uso del teléfono, correo electrónico o Internet por parte de los empleados. Un precedente importante fue la STEDH de 25/6/1997, Halford c. Reino Unido.

[56] Según reiterada jurisprudencia del TEDH, la expresión «prevista por la Ley» implica –y ello se deduce del objeto y fin del artículo 8 – que exista una medida de protección legal en la legislación interna contra las injerencias arbitrarias de las autoridades públicas en los derechos protegidos por el artículo 8.1. Es así, incluso con más motivo, en áreas como el seguimiento en cuestión, debido a la falta de vigilancia pública y el riesgo de abuso de la autoridad (Sentencia Copland, ap.45) Esta expresión no sólo requiere que la medida impugnada tenga alguna base en la legislación interna, sino que también se refiere a la calidad de la Ley en cuestión, siempre que sea compatible con la preeminencia del Derecho. Para cumplir con la exigencia de la previsibilidad, la Ley debe emplear términos lo suficientemente claros para que todos puedan conocer en qué circunstancias y en qué condiciones pueden las autoridades recurrir a tales medidas (Sentencia Copland, ap.46).

Aunque el Tribunal no excluye, en términos generales, "que el seguimiento del uso por parte de un trabajador del teléfono, el correo electrónico e Internet en el lugar de trabajo pueda considerarse "necesario en una sociedad democrática en ciertas situaciones que persigan un fin legítimo", en este caso el seguimiento no tenía fundamento en Derecho interno, por lo que la injerencia no estaba «prevista por la Ley» tal y como exige el artículo 8.2 del Convenio (ap. 48)

Por su parte, en la Sentencia Barbulescu, teniendo en cuenta especialmente el hecho de que se accedió al contenido de las comunicaciones del empleado en Yahoo Messenger y que la transcripción de estas comunicaciones fue presentado en el procedimiento ante los tribunales de trabajo, el TEDH afirmaría que estas medidas afectaron a la "vida privada" y "correspondencia" del demandante en el sentido del artículo 8.1, por lo que es aplicable al asunto (ap.45). Sin embargo en este caso el Tribunal llega a la conclusión de que las autoridades nacionales no han incumplido el art. 8 CEDH pues no hay elemento alguno que indique que las dichas autoridades incumplieran su obligación de establecer un equilibrio adecuado, dentro de su margen de apreciación, entre los intereses del empleador y el derecho del demandante al respeto de su vida privada en virtud del artículo 8 (ap. 62)[57].

Por tanto en la Sentencia Barbulescu, como después se analizará con más detalle, la no vulneración del art. 8 CEDH no se fundamentó en la inexistencia de una expectativa razonable de privacidad. En el caso Barbulescu, un supuesto de hecho en el que también concurría una prohibición de uso personal, el TEDH si consideraría afectado el citado art. 8.1CEDH, entrando a analizar el fondo del asunto para finalmente entender que no resultaba lesionado el referido precepto del Convenio.

4.3. La doctrina Constitucional y el uso extensivo la expectativa razonable de confidencialidad y de la expectativa razonable de privacidad

En relación con la utilización de ordenadores u otros medios informáticos por parte de los trabajadores, la doctrina constitucional establecida por las Sentencias 241/2012, de 17 de diciembrey 170/2913, de 7 de octubre, en primer

[57] Y ello porque "el Tribunal observa que tanto el Tribunal de Condado como el Tribunal de Apelación otorgaron particular importancia al hecho de que el empleador había accedido a la cuenta Yahoo Messenger del demandante pensando que contendría mensajes de carácter profesional, puesto que el demandante mismo había afirmado inicialmente que había usado la cuenta para asesorar a sus clientes (…). Por lo tanto, se puede deducir que el empleador actuó de conformidad con sus competencias disciplinarias puesto que, tal y como constataron los tribunales nacionales, accedió a la cuenta Yahoo Messenger basándose en el supuesto de que la información allí contenida estaba relacionada con actividades profesionales y que, por ende, acceder a ella era legítimo. El Tribunal no constata motivo alguno de poner en duda estas conclusiones" (ap. 57).

lugar, no deja lugar a dudas sobre la prevalencia del poder empresarial sobre la garantía de privacidad o la llamada "pretensión" de secreto de comunicaciones de las comunicaciones. En segundo lugar, en este contexto avala la doctrina del Tribunal Supremo, en su delimitación del ámbito de aplicación de los derechos fundamentales alegados en estos casos, es decir, el derecho a la intimidad y el secreto de las comunicaciones.

