Universidad Zaragoza
1542

Trabajo Fin de Grado

"Límites al control y vigilancia de las comunicaciones electrónicas de los trabajadores por parte del empresario"

Autor

Ana Isabel de Castro Lamarca

Director

Prof. Dra. Sara Alcázar Ortiz

Facultad de Derecho

Curso 2017/2018

ÍNDICE

ABREVIATURAS

CE: Constitución Española

CEDH: Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente

ET: Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores

NTIC: Nuevas tecnologías de la información y comunicación

TC: Tribunal Constitucional

TEDH: Tribunal Europeo de Derechos Humanos

TFG: Trabajo Fin de Grado

TS: Tribunal Supremo

I. INTRODUCCIÓN

En primer lugar, considero imprescindible delimitar adecuadamente el objeto en el que va a centrarse este Trabajo Fin de Grado (en adelante, TFG). Mi objetivo principal es analizar los límites al control y vigilancia de las comunicaciones electrónicas de los trabajadores por parte del empresario, los cuales han ido experimentados cambios con el paso de los años. Voy a internar recalcar la incuestionable presencia que tienen los derechos fundamentales dentro del puesto de trabajo, pues de lo contrario estaríamos llegando a un mundo laboral que atenta gravemente contra la dignidad de la persona.

En este TFG se va a tratar continuamente, a través del exhaustivo análisis de jurisprudencia, de resolver el conflictivo equilibrio existente entre dos intereses: por un lado, los derechos fundamentales que se manifiestan a través de comunicaciones electrónicas y, por otro, el poder de control y vigilancia empresarial de la actividad productiva.

Es preciso señalar que, para abordar este tema desde una visión adecuada, debemos ser plenamente conscientes de que, desde finales del siglo XX, las nuevas tecnologías de la información y comunicación (en adelante, NTIC) se han implantado y afianzado de una manera rápida y firme en el medio laboral, dando lugar a cambios no solo en el proceso de producción, sino también en las relaciones laborales entre empresarios y trabajadores.

Respecto a la razón de la elección de este tema, debo decir que mi inclinación por el derecho laboral se viene manifestando desde el segundo curso de la carrera, por lo que, el tema de mi TFG debía estar, indudablemente, dentro del área "Derecho del Trabajo y de la Seguridad Social".

En concreto, elegí el tema relativo a "los límites al control y vigilancia de las comunicaciones electrónicas de los trabajadores por parte del empresario" porque considero que es un tema de notoria actualidad judicial a raíz de que, el pasado 5 de septiembre de 2017, se diera a conocer a través de los medios de comunicación el caso Bârbulescu[1]. Además, buscaba un tema que no fuera meramente teórico, por lo que este tema me pareció muy apropiado, pues resulta indiscutible su aplicabilidad en los aspectos

[1] En el caso Bârbulescu hay que distinguir entre lo que se conoce como Bârbulescu I –STEDH 1/2016, de 12 de enero, Caso Bârbulescu contra Rumanía (TEDH 2016, 1)– y Bârbulescu II –STEDH (Gran Sala) 61/2017, de 5 de septiembre, Caso Bârbulescu contra Rumanía (TEDH 2017, 61)–.

cotidianos de nuestras relaciones laborales, inmersas en una sociedad profundamente tecnológica.

Para realizar el trabajo he recurrido al llamado método inductivo, es decir, he ido de lo particular a lo general. Así pues, he partido del análisis del concepto de poder de control y vigilancia como facultad empresarial y de sus límites, para continuar con la descripción de los derechos fundamentales con los que entra en conflicto, prestando especial atención al contenido esencial de los mismos. Concretamente, han sido objeto de análisis el derecho a la intimidad, el secreto de las comunicaciones y el derecho a la protección de datos de carácter personal. Estudiado todo lo anterior, me he adentrado en el análisis crítico de la doctrina de nuestros tribunales relativa al tema en cuestión a través de varios casos, para luego traspasar las fronteras nacionales y llegar al análisis de la doctrina del Tribunal Europeo de Derechos Humanos (en adelante, TEDH) sobre el caso Bârbulescu. A continuación, he puesto de manifiesto el inminente impacto de la sentencia Bârbulescu II en la doctrina sentada por nuestros tribunales –Tribunal Constitucional (en adelante, TC) y del Tribunal Supremo (en adelante, TS)–, puesto que va a suponer un giro radical respecto de lo que se venía defendiendo en los últimos años.

Finalmente, he plasmado mis conclusiones sobre el tema en cuestión, las cuales me han servido para darme cuenta de lo enriquecedor que ha sido para mi la realización de este trabajo, así como para cambiar radicalmente mi postura conforme iba empapándome de conocimiento sobre el controvertido tema.

Respecto a las fuentes utilizadas para la realización del TFG, primero recurrí a mi tutora, la doctora en Derecho Sara Alcázar. Ella me aconsejó la utilización del catálogo Roble. Además de seguir sus indicaciones, también extraje bibliografía de Dialnet. Tal y como se puede apreciar en los últimos apartados de este trabajo, la práctica totalidad de las fuentes utilizadas son libros y revistas, tan solo hay dos enlaces a páginas de internet –webgrafía–.

En el último apartado de este trabajo se recogen todas las sentencias mencionadas en el mismo, bien sea porque se ha hecho un exhaustivo análisis de las mismas o porque se han utilizado como un mero apoyo jurisprudencial en la redacción del trabajo. He considerado oportuno la inclusión de este anexo jurisprudencial, pues la doctrina sentada sobre este tema juega un papel imprescindible para su correcta comprensión.

II. PODER DE CONTROL Y VIGILANCIA SOBRE LA EJECUCIÓN DE LA PRESTACIÓN LABORAL

II.1 Poder de control y vigilancia como facultad del poder de dirección empresarial

Un trabajo sobre este tema tiene como premisa indispensable comenzar por el encuadramiento del poder de dirección empresarial para posteriormente dar una definición del mismo, así como de las facultades que lo integran.

Los dos puntos de referencia básicos en el encuadramiento del poder de dirección del empresario son: la relación jurídica de trabajo, derivada de un contrato de trabajo, y la organización de la empresa. Es este encuadramiento el que hace que nos encontremos con un poder peculiar, distinto al poder de tipo común y genérico. Como vemos, el poder de dirección del empresario encuentra su existencia en la relación laboral a través de la posición jerárquica de las partes en el marco de una empresa.

Una definición de este poder de dirección podría ser la dada por MONTOYA MELGAR[2], según el cual "el poder de dirección es el conjunto de facultades jurídicas a través de cuyo ejercicio el empresario dispone del trabajo realizado por su cuenta y a su riesgo, ordenando las singulares prestaciones laborales y organizando el trabajo de la empresa".

Delimitando el contenido del poder de dirección, tres grandes facultades lo integran. En primer lugar, la facultad de decidir cómo se va a organizar el trabajo (funciones decisorias); en segundo lugar, la facultad de organizar el trabajo a través de lo dictado previamente mediante órdenes e instrucciones (funciones ordenadoras); en tercer lugar, la facultad de comprobar y vigilar que ese trabajo está siendo realizado (funciones de control).

Esta última facultad aparece recogida en el artículo 20.3 del Estatuto de los Trabajadores (en adelante, ET): "el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".

En ciertos casos, esta facultad de vigilancia y control empresarial se traduce en una intromisión empresarial, la cual puede llegar a resultar lesiva de la esfera personal,

[2] MONTOYA MELGAR, A.: *El poder de dirección del empresario,* Instituto de Estudios Políticos, Madrid, 1965, p. 44.

llegando incluso a vulnerar los derechos inherentes al trabajador[3]. En este sentido, distinguimos cuatro tipos de actuaciones empresariales que suponen una entrada en la esfera privada y personal del trabajador. El primero serían las cuestiones directas formuladas al trabajador en la fase de contratación o en un momento posterior. El segundo bloque consistiría en el conocimiento de los informes médicos para garantizar que el trabajador cumple con su obligación de vigilancia de la salud, la cual es impuesta por la normativa de prevención de riesgos laborales[4]. El tercero –y en el que se va a basar este trabajo– guarda relación con la manera en la que el empresario controla el contenido de los medios informáticos puestos a disposición del trabajador, en especial el uso del ordenador y de las comunicaciones electrónicas. Por último, encontraríamos la contratación de un detective para el control de conductas extralaborales del trabajador[5].

II.2 Impacto de las nuevas tecnologías en el poder de supervisión empresarial

Desde finales del siglo XX, las NTIC se han implantado y afianzado de una manera rápida y firme en el medio laboral, dando lugar a cambios en el proceso de producción, así como en la relación entre trabajador y empresario. De hecho, algunos autores consideran que las NTIC han supuesto un antes y un después en el derecho del trabajo, dando lugar a una importante transformación del mismo[6].

En este sentido, es indiscutible la mejora que las NTIC suponen para la empresa en lo relativo a las necesidades productivas y organizativas de la misma, pero al mismo tiempo

[3] VALDES DAL-RÉ, F.: "Contrato de trabajo, derechos fundamentales de la persona del trabajador, y poderes empresariales: una difícil convivencia", *Relaciones Laborales,* núm. 2, 2003, p. 89-130.

[4] Según el artículo 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales: "1. El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad. En todo caso se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo. 2. Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud".

[5] RODRÍGUEZ CARDO, I. A.: *Poder de dirección empresarial y esfera personal del trabajador,* Consejo Económico y Social del Principado de Asturias, Oviedo, 2009, p. 49.

[6] SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCCONI, C.: *Nuevas Tecnologías y Relaciones Laborales,* Navarra, Aranzadi, 2012, p. 31.

conllevan un incremento del poder de control y vigilancia empresarial sobre el trabajador[7].

Esta intensificación del poder de supervisión empresarial se produce porque con las nuevas máquinas utilizadas como instrumentos de trabajo (ordenadores con acceso a internet, webcams, teléfonos móviles, ...) el control queda incorporado directamente en ellas, sometiendo al trabajador a una angosta vigilancia. Asimismo, los instrumentos de vigilancia que venía utilizado el empresario para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales han sufrido una fuerte tecnificación e informatización, lo que le permite al empresario fiscalizar muchos más elementos y de una forma más precisa y detallada.

A modo de ejemplo, en las empresas se ha pasado de un control y vigilancia a través de simples técnicas de reproducción de la imagen y sonido, o de ordenadores monitorizados a técnicas muy complejas como son la geolocalización o el control biométrico de los trabajadores.

Este nuevo poder de supervisión empresarial se traduce, en palabras de MERCADER UGUINA[8], en "un ojo electrónico penetrante, dominante y ubicuo" o, como diría TASCON LOPEZ[9], en "la profecía orwelliana del gran hermano adquiere dimensiones laborales".

Sin embargo, esta ingente supervisión que propician las NTIC y que dan lugar a un enérgico poder empresarial, no está siendo acompañada, en contra de lo que cabría pensar, de medidas flexibilizadoras de la situación de subordinación a la que se ve sometido el trabajador en su día a día. Diversos estudios[10] han inferido que los trabajadores que son objeto de una fuerte subordinación a través de la monitorización tienen más probabilidades de no aceptar puestos de responsabilidad por falta de motivación o iniciativa, así como de sentirse desconfiados por ver en gran medida mermada su privacidad.

[7] MONEREO PÉREZ, J. L. y LÓPEZ INSÚA, B.: "El control empresarial del correo electrónico tras la STC 170/2013", *Aranzadi Social*, núm. 11, 2014, p. 1.
[8] MERCADER UGUINA, J. R.: "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?, *Relaciones Laborales,* núm. 10, 2001, p. 14.
[9] TASCON LÓPEZ, R.: "El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica", *Aranzadi Social*, núm. 17, 2007, p. 2.
[10] En este sentido, GUDE FERNÁNDEZ, A.: "La videovigilancia laboral y el derecho a la protección de datos de carácter personal", *Revista de Derecho Político,* núm. 91, 2014, p. 46 y 47.

Con todo esto, nos enfrentamos a un problema que tiene, tal y como diría RODRIGUEZ ESCANCIANO[11], dos caras: "el control por la empresa del uso de las nuevas tecnologías por parte de los trabajadores y el recurso a los adelantos tecnológicos por la empresa para controlar a los trabajadores. En otras palabras, se trata de ver, de un lado, hasta qué punto puede el empresario fiscalizar la utilización de instrumentos tecnológicos por los trabajadores y, de otro, con qué limites puede valerse, a su vez, de los cauces técnicos para optimizar la vigilancia de la empresa".

III. LOS DERECHOS FUNDAMENTALES DEL TRABAJADOR COMO LÍMITE AL PODER DE CONTROL Y VIGILANCIA EMPRESARIAL DE LAS COMUNICACIONES ELECTRÓNICAS

III.1 Los derechos fundamentales del trabajador en el marco de las relaciones laborales.

En este apartado del trabajo debemos hacer referencia a una célebre afirmación que nos va a servir de guía a la hora de analizar el impacto de las NTIC en el ejercicio del poder de control y vigilancia empresarial, pero sin olvidar los límites que cabe imponer al mismo, sería la siguiente: "en el contrato, el trabajador pone a disposición del empresario la fuerza de su trabajo, pero no su persona"[12].

En el artículo 20 ET, tras indicar en el primer apartado que el trabajador está obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quién éste delegase, se señala, en el apartado tercero, que el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.

Haciendo una lectura detallada de este artículo vemos que además de adolecer de imprecisión, se muestra como un artículo desfasado al omitir por completo la implantación de las NTIC propias de las actuales formas de control empresarial.

Asimismo, no podemos hablar de una facultad de control empresarial que pueda ejecutarse con libertad absoluta, pues son dos los límites que se imponen en el mismo.

[11] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant lo Blanch, Valencia, 2015, p. 37.
[12] RIVERO, J.: "Les libertés publiques dans l'enterprise", *Droit Social*, núm. 5, 1982, p. 424.

Por un lado, el poder de control y vigilancia debe ceñirse a la supervisión de la ejecución de las prestaciones laborales previamente pactadas. Por otro lado, el medio empleado por el empresario para controlar y vigilar debe respetar ineludiblemente el derecho fundamental de la dignidad del trabajador reconocido en el artículo 10.1 de la Constitución Española[13] (en adelante, CE).

