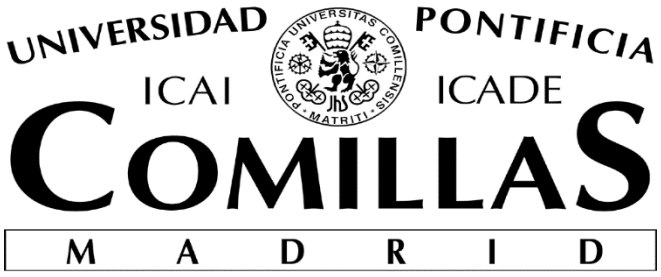

FACULTAD DE DERECHO

EL CONTROL EMPRESARIAL DE LA UTILIZACIÓN POR PARTE DE LOS EMPLEADOS DE LOS MEDIOS INFORMÁTICOS PUESTOS A SU DISPOSICIÓN

Autor: Rocío Fernández-Cuesta del Río
5º E-3 B
Área de Derecho Laboral

Tutor: María José López Álvarez

Madrid
Abril 2018

RESUMEN

El control que ejerce la empresa sobre los medios electrónicos de titularidad empresarial puestos a disposición del trabajador adquiere una importancia esencial puesto que dichos medios se configuran como instrumentos de producción laboral a través de los cuales los trabajadores ejecutan el contrato de trabajo. Dicha configuración de los medios como instrumentos de productividad laboral faculta al empresario a controlar su utilización en aras de la buena fe contractual, pero al mismo tiempo dicho control debe estar sometido a una restricción en salvaguarda de los derechos fundamentales de los trabajadores, que se erigen, asimismo, como ciudadanos. En todo caso, deben protegerse los derechos a la intimidad personal y al secreto de comunicaciones en el uso de los medios electrónicos de los trabajadores, así como la expectativa razonable de privacidad con la que cuenta el trabajador en el uso de los instrumentos informáticos. La colisión entre los intereses empresariales de control con los derechos fundamentales de los trabajadores adquiere especial relevancia pues supone cierta conflictividad que merece ser resuelta.

Palabras clave: facultad de control, medios informáticos, derecho a la intimidad, derecho al secreto de las comunicaciones, juicio de proporcionalidad, fin legítimo empresarial, derecho a la información.

ABSTRACT:

The degree of control that enterprises exercise on electronic devices used by the employees has become very important because those devices are working instruments used in order to comply with the labour contract. The employer is able to control the use of electronic devices in order to protect contractual good faith. However, at the same time, the employer's control is limited in order to protect the fundamental rights of the worker, who is at the same time, a citizen. The right to privacy and the right of communications secrecy have to be protected in the usage of electronic devices in the workplace, because workers have a reasonable expectation of privacy that cannot be breached. The collision between corporate interests and workers' fundamental rights has caused high levels of conflicts that need to be analyzed.

Key words: authority of control, electronic devices, right to privacy, right of communications secrecy, judgement of proportionality, corporate legitimate interest, right to information.

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN

1.1. Propósito y contextualización del tema elegido

El presente trabajo tiene como propósito analizar el control que puede ejercer la empresa sobre el uso que dan los empleados a los medios informáticos que esta les proporciona para que desarrollen su actividad profesional. El uso de las Tecnologías de la Información y Comunicación (en adelante, **"TIC"**) en el entorno profesional ha ido adquiriendo cada vez mayor relevancia debido a su rápida evolución y a su conversión en medio de comunicación principal de las empresas. El desarrollo de las nuevas tecnologías y medios informáticos utilizados en el entorno laboral, entre otros, el correo electrónico y el acceso a internet, ha ocasionado que se intensifique el debate sobre las garantías y posibles límites que deben estar presentes en el ejercicio de las facultades empresariales de control y vigilancia en el ámbito laboral[1]. Dentro de las TIC, la mensajería instantánea se configura como una de las vías de comunicación más utilizadas, cuyo uso se puede poner en práctica bien a través de aplicaciones del ordenador o bien a través del empleo del correo electrónico. Dicha circunstancia ha ocasionado que en la actualidad haya surgido la necesidad de analizar el uso de los medios informáticos por los trabajadores y la adaptación de las empresas a estos.

El escenario actual ha propiciado que el uso social de la tecnología en el ámbito laboral haya evolucionado más rápidamente que la adaptación de las empresas al modo de ejercer el control sobre los instrumentos tecnológicos, que, en ocasiones, se erigen como medios de transmisión de datos e información[2]. Las comunicaciones a través de medios informáticos, en concreto, a través del correo electrónico, se consideran como un sistema primordial y de los mejores posicionados dentro de las vías de comunicación de las empresas, debido a la agilidad, la rapidez y la posibilidad que propician de mantener comunicaciones en tiempo real y desde cualquier lugar[3], suponiendo dichas formas de comunicación grandes ventajas para las empresas ya que han implicado una agilización en el desarrollo profesional. Sin embargo, a su vez, se configuran como medios de comunicación que pueden ser utilizados tanto para uso personal, como para fines

[1] MUÑOZ RUIZ, A.B., "Convergencia y divergencia entre los Tribunales del Orden Social y la Agencia Española de Protección de Datos en materia de control informático de la prestación de trabajo", *Revista española de Derecho del Trabajo,* núm. 156, 2012, (BIB 2012,3125), pp. 1-2.

[2] MIRÓ MORROS, D.: "El uso del correo electrónico en la empresa: protocolos internos", *Actualidad Jurídica Aranzadi*, núm. 874, 2013 (BIB 2013, 2511), p. 7.

[3] CARRASCO DURÁN, M., "El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa", *Revista Aranzadi Doctrinal*, núm. 9, 2014, (BIB 2013, 2695), p. 1.

desleales, lo que en ocasiones ha promovido que se saque provecho de los medios telemáticos con el fin de transferir información confidencial de la empresa a terceras personas ajenas a la misma. Es por ello, que, en este contexto, es cada vez mayor el interés de las empresas por intensificar el control de los nuevos sistemas de comunicación.

En base a este contexto, la posibilidad de que un empresario ejerza el control sobre el uso que hacen sus trabajadores de los medios informáticos puestos a su disposición ha sido un tema de enorme controversia que merece un análisis. La cuestión que se trata de solventar se basa en la existencia de distintos valores jurídicos, todos ellos muy ligados con valores constitucionales[4]. Por un lado, se encuentra el derecho a la intimidad, recogido en el artículo 18.1 de la Constitución Española (en adelante, **"CE"**), y el derecho al secreto de las comunicaciones, recogido en el artículo 18.3 CE. Por otro lado, entra en juego el poder de dirección del empresario, esencial para la buena marcha de la empresa, que aparece contenido en el artículo 20 del Estatuto de los Trabajadores (en adelante, **"ET"**)[5], así como en los artículos 33 y 38 CE.

1.2.Justificación del tema elegido

El interés en el tema elegido se encuentra en que el ordenamiento jurídico español se caracteriza por no tener unas reglas especiales que puedan aplicarse a la actividad del control empresarial, es decir, no existe una regulación legal específica aplicable a los conflictos suscitados en el ejercicio de control empresarial de los medios informáticos. A pesar de haberse convertido dicho control empresarial en una potestad del empresario de especial relevancia y análisis, se ha tenido que acudir a la doctrina constitucional, a la doctrina del Tribunal Supremo y a la doctrina comunitaria con el fin de solventar los problemas que se suscitan con respecto a la relación entre el control empresarial y los derechos fundamentales de los trabajadores[6]. De lo expuesto se puede deducir que, el Derecho Laboral español se configura como un derecho Jurisprudencial en lo que respecta a las TIC y su regulación. Por ende, la doctrina general relativa al uso y control de los medios tecnológicos de información y comunicación de la empresa se ha ido

[4] GARCÍA SÁNCHEZ, J.D. y GARCÍA BEL, M., "El poder de control del empresario sobre el correo electrónico de sus trabajadores. A propósito de la Sentencia de la Sala de lo Penal del Tribunal Supremo de 16 de junio de 2014", *Revista de Actualidad Jurídica Uría Menéndez*, núm. 39, 2015, pp. 117-123.
[5] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE 24 de octubre de 2015).
[6] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", *Revista Aranzadi Doctrinal*, núm. 10, 2017, (BIB 2017, 43157), pp. 1-3.

construyendo a partir de pronunciamientos judiciales, lo que ha ocasionado ciertas discrepancias que se irán exponiendo a lo largo del presente trabajo. Esta cuestión ha sido revisada y discutida tanto por Tribunales Superiores de Justicia (en adelante, **"TSJ"**), como por Tribunal Supremo (en adelante, **"TS"**), así como por el Tribunal Constitucional (en adelante, **"TC"**), a nivel nacional; y por el Tribunal Europeo de Derechos Humanos (en adelante, **"TEDH"**), a nivel comunitario. Sin embargo, a pesar de ello, no se puede concluir en un criterio uniforme acerca de la facultad de fiscalización de la empresa del uso de los medios informáticos. Todo ello ocasiona que existan numerosas divergencias en los criterios adoptados por los distintos tribunales.

Teniendo en cuenta lo anterior, la elección del presente tema responde a la necesidad de solventar o acercar las divergencias existentes entre aspectos clave de esta cuestión. Los pronunciamientos heterogéneos de los tribunales han dotado tanto a los trabajadores como a los empresarios de cierta inseguridad jurídica en sus actuaciones que requiere ser resuelta, teniendo en cuenta que se trata de un área muy sensible referida a las nuevas tecnologías de la comunicación y a su relación con los derechos fundamentales de los trabajadores.

1.3.Objetivos

El objetivo principal del presente trabajo responde al título de este, es decir, tiene como propósito analizar el control que puede ejercer el empresario sobre los medios informáticos que pone a disposición de los trabajadores, requiriendo especial relevancia la forma en la que ha de ejercerse la potestad de control empresarial para que esta no vulnere los derechos fundamentales de los trabajadores. Para la consecución del objetivo principal, se pueden desglosar los siguientes sub-objetivos:

- Análisis de los derechos fundamentales de los trabajadores en el uso de los medios informáticos en el ámbito laboral, así como su posible modulación en aras de la buena fe contractual.
- Significado de la facultad de control empresarial y restricción de esta como consecuencia de la salvaguarda de los derechos fundamentales de los trabajadores.
- Pronunciamientos jurisprudenciales relevantes respecto al ejercicio de control empresarial.
- Propuesta y recomendaciones a la empresa acerca del modo en que debe ejercer el control empresarial en base al estudio del análisis jurisprudencial presentado.

1.4.Metodología y estructura

Con el objetivo de lograr el propósito mencionado, el trabajo se ha llevado a cabo con una metodología desde un enfoque cualitativo, analizando manuales teóricos, libros, capítulos de revista y comentarios de sentencias de autores expertos en la materia estudiada, además de las normas legales aplicables al objeto del trabajo. Asimismo, se ha llevado a cabo un análisis de sentencias de especial relevancia con el objetivo de llegar a conclusiones válidas acerca del tema en cuestión. La búsqueda de la literatura se ha realizado por medio de bases de datos jurídicas, especialmente de Aranzadi, El Derecho y Tirant Online.

El presente trabajo consta de cinco capítulos. El primer capítulo lleva a cabo una introducción que incluye el propósito, la contextualización y la justificación del tema elegido; además de los objetivos, la metodología y la estructura del trabajo.

El segundo capítulo se centra en el estado de la cuestión, presentando los derechos fundamentales erigidos, así como su posible modulación; además de analizar la facultad de control empresarial, el juicio de proporcionalidad y el deber de información al trabajador.

El tercer capítulo se centra en la evolución jurisprudencial que ha sufrido el tema de investigación, presentando las posturas divergentes del Tribunal Supremo, así como del Tribunal Constitucional y de los Tribunales Superiores de Justicia, analizando los aspectos destacadas en cada postura.

El cuarto capítulo analiza la más reciente doctrina presentada por el Tribunal Europeo de Derechos Humanos, así como la nueva postura del Tribunal Supremo que se adecúa a la misma, llegando a conclusiones válidas acerca de cierta unificación de una doctrina cada vez más garantista.

El quinto capítulo trata de otorgar propuestas y recomendaciones a la empresa acerca del modo en que ésta puede comportarse ante situaciones de control empresarial, presentando pautas clave que siempre debe tener en cuenta, así como modos en los que debe actuar si se le presentan situaciones concretas.

Por último, el sexto capítulo recoge las ideas principales analizadas en el presente trabajo, así como las conclusiones válidas a las que se han llegado. Finalmente, se hace referencia a la bibliografía utilizada.