En primer lugar, hemos de recordar que la STC 241/2012 afirmaría, insistiendo siempre en el dato de la titularidad empresarial de tales medios, que "corresponde a cada empresario, en el ejercicio de sus facultades de autoorganización, dirección y control, fijar las condiciones de uso de los medios informáticos asignados a cada trabajador", aludiendo a una regulación del uso profesional de las herramientas informáticas por medio de "órdenes, instrucciones, protocolos o códigos de buenas prácticas", y que "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" (FJ 5).

Y más concretamente, el TC afirma también que aunque en este ámbito pudiera caber la "pretensión" de secreto de las comunicaciones, actúa a su vez legítimamente el poder directivo, con la posibilidad consiguiente de establecer pautas de flujo de la información e instrucciones u órdenes del empresario que aseguren, sin interferir injustificadamente el proceso de comunicación y sus contenidos, el acceso a los datos necesarios para el desarrollo de su actividad.

En segundo lugar, esta doctrina constitucional delimita el ámbito de cobertura del derecho al secreto de las comunicaciones en la empresa, en términos, a mi juicio, restrictivos, excluyendo no sólo las comunicaciones abiertas sino toda comunicación en el interior de la empresa a través de dispositivos de titularidad empresarial cuando el empresario prohíba el uso privado de los medios electrónicos.

En efecto, en la delimitación del ámbito de cobertura del art. 18.3 CE la doctrina del TC comienza por excluir los supuestos de comunicaciones abiertas en la STC 241/2012[58], para excluir después también aquellos supuestos

[58] La demandante de amparo es una trabajadora que venía desempeñando labores de teleoperadora especialista para Global Sales Solutions Line, S.L. Dicha empleada y una compañera instalaron un programa informático denominado «Trillian», de mensajería instantánea, en el disco duro de un ordenador, que era de uso indistinto por todos los trabajadores de la empresa y al que se accedía sin clave. La instalación del programa era contraria a orden empresarial expresa. A través de dicho soporte informático, las trabajadoras entablaban conversaciones en las que vertían comentarios despectivos, críticos e insultantes en relación con compañeros de trabajo, superiores y clientes.

de prohibición empresarial expresa de uso personal de ordenadores u otros dispositivos, supuesto, al que equipara la tipificación en convenio colectivo de la infracción laboral por uso privado en la STC 170/2013[59]. En este último caso se trataría, en expresión del TC, de un canal de comunicación que, conforme a las previsiones legales y convencionales aplicables, se hallaba "abierto al ejercicio del poder de inspección reconocido al empresario"; sometido en consecuencia a su posible fiscalización, con lo que quedaba fuera de la protección constitucional del art. 18.3 CE.

Así se afirma, en efecto, que el art. 18.3 CE protege únicamente ciertas comunicaciones, las que se realizan a través de determinados medios o canales cerrados[60]. Por ello, en la STC 241/2012 se ha excluido la protección constitucional de comunicaciones, que se realizan en un canal del que no puede predicarse su confidencialidad, no vulnerándose pues el art. 18.3 CE pues es una comunicación abierta, esto es, no secreta (FJ 7)[61].

Siendo este el argumento fundamental que motiva la sentencia, también el TC en este caso consideraría que "no podía existir una expectativa razonable de confidencialidad derivada de la utilización del programa instalado", no existiendo una situación de tolerancia a la instalación de programas y, por ende, al uso personal del ordenador que era de acceso totalmente abierto y además incurría en contravención de la orden empresarial".

Dichas apreciaciones fueron descubiertas, por casualidad, por otro empleado que intentó utilizar la unidad «C» de ese ordenador, dando cuenta de ello a la empresa.

[59] Por parte de la empresa Alcaliber SA se procedió a interceptar el contenido de los correos electrónicos de un trabajador, registrados en el ordenador facilitado por la empresa, ante las sospechas de un comportamiento irregular derivado de la revelación a terceros de datos empresariales confidenciales. El convenio colectivo aplicable tipificaba como falta leve la utilización para fines privados de los medios informáticos proporcionados por la empresa.