El propio TC[14] "obliga a reconocer a cualquier persona, independientemente de la situación en que se encuentre, aquellos derechos o contenidos de los mismos imprescindibles para garantizar la dignidad humana", erigiéndose la dignidad humana como un límite muy amplio.

En este sentido, vemos cómo el trabajador no es solo titular de derechos concretos inherentes a esa condición de trabajador que posee, tales como el derecho de libertad sindical o de huelga, sino que también es titular de los llamados derechos de la persona –derechos universales, indisponibles y reconocidos expresamente en la CE–. Estos derechos fundamentales no se refieren específicamente a aspectos laborales, pero como diría PALOMEQUE LÓPEZ[15] "se tiñen de laboralidad al ejercitarse en el ámbito de una relación de trabajo".

El hecho de que la CE reconozca la eficacia de los derechos del trabajador como persona sin condicionarla a la existencia de algún instrumento jurídico intermedio, proporciona la premisa principal de la que partir. Es decir, lo que se está haciendo es que tanto el empresario como el trabajador llevan a la relación de trabajo derechos que, aunque no están recogidos en la legislación laboral, tienen una eficacia en tal relación exenta de todo tipo de dudas.

El ámbito laboral resulta ser uno de los contextos en los que más se asegura el reflejo de estos derechos subjetivos en las relaciones de derecho privado. Es el propio TC[16] el que sostiene que "la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la CE le concede como ciudadano", de modo que "ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad, ni la libertad de empresa que establece el artículo 38

[13] Así se expresan FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V.: "Nuevas tecnologías y control empresarial de la actividad laboral en España", *Labour & Law Issues,* vol. 2, núm. 1, 2016, p. 10.
[14] STC 236/2007, de 7 de noviembre (RTC 2007, 236).
[15] PALOMEQUE LÓPEZ, M. C.: *Los derechos laborales en la Constitución Española*, Madrid, CEC, 1991, p. 31.
[16] STC 88/1985, de 19 de julio (RTC 1985, 88).

del texto constitucional legitima el que quienes prestan servicios en aquéllas por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico constitucional".

Con todo esto, resulta indiscutible que los derechos fundamentales del trabajador encuentran en la propia relación laboral que les une con el empresario tanto su ámbito de ejercicio como el respeto de los mismos. Además, atendiendo al tema al que este trabajo se refiere, estos derechos suponen un límite al ejercicio del poder de control empresarial y a la propia noción intrínseca de los mismos, al no poder ser entendidos de una forma absoluta.

III.2 Debilidad en el ejercicio de los derechos fundamentales como límite al poder de control y vigilancia empresarial

Una vez hemos llegado a la conclusión de que el reconocimiento de los derechos fundamentales del trabajador como persona no queda al margen de la relación laboral, lo cierto es que se aprecia cierta debilidad de estos derechos como límite al poder de vigilancia y control empresarial.

Esta debilidad a la que hacemos referencia se explica no solo por la propia realidad práctica, sino por la combinación de otros factores, como son la propia legislación, la autonomía colectiva a través de normas convencionales y las reflexiones doctrinales[17].

En primer lugar, en lo relativo a la propia legislación, en el ET encontramos una escasa referencia a los derechos fundamentales de trabajos como límite al poder de vigilancia y control del empresario. Concretamente, esta relación queda reducida al artículo 4 –el cual recoge entre los derechos del trabajador el de la no discriminación (4.2.c), la integridad física (4.2.d) y el respeto a su intimidad y dignidad (4.2.e)–, al artículo 17, que recalca nuevamente la no discriminación y a los artículos 18 y 20, donde se garantiza la dignidad del trabajador ante los registros[18].

[17] En este sentido se expresaba el profesor Javier Gárate Castro el pasado jueves 14 de diciembre en una conferencia impartida en la Facultad de Derecho de la Universidad de Zaragoza bajo el título "Control del empresario de las nuevas tecnologías".
[18] Un análisis exhaustivo en ROMÁN DE LA TORRE, M. D.: *Poder de dirección y contrato de trabajo,* Grapheus, Valladolid, 1992, p. 304.

Como vemos, nuestro ET se limita simplemente a invocar el precepto constitucional relativo a los derechos fundamentales correspondiente, haciendo visible la carencia de un conjunto de límites, así como de unas garantías y tutelas que hagan posible su ejercicio.

A diferencia de otras legislaciones europeas, el ET no sigue la línea del *Statuto dei Lavoratori* italiano de 1970, norma cuyo propósito elemental fue limitar los poderes empresariales, "no solo intentando una alteración de ellos en la fábrica, sino contribuyendo a crear un clima de respeto a la dignidad y libertad humana en los lugares de trabajo, reconduciendo el ejercicio de los poderes directivo y disciplinario a su justo lugar, esto es, en una estrecha finalización al desenvolvimiento de las actividades productivas". Podemos afirmar, tal y como diría VALDES DAL-RE[19], que "el Estatuto de los Trabajadores perdió una ocasión histórica de incorporar a nuestro sistema de relaciones laborales las experiencias y prácticas legislativas más modernas y progresistas".

En segundo lugar, la normativa convencional tampoco se ha dedicado a afianzar esta problemática. De hecho, ni los convenios colectivos han hecho nada para encuadrar los derechos fundamentales de los trabajadores en situaciones singulares del contrato de trabajo, ni los sindicatos han desarrollado programas sindicales específicos sobre los derechos fundamentales de los trabajadores. Sin embargo, los nuevos mecanismos de control y vigilancia empleados actualmente por las empresas sí que están dejando en evidencia la palpable necesidad de comenzar una línea de reflexión, negociación, control y actuación en este ámbito, tanto desde el punto de vista colectivo como sindical.

En tercer lugar, en lo que a la doctrina se refiere, no son abundantes los trabajos realizados relativos a los derechos fundamentales de los trabajadores con carácter general. Así pues, no sería necesario afirmar que esta escasez aún resulta más manifiesta si hablamos de trabajos sobre los derechos fundamentales del trabajador como límite al poder de vigilancia y control empresarial[20].

Por lo tanto, vemos que nuestros legisladores no están regulando esta situación, la norma estatal no regula esta situación. Son nuestros órganos judiciales, a través de las resoluciones judiciales, los que resuelven la problemática abierta entre los derechos fundamentales individuales del trabajador y el poder de vigilancia y control empresarial.

[19] VALDES DAL-RE, F.: "El Estatuto de los Trabajadores", *Argumentos*, 1980, p. 18.
[20] Por todos, ROMÁN DE LA TORRE, M. D.: *Poder de dirección*… cit., p. 304.

Estas resoluciones judiciales buscan alcanzar un punto de equilibrio donde los derechos fundamentales del trabajador jueguen como límite al poder de vigilancia y control, llegando a constituir el más abundante material para resolver esta controvertida cuestión. No obstante, debemos de advertir que esto resulta peligroso porque la función de los jueces es interpretar la ley, no crearla, ya que entre ellos hay criterios contradictorios, tal y como veremos en el capítulo IV de este trabajo.

III.3 Utilización de las comunicaciones electrónicas para fines extralaborales

El uso de las comunicaciones electrónicas, a través principalmente del correo electrónico, se ha erigido como una de las principales herramientas de comunicación en el ámbito de trabajo. Esta nueva herramienta de comunicación permite el contacto interno, es decir, el contacto del trabajador con el resto de personal de la empresa, así como el contacto externo, es decir, el contacto de la empresa con terceros ajenos a la misma.

Mediante el uso de las comunicaciones electrónicas, el trabajador está al corriente y puede visualizar la información que le llega en cualquier formato para, posteriormente, responderla, almacenarla e incluso reenviarla de manera instantánea.

En este sentido, la utilización de las comunicaciones electrónicas genera una serie de efectos positivos para la empresa. De un lado, facilita la comunicación dentro y fuera de la empresa pues ofrece al trabajador la posibilidad de transferir información de manera sencilla e instantánea. De otro lado, supone un incremento de la productividad laboral.

Ahora bien, un uso desmedido o alejado de esta herramienta da lugar a numerosos e importantes inconvenientes y perjuicios para la empresa. Con carácter general, se hace referencia al daño económico, también llamado lucro cesante, entendido este como las pérdidas económicas que sufre la empresa como consecuencia de un descenso del rendimiento de aquel trabajador que invierte tiempo delante de la pantalla del ordenador realizando actividades distintas de las relacionadas con la prestación laboral propiamente dicha.

Asimismo, en ocasiones este tipo de utilización de las comunicaciones electrónicas puede poner en peligro, no solo la confidencialidad de la empresa y la imagen de la misma, sino también la eficacia de los programas informáticos utilizados para transmitir información.

En definitiva, vemos que desde el punto de vista de la productividad son muchas las ventajas (posibilidad de reenviar, responder y adjuntar archivos en tiempo real y de manera sencilla, …), pero no pocos los inconvenientes. Por tanto, son estos

inconvenientes, estas conductas incorrectas por parte de los trabajadores que pueden suponer una transgresión de la buena fe contractual o un abuso de la confianza depositada en ellos, las que despiertan el empeño de vigilancia y control del empresario[21].

Es justo en este preciso momento cuando el poder de control y vigilancia de las comunicaciones electrónicas de los trabajadores por parte del empresario va a entrar en conflicto con algunos de los derechos fundamentales del trabajador: derecho a la intimidad, derecho al secreto de las comunicaciones y derecho a la protección de datos de carácter personal.

IV. DESCRIPCIÓN DE LOS DERECHOS EN CONFLICTO

En este apartado del trabajo vamos a analizar cada uno de los tres derechos fundamentales del trabajador que pueden entran en conflicto con el poder de control empresarial cuando se produce la interceptación de una comunicación electrónica llevada a cabo por el trabajador en el centro de trabajo en horario laboral. Es preciso delimitar muy detalladamente el contenido esencial de cada uno de estos derechos, para poder comprender las interpretaciones judiciales que se han hecho en relación a casos concretos.

En primer lugar, veremos dónde queda regulado cada uno de estos derechos para después determinar su contenido esencial.

IV.1 Contenido esencial del derecho a la intimidad

El derecho a la intimidad, derecho de personalidad con rango de derecho fundamental, queda constitucionalmente consagrado en el artículo 18.1 de la Carta Magna[22]. En desarrollo del precepto constitucional, la Ley Orgánica 1/1982, de 5 mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen enuncia en su artículo 7 lo que considera "intromisiones ilegítimas" y, en particular, el emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas; así como la captación, reproducción o publicación por fotografía, filme o

[21] RODRÍGUEZ ESCANCIANO, S.: *Poder de control…* cit., p. 13.

[22] Atendiendo al artículo 18.1 de la Carta Magna: "Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia".

cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2 del mismo texto legal. Ya en el plano laboral, el derecho a la intimidad encuentra reconocimiento en el artículo 4.2.e) ET, según el cual, el trabajador tiene derecho "al respeto de su intimidad y a la consideración debida a su dignidad en la relación de trabajo"[23].

En la actualidad, el contenido esencial del derecho a la intimidad ha adquirido una doble dimensión debido a la sociedad de la comunicación de la que somos partícipes. Por un lado, es una garantía contra la intromisión ilegítima en la esfera privada propia, es decir, constituye un status negativo frente a los demás. Por otro lado, se muestra como un status positivo pues otorga al ciudadano una potestad de control sobre el flujo de información relativo a su persona que accede al escenario público[24].

A efectos de este trabajo, nos vamos a centrar en esta segunda dimensión y, especialmente, en la incidencia sobre el derecho a la intimidad que la interceptación del correo electrónico provoca.

En este caso, el derecho a la intimidad solo será susceptible de ser lesionado si el contenido de la comunicación electrónica que ha sido interceptada incide sobre el ámbito de la vida privada del trabajador que era inaccesible a los demás. Es decir, el simple hecho de que un tercero (empresario) intercepte una comunicación electrónica de otro (trabajador) no tiene como resultado, de forma inexcusable, la lesión del derecho a la intimidad.

IV.2 Contenido esencial del secreto de las comunicaciones

Este derecho fundamental se encuentra recogido en el artículo 18.3 CE, según el cual "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

Analizando el contenido del artículo, hay una opinión generalizada dentro de la doctrina y que late en la jurisprudencia de nuestro TC, la cual entendería que, "aquellas comunicaciones que tienen lugar directamente entre personas a través de la palabra, el gesto o la expresión corporal no forman parte del contenido esencial de este derecho fundamental. Es decir, el elemento esencial que activa la protección constitucional del

[23] FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V.: "Nuevas tecnologías…", cit., p. 10.
[24] Un análisis exhaustivo en CARRILLO, M.: "Los ámbitos del derecho a la intimidad en la sociedad de la comunicación", en VV. AA (Asociación de Letrados del Tribunal Constitucional): *El derecho a la privacidad en un nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, p. 49.

secreto a las comunicaciones es la intervención de un tercero en el tránsito de la comunicación. Fuera, por tanto, de este estricto ámbito habremos de acudir a la protección que nos brindan otros preceptos de la CE, mas no su artículo 18.3"[25].

Como vemos, es necesario la existencia de algún medio para que entre a jugar el secreto de las comunicaciones. A efectos de este trabajo, nos vamos a centrar en los diversos tipos de comunicaciones que podemos encontrar a través de internet. Esto nos llevaría a distinguir entre comunicaciones abiertas y comunicaciones cerradas[26]. De un lado, las comunicaciones abiertas son aquellas que son accesibles para cualquier usuario de internet –por medio de chats, foros o medios de comunicación de masas–, las mismas no tienen la consideración de privadas y, por lo tanto, no están comprendidas dentro del ámbito de protección del derecho fundamental al secreto de las comunicaciones. De otro lado, las comunicaciones cerradas o confidenciales, ya sea una comunicación bidireccional cerrada entre dos personas –correo electrónico– o multidireccional cerrada con posibilidad de aceptar nuevos interlocutores –videoconferencia–, todas ellas activan las garantías del artículo 18.3 CE.