2. ESTADO DE LA CUESTIÓN

2.1. Los derechos fundamentales de los trabajadores en el marco de las relaciones laborales

El correo electrónico se define como un servicio a través del cual dos personas se comunican transmitiéndose un mensaje entre dos ordenadores mediando un servidor. Es decir, se erige como un sistema de comunicación. Cuando el trabajador hace uso de un medio de comunicación de la empresa está promoviendo un proceso comunicativo protegido por el ordenamiento jurídico, ya que las comunicaciones de los trabajadores a través de medios informáticos propiedad de la empresa están tuteladas por el derecho fundamental al secreto a las comunicaciones, el derecho a la intimidad, y el derecho a la protección de datos. El empresario, a pesar de ser titular de las herramientas de trabajo, se configura como un tercero ajeno al trabajador, frente a quien se puede oponer el derecho al secreto a las comunicaciones y el derecho a la intimidad con el fin de que no pueda controlar las comunicaciones más íntimas entabladas por los trabajadores. Esto se debe a que el derecho a la propiedad no es jerárquicamente superior a los derechos fundamentales, por lo que no puede imponerse sobre ellos[7].

Por un lado, el derecho al secreto de comunicaciones vela por la protección de las comunicaciones de los trabajadores ya que, según recoge el artículo 18.3 CE, "se garantiza el secreto de las comunicaciones y, en especial, de las postales telegráficas y telefónicas, salvo resolución judicial" (art. 18.3 CE). A la vista de la doctrina del Tribunal Constitucional[8], que sigue la línea de lo expuesto por el Tribunal Europeo de Derechos Humanos, son dos los aspectos esenciales del derecho al secreto de las comunicaciones:

En primer lugar, únicamente se protegen las comunicaciones en sentido constitucional, que son aquellas que (i) contienen expresiones del pensamiento y mensajes dentro del proceso de comunicación; y (ii) se canalizan a través del uso de medios informáticos, por lo que en ningún caso se encuentran incluidas aquellas comunicaciones que surgen en persona. En segundo lugar, el derecho fundamental al secreto de las comunicaciones dispensa protección al contenido de la comunicación, a la identidad de los sujetos parte

[7] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", cit., p. 4.
[8] Sentencia del Tribunal Constitucional de 29 de noviembre de 1984 (RTC 1984/2014); y Sentencia del Tribunal Constitucional de 17 de diciembre de 2012 (RTC 2012/241).

de la comunicación, esto es, emisor y receptor, y al mensaje objeto de la comunicación o a la intercepción directa de la misma.

Pronunciamientos judiciales han evidenciado que este derecho no se ve vulnerado cuando la empresa fiscaliza conversaciones que mantienen dos trabajadoras en un ordenador de uso común de la empresa[9]. Asimismo, no se entiende vulnerado este derecho cuando no existe una expectativa fundada y razonable de confidencialidad en el desempeño de la actividad laboral. Dicha situación se da, por ejemplo, en los gestores de cobros o ventas por vía telefónica, donde necesariamente se lleva a cabo un control de las comunicaciones con el fin de verificar el correcto desempeño de su actividad[10].

Por otro lado, otro derecho fundamental en conflicto es el derecho a la intimidad, que se trata de un término que abarca la libertad individual, el control sobre el propio cuerpo, la potestad de información personal, la libertad ante los sistemas de control y vigilancia, la protección del honor y la reputación[11]. En este aspecto, el TEDH en la STEDH de 3 de abril de 2007[12] recoge que el derecho a la intimidad se extiende tanto al contenido de las comunicaciones electrónicas como a la información acumulada en el ordenador personal de su titular. Toda esta información forma parte de la intimidad del trabajador constitucionalmente protegida ya que, al tratarse el ordenador de una herramienta conveniente para la emisión y recepción de mensajes, puede quedar restringido el derecho a la intimidad personal siempre y cuando las comunicaciones escritas se encuentren almacenadas en la memoria del terminal informático utilizado[13]. La vulneración del derecho a la intimidad se encuentra íntimamente relacionada con el término de la expectativa razonable de intimidad; al que se ha referido el Tribunal Supremo, determinando que no considera que exista dicha expectativa si el trabajador hace uso de un instrumento tecnológico para fines privados, cuando había recibido prohibiciones expresas del uso personal del medio tecnológico, y había sido informado de los controles que efectuaría la empresa[14]. Sobre dicha consideración existe cierta controversia que será expuesta y analizada más adelante.

[9] Sentencia del Tribunal Constitucional de 17 de diciembre de 2012 (RTC 2012/241).
[10] Sentencia del Tribunal Superior de Justicia de Andalucía de 4 de septiembre de 2014 (AS 2014/3148).
[11] GALÁN MUÑOZ, A. *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación,* ed. Tirant Lo Blanch, 2014, p. 22.
[12] Sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007 (TEDH 2007/23).
[13] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", cit., p.4.
[14] Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7541).

2.2. Poder de dirección y control del empresario: límites a los derechos fundamentales

Los derechos fundamentales expuestos- derecho a la intimidad y derecho al secreto de las comunicaciones- son en todo caso reconocidos y protegidos en las relaciones laborales; si bien, se ha admitido que, en ocasiones, la buena fe contractual puede imponer determinadas restricciones a ciertos derechos fundamentales, así como limitar aspectos de la esfera personal del trabajador. En primer lugar, el reconocimiento de estos derechos proviene de que el trabajador, como tal, se erige como un ciudadano, por lo que en todo caso deben respetarse sus derechos. Sin embargo, la restricción de los mismos deriva de que el ciudadano es, al mismo tiempo, un trabajador que ha firmado un contrato de trabajo, por lo que también se erigen obligaciones de ese contrato que deben ser cumplidas[15].

Ciertamente, se puede modular la eficacia de tales derechos en algunos supuestos[16]. En concreto, el Tribunal Europeo de Derechos Humanos se refiere a que el «seguimiento del uso por parte de un trabajador del teléfono, el correo electrónico e Internet en el lugar de trabajo pueda considerarse "necesario en una sociedad democrática" en ciertas situaciones que persigan un fin legítimo» (caso Copland contra Reino Unido)[17]. Los supuestos en los que la eficacia de los derechos fundamentales se ve modulada son aquellos en los que determinados comportamientos que lleve a cabo el trabajador puedan afectar adversamente a la empresa, tales como dañar el prestigio de esta o disminuir la productividad laboral del trabajador.

En este sentido, únicamente en los supuestos en los que la buena fe contractual exija limitar la esfera personal del trabajador, deberá aceptarse el control sobre aspectos personales del trabajador y de su vida privada[18]; es decir, la restricción de derechos fundamentales en aras de la salvaguarda de la buena fe contractual debe tratarse como una excepción, por lo que ha de interpretarse de forma restrictiva. Como consecuencia, si el trabajador lleva a cabo comportamientos que afectan a la buena fe empresarial, tales

[15] PÉREZ DE LOS COBOS ORIHUEL, F. y GARCÍA RUBIO, M. A., "El control empresarial sobre las comunicaciones electrónicos del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", *Nueva Revista Española de Derecho del Trabajo*, núm.196, 2017, (BIB 2017, 814), p. 3.
[16] CARRASCO DURÁN, M., "El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa", *Revista Aranzadi Doctrinal*, núm. 9, 2014, (BIB 2013, 2695), p. 3.
[17] Sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007 (TEDH 2007/23).
[18] Sentencia del Tribunal Constitucional de 12 de junio de 1996 (RTC 1996/106).

como la realización de actos delictivos en perjuicio de intereses de la empresa[19] o comportamientos contrarios a cláusulas tipificadas en el contrato de trabajo, sus derechos pueden verse restringidos con el fin de que el empresario fiscalice el uso ilegítimo que están dando a los medios.

El control que puede ejercer el empresario sobre los medios informáticos de los trabajadores se encuentra legitimado en el «carácter de instrumento de producción del objeto sobre el que recae»[20], es decir, de la configuración del ordenador como medio de ejecutar el contrato de trabajo. La propiedad empresarial del medio de comunicación junto con la configuración del ordenador como una herramienta de trabajo, legitima al empresario a restringir y limitar el uso del correo electrónico del trabajador. Como consecuencia, el empresario, a quién le corresponden facultades directivas, puede imponer limitaciones o prohibiciones en el uso de los sistemas electrónicos puestos a disposición de los trabajadores para fines personales o extraproductivos. Por tanto, se debe reconocer la facultad empresarial de vigilancia y control sobre el cumplimento de obligaciones relativas a la utilización de los medios informáticos.

La posición del empresario en el sistema constitucional español se caracteriza por el reconocimiento de la libertad de empresa en una economía de mercado (art. 38 CE). Este derecho otorga al empresario, en su calidad de titular de la organización productiva, el poder de organización y dirección del trabajo que, con carácter general, aparece reconocido en el artículo 20 ET. Uno de los poderes comprendidos dentro del poder de organización y dirección es la potestad de dar órdenes e instrucciones a los trabajadores sobre el modo de cumplimiento de la obligación de trabajo, asumida a su vez, por el otro sujeto del contrato de trabajo, el trabajador. Este poder se configura como el poder de control del empresario, que, a su vez, incluye dos facultades específicas: por un lado, la verificación del cumplimiento del contrato de trabajo, y, por otro, la elección y utilización del medio de control con el que se lleve a cabo dicha verificación.

El artículo 20.3 ET recoge, con carácter general, la regulación de las facultades de control empresarial, que establece que el empresario podrá "adoptar las medidas de control que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales". Por lo tanto, de este artículo se

[19] Sentencia del Tribunal Supremo de 21 de septiembre de 2017 (RJ 2017/4310).
[20] Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7541).

desprende que el fin último de las facultades de control es acreditar que el trabajador ha cumplido con sus obligaciones y deberes laborales, comprobando así que el trabajador cumple con su prestación laboral de acuerdo con las directrices recibidas por el empresario. En principio, dicho control debe ejercerse con estricto análisis al cumplimiento de la obligación contractual, prohibiendo particularmente, los controles ejercidos sobre aspectos que afecten a la esfera de intimidad del trabajador; si bien, dichos controles, aun siendo ejercidos de forma legítima, pueden en ocasiones incidir en la esfera personal del trabajador, que es lo que ocasiona conflictos en las relaciones laborales.

El artículo 20.3 ET continúa estableciendo: respetando en "su adopción y aplicación la consideración debida de la dignidad humana". De dicho artículo se deriva que corresponde al empresario elegir discrecionalmente el medio que ha de emplear para ejercer su poder de control sobre el trabajador, si bien, el medio elegido siempre ha de respetar la dignidad de la persona, referida a la garantía de sus derechos fundamentales. Al tratarse dicho precepto de un precepto abstracto, la solución al conflicto que pueda derivar entre el medio de control elegido y la dignidad del trabajador deberá ser analizada caso por caso, teniendo en cuenta las circunstancias concretas de cada uno.

2.3.El juicio de proporcionalidad

El Tribunal Constitucional ha señalado en numerosas ocasiones que el empresario no está legitimado para ejercer, acogiéndose a sus facultades de control y vigilancia que le otorga el artículo 20.3 ET, intromisiones fraudulentas en la intimidad de los trabajadores. Los equilibrios recíprocos derivados del contrato de trabajo implican, además de la posible limitación de los derechos fundamentales de los trabajadores en aras de la buena fe contractual, la recíproca restricción de las facultades empresariales de control para la salvaguarda de los derechos fundamentales del trabajador, quedando obligado el empresario a respetar los mismos[21]. Por ello, el ejercicio de las facultades de control del empleador no puede en ningún caso producir resultados inconstitucionales o contrarios a los derechos fundamentales[22]. De este modo, para determinar la legitimación o no del control ejercido por el empresario, se debe llevar a cabo un juicio de proporcionalidad. Este juicio de proporcionalidad, aplicado por primera vez en la STC 99/1994, de 11 de

[21] Sentencia del Tribunal Constitucional de 10 de julio de 2000 (RTC 2000/186).
[22] FERNÁNDEZ AVILÉS, J.A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial de la actividad laboral en España", *Labour & Law Issues*, vol. 8, núm. 1, 2016, p. 55.

abril[23], determina que la doctrina constitucional no considera que los derechos de los trabajadores y los de la empresa tengan el mismo valor, por lo que el equilibrio de los mismos no se obtiene en el punto medio entre ambos, sino que únicamente cuando se supere el test de proporcionalidad, se podrán imponer límites a los derechos fundamentales. Es decir, los límites impuestos por el empresario deben ser necesarios para lograr un fin constitucionalmente legítimo, y en todo caso, deben ser respetuosos con el contenido esencial del derecho[24].

El juicio de proporcionalidad, que se asentó completamente en la jurisprudencia del TEDH[25] y se promulgó a nivel comunitario en el artículo 52 CDFUE[26], se configura como una herramienta esencial para determinar la validez de posibles acciones limitativas de derechos fundamentales. Su finalidad es determinar si la medida es idónea, necesaria y proporcional para conseguir el fin legítimo. Así, el Tribunal Constitucional entiende que, partiendo de la prevalencia de los derechos, su limitación por las facultades empresariales sólo puede fundamentarse, bien porque la propia naturaleza del trabajo contratado conlleve la restricción del derecho[27], bien por un justificado interés empresarial[28].