[60] En consecuencia no "gozan de la protección constitucional del art. 18.3 CE aquellos objetos que, pudiendo contener correspondencia, sin embargo la regulación legal prohíbe su inclusión en ellos, pues la utilización del servicio comporta la aceptación de las condiciones del mismo". 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". Así ocurre "cuando es legalmente obligatoria una declaración externa de contenido, o cuando bien su franqueo o cualquier otro signo o etiquetado externo evidencia que, como acabamos de señalar, no pueden contener correspondencia". En tales casos "pueden ser abiertos de oficio o sometidos a cualquier otro tipo de control para determinar su contenido" STC 281/2006, de 9 de octubre, FJ 3 b) citada por STC 170/2013, de 7 de octubre FJ 4.

[61] A mayor abundamiento el TC afirmaría que "no puede calificarse como vulneradora del derecho al secreto de las comunicaciones la intervención empresarial analizada, por cuanto que, además, la misma se produce a partir de un hallazgo casual de uno de los usuarios, trabajador de la empresa, que transmite su contenido a la dirección, …"(FJ 7).

Pero será la STC 170/2013 la que declare expresamente fuera del ámbito de tutela del art. 18.3 CE las comunicaciones en la empresa, cuando exista una prohibición empresarial de uso privado, supuesto al que equipararía la tipificación convencional de tal uso extralaboral como infracción laboral.

La STC 170/2013 afirmaría que en tanto que la utilización del correo electrónico para fines ajenos al contenido de la prestación laboral se encontraba tipificada como infracción sancionable regía en la empresa una prohibición expresa de uso extralaboral. A lo anterior añade que la expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales (FJ 4).

En tales circunstancias, de acuerdo con la doctrina constitucional sobre el ámbito de cobertura del art. 18.3 CE, cabe entender que no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial. En el contexto descrito, el TC concluye que en definitiva, debe descartarse la invocada lesión del derecho al secreto de las comunicaciones.

Sobre la base de esta misma motivación es decir, la tipificación como infracción del uso extralaboral de las herramientas informáticas y su consiguiente inclusión en el ámbito del poder de control empresarial, el TC, de forma similar a lo dicho respecto al derecho al secreto de las comunicaciones, tampoco en este caso aprecia que el trabajador contara con una expectativa razonable de privacidad respecto a sus correos electrónicos registrados en el ordenador de la entidad empresarial (FJ 5).

Por tanto, el régimen jurídico aplicable en la empresa hacía factible y previsible la posibilidad de que el empresario ejerciera su facultad legal de vigilancia sobre los correos electrónicos del trabajador, impidiendo tal circunstancia abrigar una expectativa razonable de privacidad, que determinara la entrada en la esfera de protección del derecho a la intimidad, de acuerdo con lo explicado en la ya citada STC 12/2012, FJ 5[62].

[62] A pesar de que el TC excluye la aplicación del ámbito de protección del art. 18.1CE pues entiende que no existía una expectativa razonable de privacidad, continua evaluando la conducta empresarial desde el canon de constitucionalidad del principio de proporcionalidad que por definición presupondría que el comportamiento empresarial afectaba al derecho de intimidad. Tales argumentos deben en consecuencia entenderse a mayor abundamiento.

Las SSTC 241/2012 y 170/2013 abordan el secreto de las comunicaciones en las relaciones laborales, bajo el test de la expectativa razonable de confidencialidad, excluyendo del ámbito de aplicación del art. 18.3 CE no sólo las comunicaciones abiertas o no secretas y confidenciales sino cualesquiera otras, considerándolas abiertas al poder empresarial de control. Solo si las comunicaciones privadas son permitidas por el empresario sería de aplicación en la empresa el citado art. 18.3 CE.