Una vez nos situamos dentro de comunicaciones cerradas o confidenciales, el derecho analizado es un derecho de carácter formal, pues no se dispensa el secreto en virtud del contenido de la comunicación, ni tiene nada que ver la protección del secreto con el hecho de que lo comunicado entre o no en el ámbito de la privacidad[27].

En conclusión, el bien constitucionalmente protegido o contenido esencial a través de la imposición a todos del secreto, es la libertad de las comunicaciones, siempre y cuando estas últimas sean a través de un medio y cerradas o confidenciales.

IV.3 Contenido esencial del derecho a la protección de datos de carácter personal

El derecho a la protección de datos aparece recogido en el artículo 18.4 CE, según el cual "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

---

[25] Por todos, RIVERO SÁNCHEZ-COVISA, F. J.: *Revisión del concepto constitucional del secreto de las comunicaciones*, Dykinson, Madrid, 2017, p. 11 - 31.

[26] En este sentido, PRECIADO DOMÈNECH, C. H.: *El Derecho de la Protección de Datos en el Contrato de Trabajo*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017, p. 142, nos remite a la Circular 1/2013 de la Fiscalía General del Estado, de 11 de enero de 2013. Esta Circular en su apartado 12, relativo a otras vías de comunicación a través de internet, hace referencia a los chats o foros, que permiten comunicarse a varias personales simultánea y públicamente, en tiempo real. En estos casos, cuando las conversaciones o comunicaciones son accesibles para cualquier usuario de internet, las mismas no pueden tener la consideración de privadas, sino de abiertas.

[27] STC 70/2002, de 3 de abril (RTC 2002, 70).

El contenido esencial de este derecho fundamental consta de tres derechos que funcionan como complementos indispensables unos de otros. En primer lugar, el derecho a consentir y el tratamiento, bien sea informático o no, de datos de carácter personal. Es decir, podríamos hablar de una facultad de consentir la recogida, la obtención y el acceso a los datos personales, así como su posterior almacenamiento y tratamiento, e incluso el uso o usos posibles, por un tercero, sea el Estado o un particular. En segundo lugar, el derecho a ser informado de quien está siendo poseedor de esos datos personales y para qué fin los está utilizando. Finalmente, el derecho a poder oponerse al responsable de poseer y usar esos datos personales exigiéndole el final de tales actuaciones[28].

Concretamente, en el ámbito laboral hay una relación muy estrecha entre el derecho fundamental a la protección de datos personales y el contrato de trabajo. Ya en la fase anterior al contrato se produce la selección de personal en la cual la empresa tiene acceso a los currículos de los candidatos, en los cuales aparece información personal de los postulantes. Más adelante, en la fase de contratación propiamente dicha tiene lugar el clausulado contractual y las disposiciones convencionales. Durante la ejecución del contrato, tiene especial relevancia el control empresarial de la prestación laboral a través de las NTIC. Por último, en la fase de extinción de la relación laboral, por ejemplo, mediante la previa obtención de pruebas, la empresa también tiene acceso a datos personales.

A efectos de este trabajo, nos vamos a centrar en el contenido esencial del derecho a la protección de datos personales como límite al poder de control y vigilancia empresarial. Es cierto, que en virtud del artículo 6.2 de la Ley Orgánica de Protección de Datos[29] y el artículo 20.3 ET, el empresario puede recabar datos sin necesidad de consentimiento. Ahora bien, el TC[30] ha venido afirmando que el derecho de información opera aun cuando no esté presente el requisito del consentimiento, pues resulta evidente 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.

Básicamente lo que viene haciendo el TC con sus resoluciones es facultar al empresario para que ejerza su poder de control y vigilancia de la prestación laboral, pero

[28] PRECIADO DOMÈNECH, C. H.: *El Derecho de la Protección …* cit., p. 142.
[29] Atendiendo al contenido del artículo 6 en su apartado 1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".
[30] STC 29/2013, de 11 de febrero (RTC 2013, 29).

garantizando en todo momento la debida información previa al trabajador, en tanto que, tal y como acabamos de ver, el derecho a la información previa es contenido esencial del derecho fundamental analizado en este apartado.

V. ANÁLISIS CRÍTICO DE LA DOCTRINA DE NUESTROS TRIBUNALES

V.1 Doctrina del Tribunal Constitucional

Nuestra jurisprudencia constitucional, a lo largo de los años, ha venido resolviendo los conflictos laborales resultantes de la profunda implantación de las NTIC en el ámbito laboral.

En concreto, en el siguiente apartado nos centraremos en la doctrina del TC sobre el control empresarial del uso por los trabajadores del correo electrónico, fundamentalmente en la STC 241/2012, de 17 de diciembre[31] y la STC 170/2013, de 7 de octubre[32].

Analizaré en primer lugar los contenidos argumentales de las citadas resoluciones para, posteriormente, destacar los aspectos comunes de tales pronunciamientos y, finalmente, proceder a realizar una crítica personal de la doctrina constitucional establecida hasta nuestros días en este ámbito.

Respecto a la primera de las sentencias (STC 241/2012), podríamos resumir los antecedentes de hecho de la siguiente manera: en una empresa existía un ordenador cuyo uso era indistinto por los empleados y sin ninguna clave de acceso. Dos trabajadoras instalaron, desobedeciendo una prohibición expresa de la empresa, el programa *Trillian* de mensajería instantánea, con el que llevaron a cabo, entre ellas y durante la jornada de trabajo sin cautela alguna que impidiese el archivo de los mensajes en el disco duro y su posterior lectura por cualquier usuario de éste, diversas conversaciones en las que se vertían "comentarios críticos, despectivos o insultantes en relación con compañeros del trabajo, superiores y clientes". Además, ninguna de las dos trabajadoras procedió al borrado de la información que había quedado almacenada, habiendo podido hacerlo. Tales conversaciones fueron descubiertas por casualidad por otro trabajador, el cual informó de ello a la empresa. El descubrimiento de esta instalación fue acompañado de la apertura de las carpetas para, posteriormente, convocar a ambas trabajadoras a una reunión en la que se les leyó el contenido de algunas conversaciones, resumiéndose el de

[31] STC 241/2012, de 17 de diciembre (RTC 2012, 241).
[32] STC 170/2013, de 7 de octubre (RTC 2013, 170).

las restantes con el propósito de comprobar tanto la finalidad y el uso como la autoría de las dos trabajadoras.

Ambas empleadas presentaron demanda ante la jurisdicción social, que concluyó con la desestimación de la misma. Una de las trabajadoras, promovió recurso de amparo ante el TC alegando que se había lesionado su derecho a la intimidad y el derecho al secreto de las comunicaciones, si bien, la respuesta del TC fue desestimatoria.

En primer lugar, el TC descarta la vulneración del derecho a la intimidad de la denunciante, pues considera que fueron las propias trabajadoras las que eliminaron la privacidad de sus conversaciones al llevar a cabo tales actos dispositivos[33].

En segundo lugar, el referido ordenador de empleo común, con el que cualquiera puede acceder al contenido de los mensajes que en él queden guardados, así como la prohibición expresa por parte de la empresa a los trabajadores de instalar de programas en dicho ordenador de uso común, impiden al TC apreciar vulneración alguna del derecho al secreto de las comunicaciones[34].

Si bien, en esta resolución hay un voto particular. El voto particular entiende que los factores considerados por el TC –accesibilidad de los mensajes y prohibición empresarial de instalar programas– para negar la violación del derecho al secreto de las comunicaciones no guardan relación con el contenido esencial de dicho derecho. De un lado, afirma el voto particular que "nadie está autorizado a abrir los archivos de correo electrónico o de mensajería de otro, siempre que puedan ser identificados como tales, como era el caso, por más que el acceso sea posible al encontrarse los archivos desprotegidos y en un ordenador de uso común" (apartado 6). De otro lado, el voto particular –haciendo uso de doctrina del propio TC[35]– considera que "el incumplimiento de las órdenes empresariales es susceptible de sanción empresarial, pero en ningún caso puede servir de justificación para entrar en la esfera personal del trabajador y llegar a lesionar algunos de sus derechos fundamentales" (apartado 4).

---

[33] El FJ 3 de la citada sentencia señala: "Por tanto, fueron la demandante de amparo y la otra trabajadora, con sus propios actos, provocaron con su voluntaria actuación que no se pudieran apreciar afectado su derecho a la intimidad al posibilitar su conocimiento de sus conversaciones por otro usuario del ordenador, que casualmente y sin ninguna intencionalidad tuvo acceso a todo su contenido, lo que finalmente provocó la intervención empresarial".

[34] El FJ 7 de la referida sentencia: "(…) estamos ante comunicaciones entre dos trabajadoras que se produjeron al introducirse el programa en un soporte de uso común para todos los trabajadores de la empresa sin ningún tipo de cautela. En este sentido, quedan fuera de la protección constitucional por tratarse de formas de envío que se configuran legalmente como comunicación abierta, esto es, no secreta".

[35] Por todas, STC 41/2006, de 13 de febrero (RTC 2006, 41).

Pasando a la segunda sentencia en cuestión (STC 170/2013), los antecedentes de hecho pueden sintetizarse de la siguiente manera: el recurrente fue despedido por la empresa tras comprobar que había proporcionado información confidencial a otra empresa a través de los medios electrónicos propiedad de la empresa, pero puestos a su disposición. Concretamente, a través del correo electrónico y del teléfono móvil. Se debe señalar que, con anterioridad al envío de la carta de despido al trabajador, tanto el ordenador como el teléfono móvil fueron entregados a un notario. Entregada la carta de despido y ante la presencia del trabajador, se realizó una copia del disco duro del ordenador.

En este segundo caso, el recurrente en amparo alega que se ha vulnerado su derecho a la intimidad, así como al secreto de las comunicaciones. Al igual que en el supuesto anterior, el TC desestima el recurso.

En primer lugar y en relación con el derecho a la intimidad, el TC considera que no ha sido vulnerado. El convenio colectivo de la empresa recoge como infracción leve el uso personal de los medios informáticos, lo que, según el TC, se traduce en una prohibición del uso extralaboral de los medios informáticos propiedad de la empresa, facultando a la empresa para el control de su utilización al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Por lo tanto, siguiendo este razonamiento, el trabajador no cuenta con la existencia de una expectativa razonable de privacidad o confidencialidad en el momento que hace un uso extralaboral del correo electrónico[36].

En segundo lugar, es esta misma prohibición y las facultades de control que lleva implícitas, la que hace que no se haya producido una lesión del derecho al secreto de las comunicaciones. El canal empleado por el trabajador se ha convertido -en virtud de un convenio colectivo- en un medio abierto, mientras que el contenido esencial del artículo 18.3 CE solo protege las comunicaciones cerradas.

Finalmente, la STC 170/2013 somete la decisión empresarial al test de proporcionalidad, llegando a la conclusión de que la misma es justificada, idónea, necesaria y ponderada, superando, por tanto, dicho test[37].

[36] En este sentido la resolución hace suya la misma argumentación manejada por la STC 241/2012 para desestimar la violación del derecho a la intimidad.

[37] El FJ 5.c de la sentencia señalada establece: "Se trataba en primer lugar de una medida justificada, puesto que, conforme consta en la sentencia de instancia, su práctica se fundó en la existencia de sospechas de un comportamiento irregular del trabajador. En segundo término, la medida era idónea para la finalidad pretendida por la empresa, consistente en verificar si el trabajador cometía efectivamente la irregularidad

Una vez analizados los argumentos de cada una de las decisiones por separado, vamos a proceder a destacar aquellos aspectos que resultan comunes a ambas resoluciones.

Por un lado, los dos procedimientos entran a resolver sendos recursos de amparo donde los respectivos recurrentes alegaron la vulneración del derecho a la intimidad (artículo 18.1 CE) y del secreto a las comunicaciones (artículo 18.3 CE). Además, en ambas resoluciones se desestimaron las lesiones de los derechos fundamentales alegados.

Por otro lado, y, entrando en el fondo de las decisiones judiciales, tanto la STC 241/2012 como la STC 170/2013 parten de la premisa de que el mero incumplimiento por el trabajador de una orden empresarial[38] tiene como inmediata consecuencia la desaparición de la expectativa de confidencialidad y privacidad a favor del trabajador y, por tanto, el trabajador no puede entender vulnerados sus derechos fundamentales del artículo 18 CE, en sus apartados 1 y 3.

Una vez estudiadas estas resoluciones, me gustaría mostrar una posición crítica respecto a esta línea jurisprudencial que, de momento, se mantiene como opinión mayoritaria dentro de nuestro TC.

Si recordamos el contenido esencial del artículo 18.3 CE es la libertad de las comunicaciones –comunicaciones que deben ser cerradas, como por ejemplo el correo electrónico–, por lo que cualquier intromisión o conocimiento antijurídico de las mismas supone una vulneración de este derecho fundamental. En palabras de VALDÉS DAL-RÉ [39], "el acceso a los mensajes del correo electrónico produce el mismo efecto lesivo para ese derecho fundamental que la apertura de una carta". En definitiva, no se puede hacer

---

sospechada: la revelación a terceros de datos empresariales de reserva obligada; al objeto de adoptar las medidas disciplinarias correspondientes. En tercer lugar, la medida podía considerarse necesaria, dado que, como instrumento de transmisión de dicha información confidencial, el contenido o texto de los correos electrónicos serviría de prueba de la citada irregularidad ante la eventual impugnación judicial de la sanción empresarial; no era pues suficiente a tal fin el mero acceso a otros elementos de la comunicación como la identificación del remitente o destinatario, que por sí solos no permitían acreditar el ilícito indicado. Finalmente, la medida podía entenderse como ponderada y equilibrada; al margen de las garantías con que se realizó el control empresarial a través de la intervención de perito informático y notario, ha de partirse de que la controversia a dirimir en este recurso se ciñe a los correos electrónicos aportados por la empresa como prueba en el proceso de despido que fueron valorados en su decisión por la resolución judicial impugnada: en concreto, los relativos a datos sobre la cosecha de 2007 y 2008".