En cualquier caso, se pueden enunciar determinadas reglas generales que establecen una relación entre la actividad de control empresarial y los derechos fundamentales de los trabajadores:

En primer lugar, en el momento de la elección del medio empresarial, debe analizarse el cumplimiento del principio de proporcionalidad. Este principio se encuentra dividido en las siguientes pautas[29]:

- Principio de idoneidad: debe justificarse la elección del medio por ser éste apto para satisfacer el interés empresarial. Es decir, la limitación de los derechos

[23] Sentencia del Tribunal Constitucional de 11 de abril de 1994 (RTC 1994/99).
[24] FERNÁNDEZ AVILÉS, J.A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial de la actividad laboral en España", cit., pp. 70-72.
[25] AROLD LORENZ, N.-L; GROUSSOT, X. y PETURSSON, G. T.: *The European Human Rights Culture - A Paradox of Human Rights Protection in Europe?,* Martinus Nijhoff Publishers, Leiden, 2013, p. 81.
[26] Carta de los Derechos Fundamentales de la Unión Europea, de 30 de marzo de 2010 (BOE 30 de marzo de 2010).
[27] Sentencias del Tribunal Constitucional, de 11 de abril de 1994 (RTC 1994/99); y de 12 de junio de 1996 (RTC 1996/106).
[28] Sentencias del Tribunal Constitucional, de 11 de abril de 1994 (RTC 1994/99); de 10 de enero de 1995 (RTC 1995/6); de 23 de julio de 1996 (RTC 1996/136); y de 10 de abril de 2000 (RTC 2000/98).
[29] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", cit., p.12.

fundamentales debe contribuir a la obtención de un fin constitucionalmente legítimo.

- Principio de necesidad: no debe existir otra medida más moderada que permita satisfacer el interés empresarial con la misma eficacia. La eficacia del medio se encuentra relacionada con los sacrificios que se imponen al derecho fundamental del trabajador con respecto al resultado que se alcanza con el medio de control. Es decir, debe compararse la medida empleada por la empresa y otros medios alternativos que esta pudiera haber escogido.
- Juicio de proporcionalidad: la medida debe ser equilibrada o ponderada, entendiéndose que lo es cuando los beneficios que se derivan para el interés general superan a los perjuicios sobre otros valores en conflicto. En este sentido, las exigencias impuestas sobre la justificación de la necesidad de la medida son mayores cuanto mayor sea la intromisión que sufra el ámbito de la intimidad del trabajador derivada del medio de control elegido.

Ahora bien, en el momento de la utilización del medio de control empresarial, debe tenerse en cuenta que, a pesar de que el uso de un medio esté admitido como tal, la utilización de este no siempre se encuentra legitimada, puesto que, en ocasiones, el uso de un medio en sí mismo legítimo puede ocasionar resultados antijurídicos. Es por ello por lo que, en todo caso, para que el empresario pueda hacer uso de un medio de control, se requiere la necesidad en la aplicación del medio, es decir, que exista una finalidad concreta que justifique su utilización, y que el emplazamiento y el empleo del medio sean adecuados y no excesivos con dicha finalidad. En este sentido, cabe decir, en términos generales que, no estaría justificado el control de un teléfono móvil facilitado como instrumento de trabajo a través de un sistema de localización permanente, requiriéndose consentimiento y conocimiento de los trabajadores[30].

A pesar de tratarse de soluciones jurisprudenciales admitidas, es cierto que existe un amplio dinamismo y soluciones divergentes con respecto a lo que concierne a las materias tecnológicas en el ámbito laboral, por lo que existe cierta dificultad en encontrar una unanimidad de criterio en este aspecto. Si bien, existen determinadas pautas básicas, tal como el juicio de proporcionalidad, que aparecen como argumentación principal de los pronunciamientos judiciales referidos a esta materia, cuya puesta en práctica depende del

[30] Sentencia del Tribunal Superior de Justicia del País Vasco de 2 de julio de (JUR 2007/95052).

caso concreto que se presente ante los tribunales, y por tanto cuenta con una marcada circunstancialidad.

Como consecuencia, la intervención por parte del empresario en las comunicaciones de los trabajadores a través de los medios otorgados al trabajador debe quedar condicionada por la existencia de ciertos indicios objetivos que acrediten la necesidad de ejercer el control. Es decir, y según estableció la sentencia del Tribunal Constitucional en resolución del recurso de amparo 2907/2011 (RTC 2013, 170)[31], el control que ejerza la empresa no puede ser caprichoso, sino que debe tener un sustento en una sospecha cierta de que el uso del correo electrónico por parte del trabajador está siendo irregular, existiendo, por tanto, un riesgo de lesión de los intereses empresariales[32]. De esto se deriva que están prohibidos los controles individuales o «controles personalizados» sin que exista ninguna razón objetiva relacionada con el cumplimiento de las obligaciones laborales; lo que implica que el uso del medio de control debe respetar el principio de no discriminación.

2.4.Deber de información o comunicación al trabajador

La superación del triple test de proporcionalidad se erige comúnmente como requisito necesario para acreditar la legalidad del control empresarial, sin embargo, dicha legalidad no se supedita exclusivamente al mismo, sino que los empresarios deben cumplir con la exigencia de la información a los trabajadores sobre la fiscalización de su actividad laboral. Al tratarse de dichos instrumentos de medios que captan datos personales, la empresa debe informar a los trabajadores de forma previa y expresa sobre la posibilidad de llevar a cabo un control de estos, y de la finalidad de control a la que va dirigida.

Resulta necesario, de acuerdo con las exigencias de la buena fe, que la empresa proporcione información a los trabajadores acerca de la existencia de un control y de los medios que van a utilizarse para comprobar la utilización de los usos que se da a los instrumentos informáticos proporcionados por la empresa a los trabajadores. Para ello, será necesario asimismo que la empresa haya determinado las reglas de uso de las herramientas para que los trabajadores conozcan cómo pueden utilizar tales medios

[31] Sentencia del Tribunal Constitucional de 7 de octubre de 2013 (RTC 2013/170).
[32] MIRÓ MORROS, D., "El uso del correo electrónico en la empresa: protocolos internos", cit., p. 2.

puestos a su disposición[33]. De la Sentencia del Tribunal Supremo de 2007[34] - la cual se expondrá más adelante- se deriva la obligación de informar al trabajador de la posibilidad del ejercicio de control por parte del empresario. Según esta, la información del empresario se configura como el vehículo a través del cual se entiende cumplido el requisito de que la intervención de las comunicaciones se ejerza mediante una previsión específica.

Asimismo, sentencias como la STC 29/2013 de 11 de febrero[35] exigen la debida información al trabajador tanto de la existencia de medios de vigilancia como de la finalidad de su implantación para que pueda estimarse la desaparición de la expectativa de intimidad del trabajador. Por otro lado, existen sentencias más flexibles del deber de información, como la STS de 6 de octubre de 2011[36], y STC de 7 de octubre de 2013[37] que estiman implícitamente cumplido dicho deber con la mera prohibición de una determinada conducta, dejando así la puerta abierta a la utilización de medios de control oportunos sin necesidad de informar expresamente al trabajador del uso de estos.

Por tanto, existen soluciones judiciales vacilantes en lo relativo al modo de ejercer el deber de información, y al momento en que se entiende cumplido dicho deber: por un lado, se establece la necesidad de determinar pautas claras del uso de los medios de control y de informar expresamente de la existencia de controles sobre la utilización de los medios informáticos; mientras que, por otro lado y contraviniendo la postura anterior, existen pronunciamientos judiciales que consideran suficiente para justificar el deber de información la prohibición expresa del uso de los medios informáticos para fines personales, puesto que entienden que existe implícitamente una expectativa de control. Es decir, no existe un criterio uniforme acerca del modo en que deben comportarse las empresas con respecto al deber de información, que se erige como un aspecto esencial en el control de los medios de comunicación. Es por ello por lo que, a lo largo del presente trabajo, se tratará de exponer más detalladamente las diversas posturas argumentadas en base a pronunciamientos jurisprudenciales, así como la postura más garantista, y, por tanto, la más recomendada.

[33] FERNÁNDEZ AVILÉS, J.A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial de la actividad laboral en España", *Labour & Law Issues*, vol. 8, núm. 1, 2016, p. 72.
[34] Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7541).
[35] Sentencia del Tribunal Constitucional de 11 de febrero de 2013 (RTC 2013/29).
[36] Sentencia del Tribunal Supremo de 6 de octubre de 2011 (RJ 2011/7699).
[37] Sentencia del Tribunal Constitucional de 7 de octubre de 2013 (RTC 2013/170).

2.5. Efectos de la ilegitimidad del control ejercido por el empresario: prueba ilícita y su efecto sobre la calificación de los despidos

Como se ha venido apuntando a lo largo del presente trabajo, las controversias que surgen entre el uso de los medios tecnológicos en el trabajo y las facultades de vigilancia y control de la empresa tienen incidencia contractual y constitucional. De igual modo, dichas controversias van a tener efectos en el ámbito procesal. La mayor parte de los conflictos suscitados en esta esfera tienen unos elementos comunes: como regla general, se trata de demandas por despido en las que, para acreditar los hechos que se imputan al trabajador, se otorgan medios de prueba que el demandado considera que han sido obtenidos en vulneración de sus derechos de intimidad y de secreto a las comunicaciones[38].

Las consecuencias que pueden tener los conflictos suscitados entre los medios informáticos y su control por la empresa dependen de la consideración del medio de prueba como lícito o ilícito. En caso de que el medio de prueba sea considerado lícito, el incumplimiento de una prohibición de uso personal de los medios informáticos puede ocasionar un despido disciplinario fundamentado en una transgresión de la buena fe contractual. De tal forma, será procedente un despido fundamentado en un incumplimiento reiterado del trabajador de una prohibición del empresario de utilizar de forma privada los medios tecnológicos empresariales, a pesar de que el empresario no haya llevado a cabo auditorías informáticas previas o no haya sancionado por ese motivo previamente[39].

En lo que respecta a la ilicitud de la prueba, su importancia procesal ha sido objeto de numerosos pronunciamientos del Tribunal Constitucional[40], que ha negado el efecto de toda prueba obtenida vulnerando algún derecho fundamental. Los efectos de la prueba ilícita han sido enunciados en el artículo 11 de la Ley Orgánica del Poder Judicial[41] (en adelante, **"LOPJ"**), que establece que «no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales». Por su parte, la Ley Reguladora de la Jurisdicción Social (en adelante, "**LRJS**")[42] incluye determinadas

[38] FALGUERA BARÓ, M. A., *Nuevas tecnologías y poderes empresariales: sus límites y su incidencia en el proceso social,* Gran Canaria, 2016, p. 101.
[39] Sentencia del Tribunal Superior de Justicia de Cataluña de 13 de junio de 2016 (JUR 2016/188647).
[40] Entre otras: SSTC 49/1999, de 5 de abril; 167/2002, de 9 de octubre; 184/2003, de 13 de noviembre; etc.
[41] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).
[42] Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social (BOE 11 de octubre de 2011).

novedades que subrayan una serie de garantías relacionadas con la posible colisión de la práctica de la prueba y su afectación a los derechos fundamentales.

En todo caso, si una prueba es considerada ilícita por un juez o tribunal, su efecto inmediato es la falta radical de eficacia, y, por tanto, la imposibilidad de su admisión como medio probatorio válido. El artículo 90.2 LRJS establece el tratamiento que debe darse a las pruebas que han sido obtenidas mediante una vulneración de los derechos fundamentales, excluyéndolas del proceso: «no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas».