Estas sentencias son un claro ejemplo de análisis de los derechos fundamentales de los trabajadores en la empresa desde la perspectiva del interés empresarial, sin duda legítimo, a sancionar usos desviados de tales dispositivos informáticos, pero que no es un interés prevalente sobre aquellos derechos en nuestro sistema constitucional[63]. Ello explicaría los términos del voto particular formulado por el Magistrado ValdesDal-Re a la STC 241/2012[64], criticando las declaraciones de la misma sobre el poder empresarial pues no terminan de corresponderse con el contenido esencial de los derechos fundamentales en presencia, toda vez que el empresario no puede disponer unilateral e ilimitadamente del uso de sus herramientas sin condicionante alguno. Esa concepción, afirma el citado voto particular, expresa una noción ya superada de los derechos del ciudadano trabajador, porque el derecho de libertad, que contiene el art. 18.3 CE, limita sus actos de disposición y limitación de uso o prohibición, sin perjuicio de que quepa, obviamente, la reglamentación del mismo. Más concretamente considera que la titularidad de esos medios y herramientas tampoco confiere al empresario un derecho a restricciones caprichosas y afirma expresamente que cualquier intervención empresarial debe producirse con las prevenciones y cánones de la autorización judicial que cita el art. 18.3 CE, en cuya definición

[63] Claramente se aprecia pues el TC afirmará que el ejercicio de la potestad de control empresarial resulta limitada por la vigencia de los derechos fundamentales, si bien los grados de intensidad o rigidez con que deben ser valoradas "las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin".

[64] La Sentencia de la que me distancio, afirma el voto, responde a un concepto de las relaciones laborales que, con todo el respeto que me merece la decisión de la Sala, no se corresponde con el modelo que impone la cláusula constitucional del Estado social y democrático de Derecho (art. 1.1 CE) que las informa; atribuye al empresario facultades de las que carece; soslaya los condicionantes que en un juicio como el actual imponen la libertad de las comunicaciones y el derecho al secreto de las mismas, con su carácter formal y que, en fin y en el contexto moderno de las innovaciones tecnológicas, brinda indudables ventajas para los procesos productivos y para el desarrollo de la personalidad de los ciudadanos, y, en última instancia, opta por avalar los instrumentos de fiscalización incluso cuando, como en este caso, se actualizan en términos abiertamente invasivos, lo que, al margen de acentuar la dependencia jurídica y la presión sicológica a los trabajadores, repercute negativamente en la efectividad de los derechos fundamentales constitucionalmente reconocidos a los trabajadores.

nuestra jurisprudencia incorpora la exigencia de una norma legal que habilite la injerencia -"una ley de singular precisión" (STC 49/1999, FJ 4)- y dispone que los Jueces y Tribunales podrán adoptar la medida sólo cuando concurran los presupuestos materiales pertinentes.

Pues bien, efectivamente la doctrina constitucional sobre uso de dispositivos electrónicos en la empresa se aparta de la doctrina general que protege la comunicación con independencia del medio utilizado y como un derecho autónomo de la intimidad. Desde la STC 114/1984, de 29 de noviembre, el TC sostiene que el bien jurídico protegido por el art. 18.3 CE es la libertad de las comunicaciones cualquiera que sea el sistema empleado para interceptarlas (FJ7). Desde esta primera sentencia de referencia y de forma reiterada, el TC ha incidido en la delimitación del ámbito del derecho al secreto de las comunicaciones (art. 18.3 CE) frente al ámbito del derecho a la intimidad (art. 18.1 CE)[65]. Lo protegido por el derecho garantizado en el art. 18.3 CE es el proceso de comunicación mismo frente a cualquier interferencia no consentida o judicialmente autorizada. Por lo demás y como se sabe, las garantías constitucionales que legitiman la intervención de las comunicaciones son, con carácter general, la existencia de previsión legal de la medida de intervención con suficiente previsión, la autorización judicial y la ejecución de la medida con estricta observancia del principio de proporcionalidad.

Por último, no puede dejar de señalarse que, a mi juicio, esta doctrina no se deduce directamente de la doctrina del TEDH en la Sentencia Barbulescu, al negar la existencia de una expectativa razonable de privacidad, en los casos de expresa prohibición de los usos privados de medios electrónicos empresariales.

Aunque ciertamente en la Sentencia BarBulescu se distingue entre el supuesto de hecho enjuiciado donde existía una prohibición uso personal y los resueltos por las Sentencias Copland o Halford donde existía tolerancia empresarial a los usos privados, la *ratio decidenci* de la Sentencia Barbulescu para negar la violación del art. 8.1 CEDH no fue la inexistencia de una expectativa razonable de privacidad, derivada de la prohibición expresa de uso personal de herramientas informáticas en la empresa. Por el contrario, para el TEDH si existió tal expectativa, por ello resultó aplicable el art. 8 CEDH, con independencia de que finalmente, en la decisión de fondo se declarara la no vulneración del art. 8 CEDH.