[38] En la STC 241/2012 esta ausencia venía motivada por dos factores: el carácter abierto del ordenador, calificado de uso común, y la expresa prohibición acordada por la empresa de instalar programas. En la STC 170/2013 la inexistencia se hizo derivar no ya de una prohibición expresa, sino de una simple calificación por el convenio colectivo aplicable como infracción leve del "uso personal de los medios informáticos".

[39] VALDÉS DAL-RÉ, F.: "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", *Revista de Derecho Social*, núm. 79, 2017, p. 33.

depender el secreto de las comunicaciones de que el medio en cuestión sea propiedad de la empresa y deje o no rastro informático de las conversaciones llevadas a cabo a través de él, pues en la mayoría de los casos ni siquiera los propios comunicantes tienen ese conocimiento.

Es cierto que, cuando existen indicios fundados de la comisión de un delito y siempre que se cuente con la debida autorización judicial, el derecho al secreto de las comunicaciones puede verse relegado a un segundo plano. En mi opinión, esta autorización judicial debería extenderse al ámbito laboral porque de otro modo nos estamos enfrentando a decisiones judiciales, como las ahora analizadas, donde basta con la mera sospecha de que el trabajador no estaba desempeñando adecuadamente la prestación laboral, por ejemplo, porque estaba facilitando información confidencial a una empresa competidora para justificar la lesión artículo 18.3 CE.

Debemos destacar también que en la sentencia 241/2012, el TC debería de haber entrado a valorar de una manera más detallada la posible lesión del derecho a la intimidad (artículo 18.1 CE). Se me hace difícil imaginar, dado el tipo de conversaciones que se vertieron a través de ese programa entre dos compañeras, que la empresa no hubiera tenido conocimiento de aspectos de la vida privada de las trabajadoras, los cuales eran inaccesibles a los demás.

Por último, considero que en la sanción laboral deben terminar las facultades del empresario, es decir, bajo ningún concepto estas facultades pueden suponer una lesión de los derechos fundamentales del trabajador en el ámbito de una relación laboral.

V.2 Doctrina del Tribunal Supremo

En la doctrina del TS podemos distinguir claramente dos posturas en relación con los límites al control empresarial de las comunicaciones electrónicas de los trabajadores[40].

El punto de inflexión en la jurisprudencia del TS lo encontramos en la STS 2011/7699, de 6 de octubre[41], la cual supone un retroceso en la protección del derecho a la intimidad del trabajador, según venía siendo interpretada por la jurisprudencia del TS en sentencias como la STS 2011/932, de 8 de marzo[42] y STS 2007/7514, de 26 septiembre[43].

[40] PRECIADO DOMÈNECH, C. H.: *El Derecho de la Protección…*, cit., p. 256.
[41] STS 2011/7699, de 6 de octubre (RJ 2011, 7699).
[42] STS 2011/932, de 8 de marzo (RJ 2011, 932).
[43] STS 7514/2007, de 26 septiembre (RJ 2007, 7514).

En la STS 2011/932, de 8 de marzo, se procede al despido de un directivo tras haber sido comprobado por la empresa la presencia de antiguos accesos a páginas pornográficas desde el ordenador del citado trabajador. Se debe señalar que el ordenador estaba en un despacho sin llave, no tenía clave de acceso alguna y estaba conectado a la red de la empresa.

En esta importante sentencia se considera que tal actuación ha constituido una lesión del derecho a la intimidad del trabajador. En sus fundamentos jurídicos, la doctrina que emana es, en primer lugar, la consistente en delimitar el ámbito normativo de aplicación. Así pues, afirma que el poder de control y vigilancia del uso del ordenador puesto a disposición del trabajador por el empresario no encuentra su regulación en el artículo 18 ET[44], sino en el ya analizado artículo 20.3 ET.

Añade la sentencia en su FJ 4 dos precisiones. Por un lado, tanto los archivos personales del trabajador como el historial de navegación por internet que se hallen en el ordenador están incluidos dentro del contenido esencial que protege el derecho a la intimidad y el secreto de las comunicaciones. Por otro lado, existe un hábito social generalizado de tolerancia de ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores, creándose una expectativa de confidencialidad en esos usos a favor de los trabajadores.

De este modo, si la empresa quisiera destruir esa expectativa de confidencialidad y controlar plenamente el uso del ordenador por parte del trabajador, debería –atendiendo al tenor literal del FJ 4 de la citada sentencia– "establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que va 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, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones".

[44] Según el artículo 18, relativo a la inviolabilidad de la persona del trabajador: "Solo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible".

Por tanto, en aquellos casos en los que, a pesar de cumplirse tales exigencias, el trabajador utilice el ordenador para usos privativos, vulnerando las prohibiciones impuestas por la empresa, el control que esta última realice no lesionará esa expectativa de confidencialidad creada a favor del trabajador.

Esta doctrina que acabamos de exponer es seguida por otras sentencias posteriores como la citada STS 2011/932, de 8 de marzo. En esta sentencia se trata de enjuiciar nuevamente un despido producido tras comprobar la empresa, a través de una auditoria informática, que uno de sus trabajadores había realizado un total de 5.566 visitas a páginas web (multimedia-vídeos, piratería informática, anuncios, televisión, contactos, …) durante los turnos de trabajo.

Pues bien, en esta sentencia se declara la nulidad de la prueba obtenida a través de esa auditoría informática porque considera que tal prueba se había conseguido de una manera ilícita al no respetarse las exigencias fijadas en la STS 2007/7514, de 26 septiembre para destruir la "expectativa razonable de intimidad" por parte del empresario.

En el mes de octubre del año 2011, como ya hemos advertido anteriormente, se produce un giro doctrinal. Concretamente, este retroceso en la tutela de los derechos fundamentales se produce con la STS 2011/7699, de 6 de octubre. En este caso, la empresa comunicó a todos sus trabajadores la prohibición del uso particular de los ordenadores y demás medios puestos a su disposición. Además, se procedió a monitorizar a dos trabajadoras, las cuales habían desarrollado un bajo rendimiento en los últimos meses, dando como resultado el despido de la recurrente cuyas visitas a internet habían sido continuas durante su jornada de trabajo.

A la vista de los anteriores hechos, el TS en su FJ 4 considera que en el momento en el que la empresa impuso una prohibición del uso del ordenador para fines particulares, desapareció el derecho de la trabajadora para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones. En otras palabras, el TS afirmó que, si no existía una situación de tolerancia del uso personal, por ende, tampoco existía ninguna expectativa razonable de intimidad a favor de la trabajadora despedida. Además, la doctrina del TS sentada en esta sentencia afirma que cuando un trabajador hace un uso personal del ordenador –uso ilícito–, resulta inadmisible exigir al empresario que, además de soportarlo, deba abstenerse de controlarlo.

De este modo, la STS 2011/7699, de 6 de octubre no considera vulnerados el derecho a la intimidad ni al secreto de las comunicaciones de la recurrente, si bien, hay un voto particular que afirma que, en la medida en que el control empresarial ha sido realizado sin advertir previamente de los controles y medidas aplicables, esa "expectativa razonable de intimidad" con la que cuenta el trabajador ha resultado dañada. Es decir, el voto particular entiende que tal prohibición empresarial debe ir, en todo caso, acompañada de información clara, previa y expresa sobre la existencia de un control, así como de los concretos medios que van a emplearse. Concluye diciendo que en ningún caso resulta suficiente ni proporcionada la simple prohibición del uso del ordenador para fines particulares.

Con todo esto, podemos hablar de un TS que ha pasado de mostrar una cierta sensibilidad hacía el hábito de un uso adecuado y racional de los medios proporcionados por la empresa para fines particulares –lo cual conlleva una expectativa razonable de confidencialidad cuya única manera de ser destruida es a través de una advertencia clara, previa y expresa–, a un TS que, en cierto modo, parece otorgar una posición privilegiada al empresario en las relaciones laborales pues ahora basta con una simple prohibición empresarial del uso del ordenador para fines particulares para que la expectativa de confidencialidad y privacidad a favor del trabajador –en caso de usar el ordenador para fines personales– quede destruida y, por tanto, no puede entender vulnerados sus derechos fundamentales del artículo 18 CE, en sus apartados 1 y 3.

En mi opinión, en apenas cuatro años la doctrina del TS ha olvidado, o más bien ha querido olvidar, que tanto el empresario como el trabajador llevan a la relación laboral derechos que, aunque no están recogidos en la legislación laboral, tienen una eficacia en la prestación laboral incuestionable.

Sin embargo, es necesario tener en cuenta el recurso de casación resuelto por el TS el pasado 8 de febrero de 2018, con el fin principal de unificar la doctrina[45]. En este recurso se analiza nuevamente la licitud del acceso al correo electrónico de un trabajador por parte de su empleador, así como su posterior utilización como prueba para fundar el despido disciplinario.

[45] STS 119/2018, de 8 de febrero (RJ 2018/666).

En este caso, el TS[46] presta especial atención al hecho de que la empresa contaba con una política interna, la cual limitaba el uso de los medios informáticos –especialmente el correo electrónico– únicamente para fines profesionales y prohibía su utilización para cuestiones personales. Asimismo, el TS señala que en las normas internas de la empresa ya se advertía, de una manera suficientemente clara, de la facultad que disponía la empresa para supervisar o monitorizar la utilización de los medios informáticos por los trabajadores, así como del hecho de que el propio trabajador debía conocer de esas normas y las aceptada diariamente cuando accedía a su ordenador. Además, a la hora de revisar los correos electrónicos del demandante, la empresa no lo hizo de un modo genérico, sino que utilizó palabras clave, las cuales le permitieran encontrar aquellos correos que contenían información relevante para la investigación.

Como consecuencia de todo lo anterior, el TS considera que el control llevado a cabo por la empresa ha superado los juicios de idoneidad, necesidad y proporcionalidad, así como el filtro de los requisitos del TEDH en el caso Bârbulescu[47], ya que el control del correo electrónico del trabajador fue realizado a través de un medio idóneo y necesario dadas las circunstancias concretas del caso. El TS concluye afirmando que el despido es procedente y no se ha vulnerado ningún derecho fundamental del trabajador.

En mi opinión, lo que hace el TS en esta reciente sentencia es corroborar la pérdida de esa expectativa razonable de intimidad del trabajador cuando el empleador cuenta con una organizada y adecuada política interna de control de los medios informáticos puestos a disposición del trabajador.

[46] El FJ 5 de la analizada sentencia nos muestra con gran exhaustividad la argumentación seguida por el TS en este reciente caso.

[47] El FJ 6 de la citada sentencia se refiere a la doctrina Bârbulescu. Esta doctrina Bârbulescu, será analizada de manera detallada en el apartado VI.1 del presente trabajo. Sin embargo, debido a que en este apartado se estudiaba la doctrina del TS he considerado que era de vital importancia entrar a valorar esta reciente sentencia del TS donde "aunque por razones temporales en el presente procedimiento no se pudo tener en cuenta hasta la fecha la STEDH -Gran Sala- 05/Septiembre/2017 [Caso "Bârbulescu"], parece conveniente que nos refiramos a tan reciente doctrina, no sólo para evidenciar que sus criterios son sustancialmente coincidentes con los de la jurisprudencia constitucional (…), sino también que -precisamente por ello- la conducta empresarial de autos pasa holgadamente el filtro de los requisitos que el Alto Tribunal europeo exige para atribuir legitimidad a la actividad de control que acabamos de enjuiciar".

VI. LA DOCTRINA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

VI.1 Caso concreto: Bârbulescu contra Rumanía

Una vez hemos analizado la doctrina de los tribunales españoles en lo que se refiere a los límites al control y vigilancia de las comunicaciones electrónicas de los trabajadores por parte del empresario, en este apartado vamos a adentrarnos en el estudio de la doctrina del TEDH acerca del tema en cuestión, y lo haremos a través del importantísimo caso Bârbulescu[48].

En el caso Bârbulescu, se va a debatir sobre el presunto incumplimiento por parte del gobierno de Rumanía del artículo 8 del Convenio Europeo de Derechos Humanos (en adelante, CEDH), el cual reconoce –en su apartado primero– el derecho que toda persona tiene al respeto de su vida privada y familiar, de su domicilio y de su correspondencia, y dispone –en su apartado segundo– que, " no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por 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 la libertades de los demás".

Concretamente, el caso Bârbulescu del que va a conocer el TEDH encuentra su origen en el despido de un trabajador, el cual, a petición de su empresa, creó una cuenta de Yahoo Messenger con el fin de recibir y responder a preguntas de los clientes. El 1 de agosto de 2007 la empresa procedió al despido del trabajador. La empresa alegaba que se habían vulnerado las normas internas de la empresa, las cuales prohibían el uso de recursos tecnológicos puestos a disposición del trabajador por parte del empleador para usos o fines personales, tras haber vigilado las comunicaciones electrónicas del trabajador vía Yahoo y haber comprobado que este había intercambiado mensajes que guardaban relación con su vida privada con su hermano y su novia.

El demandante, en instancia, impugnó la decisión de la empresa ante el Tribunal del Condado de Bucarest por vulneración de la Constitución y del Código Penal Rumano,

[48] En el caso Bârbulescu hay que distinguir entre lo que se conoce como Bârbulescu I – STEDH 1/2016, de 12 de enero, Caso Bârbulescu contra Rumanía (TEDH 2016, 1)– y Bârbulescu II –STEDH (Gran Sala) 61/2017, de 5 de septiembre, Caso Bârbulescu contra Rumanía (TEDH 2017, 61)–.

argumentado que se había vulnerado el derecho a la privacidad de la correspondencia. Sin embargo, el Tribunal del Condado desestimó la queja, estimando que la empresa había cumplido con el procedimiento de despido establecido por el Código del Trabajo, y observó –más correcto sería decir que "pareció observar"– que el demandante había sido debidamente informado de las normas de la empresa que prohibían el uso de recursos internos de ésta con fines personales.

En fase de recurso, el trabajador –principalmente– alegó la vulneración del artículo 8 del CEDH. Si bien, el Tribunal de Apelación de Bucarest desestimó tal recurso[49]. Ante tal decisión, el Señor Bârbulescu planteó un recurso ante el TEDH, el cual fue declarado admisible ante las dudas jurídicas que se venían planteando sobre si la actuación de la empresa había sido proporcionada y razonable.