La ilicitud de la prueba obtenida vulnerando los derechos fundamentales ha supuesto un conflicto con respecto a la calificación del despido. Actualmente concurre un amplio debate relacionado con la consideración del despido nulo o improcedente. El debate que se plantea versa sobre un despido que se ocasiona no como consecuencia del ejercicio de la libertad sindical del trabajador, sino por unos hechos que no tienen que ver con los derechos fundamentales del trabajador, pero cuya prueba sí que se ha producido vulnerando los mismos[43]. En este contexto, surgen dos posturas claramente diferenciadas, que defienden tanto la nulidad del despido como la improcedencia de este:

En primer lugar, parte de la doctrina considera que el despido debe ser declarado improcedente, puesto que la vulneración de los derechos fundamentales se encuentra presente en el modo de obtener la prueba, pero no en la calificación del acto extintivo. Esta postura entiende que la infracción constitucional no se ha producido en la motivación patronal de despido, sino que, el motivo extintivo se intenta acreditar mediante el empleo de un medio de prueba cuya obtención sí que proviene de una vulneración de derechos fundamentales y que, por lo tanto, conforme al art. 90.2 LRJS, no podrá admitirse[44]. Los defensores de esta postura consideran que el elemento clave de interpretación es el artículo 55.5 ET, que se refiere a la nulidad del despido, y establece que será nulo «(…) cuando se produzca con violación de derechos fundamentales y libertades públicas del trabajador», y, como tal, la obtención ilícita de un medio de prueba no «contamina» la

[43] LLUCH CORELL, F. J., "La prueba ilícita y sus efectos sobre la calificación del despido. Foro abierto", *Revista de Jurisprudencia El Derecho*, núm. 1, 2015, p. 4.
[44] Véanse al respecto las distintas posiciones de magistrados del orden social en el foro, coordinado por LLUCH CORELL, F. J., "La prueba ilícita y sus efectos sobre la calificación del despido. Foro abierto", cit., pp. 7-12. También, LOUSADA AROCHENA, J.F.; "La prueba ilícita en el proceso laboral", *Revista Doctrinal Aranzadi Social*, núm. 11, 2006, p. 9.

decisión de un despido. Por ello, la calificación de un despido del que no se ha podido acreditar su procedencia, será la propia de un proceso ordinario de despido, es decir, su calificación de improcedente. Esta postura la comparten, entre otros, magistrados de TSJ de Castilla La Mancha (Jesús Rentero Jover), de Cataluña (Sebastián Moralo Gallego), así como decisiones judiciales[45], entre las que destaca la STSJ de Madrid de 5 de mayo de 2008[46], que afirma que «el despido se ha basado en unos hechos concretos que se imputan al trabajador como realizados en su puesto de trabajo y con ocasión de éste y que, de haberse acreditado, podrían ser sancionables por el empresario (…) centrándose el recurrente, para solicitar la declaración de la nulidad, no en la voluntad vulneradora de la empleadora al despedir, sino en la violación de sus derechos fundamentales en la obtención de la prueba de esos hechos imputados, supuesto bien distinto que afectaría, no al despido, sino a la actividad probatoria previa al mismo, de manera que la prueba obtenida con tal vulneración es ilícita y no puede tenerse en ningún caso en cuenta en el proceso, como tampoco aquéllas que derivan de la inicial ilicitud, pero en ningún caso cabría aquí hablar de despido nulo sino improcedente, de conformidad con lo dispuesto en el artículo 55.4 del Estatuto de los Trabajadores».

En segundo lugar, frente a esta postura, se invoca la denominada «doctrina de los frutos del árbol envenado», que proviene de la teoría desarrollada en la Sentencia del Tribunal Supremo (Sala Penal) de 18 de julio de 2002, que se refiere al "efecto dominó". Esta postura sostiene el reconocimiento del despido como nulo, pues considera que la nulidad de la prueba ilícita puede extender sus efectos a la nulidad del acto extintivo, del despido. Dicha argumentación se basa en el mencionado "efecto dominó", que supone que, si una prueba inicial es ilícita, puede producir el decaimiento de las pruebas derivadas de esta, pues «prohibir el uso directo de estos medios probatorios y tolerar su aprovechamiento indirecto constituiría una proclamación vacía de contenido efectivo»[47]. La proyección de esta tesis al ámbito laboral tiene su base en la argumentación de que los artículos 11 LOPJ y 90.2 LRJS establecen la nulidad de la prueba, pero no impiden que dicha nulidad refleje sus efectos sobre el despido, que se encuentra fundamentado en una evidencia nula[48].

[45] Entre otras: SSTSJ Castilla La Mancha 10-06-2014; Madrid 21-03-2014 [EDJ 2014/50774]; STSJ de Madrid 05-05-2008 [REC 4747/2008]; etc.
[46] Sentencia del Tribunal Superior de Justicia de Madrid de 5 de mayo de 2008 (REC 2008/4747).
[47] VIDAL, P., "El control del e-mail de los empleados y los frutos del árbol envenenado", *Actualidad Jurídica Aranzadi*, núm. 924, 2016, (BIB 2016, 9827), p. 2.
[48] LLUCH CORELL, F. J., "La prueba ilícita y sus efectos sobre la calificación del despido. Foro abierto", cit., p. 7.

Asimismo, esta teoría reconoce de forma amplia los derechos fundamentales y, por tanto, cuando la única prueba de los hechos que se imputa en la carta de despido se ha obtenido con vulneración de dichos derechos, el despido debe ser calificado como nulo[49]. Dicha afirmación es matizada en el caso de que existan múltiples pruebas que sustenten el despido y no guarden relación causal con la prueba ilícita, en cuyo caso la presunción de inocencia no se entiende infringida[50], lo que lleva a poder considerar el despido como procedente si el resto de las pruebas justifican el incumplimiento contractual por parte del trabajador. La conclusión de nulidad del despido se obtiene asimismo a la luz de los valores constitucionales, considerando que la calificación del despido como nulo tiene su base en la satisfacción frente al derecho fundamental infringido. Esta tesis es defendida y argumentada por diversos magistrados del TSJ de Valencia (Teresa Pilar Blanco Pertegaz), de Madrid (Ignacio Moreno González-Aller), así como por diversos pronunciamientos judiciales[51], tales como la STSJ País Vasco de 10 de mayo de 2011[52], que considera que la exclusión de las pruebas obtenidas que vulnera los derechos fundamentales se extiende a todos los frutos del árbol envenenado.

[49] LLUCH CORELL, F. J., "La prueba ilícita y sus efectos sobre la calificación del despido. Foro abierto", cit., p. 8.
[50] Sentencia del Tribunal Constitucional de 2 de abril de 1998 (RTC 1998/81); y Sentencia del Tribunal Constitucional de 26 de marzo de 1996 (RTC 1996/54).
[51] Entre otras: SSTSJ Castilla La Mancha 24-03-2009 [REC 1356/2008]; Extremadura 30-07-2014 [284/2014]; así como STC 15-11-2004 [EDJ 2004/157278]; etc.
[52] Sentencia del Tribunal Superior de Justicia del País Vasco de 10 de mayo de 2011 (REC 2011/644).

3. EVOLUCIÓN JURISPRUDENCIAL

3.1. Doctrina del Tribunal Supremo: Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7514)

El control ejercido por el empresario de los medios informáticos puestos a disposición del trabajador ha sido una cuestión de gran relevancia jurisprudencial, habiendo sido analizada por un elevado número de resoluciones judiciales en distintas instancias. A pesar de los numerosos pronunciamientos, hasta la sentencia del Tribunal Supremo de 26 de septiembre de 2007[53] (en adelante, la "**Sentencia**") no se había conseguido alcanzar una conclusión clara sobre el contenido y los límites del control empresarial. Es por ello por lo que la mencionada sentencia tiene gran trascendencia ya que supone una primera unificación acerca del «alcance y la forma del control empresarial sobre el uso por el trabajador del ordenador que se le ha facilitado por la empresa como instrumento de trabajo»[54]. A pesar de que la Sentencia deja algunos puntos sin resolver, tiene amplia importancia y repercusión ya que clarifica determinados aspectos relevantes que se venían discutiendo doctrinal y judicialmente. La Sentencia insiste en que el objeto de la unificación no se trata de la valoración de la conducta del trabajador, sino de la resolución de un problema relativo al alcance y a la forma de control empresarial sobre el uso del ordenador instrumento de trabajo. Es decir, la Sentencia asienta las bases sobre los «límites de control empresarial» sobre el uso del ordenador facilitado por la empresa[55].

La Sentencia versa sobre el despido de un trabajador que prestaba servicios en una empresa como director general, y desempeñaba su puesto de trabajo en un despacho sin llave, en el que disponía de un ordenador que no contaba con clave de acceso. Debido a la existencia de diversos fallos en el sistema del ordenador, se solicitó la intervención de un técnico para que examinara el ordenador, quién encontró varios virus informáticos que eran consecuencia de la navegación por internet por paginas poco seguras. Frente a esto, se procedió a la investigación del ordenador y se encontraron unos archivos en el ordenador de contenido pornográfico que llevaron al despido de este. Las actuaciones de investigación se llevaron a cabo sin la presencia del interesado ni de representantes de los trabajadores. Dicha situación suscitó un conflicto presentado ante los tribunales que se

[53] Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7514).
[54] PONCE RODRÍGUEZ, S., "El poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador. Sentencia del Tribunal Supremo de 26 de septiembre de 2007", *Actualidad Jurídica Uría Menéndez*, núm. 19, 2008, p. 67.
[55] PONCE RODRÍGUEZ, S., "El poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador. Sentencia del Tribunal Supremo de 26 de septiembre de 2007", cit., pp. 67-71.

basaba en determinar si el control ejercido había vulnerado o no el derecho a la intimidad de trabajador.

En primer término, la Sentencia hace alusión al concepto de intimidad, refiriéndose al mismo como «la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario para mantener una calidad mínima de vida humana en nuestro entorno cultural». La Sentencia se refiere a que la utilización de los medios informáticos por parte del trabajador puede suscitar conflictos que incidan en la intimidad personal del trabajador ya que existe cierta tolerancia de un uso personal moderado de los medios laborales del trabajador. Al mismo tiempo, la Sentencia recalca la importancia de considerar los medios puestos a disposición del trabajador como propiedad de la empresa, y cuyo fin es el desarrollo de la prestación laboral, por lo que el uso de estos debe quedar dentro del poder de vigilancia y control del empresario para que este pueda verificar el cumplimiento de las prestaciones laborales[56]. Si bien, la legitimidad de control de la empresa deriva del carácter de instrumento de producción de trabajo del medio controlado en cuestión.

Asimismo, la Sentencia solventa uno de los debates tradicionales con respecto al poder de control empresarial en este ámbito, en lo que respecta al amparo del control empresarial en el artículo 18 ET o en el artículo 20.3 ET. El Tribunal establece que los requisitos legales del artículo 18 ET no pueden aplicarse al control del empresario de los medios informáticos puestos a disposición de sus empleados. El control ejercido por el empresario tiene su sustento en el artículo 20 ET ya que dicho control se justifica por encontrarse dentro del ámbito de ejecución del contrato de trabajo al que pueden extenderse dichos poderes empresariales. La inclusión de dichas medidas de control dentro del ámbito habitual de los poderes de control del empresario se justifica en que el ordenador se configura como un instrumento de producción de titularidad empresarial, a través del cual el trabajador cumple con la prestación laboral, y, por lo tanto, el empresario tiene facultad de controlarlo con el fin de verificar el correcto cumplimiento de la misma. Por el contrario, el artículo 18 ET establece que «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,

[56] MANTECA VALDELANDE, V., "Control del empresario sobre el uso del ordenador por los trabajadores: alcance, contenido y límites", *Actualidad Jurídica Aranzadi*, núm. 749, 2008 (BIB 2008, 456), pp. 5 y ss.

dentro del centro de trabajo y en horas de trabajo». Dicho artículo se refiere a la persona del trabajador y a sus bienes propios, incluidos dentro de su esfera privada, y atribuye al empresario un control que excede de lo que deriva de su posición en el contrato de trabajo. Se trata de registros en los que el empresario actúa fuera del ámbito de ejecución del contrato de trabajo al que se extiende el artículo 20 ET[57]. Por lo tanto, en base a la legitimidad de control en el artículo 20.3 ET, el Tribunal reconoce el establecimiento de límites a ese control, así como el respeto a la dignidad que debe estar presente en el control ejercido en todo momento. En este sentido, considera que la presencia de un representante de los trabajadores o de un trabajador de la empresa no se trata de un requisito necesario que no respete la dignidad del trabajador. En términos generales, el TS concluye lo siguiente[58]:

El TS reconoce la existencia de un hábito social generalizado de tolerancia a determinados usos personales de los medios informáticos. Dicha tolerancia crea una expectativa general de confidencialidad que, a pesar de que no puede ser desconocida, tampoco puede suponer un obstáculo permanente en el control empresarial. Por ello, para salvaguardar la buena fe, la empresa debe establecer las reglas de uso de los medios informáticos- incluyendo prohibiciones absolutas y parciales- y proporcionar información a los trabajadores de los controles de uso que se llevarán a cabo y de las medidas que deban adoptarse para garantizar la correcta utilización de la herramienta de trabajo. Por todo ello, si el ordenador se utiliza de forma privada infringiendo dichas prohibiciones y con conocimiento de los posibles controles, no se entenderá vulnerada la expectativa de intimidad.

Por otro lado, la protección de la intimidad debe ser compatible con la existencia de controles legales de los ordenadores. El TS ha declarado que los archivos temporales del ordenador se incluyen también dentro del ámbito de intimidad personal ya que así lo ha declarado el TEDH al determinar que se encuentran incluidos dentro del artículo 8 del Convenio[59], debido a que dichos archivos pueden contener datos sensibles de intimidad al poder incluir datos relevantes de la vida privada. Por último, la inexistencia de una

[57] PONCE RODRÍGUEZ, S., "El poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador. Sentencia del Tribunal Supremo de 26 de septiembre de 2007", cit., pp. 67-71.
[58] MANTECA VALDELANDE, V., "Control del empresario sobre el uso del ordenador por los trabajadores: alcance, contenido y límites", cit., pp. 5 y ss.
[59] Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma 4 de noviembre de 1950 (BOE 6 de mayo de 1999).

clave de acceso al ordenador no se considera como un obstáculo para la protección de la intimidad, es decir, no implica que el trabajador acepte el acceso a la información de su ordenador.