[65] Se garantiza la impenetrabilidad de la comunicación para terceros, públicos y privados, tanto en lo referido al contenido del mensaje como a la identidad de los interlocutores, y ello con independencia de que los datos pertenezcan o nó al ámbito de lo personal, íntimo o reservado pues el concepto de lo secreto tiene carácter formal y no material

En efecto, puede comprobarse que la sentencia Barbulescu, cuando analiza la admisibilidad y ante la alegación del Gobierno rumano de que no resulta aplicable el art. 8 del Convenio es cuando el TEDH se plantea la pregunta de "si, en el presente asunto, el demandante podía razonablemente esperar que sus comunicaciones serían privadas al usar la cuenta de Yahoo Messenger que creó a petición de su empleado", afirmando que está convencido de que estas medidas afectaron a la "vida privada" y "correspondencia" del demandante en el sentido del art. 8.1 CEDH, que es aplicable al presente asunto (ap. 45). Por lo que, pasando ya a analizando el fondo del asunto, concluye que no se ha producido violación alguna del artículo 8 del Convenio, pues no hay elemento alguno, en el presente asunto, que indique que las autoridades nacionales incumplieran su obligación de establecer un equilibrio adecuado, dentro de su margen de apreciación, entre los intereses del empleador y el derecho del demandante al respeto de su vida privada (ap. 63).

4.4. Aplicación de la doctrina del Tribunal Supremo y del Tribunal Constitucional

El control empresarial del uso por el trabajador de los medios tecnológicos ha sido analizado en sede judicial de forma unitaria, sin distinguir en virtud de los derechos fundamentales afectados y ello a pesar de que en el control del correo electrónico, el acceso a los mensajes no abiertos está protegido por el secreto de las comunicaciones ex art. 18.3 CE.

La doctrina de nuestros tribunales, en términos generales[66], aplica la doctrina antes vista sobre la inexistencia de lesión del derecho a la intimidad, no solo si la empresa tiene establecido un detallado, preciso, riguroso y bien perfilado protocolo de actuación en el uso del ordenador, del que el trabajador que lo usa tiene cabal y perfecto conocimiento[67], sino también si existe una prohibición absoluta sobre el uso de medios de la empresa para fines ajenos al trabajo[68].

[66] V. STSJ Cataluña, de 16/12/2016 (AS 2016\1921) en un supuesto de vulneración empresarial del derecho a la intimidad a través de un acceso unilateral al ordenador de la empresa, utilizado por el trabajador, constituyendo una extralimitación del poder de vigilancia y control del empresario. En esta sentencia se afirma 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 considerarse como una prohibición absoluta de utilización del ordenador y teléfono móvil entregado al trabajador por la empresa. STSJ Madrid, de 13/05/2016 (AS 2016\1166) si ha existido vulneración del derecho a la intimidad y al secreto de las comunicaciones en un supuesto de examen del disco duro del ordenador facilitado por la empresa con apertura y restauración en parte de un archivo temporal que condujo a una cuenta privada de correo electrónico del trabajador.

[67] STSJ Madrid, de 16/12/2013 (JUR 2014\19902) y en este mismo sentido, STSJ Cataluña, de 13/6/2016.

[68] STSJ País Vasco, de 29/09/2015 (AS 2015\1922).

En el ámbito de las redes sociales el control de las declaraciones de los trabajadores y legitimidad en la obtención de la prueba por parte del empresario se funda en el carácter no privado de estos medios[69].

4.5. Valoración de la doctrina constitucional y jurisprudencial

La doctrina constitucional y la jurisprudencia del TS que la precede, sobre uso de dispositivos electrónicos en la empresa no tutela, a mi juicio, suficientemente los derechos de los trabajadores, al desconocer una esfera legítima de privacidad y de libertad en las comunicaciones empresariales.