Básicamente, lo que se tenía que esclarecer era si el recurrente tenía –o no– unas expectativas razonables de que sus conversaciones no iban a ser controladas o monitorizadas y, por ende, tal situación estaba –o no– bajo la protección del artículo 8 CEDH.

El litigio se centra en la obligación de respeto de los derechos contenidos en el artículo 8 CEDH por parte de los gobiernos nacionales, es decir, de combinar de un modo adecuado, por una parte, la protección del derecho a la vida privada y a la correspondencia del trabajador y, por otro lado, el interés empresarial de vigilancia y control del correcto desarrollo de la actividad laboral por parte de sus empleados.

Puestas de manifiesto las circunstancias del caso Bârbulescu, en los siguientes apartados se analizará la doctrina seguida por el TEDH en Bârbulescu I para, posteriormente, analizar el giro doctrinal defendido por la Gran Sala del TEDH en Bârbulescu II.

VI.1.1 Bârbulescu I

En Bârbulescu I, el TEDH con carácter previo a entrar en el fondo del asunto analiza tanto la normativa interna como internacional aplicable al caso concreto. De un lado, en lo que a la normativa internacional se refiere, la Constitución rumana consagra el derecho a la protección de la vida íntima, privada y familiar, así como al respeto de la

[49] La argumentación del Tribunal de Apelación de Bucarest queda recogida en el apartado 12 de la STEDH 1/2016, de 12 enero (TEDH 2016, 1). De este modo, invocando la Directiva de la Unión Europea Núm. 95/46/EC (LCEur 1995, 2977), el Tribunal de Apelación estimó que el comportamiento de la empresa empleadora había sido razonable y que vigilar las comunicaciones del demandante era la única manera de determinar si había incumplido las normas disciplinarias.

correspondencia privada[50]. Además, el Código Penal rumano[51] impone penas de prisión de entre seis meses y tres años para aquel que acceda de forma ilegal o intercepte correspondencia privada de otra persona. En el ámbito jurídico laboral, el Código de Trabajo[52] vigente en el momento de los hechos disponía que la dirección de la empresa tenía el derecho de controlar la manera en la que los empleados llevaban a cabo sus tareas profesionales, pero también tenía la obligación de garantizar la confidencialidad de los datos personales de sus empleados. De otro lado, en lo relativo a la normativa internacional, se hace referencia a la Directiva de la Unión Europea 95/46/EC (LCEur 1995, 2977) y al Convenio del Consejo de Europa de 1981 (LCEur 1981,362).

Entrando en el fondo del asunto, el TEDH se encuentra con dos cuestiones de gran relevancia jurídica, las cuales debe resolver. En primer lugar, el TEDH entra a decidir si es o no conforme a derecho que el empresario pueda acceder a la cuenta del trabajador con el objetivo de descubrir pruebas que corroboren la desconfianza que pudiera tener sobre un correcto desempeño de la actividad laboral por parte del trabajador. Pues bien, el TEDH[53] no entiende abusivo, sino que entraría dentro del poder de control y vigilancia empresarial, que el empleador desee controlar el correcto cumplimiento de la prestación laboral por parte de un trabajador accediendo a la cuenta profesional –Yahoo Messenger– del empleado con la certeza de que solo incluía información de carácter profesional, la cual era la que deseaba controlar. Es decir, el TEDH considera que ante una cuenta de carácter profesional, la expectativa de privacidad del trabajador desaparece y, por tanto, no es de aplicación el artículo 8 CEDH. En segundo lugar, el TEDH entra a valorar si la normativa interna de la empresa sobre la prohibición del correo para uso personal era o no conocida plenamente por el trabajador. A pesar de que, con la información disponible,

[50] Concretamente, es el artículo 26 de la citada Constitución donde se recoge el derecho a la protección de la vida íntima, privada y familiar, mientras que el respeto de la correspondencia privada queda recogido en el artículo 28.

[51] En este sentido, es el artículo 195 del Código Penal rumano el que recoge este tipo delictivo. Concretamente, en el apartado 14 de la analizada sentencia se cita el tenor literal de dicho artículo disponiendo lo siguiente: "Todo individuo que abra ilegítimamente la correspondencia de otra persona o intercepte sus conversaciones o comunicaciones por teléfono, telégrafo u otro medio de transmisión a larga distancia podrá ser sometido a una pena de prisión de entre seis meses y tres años".

[52] Es el apartado 15 de la sentencia en cuestión el que hace referencia expresamente al artículo 40.1.d) y al artículo 40.2.i), ambos del Código de Trabajo rumano, en los cuales aparece consagrado el derecho y la obligación empresarial respectivamente.

[53] La solución a esta primera pregunta planteada al TEDH la encontramos en el apartado 57 de la sentencia analizada. El tenor literal de la argumentación seguida por el TEDH es el siguiente: "(…) se puede deducir que el empleador actuó de conformidad con sus competencias disciplinares 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".

la respuesta –a mi parecer[54]– no está nada clara (la tesis del empleador y del gobierno rumano es afirmativa, pero el trabajador afirma no haber tenido tal conocimiento), el TEDH entiende probado el conocimiento pleno de la prohibición por parte del trabajador.

A la vista de estas consideraciones, en Bârbulescu I, el TEDH llega a la conclusión de que las autoridades nacionales rumanas realizaron un equilibrio adecuado entre los intereses de la empresa y los derechos fundamentales del trabajador recogidos en el artículo 8 CEDH, en tanto en cuanto la injerencia empresarial tuvo lugar únicamente sobre una cuenta de tipo profesional, en la cual la expectativa de confidencialidad había desaparecido, y no sobre su vida y correspondencia privada.

Sin embargo, resulta esencial señalar que en la sentencia hay un extenso voto particular del magistrado portugués Paulo Pinto cuya tesis fundamental se basa en la idea de que el empresario no cuenta con un poder absoluto de control y vigilancia de las relaciones en el trabajo por cualquier medio informático. Añade que, en el caso objeto de análisis, en ningún momento se ha respetado por parte de la empresa una política transparente en lo que a la información se refiere, así como a las restricciones a imponer. Concluye el magistrado diciendo que los derechos a la vida y correspondencia privada del trabajador, recogidos en el artículo 8 CEDH, han sido vulnerados tanto por los tribunales nacionales rumanos como por el propio TEDH.

Según mi parecer, con Bârbulescu I el TEDH amplía el poder de control y vigilancia empresarial ya que entiende que no resulta ilógico que un empleador desee comprobar el correcto cumplimiento de la prestación laboral por parte del trabajador, aún cuando no haya motivos para desconfiar del rendimiento del trabajador.

VI.1.2 Bârbulescu II

Ante la anterior sentencia del TEDH, el señor Bârbulescu pidió que el litigio en cuestión fuera conocido por la Gran Sala del TEDH[55]. La petición del demandante fue aceptada,

[54] En esta misma línea se han expresado otros autores como ROJO TORRECILLA, E.: "El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales", *El blog de Eduardo Rojo,* http://www.eduardorojotorrecilla.es/ (miércoles, 6 de septiembre de 2017). Este autor señala que "ni en la sentencia, ni en la argumentación del TEDH ni en la de los tribunales nacionales se encuentra referencia a alguna medida precautoria tales como el conocimiento por parte de los representantes de los trabajadores que iba a realizarse dicho seguimiento (…)".

[55] Atendiendo al contenido del artículo 43 del CEDH, relativo a la remisión ante la Gran Sala, vemos como se regula tal posibilidad: "1. En el plazo de tres meses a partir de la fecha de la sentencia de una Sala, cualquier parte en el asunto podrá solicitar, en casos excepcionales, la remisión del asunto ante la Gran Sala. 2. Un colegio de cinco jueces de la Gran Sala aceptará la solicitud si el asunto plantea una cuestión grave relativa a la interpretación o a la aplicación del Convenio o de sus Protocolos o una cuestión grave de

pues se reconoció que el asunto planteaba una cuestión grave relativa a la interpretación o a la aplicación del CEDH. Por tanto, será objeto de análisis en este trabajo el obligado pronunciamiento en forma de sentencia de la Gran Sala sobre este asunto.

Al igual que en Bârbulescu I, la Gran Sala antes de entrar en la argumentación jurídica sustantiva hace un exhaustivo repaso de la legislación interna aplicable[56]; de la legislación y jurisprudencia internacional[57], de la legislación de la Unión Europea[58] y de la legislación comparada. En relación con la legislación comparada, considero muy relevante la información que el estudio de la misma –a través treinta y cuatro Estado Miembros– le ha proporcionado a la Gran Sala: aunque todos los Estados objeto de estudio protegen por vía constitucional o legal el derecho al respeto de la privacidad y al secreto de la correspondencia, solo en unos pocos hay una precisión o puntualización de cómo deben respetarse tales derechos del trabajador por parte del empleador en el ámbito de las relaciones laborales.

Entrando ya en los Fundamentos de Derecho, la Gran Sala se va a centrar en la violación o no del artículo 8 CEDH. Para ello, en primer lugar, analiza si el citado artículo es aplicable o no en el caso y, en caso de ser aplicable al litigio, trata de determinar si las autoridades nacionales lo han respetado o no.

Sobre la aplicación del artículo 8 CEDH, frente a la postura negativa del gobierno rumano y la postura positiva del recurrente, la Gran Sala considera que el artículo 8 CEDH sí que es aplicable al litigio enjuiciado puesto que las comunicaciones llevadas a cabo desde el lugar de trabajo están amparadas bajo la protección de los términos "vida privada" y "correspondencia".

---

carácter general. 3. Si el colegio acepta la solicitud, la Gran Sala se pronunciará sobre el asunto mediante sentencia".

[56] En este sentido, la Gran Sala transcribe la normativa interna que previamente ya había sido referenciada por el TEDH en Bârbulescu I, adicionando los artículos 998 y 999 del Código Civil rumano. Concretamente, en el artículo 998 se dice que "cualquiera que cause a otro un daño por una falta, está obligado a repararle" y en el artículo 999 se dice que "cualquiera es responsable del daño causado no solo por el hecho, sino por su negligencia o imprudencia".

[57] Respecto a la legislación y jurisprudencia internacional, en Bârbulescu II se observan grandes diferencias con respecto a Bârbulescu I. Además de hacer referencia a normas ya citadas por el TEDH, aparecen como novedades normas de las Naciones Unidas y ciertas normas del Consejo de Europa, como la Recomendación del Comité de Ministros a los Estados Miembros sobre el tratamiento de datos de carácter personal en el ámbito de trabajo de 1 de abril de 2015.

[58] Dentro de la legislación de la Unión Europea se hace referencia a la Carta de Derechos Fundamentales de la Unión Europea (LCEur 2007,2329) y a la Directiva 95/46/CE (LCEur 1995, 2977), de 24 de octubre de 1995 del Parlamento Europeo y del Consejo de la Unión Europea sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la cual afirma en su apartado 10 que el objeto de las legislaciones nacionales relativas al tratamiento de datos de carácter personal es principalmente el de garantizar el respeto del derecho a la vida privada reconocido por el artículo 8 del CEDH y en los principios generales del derecho comunitario.

A la anterior valoración se llega porque para la Gran Sala el concepto de vida privada debe interpretarse de manera amplia[59], incluyendo dentro del mismo las actividades profesionales, de modo que: "Las restricciones establecidas en la vida laboral pueden incluirse en el artículo 8 cuando repercuten en la forma en que el individuo forja su identidad social a través del desarrollo de relaciones con otros (…) es en el marco de la vida laboral donde la mayoría de la gente tiene muchas, sino la mayoría, de las oportunidades para fortalecer sus lazos con el mundo exterior". Respecto al término de comunicación electrónica[60], la Gran Sala señala que: "(…) el tipo de mensajería instantánea en internet no es otra cosa que una forma de comunicación que forma parte del ejercicio de la intimidad social (…)".

Una vez sabemos que el artículo 8 CEDH es aplicable al caso concreto, la Gran Sala debe resolver si ha sido respetado o no por el gobierno rumano. Para ello analiza tres cuestiones clave. En primer lugar, para la mayoría de la Gran Sala, no queda acreditado que el empleador hubiera cumplido con la obligación de informar con antelación[61] sobre la prohibición del uso personal de los medios puestos a disposición del trabajador, así como de la extensión, alcance y naturaleza de los medios de vigilancia que se iban a emplear. Así pues, tampoco puede llegarse a la conclusión de que el trabajador tuviera pleno conocimiento de las limitaciones que iban a imponerse a su vida y comunicaciones privadas. En segundo lugar, la Gran Sala considera que, como la vigilancia del contenido de las comunicaciones electrónicas es un método muy invasivo, se harán necesarias justificaciones más fundamentadas, las cuales quedan muy lejos de las meramente teóricas defendidas por el Tribunal del Condado (tribunal de instancia), tales como: la necesidad de impedir daños a los sistemas informáticos de la empresa, o de evitar responsabilidad empresarial por actos ilícitos perpetrados por el trabajador, o la difusión

[59] Es preciso señalar que a esta interpretación de carácter amplio del concepto llega la Gran Sala tras hacer un exhaustivo repaso de su extensa jurisprudencia sobre el concepto "vida privada". Toma en consideración algunos casos como:
STEDH 55/2004, de 27 de julio, Caso Sidabras y Džiautas contra Lituania (TEDH 2004, 55).
STEDH77/1992, de 16 de diciembre, Caso Niemietz contra Alemania (TEDH 1992, 77).
STEDH 61/2009, de 28 de mayo, Caso Bigaeva contra Grecia (TEDH 2009, 61).
STEDH 103/2010, de 19 de octubre, Caso Özpinar contra Turquía (TEDH 2010, 103).

[60] Con respecto a la privacidad de las comunicaciones electrónicas, la Gran Sala también recurre a la revisión de amplia jurisprudencia al respecto. Por ejemplo, destaca la STEDH 23/2007, de 3 de abril, Caso Copland contra Reino Unido (TEDH 2007, 23).