En conclusión, el TS desestima la pretensión planteada estableciendo que la empresa no llevó a cabo un control legítimo del ordenador puesto que el acceso a los datos vulneró el derecho a la intimidad del trabajador. A pesar de que el ordenador se revisó inicialmente como consecuencia de la existencia de un virus, la actuación de la empresa se extralimitó ya que examinó contenido del ordenador, apoderándose así de un archivo cuyo análisis no se requería para llevar a cabo la reparación, y cuyo control no se llevó a cabo cumpliendo con los requisitos exigidos.

3.2. Doctrina del Tribunal Constitucional: STC 241/2012 (RTC 2012/241) y STC 170/2013 (RTC 2013/170)

Consolidada la solución entablada por el Tribunal Supremo, el Tribunal Constitucional se ha pronunciado sobre el equilibrio entre los derechos fundamentales de los trabajadores y la facultad de control de los empresarios de las herramientas tecnológicas, incluyendo una nueva línea interpretativa.

En primer lugar, la STC 241/2012[60] versa sobre un conflicto en el que intervinieron una trabajadora y una compañera, que habían instalado un programa de mensajería instantánea en el ordenador de la empresa, a través del cual criticaban a sus compañeros, superiores y clientes. Un trabajador, tras encontrar y leer dichos mensajes, lo puso en conocimiento de la empresa, la que, tras revisar el contenido de los mensajes, procedió a despedir a las trabajadoras.

El supuesto planteado no cuestiona como tal la acción de control entablada por la empresa, sino la lesión de derechos fundamentales en el acceso a dichas comunicaciones. El análisis argumental se centra primordialmente en la determinación de la existencia o no de una esfera de privacidad para la trabajadora, es decir, si la trabajadora podía tener una expectativa razonable de privacidad[61]. En este supuesto, el Tribunal Constitucional no hace uso del test de proporcionalidad, y, además, establece que no se vulnera el derecho a la intimidad puesto que los mensajes en este supuesto se consideran como una

[60] Sentencia del Tribunal Constitucional de 17 de diciembre de 2012 (RTC 2012/241).
[61] GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos del trabajo", *Revista Española de Derecho de Trabajo*, núm. 164, 2014, (BIB 2014, 1065), p. 20.

«comunicación abierta», por lo que fue la propia trabajadora la que eliminó la privacidad de sus conversaciones, ya que los mensajes tuvieron lugar en un ordenador de uso común al cual podía acceder cualquier usuario[62].

Con respecto al derecho al secreto de las comunicaciones, el Tribunal Constitucional no cuestiona que, en el desarrollo de la prestación laboral, el trabajador puede efectuar comunicaciones que queden cubiertas por el derecho fundamental al secreto de las comunicaciones, si bien considera que es al empresario a quién le corresponde «fijar las condiciones de uso de los medios informáticos asignados a cada trabajador». En el supuesto en cuestión, el ordenador era de uso común de los trabajadores, por lo que el Tribunal considera que era incompatible con los usos personales, por lo que el secreto de las comunicaciones carece de cobertura constitucional. Asimismo, la empresa había prohibido expresamente a los trabajadores la instalación de programas en el ordenador, por lo que el Tribunal, basándose en la inexistencia de una situación de tolerancia empresarial de la instalación de programas y, por consiguiente, de uso personal, entiende que no podía existir una «expectativa razonable de confidencialidad»[63].

A continuación, el Tribunal Constitucional establece que pueden utilizarse diferentes instrumentos, tales como órdenes, instrucciones o protocolos, para regular el uso de los medios tecnológicos empresariales, con el fin de no privar a la empresa de sus poderes directivos ni permitir cualquier uso de los instrumentos informáticos. Por tanto, parece deducirse que no es suficiente la regulación legal del artículo 20.3 ET para justificar el control de las herramientas informáticas, sino que es necesario además establecer unas pautas de uso de estas[64]. En efecto, el Tribunal Constitucional, prescindiendo del principio de proporcionalidad, afirma que la existencia de pautas de uso de los instrumentos empresariales, y la solución que estas contemplen, deben ser instrumentos en base a los cuales se valore la posible vulneración de los derechos fundamentales del acceso al contenido de los ordenadores de los trabajadores. Es decir, el Tribunal Constitucional establece que «el ejercicio de la potestad de vigilancia o control empresarial sobre tales elementos resultada limitada por la vigencia de los derechos

[62] CARRASCO DURÁN, M., "El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa", cit., p. 4.
[63] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", cit., p. 6.
[64] GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos del trabajo", cit., pp. 20 y ss.

fundamentales, si bien los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin». De todo lo expuesto se deriva que, para el TC, la prohibición empresarial de un uso personal de los medios utilizados por los trabajadores supone que no existe una tolerancia empresarial del uso personal, lo que elimina absolutamente la expectativa de confidencialidad, permitiendo así controlar libremente el uso de los medios que se lleva a cabo por los trabajadores[65].

Por otro lado, el Tribunal Constitucional, en su STC 170/2013[66], reproduce una pauta interpretativa muy similar a la expuesta anteriormente. Esta sentencia versa sobre el despido de un trabajador tras haber comprobado la empresa, a través del acceso al correo electrónico del trabajador en un ordenador de titularidad empresarial puesto a su disposición, que el trabajador estaba proporcionando información de la compañía a una empresa de la competencia.

A pesar de que el Tribunal Constitucional entiende que el correo electrónico se encuentra dentro del ámbito del secreto de las comunicaciones, el mismo considera que no se verifica la existencia de una «expectativa razonable y fundada de confidencialidad» ya que el convenio colectivo de la empresa pertinente tipifica como falta la utilización de los medios informáticos propiedad de la empresa para fines distintos de los exigidos por la prestación laboral. De la tipificación en el convenio de la imposibilidad de uso personal de los ordenadores, el Tribunal Constitucional entiende que se deriva implícitamente la facultad de la empresa de controlar los mismos, y es por ello por lo que considera que el empresario está facultado para fiscalizar el uso del correo electrónico con el objetivo de verificar el cumplimiento de las obligaciones y deberes laborales del trabajador. Es decir, con el fin de acreditar el correcto ejercicio de la facultad de control sobre el uso de los instrumentos informáticos, determinando la existencia o inexistencia de una lesión de un derecho fundamental, debe llevarse a cabo un análisis en base el régimen de uso de estos establecido por el empresario[67]. Por tanto, en el presente supuesto, al prever el convenio

[65] GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos del trabajo", cit., pp. 20 y ss.
[66] Sentencia del Tribunal Constitucional de 7 de octubre de 2013 (RTC 2013/170).
[67] GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos del trabajo", cit., p. 22.

colectivo la prohibición expresa del uso extralaboral de las herramientas informáticas, «el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse, ex art. 20.3 ET, tanto a efectos de vigilar el cumplimiento de la prestación laboral realizada a través del uso profesional de estos instrumentos, como para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo». De dicha afirmación se deduce que el presupuesto recogido en el artículo 20.3 ET parece no ser suficiente para justificar el control empresarial. En relación con la posible lesión de la intimidad, el Tribunal Constitucional alega su falta de vulneración ya que el acceso al contenido de los correos debe valorarse en función de las instrucciones impartidas por el empresario para el uso de las herramientas informáticas, y, por tanto, en virtud de las previsiones convencionales de la empresa, el trabajador no contaba con una expectativa razonable de privacidad. Por último, el Tribunal Constitucional, habiendo descartado la expectativa de privacidad y habiendo afirmado la potestad del empresario de desplegar el control empresarial, lleva a cabo un test de proporcionalidad para examinar si la facultad empresarial ha sido respetuosa con los derechos fundamentales, concluyendo finalmente que sí supera el mencionado test[68].

En suma, el Tribunal Constitucional, al entender como suficiente lo previsto en el ET y en el convenio colectivo para habilitar al empresario a fiscalizar el uso de los medios informáticos, añade una interpretación del control empresarial de los medios tecnológicos novedosa, retrocediendo en lo que respecta a la garantía del derecho a la intimidad y del derecho al secreto de las comunicaciones. Es decir, la doctrina constitucional considera que es suficiente una prohibición expresa del uso personal de los trabajadores de los medios electrónicos puestos a su disposición para legitimar el control ejercido por la empresa de dichos medios, sin requerir informar previamente y de forma expresa a los empleados de la posibilidad de llevar a cabo dicho control.

3.3.Doctrina de los Tribunales Superiores de Justicia

Por regla general, la doctrina de los TSJ ha seguido parámetros similares a los del Tribunal Supremo[69]. Precisamente, no se entiende infringido el art. 18.1 CE en casos en

[68] GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos del trabajo", cit., pp. 20 y ss.
[69] FALGUERA BARÓ, M. A., *Nuevas tecnologías y poderes empresariales: sus límites y su incidencia en el proceso social,* cit., pp. 75-77.

los que el empresario accede a los mensajes personales de los trabajadores en ordenadores de la empresa cuando había avisado previamente de la instalación de un sistema de control[70], o en los casos en los que el trabajador era consciente de la posibilidad de acceso a sus sistemas informáticos por su estipulación en el manual de uso de las herramientas tecnológicas[71]. Asimismo, se ha descartado la intromisión en la vida privada del trabajador en los casos en los que se accede a un contenido del correo electrónico profesional y no personal[72].

De igual forma, existen pronunciamientos de Tribunales Superiores de Justicia que, de forma previa a la STS de 26 de septiembre de 2009[73], venían aplicando garantías del artículo 18 ET en lo que respecta a los medios informáticos en el ámbito laboral[74]. Si bien, como ya se ha argumentado en el apartado correspondiente a la doctrina del Tribunal Supremo, el rechazo de esa tesis se generalizó tras la promulgación de la STS de 26 de septiembre de 2009. Los TSJ en todo caso han ponderado los derechos fundamentales de los trabajadores en relación con el control de la empresa de los medios informáticos, y en varios pronunciamientos han afirmado que en caso de que exista tolerancia empresarial para el uso extraproductivo de los medios tecnológicos, sin existir una prohibición total o parcial al respecto, se entiende que los trabajadores tienen una expectativa de intimidad y, por tanto, el acceso a los registros informáticos supone una intromisión al derecho a la intimidad[75].

También destacan pronunciamientos que valoran el posicionamiento o no de un trabajador en un ámbito de privacidad. En ese sentido, se ha descartado una posible vulneración al artículo 18 CE cuando el ordenador o los programas son de uso común[76], o en los casos en los que el trabajador ha firmado un documento de confidencialidad en el que permite el acceso del empresario a su correo electrónico[77]. Por último, la prueba

[70] Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 5 de octubre de 2010 (REC 2010/2195).
[71] Sentencia del Tribunal Superior de Justicia de Andalucía, Granada de 17 de julio de 2014 (REC 2014/1136).
[72] Sentencia del Tribunal Superior de Justicia de Islas Baleares de 14 de diciembre de 2011 (REC 2011/503).
[73] Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7541).
[74] Entre otras: SSTSJ Cantabria 20-02-2004 [REC 47/2004]; Castilla La Mancha 17-05-2006 [REC 1282/2005]; Comunidad Valenciana 22-12-2005 [REC 3503/2005]; etc.
[75] Entre otras: SSTSJ Asturias 26-07-2013 [REC 1293/2013]; Cantabria 24-06-2009 [REC 381/2009]; País Vasco 27-09-2011 [REC 1973/2011]; etc.
[76] Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 16 de diciembre de 2014 (REC 2014/2422); País Vasco de 18 de octubre de 2011 (REC 2011/2081).
[77] Sentencia del Tribunal Superior de Justicia de Asturias de 30 de enero de 2015 (REC 2015/20).

aportada judicialmente se ha considerado como vulneradora de los derechos fundamentales en supuestos en los que una empresa, sin haber realizado ninguna advertencia en relación con el uso de los ordenadores, instala un programa que monitoriza las conexiones informáticas de un empleado, entendiendo que supone una intromisión en la privacidad del trabajador[78].

[78] Sentencia del Tribunal Superior de Justicia de Madrid 15 de enero de 2010 (REC 2009/4921).

4. DOCTRINA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS Y ADECUACIÓN DE LA RECIENTE DOCTRINA DEL TRIBUNAL SUPREMO

4.1. Barbulescû I y Barbulescû II

La Sentencia del TEDH de 12 de enero de 2016[79], también conocida como Barbulescû I, caso Barbulescû contra Rumanía, versa sobre el acceso por un empresario a las comunicaciones que un trabajador tenía registradas en el ordenador de la empresa, y que había mantenido a través de una cuenta de *Messenger* creada por petición del empresario para entablar conversaciones con los clientes. La empresa, que procedió a una monitorización de la aplicación, evidenció que el trabajador había hecho uso personal de la aplicación. Tras comunicárselo la empresa al trabajador, y éste negarse de lo mismo, la empresa transcribió el contenido de los mensajes, acreditando las conversaciones personales que había entablado el trabajador, lo que determinó el despido del trabajador. Frente a este despido, el trabajador interpuso una demanda ante los tribunales rumanos contraviniendo una vulneración al derecho a la privacidad. Los tribunales rumanos desestimaron la demanda en base a la argumentación de que la empresa había prohibido expresamente el uso de los ordenadores para fines personales. Llevado el caso al TEDH, este llega a la misma conclusión que los órganos rumanos, considerando que no existe violación de la privacidad del trabajador recogido en el art. 8 del Convenio Europeo de Derechos Humanos: el trabajador incumplió el código de conducta de la empresa del uso de las tecnologías puesto que existía una prohibición de uso personal de los medios informáticos, de lo que se deriva que el empresario podía controlar las comunicaciones profesionales de sus trabajadores[80].