En definitiva, el razonamiento base de esta doctrina, "la prohibición empresarial de uso privado implica la inexistencia de una expectativa razonable de confidencialidad y la inexistencia de una expectativa razonable privacidad" situaría el uso de estos medios por el trabajador fuera del ámbito de protección de la libertad de comunicaciones y de su derecho a la privacidad en los centros de trabajo. Los trabajadores tendrán reconocido el derecho al secreto de las comunicaciones en la medida y en los términos que establezca el empresario[70]. Las comunicaciones cubiertas por el derecho al secreto del art. 18.3 CE se limitarían a aquellos supuestos de tolerancia empresarial del uso privado.

Esta doctrina creo que no se ajusta completamente a la doctrina europea, como antes señalé, y se fundamenta en el tradicional argumento de la titularidad empresarial de las herramientas informáticas, que es, a mi juicio, un débil argumento jurídico y en todo caso de incierto recorrido futuro[71]. Un argumento débil pues el correo electrónico, internet o el ordenador no son sólo instrumentos

[69] STSJ País Vasco de 26/10/2010, de STSJ Andalucía de 10/11/2011 y STSJ Madrid de 26/7/2016.

[70] Para determinar si se vulnera el art. 18.3 CE, habrá de estarse, afirma la STC 241/2012, a "las condiciones de puesta a disposición", pudiendo aseverarse que "la atribución de espacios individualizados o exclusivos puede tener relevancia desde el punto de vista de la actuación empresarial de control". Es el caso de "asignación de cuentas personales de correo electrónico" a los trabajadores, o incluso a las entidades sindicales, aspecto éste que fue abordado en nuestra STC 281/2005, de 7 de noviembre.

[71] La doctrina de los tribunales ha recaído fundamentalmente sobre el uso de los medios digitales iniciales como ordenadores fijos o portátiles email corporativo y navegación por internet. En los últimos años, las redes sociales de empresa o redes sociales corporativas y plataformas (como Yammer) son utilizadas como medios de comunicación entre la empresa y los empleados y que también pueden constituir formas de trabajar en grupos por proyectos. Los criterios sobre la utilización de estas redes sociales corporativas, las facultades de control empresarial y la afectación de los derechos de libre expresión e información de los trabajadores pueden precisar de nuevas respuestas pues los límites a tal uso serán más difíciles de articular dado que el trabajador accederá a tales plataformas o redes en muchas ocasiones a través de dispositivos particulares: V. V. AAVV., Nuevas Tecnologías y gestión de recursos humanos, Proyecto Technos: Impacto de las redes sociales y marco laboral tecnológico (Del Rey Guanter dir.), WolterKluwer, 2017.

de trabajo sino herramientas de comunicación y espacios, eso si no físicos sino virtuales, en los que el trabajador puede disponer, a mi juicio, de una esfera legítima de privacidad.

Además, la aplicación de esta doctrina sobre la expectativa razonable de confidencialidad[72] está determinando que entre nosotros, a diferencia de lo acontece en países vecinos, no puede afirmarse la existencia de un derecho del trabajador al uso personal de los medios tecnológicos puestos a su disposición. A falta de reconocimiento legal, si éste no se establece en convenio colectivo, será el poder empresarial el que determine su existencia y condiciones de ejercicio.

En definitiva y a pesar del reconocimiento constitucional de los derechos fundamentales de los trabajadores, son admisibles prohibiciones empresariales absolutas de desarrollo de los mismos. Afirmar que el trabajador es ciudadano de la empresa y que también desarrolla su vida personal en los lugares de trabajo conllevaría, a mi juicio, el derecho a ciertos usos privados no abusivos de tales medios de comunicación, siempre que no afecten a la productividad del trabajador ni causen perjuicio a la empresa. Es razonable pensar que evitar usos abusivos no es título suficiente para prohibir completamente todo o cualquier uso personal de los medios tecnológicos de comunicación. En fin, el desarrollo de la vida personal de los trabajadores no puede depender de la voluntad o tolerancia de la empresa, pues expresa un valor e interés de relevancia constitucional protegido a través del reconocimiento de derechos fundamentales en nuestro sistema constitucional.

[72] La aplicación del canon de la "expectativa razonable de confidencialidad", a diferencia del control de proporcionalidad, opera en el momento previo al análisis de fondo sobre la violación del derecho fundamental pues su inexistencia implica la inaplicación del derecho a la libertad de comunicaciones o del derecho a la privacidad.