[61] En el apartado 137 de la analizada sentencia, el tribunal argumenta que la obligación del empleador de informar sobre la vigilancia debe ser previa al inicio de la actividad laboral por parte del trabajador. De lo contrario, se estaría yendo en contra del principio de transparencia recogido en el apartado 63 de la Recomendación del Comité de Ministros a los Estados Miembros sobre el tratamiento de datos de carácter personal en el ámbito de trabajo de 1 de abril de 2015.

de secretos comerciales[62]. En tercer lugar, la Gran Sala recrimina que en ningún momento se ha analizado si el objetivo de vigilancia y control de la empresa se podía haber conseguido con otras medidas menos invasivas. Del mismo modo, tampoco se ha entrado a examinar la gravedad de las consecuencias que podía causar tal medida, la cual en el caso objeto de litigio resultó ser la máxima en el ámbito laboral: el despido.

Resueltas estas tres cuestiones clave, la Gran Sala considera que los tribunales nacionales no valoraron el justo equilibrio entre los intereses en juego: el derecho al respeto de la vida privada a través de las comunicaciones electrónicas, por una parte, y, el poder de vigilancia y control empresarial, de otro. En consecuencia, el artículo 8 CEDH ha sido transgredido.

VI.2 Caso concreto: Libert contra Francia

El pasado 22 de febrero de 2018, el TEDH volvió a conocer sobre un nuevo caso de presunta vulneración del artículo 8 CEDH –STEDH de 22 de febrero de 2018, Caso Libert contra Francia[63]–. Se debe señalar que la Sala decidió posponer el examen del caso hasta que hubiera un pronunciamiento de la Gran Sala en Bârbulescu II, por lo que –a priori– podríamos pensar que la doctrina Bârbulescu ha debido ser tenida en cuenta por el TEDH en la resolución del litigio.

En este caso, se procede al despido de un trabajador de la Société Nationale des Chemins de Fer (en adelante, SNCF) (empresa nacional de trenes), tras la incautación de su ordenador profesional, el cual revelaba que el trabajador había expedido algunas certificaciones a favor de terceros –vulnerando las normas internas que regulaban su obtención– y había almacenado material pornográfico en el mismo.

Por tanto, nuevamente el TEDH debe abordar los límites al poder de vigilancia y control empresarial del uso profesional del ordenador puesto a disposición del trabajador. Para ello, en primer lugar, el TEDH analiza la legislación y jurisprudencia internas aplicables[64]. En segundo lugar, el TEDH presta atención a las normas internas de la

[62] En concreto, es el apartado 134 de la sentencia analizada el que nos recuerda tales justificaciones del tribunal de instancia. Añade que, para la Gran Sala, no son justificaciones fundamentadas sino simplemente meras "(…) indicaciones teóricas, ya que no se le ha reprochado al recurrente haber expuesto a la empresa a ninguno de estos riesgos".

[63] STEDH 82241/2018, de 22 de febrero, Caso Libert contra Francia (TEDH 2018, 82241).

[64] En este sentido, en el apartado 17 de la citada sentencia se hace referencia a los artículos L.1121-1 y L.1321-3 del Code du Travail, los cuales prohíben cualquier restricción al ejercicio de las libertades

SNCF para la utilización del sistema informático por parte de los trabajadores, las cuales permitían un uso privado del ordenador, siempre que se mantuviera la calidad de la prestación laboral[65]. Por último, el TEDH entra en la exposición de los Fundamentos de Derecho, analizando la existencia, o no, de una "injerencia de una autoridad pública".

En este sentido, para el TEDH sí hubo una injerencia en el derecho del trabajador al respeto de su vida privada porque los archivos que el trabajador tenía en su ordenador fueron abiertos sin ser informado previamente y en su ausencia[66].

Como vemos, el presente asunto dista del ya analizado caso Bârbulescu, en la medida en que la vulneración del artículo 8 CEDH alegada por el demandante provenía de un empleador del sector privado y no de una autoridad pública. Así pues, siendo en el presente litigio una injerencia proveniente de una autoridad pública, "tal injerencia incumplirá el artículo 8 CEDH excepto si estando previsto por la ley, persigue uno o varios de los objetivos legítimos establecidos en el segundo párrafo de esta disposición, y es necesaria en una sociedad democrática para alcanzarlos"[67].

Por tanto, el siguiente paso del TEDH en esta sentencia es tratar de dar respuesta a cada una de las justificaciones exigidas por el apartado 2 del artículo 8 CEDH.

En primer lugar, respecto a la posibilidad de que tal injerencia esta prevista por la ley, el TEDH concluye que, en el momento de los hechos, del derecho positivo –normativa y jurisprudencia francesa–, se podía deducir que el empleador tenía la certeza de que podía

---

individuales y colectivas cuando no estén justificadas por la naturaleza de la actividad a desempeñar y por ser proporcionales al fin perseguido.

[65] En el apartado 19 de la analizada sentencia se reproduce el tenor literal del manual de usuario para la utilización del sistema de información de la SNCF: "(...) El uso de los recursos del sistema de información de la SNCF es posible como parte de la actividad profesional del personal, definido por sus funciones y dentro de los límites de las atribuciones concedidas. No obstante, se tolera un uso personal puntual y razonable del correo electrónico y de Internet con el fin de facilitar la vida práctica o familiar siempre que no sea susceptible de afectar a la calidad del servicio asociado. La información privada debe identificarse claramente como tal (la opción "Privado" en los criterios OUTLOOK, en particular); asimismo, para los receptores de esa información (repertorio "PRIVADO"). Este uso está sujeto a una autorización estrictamente personal que no puede, de ninguna manera, ser cedida, ni siquiera temporalmente, a un tercero sin comprometer la responsabilidad del titular. Puede ser revocada en cualquier momento y termina en caso de suspensión temporal o definitiva de la actividad profesional que la haya justificado. (...)"

[66] El apartado 37 de la controvertida sentencia es en el que recoge la anterior afirmación, puesto que "El Tribunal no está convencido de la tesis del Gobierno según la cual no existe un "injerencia" en el derecho al respeto de la vida privada del demandante porque éste no habría marcado correctamente como privados los archivos abiertos por sus superiores".

[67] A esta afirmación llega el TEDH en el apartado 42 de la estudiada sentencia. Concretamente, se está haciendo referencia al apartado 2 del artículo 8 CEDH: "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

acceder a las comunicaciones electrónicas del ordenador personal del trabajador salvo que estuvieran rigurosamente identificadas como privadas.

En segundo lugar, para la Sala, sí que existe un objetivo legitimo cuando el empleador quiere asegurarse de que sus empleados hacen un uso adecuado de los medios informáticos puestos a su disposición, conforme a sus obligaciones contractuales y a la reglamentación aplicable[68].

En tercer lugar, para la Sala del TEDH "la noción de necesidad implica una injerencia basada en una necesidad social imperiosa y especialmente proporcionada al objetivo legítimo perseguido". En este sentido, el TEDH entiende que la SNCF y los tribunales franceses tenían derecho a examinar su caso con rigor, puesto que en la medida en que los ficheros no estaban debidamente identificados como "privados" sino como "personales", no se ha producido ninguna vulneración de la privacidad del trabajador. Este "juego de palabras" no ha sido tenido en cuenta por el TEDH y quizás sea una de las cuestiones más relevantes del caso, pues comparto la opinión de TORRECILLA ROJO[69] al afirmar que "esa diferencia conceptual no es suficiente para cuestionar la validez de las decisiones adoptadas por los tribunales nacionales al juzgar el TEDH si se ha respetado el art.8 CEDH".

La conclusión de toda esta argumentación es que el TEDH estima que "los tribunales internos no excedieron el margen de apreciación del que disponían, y que, por lo tanto, no ha habido violación del artículo 8 CEDH".

En mi opinión, a la vista de esta reciente sentencia del TEDH, el poder de control del empleador público goza de una posición más amplia y más privilegiada respecto al poder de control del empleador privado, la cual -personalmente- no comparto porque el poder de control y vigilancia empresarial debería tener los mismos límites, con independencia de ser este público o privado. Además, el hecho de que el TEDH solo tomará en consideración el término "privado" (sin tan siquiera entrar a valorar el término

[68] En este punto el TEDH acude a la sentencia Bârbulescu II, la cual en su apartado 127 afirma que "el empleador tiene un legítimo interés en asegurar el buen funcionamiento de su empresa, aplicando medidas que le permitan verificar que sus empleados cumplen con sus deberes profesionales de manera adecuada y con la celeridad requerida".

[69] ROJO TORRECILLA, E.: "Nuevamente sobre la privacidad del trabajador, y sus límites en el ámbito de la prestación laboral. La sutil diferencia entre "personal" y "privado". Notas a la sentencia del TEDH de 22 de febrero de 2018 (¿a la espera de intervención de la Gran Sala?)", *El blog de Eduardo Rojo,* http://www.eduardorojotorrecilla.es/2018/02/nuevamente-sobre-la-privacidad-del.html (martes, 27 de febrero de 2018).

"particular" empleado por el trabajador), pues era el primero de ellos el que aparecía en la normativa interna de aplicación al caso, hará presumible que esta sentencia sea recurrida para que pueda ser conocida por la Gran Sala, al igual que sucedió en el caso Bârbulescu.

VII. IMPACTO DE LA SENTENCIA BÂRBULESCU II EN LA DOCTRINA DEL TRIBUNAL CONSTITUCIONAL Y DEL TRIBUNAL SUPREMO

La sentencia del TEDH que acabamos de examinar ha dado lugar a una nueva doctrina: la doctrina Bârbulescu. Esta nueva doctrina viene a contradecir la doctrina sentada por el TC y el TS en los últimos años, la cual venía a considerar que, el mero incumplimiento por el trabajador de una orden empresarial tiene como inmediata consecuencia la desaparición de la protección que los derechos fundamentales ofrecen al mismo en el ámbito de una relación laboral –STC 241/2012, de 17 de diciembre y STC 170/2013, de 7 de octubre– o que, cuando un trabajador hace un uso personal del ordenador –uso ilícito–, resulta inadmisible exigir al empresario que, además de soportarlo, deba abstenerse de controlarlo –STS 2011/7699, de 6 de octubre–.

Con la doctrina Bârbulescu, el TEDH impone una serie de requisitos que deben ser examinados por cualquier órgano jurisdiccional en aquellos casos en los que el empleador haya hecho uso de su poder de vigilancia y control de las comunicaciones electrónicas de los trabajadores llevadas a cabo a través de los medios propiedad de la empresa. Así, de manera muy esquemática, serían[70]:

- Informar con antelación al trabajador sobre la prohibición del uso personal de los medios puestos a su disposición, así como de la extensión, alcance y naturaleza de los medios de vigilancia que van a ser empleados por la empresa. El carácter previo de la información significa que esta ha de ser anterior al inicio de la actividad laboral y, por tanto, también al de la vigilancia (principio de transparencia).
- El empleador ha de aportar razones muy fundamentadas que justifiquen la vigilancia del contenido de las comunicaciones electrónicas. Por ejemplo, en el

[70] En este sentido se expresa PRECIADO DOMÈNECH, C. H.: "Comentario de urgencia a la STEDH de 5 de septiembre de 2017. Caso Bârbulescu contra Rumanía (Gran Sala). –Recuperando la dignidad en el trabajo–", *Blog de la Comisión de lo Social de Jueces y Juezas para la Democracia*, http://jpdsocial.blogspot.com.es/2017/09/comentario-de-urgencia-la-stedh-de-05.html (martes, 5 de septiembre de 2017).

caso de España, la alusión al artículo 20.3 ET sería una justificación meramente teórica –y no fundamental– que deberá ser rechazada por nuestros tribunales.

- Se debe cumplir el principio de proporcionalidad de la medida de vigilancia, es decir, hay que examinar si el fin perseguido por la empresa hubiera podido alcanzarse por vías menos invasivas.
- Hay que examinar las consecuencias de la medida de vigilancia. En todos los casos analizados el procedimiento disciplinario ha terminado con la mayor de las sanciones en el ámbito de la relación contractual laboral: el despido.
- El empleador debe proporcionar al trabajador unas adecuadas garantías, sobre todo, cuando la medida de vigilancia posea un carácter intrusivo.

En este sentido, parece que la doctrina del TC y del TS debería dar un giro radical y observar estos estándares mínimos en los casos de vigilancia de las comunicaciones electrónicas. De hecho, nuestro TC[71] ya ha afirmado en varias ocasiones que "la jurisprudencia del TEDH no solo ha de servir de criterio interpretativo en la aplicación de los preceptos constitucionales tuteladores de los derechos fundamentales" sino que también "resulta de aplicación inmediata en nuestro ordenamiento". Es preciso aclarar que cuando el TC hace referencia a la jurisprudencia del TEDH se refiere a toda ella, es decir, no únicamente a aquella recaída en procesos donde nuestro país haya sido parte.

Adicionalmente, la STEDH pone de manifiesto la imperiosa necesidad de que el legislador español –de una vez por todas– dicte una norma que concrete cómo deben respetarse los derechos fundamentales del trabajador por parte del empleador en el ámbito de las relaciones laborales. En este sentido, no debemos olvidar que, a partir de mayo de 2018, el nuevo Reglamento 679/2016 del Parlamento Europeo y del Consejo de abril de 2016[72], con el que se pretende unificar la regulación de los 28 países en materia de protección de datos, será de obligado cumplimiento para todos los Estados Miembros[73].

[71] Por todas, STC 303/1993, de 25 de octubre (RTC 1993, 303).
[72] Es concretamente en el artículo 88 donde se regula el tratamiento de los datos en el ámbito de las relaciones laborales, según el cual: "Los Estados Miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más 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, (…)"
[73] GALLARDO MORA, R.: "Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Bârbulescu II C. Rumanía", *Revista de Derecho Social*, núm. 79, 2017, p. 141-157.

Por último, se debe destacar que la nueva doctrina Bârbulescu –como diría PRECIADO DOMÈNECH[74]– "no ha conseguido otra cosa que recuperar la dignidad en el puesto de trabajo y situar la tutela de los derechos fundamentales del trabajador/a al mismo nivel que los de cualquier otro ciudadano/a no trabajador/a".