Para argumentar el justo equilibrio entre el derecho del trabajador al respeto a su privacidad y los intereses empresariales del supuesto en cuestión, el Tribunal se basó en que el acceso del empresario a las comunicaciones se había fundado en la creencia de este de que tenían contenido profesional (puesto que lo había afirmado el trabajador). Por otro lado, el Tribunal Europeo destaca que el control ejercido por el empresario fue proporcionado (se limitó al control del *Messenger* y no del resto de contenidos del ordenador) puesto que el trabajador podría haber dañado a la empresa con su conducta,

[79] Sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016 (TEDH 2016/1).
[80] PÉREZ DE LOS COBOS ORIHUEL, F., y GARCÍA RUBIO M.A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", *Nueva Revista Española de Derecho de Trabajo,* núm. 196, 2017, (BIB 2017/84), p. 4.

considerando legítimo que el empresario llevase a cabo una comprobación del cumplimiento de las tareas profesionales de sus trabajadores durante las horas del trabajo; teniendo en cuenta a su vez que la empresa había prohibido expresamente el uso de las herramientas informáticas para fines personales.

Por lo tanto, en esta primera resolución el TEDH considera legítima la fiscalización de la empresa de las comunicaciones del trabajador en base a su facultad empresarial de control de la prestación laboral y de la prohibición expresa de la empresa del uso personal de los instrumentos proporcionados por esta; no haciendo mención en ningún caso a la necesidad de comunicación por parte de la empresa del ejercicio de control que podrían llevar a cabo los empresarios[81]. Si bien, ante dicha resolución se erige un voto particular que discrepa de la fundamentación de la decisión del TEDH: considera que el particular no tenía suficiente conocimiento del uso de los medios tecnológicos ni de la limitación del uso personal de los mismos, reconociendo que el control de la empresa debía estar justificado y ser conocido por los trabajadores, no pudiendo erigirse como discrecional ni arbitrario. Por ello, para que la medida fiscalizadora no vulnerara el art. 8 del CEDH, el trabajador debería haber conocido de forma previa y clara la misma, lo que no ocurre en el presente supuesto.

Frente a la resolución de Barbulescû I, y debido a que la sentencia emitida era contraria a los intereses de una de las partes, se solicitó una remisión excepcional de la cuestión a la Gran Sala, que dictó sentencia el 5 de septiembre de 2017[82], conocida como Barbulescû II. Dicha sentencia adquiere gran importancia ya que se trata de la primera vez en la que la Gran Sala hace referencia a la vulneración del art. 8 CEDH por parte de un empresario privado[83].

En primer lugar, la Gran Sala se refiere a que la gran mayoría de los Estados europeos reconocen el derecho a la privacidad de sus trabajadores, pero muy pocos regulan legislativamente el modo en que el empresario debe respetar ese derecho en el ámbito

[81] PÉREZ DE LOS COBOS ORIHUEL, F., y GARCÍA RUBIO M.A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", p. 7.
[82] Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (TEDH 2017/61).
[83] ECHR (2017, 5 de septiembre). Grand Chamber judgement in the case of Barbulescû v. Rumania. https://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF.

laboral de las TIC[84]. Asimismo, el TEDH considera que los tribunales rumanos no han procedido a verificar si el empresario había advertido previamente al trabajador de la posibilidad de fiscalizar sus comunicaciones, así como de la necesidad de que se proporcionase información previa y clara de la naturaleza, alcance y grado de afectación del control en la vida privada del trabajador. Es decir, el TEDH considera que para que se entienda cumplido el art. 8 CEDH, es necesario verificar previamente el cumplimiento de las siguientes cuestiones[85]:

- Informar al trabajador de la posibilidad que tiene el empresario de adoptar medidas con el fin de controlar las comunicaciones del trabajador: dicha información ha de ser clara, y en el presente supuesto no lo ha sido.
- Comprobar el alcance de la vigilancia ejercida por el empresario y el grado de intromisión en la vida privada del empleado: en el supuesto enjuiciado no se especifica si el empresario pudiera haber ejercido el control a través de medios menos intrusivos, ni se detalla por qué la empresa ha optado por el medio más intrusivo ni se explica si se podría haber alcanzado el mismo resultado con medidas menos invasoras.
- Verificar la existencia de intereses legítimos, debidamente justificados por el empresario, que justifiquen el control y acceso a las comunicaciones: en el caso en cuestión no se acreditan las razones que mueven al empresario a fiscalizar la cuenta del trabajador.

Por todo lo expuesto, el TEDH concluye que el derecho de privacidad del trabajador no se ha protegido debidamente, y, por tanto, no ha habido una ponderación adecuada de los intereses del empresario ni del derecho del trabajador, vulnerando así el art. 8 CEDH.

Adquiere especial relevancia que los fundamentos en los que se basa la argumentación de la Gran Sala se equiparan con el canon de enjuiciamiento del principio de proporcionalidad, que elabora un triple test dividido en el principio de idoneidad, principio de necesidad y juicio de proporcionalidad.

[84] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", cit., p. 11.
[85] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", cit., p. 11.

En suma, Barbulescû II se configura como una sentencia de especial relevancia puesto que establece las bases que debe seguir un empresario para controlar el uso de los medios electrónicos de sus empleados en el marco de un contrato laboral[86]. Asimismo, y recordando lo expuesto con anterioridad acerca de la STS de 26 de septiembre de 2007, Barbulescû II reitera la misma doctrina puesto que reconoce la necesidad de proporcionar información al trabajador de la existencia de control, así como de determinar las reglas de uso de los medios informáticos, reconociendo una expectativa razonable de intimidad del trabajador. Al mismo tiempo, la doctrina recogida por la Gran Sala difiere de los posteriores criterios recogidos por el Tribunal Constitucional que entienden cumplido el deber de información de una forma más flexible.

4.2.Sentencia del Tribunal Supremo de 8 de febrero de 2018 (JUR 2018/58399)

Con respecto a la doctrina del TEDH, se ha considerado conveniente analizar el más reciente pronunciamiento del Tribunal Supremo español, la Sentencia del Tribunal Supremo de 8 de febrero de 2018 (JUR 2018/58399), que recoge criterios coincidentes con la doctrina comunitaria. El caso versa sobre la declaración del despido de un trabajador de Inditex basado en una transgresión de la buena fe contractual y abuso de confianza, por haber recibido una cantidad de dinero de una entidad proveedora. La empresa tuvo conocimiento de dicho comportamiento desleal debido a un «hallazgo casual» de unas facturas por parte de un trabajador, tras lo cual, procedió a una revisión de los correos electrónicos del trabajador. Ante esto, el trabajador considera que las pruebas fueron obtenidas ilícitamente por una vulneración a su derecho a la intimidad. El Tribunal Supremo resuelve el caso en base a los siguientes fundamentos:

- En primer lugar, tiene en cuenta que la empresa había prohibido expresamente el uso de los ordenadores para cuestiones personales;
- Asimismo, la empresa contaba con una «política de seguridad de información», y cada vez que un trabajador accedía a su ordenador, se le exigía aceptar las directrices de la política de seguridad, así como se le advertía que la empresa se reservaba el derecho de la adopción de medidas de vigilancia y control;

[86] CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", cit., p. 12.

- El motivo que llevó a la empresa a comenzar el control fue un «hallazgo casual» de unas fotocopias de transferencias recibidas por el trabajador de un cliente, conducta prohibida expresamente;
- El contenido de los correos no fue examinado de «modo genérico e indiscriminado», sino que se buscaron elementos relacionados con las transferencias en cuestión.

Por todo lo expuesto, el TS se basó en cuatro factores primordiales que justificaron la legitimidad de su control y determinaron la procedencia del despido del trabajador: el trabajador tenía conocimiento y había sido informado del derecho de control que podía ejercer el empresario, la empresa tuvo un interés legítimo para actuar, y el grado de intromisión de la empresa fue el menor posible para la consecución de sus objetivos.

En suma, el pronunciamiento más reciente del Tribunal Supremo reitera la doctrina del TEDH y vuelve a adoptar la postura garantista que adoptó años atrás, en 2007, exigiendo una determinación de las reglas de uso del ordenador, así como información expresa al trabajador del ejercicio de control.

5. PROPUESTA Y RECOMENDACIONES A LA EMPRESA

Una vez expuesto el conflicto suscitado entre los intereses de los empresarios y los derechos fundamentales de los trabajadores en el ámbito laboral del uso de los medios tecnológicos, conviene reiterar que no existe un pronunciamiento único acerca del modo en que debe comportarse el empresario en lo que respecta al uso de los medios informáticos en el ámbito laboral, sino que existen numerosos pronunciamientos que, pese a llegar a conclusiones similares, no todas ellas son homogéneas, sino que establecen criterios que difieren en aspectos trascendentales (tal y como lo es el ejercicio del deber de información al trabajador). La realidad es que no existe como tal una regulación legal específica en lo que respecta al uso de los medios informáticos. Esta situación, junto con el incremento continuo de la digitalización de los medios utilizados para el ejercicio de la prestación laboral, ha multiplicado la conflictividad en este punto. Ante esto, los órganos jurisdiccionales se han visto obligados a establecer criterios interpretativos con el fin de dar una solución a los conflictos suscitados entre trabajador y empresario.

Cabe destacar asimismo que la enorme conflictividad que surge con respecto al control del uso de las TIC en el ámbito laboral se debe a que existe una ingente cantidad de casos dispares que pueden suscitarse con respecto a esta cuestión, y, por lo tanto, las soluciones que han ido dando los órganos jurisdiccionales no versan sobre los mismos supuestos, sino que se adhieren a supuestos concretos. Es decir, a pesar de que haya numerosas interpretaciones jurisdiccionales, las mismas versan sobre supuestos distintos, lo que ocasiona que el conflicto suscitado al que nos estamos refiriendo se erija como una cuestión *ad casum* en donde los tribunales responden al caso concreto que se les presenta. Por lo tanto, esto implica que debe llevarse a cabo un análisis individual de cada caso, en base a las circunstancias y características particulares de cada uno, con el fin de evaluar la licitud o no de las mismas[87].

Ahora bien, dentro de la disparidad de las soluciones de los tribunales, adquiere especial relevancia el cambio de criterio que han ido adoptando tanto el Tribunal Supremo como la doctrina constitucional, así como la doctrina asentada por el Tribunal Europeo de Derechos Humanos. Si bien es cierto que en el presente no existe un criterio unificado ni una resolución correcta de los casos que se suscitan en este ámbito, la doctrina que se ha

[87] TOSCANI GIMÉNEZ, D. y CALVO MORALES, D., "El uso de internet y el correo electrónico en la empresa: límites y garantías", *Revista Española de Derecho del Trabajo,* núm. 165, 2014 (BIB 2014/1659), p. 6.

ido exponiendo a lo largo del trabajo da a conocer que es cada vez mayor la preocupación de los tribunales de dar mayores garantías a los trabajadores acerca del posible control que se vaya a ejercer sobre los medios informáticos que den a conocer aspectos de su vida privada. Es decir, en septiembre de 2007, el TS reconoció la importancia informar expresamente al trabajador del control ejercido sobre los medios electrónicos, mientras que, en los años 2012 y 2013, el Tribunal Constitucional flexibilizó este criterio entendiéndolo cumplido con la mera prohibición del uso personal de los medios. En este contexto, surgió la novedosa sentencia Barbulescû I, la que no se refirió de forma expresa a la necesidad de informar de forma clara y previa al trabajador de la fiscalización llevada a cabo por la empresa de los útiles electrónicos. Frente al carácter no definitivo de esta sentencia, surgió la sentencia Barbulescû II que recogió la enorme trascendencia que tiene la comunicación por parte de la empresa de las reglas de uso al trabajador, así como de la necesidad de informar al trabajador del control ejercido por la empresa. Recientemente, ha surgido un pronunciamiento del Tribunal Supremo[88] que sigue las mismas pautas expuestas por el TEDH, destacando la importancia de la información recibida por el trabajador. Es decir, a pesar de que actualmente no se pueda concluir en la existencia de una doctrina uniforme en lo que respecta a estos conflictos, los pronunciamientos más actuales parecen sugerir la adopción de una postura concreta que es la que parece ofrecer mayor seguridad jurídica.

5.1.Pautas clave de la fiscalización de los medios informáticos

El estudio de la presente problemática, así como de los criterios divergentes presentados, hace necesario el desarrollo de unas pautas generales que debe tener en cuenta todo empresario a la hora de fiscalizar el uso del correo electrónico de sus empleados. Dichas pautas, que son fruto de una síntesis de construcciones jurisprudenciales, se erigen como recomendaciones a la empresa.