VII.1 Sentencia Inditex: STS 119/2018, de 8 de febrero

La primera referencia a la doctrina Bârbulescu en la jurisprudencia española la podemos observar en el "sentencia Inditex"[75], concretamente en el en el FJ 6 de la referida sentencia.

En este sentido, el TS estudia –siguiendo la doctrina Bârbulescu– aquellos requisitos que deben ser examinados por cualquier órgano jurisdiccional en aquellos casos en los que el empleador haya hecho uso de su poder de vigilancia y control de las comunicaciones electrónicas de los trabajadores llevadas a cabo a través de los medios propiedad de la empresa (información previa, conocimiento del trabajador, adecuación e idoneidad de la medida, consecuencias de la media…) y llega a la conclusión de que el despido debe ser calificado como procedente, pues no se ha vulnerado ningún derecho fundamental del trabajador.

El TS concluye de esta manera porque considera que, cuando el empleador cuenta con una organizada y adecuada política interna de control de los medios informáticos puestos a disposición del trabajador, se superan todos los filtros del TEDH fijados en la doctrina Bârbulescu y, por tanto, el trabajador pierde esa expectativa razonable de intimidad. En palabras de ROJO TORRECILLA[76] "el poder de control empresarial, incluso bien organizado jurídicamente, pasa por delante del derecho constitucional del trabajador a la protección de sus datos".

Con todo esto, para decepción de aquellos que pensamos que la sentencia Bârbulescu II iba a suponer la recuperación de la dignidad en el puesto del trabajo al incrementar la protección de los derechos fundamentales de los trabajadores, el TS entiende que "la

[74] PRECIADO DOMÈNECH, C. H.: "Comentario de urgencia… cit,.
[75] Esta sentencia ha sido analizada anteriormente en el apartado V.2 del presente trabajo.
[76] ROJO TORRECILLA, E.: "Sobre la privacidad del trabajador en su vida laboral tras la jurisprudencia Bârbulescu II, del TEDH. A propósito de la sentencia del TS de 8 de febrero de 2018 y la recuperación de la doctrina del TC en sentencia núm.170/2013 de 30 de octubre", *El blog de Eduardo Rojo,* http://www.eduardorojotorrecilla.es/2018/04/sobre-la-privacidad-del-trabajador-en.html (domingo, 1 de abril de 2018).

doctrina del TEDH en Bârbulescu II nada sustancial añade a la doctrina tradicional de la Sala y a la expuesta por el TC en la sentencia 170/2013 (…)".

En definitiva, considero que, los requisitos fijados en TEDH en Bârbulescu II a la hora de ponderar intereses, para el TS se reconducen básicamente a los tres sucesivos juicios de idoneidad, necesidad y proporcionalidad, olvidando que el cumplimiento de esos juicios debe hacerse siempre desde el respeto previo a los derechos fundamentales del trabajador –en concreto: derecho a la intimidad, al secreto a las comunicaciones y a la protección de datos personales–.

VIII. CONCLUSIONES

Una vez elaborado el contenido del trabajo considero pertinente terminar el mismo incluyendo un apartado de conclusiones.

-. PRIMERA

El tema sobre el que versa este trabajo se debe estudiar siendo plenamente conscientes de que somos parte de la llamada era digital, en la cual el desarrollo tecnológico que hoy forma parte de nuestro día a día, de nuestras vidas…, ha cambiado radicalmente nuestra manera de compartir, interactuar y transmitir información. Los avances tecnológicos han sido, sin lugar a dudas, un fenómeno que ha contribuido a la creación de riqueza y bienestar, así como a facilitar la vida de las personas –en especial del mundo desarrollado–.

Concretamente, desde finales del siglo XX, las NTIC se han instaurado y consolidado de una manera rápida y firme en el medio laboral, dando lugar a cambios no solo en el proceso de producción –mayor capacidad de las empresas para atender las necesidades productivas y organizativas–, sino también en las relaciones laborales entre empresarios y trabajadores desde dos perspectivas. De un lado, los instrumentos de vigilancia que se venían utilizado por el empresario –para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales– han sufrido una fuerte tecnificación e informatización, lo que le permite –al empresario– fiscalizar muchos más elementos y de una forma más precisa y detallada, es decir, nos encontramos con un empresario más "poderoso" en lo relativo al poder de control y supervisión recogido en el artículo 20.3 ET. De otro lado, la mayoría de los trabajadores parecen incapaces de abstenerse del uso, durante la jornada de trabajo, de la multitud de instrumentos tecnológicos que les

permiten mantener comunicaciones electrónicas (ordenadores, teléfonos móviles, tablets, …), los cuales les acompañan en el resto de ámbitos de su vida las restantes horas del día.

-. SEGUNDA

Es evidente que las NTIC han producido significativos cambios en las relaciones laborales entre el empresario y el trabajador, si bien, hay un aspecto que siempre debe estar presente en las relaciones laborales: los derechos fundamentales recogidos en la CE.

En este sentido, vemos cómo el trabajador no es solo titular de derechos concretos inherentes a esa condición de trabajador que posee, tales como el derecho de libertad sindical o de huelga, sino que también es titular de los llamados derechos de la persona –derechos universales, indisponibles y reconocidos expresamente en la CE–.

En el momento en el que la CE reconoce la eficacia de los derechos del trabajador como persona sin condicionarla a la existencia de algún instrumento jurídico intermedio, lo que verdaderamente está haciendo es evidenciar que tanto el empresario como el trabajador llevan a la relación de trabajo derechos que, aunque no están recogidos en la legislación laboral, tienen una eficacia en tal relación libre de cualquier duda. En otras palabras, se podría afirmar que la celebración de un contrato de trabajo no puede privar al trabajador de los derechos que la CE le concede como ciudadano –trabajador o no trabajador–.

A pesar de que el reconocimiento de los derechos fundamentales del trabajador como persona no queda al margen de la relación laboral, lo cierto es que se aprecia debilidad de estos derechos como límite al incremento en el poder de control y vigilancia empresarial. La razón se encuentra en que la norma estatal no regula esta situación. Nuestra propia legislación –ET– se limita a exponer el precepto constitucional relativo a los derechos fundamentales correspondientes sin llegar a incluir una serie de garantías y tutelas que hagan posible su efectivo ejercicio. Además, ni la normativa convencional ni la doctrina han mostrado especial interés en afianzar esta problemática.

Por lo tanto, vemos cómo nuestros legisladores no están regulando esta situación. Son nuestros órganos judiciales, a través de las resoluciones judiciales, los que resuelven el conflictivo equilibrio existente entre los derechos fundamentales que se manifiestan a través de comunicaciones electrónicas y el poder de control y vigilancia empresarial de la actividad productiva, llegando a constituir el más abundante material para resolver esta controvertida cuestión. No obstante, considero que esto resulta peligroso porque la función de los jueces es interpretar la ley, no crearla, ya que entre ellos hay criterios

contradictorios, llegando incluso a cambios radicales en las posturas doctrinales con el transcurso de los años.

-. TERCERA

En este juego que realizan nuestros órganos jurisdiccionales –TC y TS–, para tratar de alcanzar un equilibrio entre los dos intereses enfrentados, se analiza la vulneración o no de dos derechos fundamentales: el derecho a la intimidad y el derecho al secreto de las comunicaciones, los cuales están recogidos en el artículo 18 CE, apartados 1 y 3.

Por un lado, si nos fijamos, en primer lugar, en la doctrina del TC sobre el control empresarial del uso por los trabajadores del correo electrónico durante la jornada de trabajo, fundamentalmente a través del análisis de la STC 241/2012, de 17 de diciembre y la STC 170/2013, de 7 de octubre –las cuales son un una muestra de la opinión mayoritaria de nuestro TC–, podemos ver cómo en ambas resoluciones se parte de la premisa de que el mero incumplimiento por el trabajador de una orden empresarial tiene como inmediata consecuencia la desaparición de la expectativa de confidencialidad y privacidad a favor del trabajador y, por tanto, el trabajador no puede entender vulnerados sus derechos fundamentales del artículo 18 CE, en sus apartados 1 y 3. En la STC 241/201 esta ausencia venía motivada por dos factores: el carácter abierto del ordenador empleado, calificado de uso común y la expresa prohibición acordada por la empresa de instalar programas, y en la STC 170/2013 la inexistencia se hizo derivar, no ya de una prohibición expresa, sino de una simple calificación por el convenio colectivo aplicable como infracción leve el uso personal de los medios informáticos.

Por otro lado, si analizamos la doctrina del TS podemos distinguir claramente dos posturas en relación con los límites al control empresarial de las comunicaciones electrónicas de los trabajadores. El punto de inflexión en la jurisprudencia del TS lo encontramos en la STS 2011/7699, de 6 de octubre, la cual supone un retroceso en la protección del derecho a la intimidad del trabajador, según venía siendo interpretada por la jurisprudencia del TS en sentencias como la STS 2011/932, de 8 de marzo, y STS 2007/7514, de 26 septiembre. Actualmente, –tomando como última referencia la STS 2011/7699, de 6 de octubre– la doctrina del TS afirma que, si no existe una situación de tolerancia del uso personal de los medios informáticos propiedad de la empresa por parte del trabajador, por ende, tampoco existe ninguna expectativa razonable de intimidad a favor del trabajador. Además, la doctrina del TS sentada en esta sentencia afirma que cuando un trabajador hace un uso personal del ordenador –uso ilícito–, resulta

inadmisible exigir al empresario que, además de soportarlo, deba abstenerse de controlarlo.

Además, en estas conclusiones se debe hacer referencia a la reciente STS 119/2018, de 8 de febrero (sentencia Inditex), relativa al despido de un trabajador tras el control de sus comunicaciones electrónicas. En este caso, el TS considera que cuando una empresa cuenta con una organizada y adecuada política interna de control de los medios informáticos puestos a disposición del trabajador, el hipotético control llevado a cabo por la misma supera ampliamente los juicios de idoneidad, necesidad y proporcionalidad, perdiendo el trabajador toda expectativa razonable de intimidad. En esta sentencia se encuentra la primera referencia a la doctrina Bârbulescu, pero de una manera que no era la esperada -por lo menos, personalmente-. La propia Sala señala que "la doctrina del TEDH en Bârbulescu II nada sustancial añade a la doctrina tradicional de la Sala y a la expuesta por el TC en la sentencia 170/2013 (…)".

Respecto a la línea jurisprudencial que, de momento, se mantiene como opinión mayoritaria dentro de nuestros órganos jurisdiccionales, me gustaría expresar mi posición personal crítica:

- La vulneración o no del secreto de las comunicaciones no se puede hacer depender de que el medio en cuestión sea propiedad de la empresa y deje rastro informático o no de las conversaciones llevadas a través de él, pues el contenido esencial del artículo 18.3 CE protege la libertad de las comunicaciones realizadas a través de un medio y cerradas o confidenciales –como, por ejemplo, el correo electrónico–, pero no añade ningún requisito más.
- En relación también con el secreto de las comunicaciones es cierto que, cuando existen indicios fundados de la comisión de un delito y siempre que se cuente con la debida autorización judicial, el derecho al secreto de las comunicaciones puede verse relegado a un segundo plano. En mi opinión, esta autorización judicial debería extenderse al ámbito laboral porque de otro modo nos estamos enfrentando a decisiones judiciales, como las ahora analizadas, donde basta con la mera sospecha de que el trabajador no estaba desempeñando adecuadamente la prestación laboral, por ejemplo, porque estaba facilitando información confidencial a una empresa competidora, para justificar la lesión del artículo 18.3 CE.

- Bajo mi parecer, tanto el TC como el TS, deberían de haber entrado a valorar de una manera más detallada la posible lesión del derecho a la intimidad (artículo 18.1 CE). Se me hace difícil imaginar, dado el tipo de conversaciones llevadas a cabo por los trabajadores despedidos, que el empresario –aprovechando su poder de vigilancia y control– no hubiera tenido conocimiento de aspectos de la vida privada de los trabajadores, los cuales eran inaccesibles a los demás.
- Además, a mi juicio, hay un derecho fundamental que ha sido el gran olvidado en todas las anteriores sentencias: el derecho a la protección de datos personales (artículo 18.4 CE). El empresario está facultado para ejercer su poder de vigilancia y control de la prestación laboral, pero garantizando en todo momento la debida información previa al trabajador sobre el poseedor y propósito del tratamiento de sus datos, en tanto que el derecho a la información previa es contenido esencial de este derecho fundamental.
- Por último, se debe señalar que, en la sanción laboral terminan las facultades del empresario, es decir, bajo ningún concepto estas facultades pueden suponer una lesión de los derechos fundamentales del trabajador en el ámbito de una relación laboral.

-. CUARTA

Resulta evidente que las NTIC no solo se han implantado y afianzado en España, sino que también han llegado a la mayoría de países del mundo. De hecho, son numerosos los litigios que se han planteado en casi todos los Estados Miembros relativos a este controvertido tema. Algunos de estos litigios han llegado, incluso, hasta el TJUE, tal y como ha ocurrido con el mediático caso Bârbulescu, en el cual se va a debatir sobre el presunto incumplimiento por parte del gobierno de Rumanía del artículo 8 CEDH.

En el caso Bârbulescu hay que distinguir entre lo que se conoce como Bârbulescu I– STEDH 1/2016, de 12 enero, Caso Bârbulescu contra Rumanía (TEDH 2016, 1)– y Bârbulescu II –STEDH (Gran Sala) 61/2017, de 5 de septiembre, Caso Bârbulescu contra Rumanía (TEDH 2017, 61)–. Mientras que en Bârbulescu I, el TEDH llega a la conclusión de que las autoridades nacionales rumanas realizaron un equilibrio adecuado entre los intereses de la empresa y los derechos fundamentales del trabajador recogidos en el artículo 8 CEDH, –en tanto en cuanto la injerencia empresarial tuvo lugar únicamente sobre una cuenta de tipo profesional, en la cual la expectativa de

confidencialidad había desaparecido, y no sobre su vida y correspondencia privada–, con Bârbulescu II se produce un giro radical en la doctrina. En este caso, la Gran Sala del TEDH considera que el artículo 8 CEDH sí que es aplicable al litigio enjuiciado puesto que las comunicaciones llevadas a cabo desde el lugar de trabajo están amparadas bajo la protección de los términos "vida privada" y "correspondencia", y que además este ha resultado transgredido al entender que los tribunales nacionales no valoraron el justo equilibrio entre los intereses en juego: el derecho al respeto de la vida privada a través de las comunicaciones electrónicas, por una parte, y, el poder de vigilancia y control empresarial, de otro.

En este sentido, la sentencia Bârbulescu II va a tener un importante impacto en la doctrina de los Estados Miembros de la UE y, en especial, en la doctrina de nuestros tribunales, al imponer una serie de requisitos que deben ser examinados por cualquier órgano jurisdiccional en aquellos casos en los que el empleador haya hecho uso de su poder de vigilancia y control de las comunicaciones electrónicas de los trabajadores llevadas a cabo a través de los medios propiedad de la empresa. Así, de manera muy esquemática, los límites al poder de vigilancia y control empresarial serían:

- Informar con antelación al trabajador sobre la prohibición del uso personal de los medios puestos a su disposición, así como de la extensión, alcance y naturaleza de los medios de vigilancia que van a ser empleados por la empresa. El carácter previo de la información significa que esta ha de ser anterior al inicio de la actividad laboral y, por tanto, también al de la vigilancia (principio de transparencia).
- El empleador ha de aportar razones muy fundamentadas que justifiquen la vigilancia del contenido de las comunicaciones electrónicas. Por ejemplo, en el caso de España, la alusión al artículo 20.3 ET sería una justificación meramente teórica –y no fundamental– que deberá ser rechazada por nuestros tribunales.
- Se debe cumplir el principio de proporcionalidad de la medida de vigilancia, es decir, hay que examinar si el fin perseguido por la empresa hubiera podido alcanzarse por vías menos invasivas.
- Hay que examinar las consecuencias de la medida de vigilancia. En todos los casos analizados el procedimiento disciplinario ha terminado con la mayor de las sanciones en el ámbito de la relación contractual laboral: el despido.

- El empleador debe proporcionar al trabajador unas adecuadas garantías, sobre todo, cuando la medida de vigilancia posea un carácter intrusivo.

Es cierto que el pasado 22 de febrero de 2018, el TEDH volvió a conocer sobre un nuevo caso de presunta vulneración del artículo 8 CEDH –STEDH de 22 de febrero de 2018, Caso Libert contra Francia–, si bien, personalmente considero que esta sentencia va a ser recurrida para que conozca de la misma la Gran Sala del TEDH debido a la estricta interpretación del término "privado" que ha llevado a cabo la Sala. Por lo tanto, considero prudente estar a la espera de conocer si la Gran Sala debe pronunciarse nuevamente sobre este controvertido tema.

-. QUINTA

En mi opinión, la doctrina sentada por la Gran Sala del TEDH a través de Bârbulescu II era absolutamente necesaria en el ámbito de las actuales relaciones laborales, obligando a los órganos judiciales a observar unos estándares mínimos en aquellos litigios derivados del control y vigilancia de las comunicaciones electrónicas de los trabajadores por parte de la empresa.

En España, las sentencias dictadas en los últimos años por el TC y el TS parecían otorgar una posición privilegiada al empresario en las relaciones laborales, pues valía una simple prohibición empresarial del uso del ordenador para fines particulares para que la expectativa de confidencialidad y privacidad a favor del trabajador –en caso de usar el ordenador para fines personales– quedara destruida y, por tanto, no podían entenderse vulnerados los derechos fundamentales del artículo 18 CE, en sus apartados 1 y 3.

Bajo mi parecer, las decisiones de nuestros órganos judiciales en los últimos años se habrían alejado de la realidad social en la que estamos inmersos donde –en la mayoría de los casos– hay un uso admisible, habitual, racional e inteligente del ordenador y, por ende, de las comunicaciones electrónicas por parte de los trabajadores. Esta forma de actuar del TC y TS les habría llevado a olvidar que, tanto el empresario como el trabajador llevan a la relación laboral derechos que, aunque no están recogidos en la legislación laboral, tienen una eficacia en la prestación laboral incuestionable.

Sin embargo, considero que a raíz de Bârbulescu II la doctrina del TC y del TS debería dar un giro radical, recuperando así la dignidad en el puesto de trabajo y situando la tutela de los derechos fundamentales del trabajador al mismo nivel que los de cualquier otro ciudadano no trabajador.

Este pensamiento personal esperanzador -desde el punto de vista de los derechos de los trabajadores- que he venido manteniendo desde el análisis de Bârbulescu II, se ha visto debilitado con la reciente STS 119/2018, de 8 de febrero, cuya argumentación jurídica deja bastante confuso el derecho a la privacidad del trabajador dentro del ámbito laboral cuando el empleador cuenta con una organizada y adecuada política interna de control de los medios informáticos puestos a disposición del trabajador. El propio TS entiende que "la doctrina del TEDH en Bârbulescu II nada sustancial añade a la doctrina tradicional de la Sala y a la expuesta por el TC en la sentencia 170/2013 (…)" y para el TS los requisitos fijados en TEDH en Bârbulescu II a la hora de ponderar intereses se reconducen básicamente a los tres sucesivos juicios de idoneidad, necesidad y proporcionalidad, olvidando que el cumplimiento de esos juicios debe hacerse siempre desde el respeto previo al derecho a la privacidad del trabajador.

Ahora bien, considero que debemos ser prudentes y esperar a un nuevo –y espero que próximo– pronunciamiento por parte de nuestro TS en relación con un caso semejante para comprobar si se confirma esta tesis –creando jurisprudencia– y si también será de aplicación en aquellos casos en los que no se aprecie con tanta claridad la existencia de una organizada y adecuada política interna de control de los medios informáticos puestos a disposición del trabajador.

-. SEXTA

En este último apartado de conclusiones me gustaría reflejar lo que ha significado para mi la realización de este TFG con un tema como el elegido. Por un lado, la búsqueda de bibliografía, su posterior análisis y, finalmente, la elaboración de una postura personal crítica, ha supuesto para mi un considerable esfuerzo, el cual vengo realizando desde el mes de diciembre. Sin embargo, este esfuerzo se ha visto plenamente compensado por los conocimientos adquiridos sobre un tema de notoria actualidad judicial y aplicabilidad en los aspectos cotidianos de nuestras relaciones laborales, inmersas en una sociedad profundamente tecnológica. De hecho, la propia actualidad del tema me ha llevado a la necesidad de añadir nuevos apartados conforme se dictaban sentencias por parte del TEDH y del TS en los últimos meses. Por otro lado, he experimentado en primera persona la expresión "el Derecho no es una ciencia exacta, sino que admite varias interpretaciones de la norma jurídica" puesto que mi postura personal cambiaba cuanto más leía y más conocimientos adquiría sobre el controvertido tema.

Por último, en la realización de este TFG he contado con la excepcional ayuda de la doctora en Derecho Sara Alcázar, orientándome en todo momento en la realización de este trabajo.

BIBLIOGRAFÍA

CARRILLO, M.: "Los ámbitos del derecho a la intimidad en la sociedad de la comunicación", en VV. AA (Asociación de Letrados del Tribunal Constitucional): *El derecho a la privacidad en un nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, p. 49.

FERNÁNDEZ AVILÉS, J. A. y RODRÍGUEZ-RICO ROLDÁN, V.: "Nuevas tecnologías y control empresarial de la actividad laboral en España", *Labour & Law Issues,* vol. 2, núm. 1, 2016, p. 10.

GALLARDO MORA, R.: "Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Bârbulescu II C. Rumanía", *Revista de Derecho Social*, núm. 79, 2017, p. 141-157.

GÁRATE CASTRO, J.: "Control del empresario de las nuevas tecnologías", *Ejemplar facilitado por el autor en una conferencia impartida en la Facultad de Derecho de la Universidad de Zaragoza* (jueves 14 de diciembre de 2017).

GUDE FERNÁNDEZ, A.: "La videovigilancia laboral y el derecho a la protección de datos de carácter personal", *Revista de Derecho Político,* núm. 91, 2014, p. 46 y 47.

MERCADER UGUINA, J. R.: "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?, *Relaciones Laborales,* núm. 10, 2001, p. 14.

MONEREO PÉREZ, J. L. y LÓPEZ INSÚA, B.: "El control empresarial del correo electrónico tras la STC 170/2013", *Aranzadi Social*, núm. 11, 2014, p. 1.

MONTOYA MELGAR, A.: *El poder de dirección del empresario,* Instituto de Estudios Políticos, Madrid, 1965.

PALOMEQUE LÓPEZ, M. C.: *Los derechos laborales en la Constitución Española*, Madrid, CEC, 1991.

PRECIADO DOMÈNECH, C. H.: *El Derecho de la Protección de Datos en el Contrato de Trabajo*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017.

RIVERO, J.: "Les libertés publiques dans l'enterprise", *Droit Social*, núm. 5, 1982, p. 424.

RIVERO SÁNCHEZ-COVISA, F. J.: *Revisión del concepto constitucional del secreto de las comunicaciones,* Dykinson, Madrid, 2017.

RODRÍGUEZ CARDO, I. A.: *Poder de dirección empresarial y esfera personal de trabajador,* Consejo Económico y Social del Principado de Asturias, Oviedo, 2009.

RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores,* Tirant lo Blanch, Valencia, 2015.

ROMÁN DE LA TORRE, M. D.: *Poder de dirección y contrato de trabajo,* Grapheus, Valladolid, 1992.

SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCCONI, C.: *Nuevas Tecnologías y Relaciones Laborales,* Navarra, Aranzadi, 2012.

TASCON LÓPEZ, R.: "El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica", *Aranzadi Social*, núm. 17, 2007, p. 2.

VALDES DAL-RÉ, F.: "Contrato de trabajo, derechos fundamentales de la persona del trabajador, y poderes empresariales: una difícil convivencia", *Relaciones Laborales,* núm. 2, 2003, p. 89-130.

VALDÉS DAL-RÉ, F.: "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", *Revista de Derecho Social*, núm. 79, 2017, p. 15-35.

VALDES DAL-RÉ, F.: "El Estatuto de los Trabajadores", *Argumentos*, núm. 34, 1980, p. 18.

WEBGRAFÍA

PRECIADO DOMÈNECH, C. H.: "Comentario de urgencia a la STEDH de 5 de septiembre de 2017. Caso Bârbulescu contra Rumanía (Gran Sala). – Recuperando la dignidad en el trabajo-", *Blog de la Comisión de lo Social de Juezas y Jueces para la Democracia,* http://jpdsocial.blogspot.com.es/2017/09/comentario-de-urgencia-la-stedh-de-05.html (martes, 5 de septiembre de 2017).

ROJO TORRECILLA, E.: "Sobre la privacidad del trabajador en su vida laboral tras la jurisprudencia Bârbulescu II, del TEDH. A propósito de la sentencia del TS de 8 de febrero de 2018 y la recuperación de la doctrina del TC en sentencia núm.170/2013 de 30 de octubre", *El blog de Eduardo Rojo,* *http://www.eduardorojotorrecilla.es/2018/04/sobre-la-privacidad-del-trabajador-en.html* (domingo, 1 de abril de 2018).

ROJO TORRECILLA, E.: "Nuevamente sobre la privacidad del trabajador, y sus límites en el ámbito de la prestación laboral. La sutil diferencia entre "personal" y "privado". Notas a la sentencia del TEDH de 22 de febrero de 2018 (¿a la espera de intervención de la Gran Sala?)", *El blog de Eduardo Rojo,* *http://www.eduardorojotorrecilla.es/2018/02/nuevamente-sobre-la-privacidad-del.html* (martes, 27 de febrero de 2018).

ROJO TORRECILLA, E.: "El nuevo y cambiante mundo del trabajo. Una mirada abierta y crítica a las nuevas realidades laborales", *El blog de Eduardo Rojo,* *http://www.eduardorojotorrecilla.es/* (miércoles, 6 de septiembre de 2017).

ANEXO JURISPRUDENCIAL

Tribunal Europeo de Derechos Humanos:

STEDH 82241/2018, de 22 de febrero, Caso Libert contra Francia (JUR 2018, 2241).

STEDH (Gran Sala) 61/2017, de 5 de septiembre, Caso Bârbulescu contra Rumanía (TEDH 2017, 61).

STEDH 1/2016, de 12 de enero, Caso Bârbulescu contra Rumanía (TEDH 2016, 1).

STEDH 103/2010, de 19 de octubre, Caso Özpinar contra Turquía (TEDH 2010, 103).

STEDH 61/2009, de 28 de mayo, Caso Bigaeva contra Grecia (TEDH 2009, 61).

STEDH 23/2007, de 3 de abril, Caso Copland contra Reino Unido (TEDH 2007, 23).

STEDH 55/2004, de 27 de julio, Caso Sidabras y Džiautas contra Lituania (TEDH 2004, 55).

STEDH 77/1992, de 16 de diciembre, Caso Niemietz contra Alemania (TEDH 1992, 77).

Tribunal Constitucional:

STC 170/2013, de 7 de octubre (RTC 2013, 170).

STC 29/2013, de 11 de febrero (RTC 2013, 29).

STC 241/2012, de 17 de diciembre (RTC 2012, 241).

STC 236/2007, de 7 de noviembre (RTC 2007, 236).

STC 41/2006, de 13 de febrero (RTC 2006, 41)

STC 70/2002, de 3 de abril (RTC 2002, 70).

STC 88/1985, de 19 de julio (RTC 1985, 88).

STC 114/1984, de 29 de noviembre (RTC 1984,114).

Tribunal Supremo (Sala de lo Social):

STS 119/2018, de 8 de febrero (RJ 2018, 666).

STS 2011/7699, de 6 de octubre (RJ 2011, 7699).

STS 2011/932, de 8 de marzo (RJ 2011, 932).

STS 7514/2007, de 26 septiembre (RJ 2007, 7514).