- En la esfera laboral, las comunicaciones electrónicas que se encuentren en los ordenadores de los trabajadores propiedad de la empresa quedan en principio amparadas por los derechos al secreto de las comunicaciones y a la intimidad[89]. De acuerdo con los usos y costumbres de la realidad social, el uso privativo de los

[88] Sentencia del Tribunal Supremo de 8 de febrero de 2018 (JUR 2018/58399).
[89] PÉREZ DE LOS COBOS ORIHUEL, F., y GARCÍA RUBIO M.A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", cit., p. 3.

ordenadores está generalizado y comúnmente tolerado: siempre dentro de unos límites que respeten la buena fe contractual y el equilibrio de los intereses en cuestión. Es por ello por lo que el uso que se da a los medios de trabajo es, de forma general, bajo una expectativa de confidencialidad e intimidad[90].

- En este contexto, la empresa no tiene acceso libre a las comunicaciones de sus trabajadores, pero, en virtud de su libertad de empresa, posee la facultad de regular y ordenar el uso que llevan a cabo los trabajadores de los medios propiedad de la empresa que ésta pone a disposición de los trabajadores. Las medidas que el empresario adopte con el fin de controlar el uso de los medios informáticos se encuentran dentro de sus facultades de vigilancia y control ya que el ordenador se erige como un instrumento de producción titularidad de la empresa[91]. Si bien, en todo caso, la fiscalización empresarial sobre el uso de los medios debe respetar los derechos fundamentales.
- Debido a la presencia de dos derechos puestos en relación, se valora la existencia de un posible conflicto entre el poder de dirección del empresario y los derechos de los trabajadores al secreto de comunicaciones y a la intimidad: la colisión de estos intereses ocasiona que los derechos fundamentales del trabajador puedan someterse a una modulación, pero únicamente cuando resulte esencial para un desarrollo adecuado de la actividad laboral[92].
- Para que la empresa pueda ejercer control sobre el uso de los medios informáticos, deberá en primer lugar, **establecer las reglas de uso de los medios puestos a disposición del trabajador:** a través de directrices o prohibiciones de uso de los medios informáticos. Es decir, se requiere una comunicación previa a los trabajadores tanto de la política de uso de los ordenadores, como de la política de vigilancia de estos para legitimar el control empresarial. La empresa no está obligada a permitir cualquier uso sobre los medios informáticos; por lo que puede admitir cierto uso personal, pero también puede prohibir y limitar el uso a fines estrictamente laborales. En este sentido, a pesar de que tanto el TC como el TS hayan otorgado validez a las prohibiciones absolutas de utilización personal de

[90] GARCÍA SALAS, A.I. "La adopción de medidas empresariales de vigilancia y control de la prestación de trabajo". En GARCÍA SALAS, A.I. *Necesidades empresariales de vigilancia y control de la prestación de trabajo.* Madrid, 2016, pp. 2.
[91] Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7514).
[92] PÉREZ DE LOS COBOS ORIHUEL, F., y GARCÍA RUBIO M.A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", cit., p. 3.

los instrumentos que el empleador pone a disposición del empleado, se han erigido críticas que establecen la necesidad de cierto margen de permisividad con el fin de que se puedan atender necesidad personales y familiares, coadyuvando así la conciliación personal y laboral[93]. En determinados casos, dichas prohibiciones absolutas se han considerado vulneradoras del derecho a la dignidad del trabajador. Esto se debe a que el contrato de trabajo no se erige para incomunicar al trabajador, «instalándose, en la organización empresarial en la que presta servicios, en una situación de soledad hacia el exterior; y, de su lado, la titularidad de esos medios y herramientas tampoco confiere al empresario un derecho a restricciones caprichosas»[94]. Dada la importancia que implica el uso del correo para el mantenimiento de comunicaciones sociales de los trabajadores, siempre que éstas no impliquen un apartamiento de las tareas del trabajador o un perjuicio para la empresa, ésta ha de considerar la posibilidad de uso personal del ordenador por el trabajador que depende de un debate constitucional, no pudiendo resolverse de forma exclusiva con una advertencia a los trabajadores[95].

Asimismo, el TC ha reconocido la necesidad de fijar las condiciones de uso de los útiles informáticos a través de instrumentos tales como órdenes, instrucciones, protocolos y códigos de buenas prácticas. Uno de los instrumentos más utilizados para informar a los trabajadores del uso que deben hacer de los medios informáticos son los códigos de conducta o códigos éticos. En los mismos, el empresario puede establecer las condiciones de conducta, así como prohibiciones absolutas o parciales del uso del ordenador. Si bien, en todo caso, dichas prohibiciones y condiciones deben respetar las leyes y los preceptos constitucionales, configurándose como un desarrollo estricto de la facultad de control empresarial, amparado en el art. 20 ET[96]. Debe tenerse en cuenta que los códigos unilaterales de conducta no deben ir «más allá de las exigencias derivadas del programa obligacional deducido del contrato»[97], como sería exigir a un trabajador que mantenga un equipo informático.

---

[93] SAN MARTÍN MAZZUCCONI, C. "Navegar por internet en horas de trabajo… ¿Quién? ¿Yo?", *Aranzadi Social,* parte Presentación, 2010, (BIB 2010/147).
[94] Voto particular STC 241/2012 (RTC 2012/241).
[95] Sentencia del Tribunal Superior de Justicia del País Vasco de 6 de noviembre de 2007 (AS 2008/1556).
[96] CALVO GALLEGO, F.J., *Códigos éticos y derechos de los trabajadores.* Ediciones Bomarzo. Publicación 5.1.2009, p. 68.
[97] CALVO GALLEGO, F.J., *Códigos éticos y derechos de los trabajadores.* Cit., p.75.

Con el objetivo de otorgar mayor seguridad al trabajador, adquiere relevancia que la empresa establezca en los códigos internos de la empresa tanto la descripción de los comportamientos que puede realizar y de los que no, como la determinación clara de cuáles son las acciones permitidas y cuáles las prohibidas. Asimismo, resulta conveniente establecer qué nivel de gravedad tiene cada conducta llevada a cabo por el trabajador, así como la consecuencia punible que tendría su infracción. De tal forma, el trabajador tendría conocimiento de las consecuencias de su actuar, y el empresario tendría un soporte sobre el cual poder apoyarse para poder sancionar a un trabajador que realiza conductas indebidas[98].

- La empresa, asimismo, tiene la facultad de **ejercer el control del cumplimiento de las directrices:** dicho control lo ejercerá a través de medidas adoptadas en virtud de las facultades de control y vigilancia del empresario, que, en todo caso, deben respetar el juicio de proporcionalidad, con el fin de determinar si la acción de fiscalización empresarial es o no excesiva respecto a la afectación que sufre la privacidad del trabajador[99]. Para que se cumpla el juicio de proporcionalidad, la medida debe ser proporcional (equilibrada y ponderada), necesaria (que concurra un fin legítimo) e idónea (que el medio sea apto para satisfacer el interés empresarial). El grado de intensidad de la fiscalización ejercida por el empresario va a depender de las condiciones de uso y disposición establecidas en cada caso. Es decir, el poder de control empresarial sobre el uso de los medios informáticos no es absoluto, discrecional y arbitrario, requiriéndose una justificación que vaya más allá de la mera productividad[100]. Si se ocasiona una colisión entre los poderes de control del empresario y los derechos fundamentales del trabajador, el sacrificio de estos debe ser necesario, adecuado y no excesivo[101], debiendo ponderarse tanto el derecho del trabajador como el poder del empresario.

  La existencia de un fin legítimo empresarial es necesario para que la empresa pueda llevar a cabo la fiscalización, no cabiendo, por tanto, la fiscalización

[98] TOSCANI GIMÉNEZ, D. y CALVO MORALES, D., "El uso de internet y el correo electrónico en la empresa: límites y garantías", cit., p. 10.
[99] PÉREZ DE LOS COBOS ORIHUEL, F., y GARCÍA RUBIO M.A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", cit., p. 4.
[100] FALGUERA BARÓ, M. A., *Nuevas tecnologías y poderes empresariales: sus límites y su incidencia en el proceso social,* cit., p. 101.
[101] Sentencia del Tribunal Constitucional de 1 de febrero de 2000 (RTC 2000/98); y de 10 de julio de 2000 (RTC 2000/186).

gratuita. Dicho fin legítimo excluye el deseo de obtener información privada acerca de los trabajadores que no guarde relación con la prestación laboral. Si bien, la empresa puede encontrar abundantes intereses legítimos amenazados, tales como el gasto que le ocasiona directamente un uso incorrecto de los medios, así como la falta de dedicación a actividades laborales que se utiliza en intereses personales, o incluso el temor de que se estén ocasionando situaciones de mayor gravedad, tales como la competencia desleal o el espionaje industrial.

- Por último, la empresa tiene la **necesidad de proporcionar información a los trabajadores acerca de la existencia de medidas de control** en base al respeto al derecho de intimidad de los trabajadores, tal y como recoge la STS de 16 de septiembre de 2007 (RJ 2007/7514). Dicha exigencia aparece matizada en variadas sentencias, estableciendo criterios más flexibles, considerando que la prohibición absoluta del uso personal del ordenador como suficiente para romper la expectativa razonable de intimidad. Sin embargo, siguiendo los criterios más garantistas adoptados por la jurisprudencia más reciente[102], parece conveniente que la empresa informe explícitamente a los trabajadores del control que ejercerá. Es decir, con el fin de que la empresa se evite problemas de justificación del control ejercido, será ventajoso que esta otorgue información directa al trabajador, con el fin de que tenga conocimiento de la posibilidad de que la empresa ejerza dicho control.

5.2. Situaciones a las que se puede enfrentar un empresario y manera de actuar frente a las mismas

A pesar de que existen criterios contundentes de los tribunales, cada vez más garantistas, la realidad es que, debido a la existencia de una gran variedad de casos y conflictos suscitados en relación con el control de los instrumentos informáticos, a continuación, se va a proceder a recopilar las situaciones más destacadas a las que se han visto expuestas empresas y trabajadores, y, en base a distintos pronunciamientos judiciales, se van a incluir recomendaciones acerca de la posible respuesta que puede otorgar empresa ante la situación planteada:

[102] STS de 26 de septiembre de 2007 (RJ 2007/7514); STEDH de 5 de septiembre de 2017 (TEDH 2017/61), y STS de 8 de febrero de 2018 (JUR 2018/58399).

i. En el caso de que se consiga información de un trabajador debido a una situación de «hallazgo casual».

- Como «hallazgo casual» debe entenderse aquella situación en la que la empresa conoce información personal del trabajador sin haber investigado de forma activa[103]. En este supuesto, la actuación empresarial es consecuencia de dicho hallazgo, por lo que no se entiende que la empresa haya obtenido la información a través de una intromisión ilegítima.
- Sin embargo, debe distinguirse esta situación de «hallazgo casual» de otras situaciones en las que, a pesar de que la entrada inicial en el ordenador esté justificada, no implica necesariamente que la actuación empresarial posterior a la entrada en el ordenador sea consecuencia de un «hallazgo casual». Es decir, en caso de que la entrada en el ordenador del trabajador por parte del empresario se encuentre justificada por la existencia de un virus, si la actuación empresarial va más allá de las tareas de reparación, y la empresa se apodera de archivos no necesarios para dicha reparación, la empresa está llevando a cabo una intromisión ilegítima en los datos del trabajador[104]. Por todo ello, en este supuesto, la entrada en el ordenador como consecuencia del «hallazgo casual» no estaría justificada, al realizar la empresa acciones que van más allá[105].

  Es decir, en el supuesto de «hallazgo casual» únicamente se entenderá justificada la obtención de información por parte de la empresa siempre y cuando dicha información se limite a aquella que el empresario ha obtenido sin buscar de forma activa. En el momento que el empresario obtenga información por llevar a cabo actuaciones adicionales, se entenderá que existe una intromisión ilegítima de la empresa, sin encontrarse justificada.

ii. En el caso de que exista una prohibición expresa del uso personal de los trabajadores de los sistemas informáticos.

- En numerosos criterios jurisprudenciales, se matiza la exigencia de información ya que se considera que la prohibición expresa elimina la expectativa razonable de intimidad por no darse una situación de tolerancia del uso personal, por lo que no se

[103] Sentencia del Tribunal Superior de Justicia de Madrid de 8 de mayo de 2013 (AS 2013/2695).
[104] Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7514).
[105] GARCÍA SALAS, A.I. "La adopción de medidas empresariales de vigilancia y control de la prestación de trabajo". En GARCÍA SALAS, A.I. *Necesidades empresariales de vigilancia y control de la prestación de trabajo.* Madrid, 2016, p. 2.

requiere informar expresamente del control realizado, bastando con la prohibición. Dicha flexibilidad de la exigencia se ve expuesta en los siguientes pronunciamientos:

- **STS de 6 de octubre de 2011 (RJ 2011/7699):** la instalación de un software espía de los ordenadores no vulnera el derecho a la intimidad ni el derecho al secreto de las comunicaciones por encontrarse absolutamente prohibido su uso personal. El caso versa sobre una trabajadora que utiliza inadecuadamente el ordenador, no respetando las instrucciones de la empresa ya que la empresa había prohibido expresamente el uso personal de los medios electrónicos. En base a que el trabajador había sido informado previamente de la prohibición absoluta del uso personal del ordenador, se considera que no se puede argumentar la intimidad del trabajador, y, por lo tanto, la empresa puede llevar a cabo una fiscalización de la actividad del trabajador[106], sin estar vulnerando el derecho a la intimidad del trabajador.
- **STC de 7 de octubre de 2013 (RTC 2013/170):** el acceso a ficheros informáticos de correos privados del trabajador no vulnera el derecho al secreto de comunicaciones por existir una prohibición expresa del uso extralaboral del mismo. En este caso, el TC faculta a la empresa a intervenir el contenido de los correos de un trabajador fundamentando su argumentación en que el convenio colectivo aplicable a dicha empresa prohibía expresamente que los trabajadores diesen un uso a los medios electrónicos que difiriese de los medios estrictamente laborales. De tal forma, la intervención de la empresa en las comunicaciones electrónicas del trabajador se basa en una facultad de control implícita, derivada de una prohibición convencional.

- Criterios jurisprudenciales más recientes no han considerado suficiente la existencia de una prohibición expresa del uso personal de los ordenadores para entender cumplido el deber de información del control ejercido, y no entender vulnerada la expectativa de intimidad y confidencialidad. Es decir, dichos pronunciamientos han exigido que se informe al trabajador de forma expresa sobre la posibilidad del ejercicio de control sobre los medios informáticos para que este no tenga expectativa de confidencialidad y se justifique dicho control[107].

[106] TOSCANI GIMÉNEZ, D. y CALVO MORALES, D., "El uso de internet y el correo electrónico en la empresa: límites y garantías", cit., p. 6.
[107] STS de 26 de septiembre de 2007 (RJ 2007/7514), STEDH de 5 de septiembre de 2017 (TEDH 2017/61), y STS de 8 de febrero de 2018 (JUR 2018/58399).

Siguiendo esta postura, se recomienda a la empresa que no lleve a cabo un control de los medios electrónicos del trabajador sin haberles informado expresa y previamente de la posibilidad de dicho control, puesto que la aplicación a dichos supuestos de criterios jurisprudenciales más garantistas no permitiría justificar el control del empresario en base a una prohibición expresa del uso privado de los medios.

iii. En el supuesto de que la imposibilidad del uso de los medios electrónicos proporcionados por la empresa para fines laborales se encuentre tipificada en el convenio colectivo.

Dicho supuesto tiene relación con el caso presentado anteriormente, ya que se refiere a la forma en la que un empresario debe informar del ejercicio de fiscalización a los trabajadores para que se entienda justificado el control ejercido:

- Por un lado, pronunciamientos judiciales han considerado que el carácter vinculante del convenio colectivo implica de forma implícita que el empresario tiene facultad de supervisar el correo electrónico del trabajador[108].
- Por otro lado, pronunciamientos más recientes[109] han exigido proporcionar información expresa, clara y precisa del control que pueda ejercer el empresario para que no se entienda vulnerada la expectativa razonable de intimidad. Es decir, en este sentido, han surgido críticas[110] con respecto a la fundamentación exclusiva del acceso al correo electrónico en base a la prohibición del uso personal del mismo en el convenio colectivo aplicable a la empresa. Dichos pronunciamientos alegan la insuficiencia del convenio pata poder sancionar una determinada conducta, y abogan por la necesidad de transmitir de forma explícita qué conductas están prohibidas y cuáles están permitidas.

iv. En el supuesto de que la empresa acceda a un ordenador de uso común y sin clave de acceso (caso STC 241/2012).

Un ordenador de uso común se configura comúnmente como un medio de comunicación abierta que permite el acceso a toda persona, pues en ningún caso se encuentra sujeto a una restricción de acceso. Así, puede entenderse que no existe expectativa de

[108] Sentencia del Tribunal Constitucional de 13 de octubre de 2013 (RTC 2013/170).
[109] STEDH de 5 de septiembre de 2017 (TEDH 2017/61), y STS de 8 de febrero de 2018 (JUR 2018/58399).
[110] TOSCANI GIMÉNEZ, D. y CALVO MORALES, D., "El uso de internet y el correo electrónico en la empresa: límites y garantías", cit., p. 14.

confidencialidad, por lo que no se requiere el consentimiento de un tercero para su utilización[111]. Como consecuencia:

- La instalación de un programa de mensajería en un ordenador de uso común implica el permiso voluntario del acceso de cualquier usuario, conllevando así la eliminación de privacidad de las conversaciones (STC 241/2012).
- El uso compartido de los medios de trabajo, que permite a cualquier tercero acceder libremente a un ordenador se conoce como comunicación abierta. Dicha comunicación implica que no se requiere que el empresario advierta previamente de la preservación de los datos y del acceso a ellos de terceros (STC 170/2013).

  Es decir, numerosos pronunciamientos jurisprudenciales han evidenciado la omisión de la expectativa de confidencialidad en la información recogido en un ordenador común sin clave de acceso.

v. Ante el supuesto en que el trabajador está llevando a cabo actos abusivos e ilegales y surja la necesidad de corroborar una infracción.

Debe tenerse en cuenta que la realización de comportamientos abusivos o la sospecha de comisión de delitos a través de los medios informáticos puestos a disposición del trabajador no requieren ser prohibidos por la empresa expresamente, ya que se trata de comportamientos sancionados por la propia normativa laboral[112]. A continuación, se analizará la necesidad o no de informar expresamente del ejercicio de control ante la sospecha de una irregularidad cometida por los trabajadores, debido a la posible frustración de la investigación que la información de dicho control pueda suponer. El análisis jurisprudencial que se va a exponer seguidamente se centra en la videovigilancia de los empresarios, y no en el uso de los medios informáticos, si bien, sus conclusiones son extrapolables al ámbito del control de las comunicaciones electrónicas de los empleados.

- Determinados pronunciamientos judiciales han entendido que las sospechas fundadas de la comisión del trabajador de irregularidades en el ejercicio de su prestación laboral, así como el posible perjuicio a la empresa justifican el establecimiento de medidas, aunque las mismas no se hubiesen comunicado. Dicho criterio es reconocido en los siguientes pronunciamientos:

[111] TOSCANI GIMÉNEZ, D. y CALVO MORALES, D., "El uso de internet y el correo electrónico en la empresa: límites y garantías", cit., p. 13.
[112] Sentencia del Tribunal Superior de Justicia de la C. Valenciana de 19 de julio de 2005 (AS 2005/3205).

- **Sentencia del Tribunal Constitucional de 10 de julio de 2000 (RTC 2000/186)**
  En julio de 2000[113], el Tribunal Constitucional consideró que la instalación de una cámara de videovigilancia secreta en tres cajas registradoras era una medida aceptable puesto que superaba el triple test: «tenía un objetivo legítimo ("un test de conveniencia"), necesario ("una prueba de necesidad") y proporcional ("una estricta prueba de proporcionalidad")». Es decir, en la decisión del Tribunal, careció de importancia la ausencia de comunicación de dicha medida de control tanto al Comité de empresa como a los trabajadores afectados puesto que se había ponderado un «justo equilibrio» entre la importancia que tenía el fin legítimo perseguido- resolver la irregularidad que se estaba cometiendo- y la injerencia en el derecho fundamental del trabajador. Por lo tanto, en este supuesto, el TC, ante la existencia de una sospecha fundada de la comisión de una irregularidad, considera que no se requiere informar al trabajador del control ejercido por la empresa. El fundamento de este argumento se basa en la prioridad que se otorga a la protección de los intereses empresariales frente al derecho de información del trabajador, puesto que el otorgamiento de dicha información puede frustrar la consecución del fin legítimo empresarial[114]- poner fin a las irregularidades.

- Pronunciamientos jurisprudenciales más recientes no han considerado suficiente para justificar el control ejercido por la empresa la protección de los intereses empresariales ante la posible frustración de una investigación por la proporción de información acerca del control ejercido, recalcando la necesidad de informar al trabajador de forma expresa de la fiscalización llevada a cabo por el empresario de los medios informáticos:
  - **Sentencia del Tribunal Constitucional de 3 de marzo de 2016 (RTC 2016/39)**
    En este supuesto, una empresa instaló de forma temporal cámaras de videovigilancia encubiertas apuntando a una caja registradora por la detección de ciertas irregularidades, y a su vez, instaló de forma general una señal que indicaba la presencia de videovigilancia. Ante esto, el TC concluyó en que la medida era justificada (existían sospechas razonables), idónea para verificar las irregularidades, necesaria y equilibrada (la grabación únicamente grabó la zona

[113] Sentencia del Tribunal Constitucional de 10 de julio de 2000 (RTC 2000/186).
[114] GARCÍA SALAS, A.I., "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018", *Revista de Información Laboral*, núm. 2, 2018, (BIB 2018/6596), p. 2.

de la caja). Asimismo, argumentó que el artículo 18.4 ET relativo a la protección de datos no se violó debido a la información proporcionada acerca de la videovigilancia.

Al contrario que el caso anterior, a pesar de que el TC hace referencia a la justificación, idoneidad, necesidad y equilibrio de la medida; también se refiere a la necesidad de la información para legitimar dicho control. El TC adopta por tanto un criterio más garantista que años atrás; si bien, únicamente se exige que se proporcione dicha información de forma general, y no de forma expresa, clara y precisa[115] como ocurre en otros supuestos en los que no concurre una irregularidad.

- **Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018 (TEDH 2018/1)**

  Dicha sentencia versa sobre un conflicto que surge debido a ciertas irregularidades que se estaban ocasionando en un supermercado entre la mercancía almacenada y las ventas reales. Como consecuencia de lo mismo, la empresa procedió a la instalación de cámaras, tanto ocultas como visibles, con el fin de controlar dichas irregularidades. Si bien, únicamente informó a los empleados y al comité de empresa de la existencia de las cámaras visibles y en ningún caso de las ocultas. Dichas cámaras capturaron a las empleadas sustrayendo artículos, por lo que fueron despedidas. Frente a esto, las demandantes ejercitaron acciones hasta que los tribunales acabaron por admitir la licitud de la obtención de las grabaciones como pruebas.

  Una vez elevada la cuestión al TEDH, las demandantes consideraron que la vigilancia encubierta suponía una violación al art. 8 del CEDH. El TEDH en este caso, no consideró que la omisión de información a las trabajadoras se encontraba justificada por la sospecha fundada de robo, como ocurría en la STC 186/00 (RTC 2000/186), sino que consideró que la instalación de cámaras ocultas de un trabajador en su puesto laboral, sin informarle previamente, se erige como una injerencia al derecho a la vida privada del trabajador[116], pues las trabajadoras

[115] STEDH de 5 de septiembre de 2017 (TEDH 2017/61), y STS de 8 de febrero de 2018 (JUR 2018/58399): en base a los criterios asentados, se debería exigir información suficiente y específica con carácter previo del control ejercido- en este caso, la instalación de las videograbaciones.

[116] PRECIADO DOMÈNECH, C.H., "Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalta y otras c. España", *Revista de Información Laboral,* núm. 1, 2018, (BIB 2018/6060), pp. 5-7.

tenían en todo caso una expectativa razonable de privacidad. Asimismo, establece que la empresa no respetó la legislación vigente que establecía la necesidad de informar acerca de la existencia de un sistema de captación de datos, así como las finalidades de este. Es decir, el TEDH considera que la proporcionalidad de las medidas adoptadas no es suficiente como para legitimar la videovigilancia encubierta, a pesar de existir indicios de la comisión de una infracción. Por lo tanto, el TEDH, en contra de la resolución de los tribunales españoles, resuelve que no se llevó a cabo una justa ponderación entre el interés de la empresa de proteger su derecho a la propiedad, y el derecho a las trabajadoras del respeto a su derecho a la privacidad.

Por consiguiente, la doctrina más reciente ha supuesto un criterio modificador del requisito del deber de información del control ejercido por el empresario en caso de que exista una sospecha fundada de la comisión de una infracción, estableciendo la necesidad de proporcionar dicha información para que no se vulnere la expectativa razonable de privacidad de los trabajadores. En base a esta doctrina cada vez más garantista, actualmente, resulta conveniente que toda empresa adopte esta postura con el fin de evitar cualquier conflicto, informando así a sus trabajadores del ejercicio de control que puede ejercer sobre el uso de los medios electrónicos de sus empleados.

6. CONCLUSIONES

El objetivo principal de la realización del presente trabajo de investigación era el análisis del control empresarial de la utilización por parte de los empleados de los medios informáticos puestos a su disposición. El especial interés de la presente cuestión se encontraba en la existencia de cierta controversia debido a la inexistencia de una regulación legal específica, haciendo depender su solución en las interpretaciones jurisprudenciales dadas en cada caso, careciendo así de un criterio uniforme. Es por ello por lo que en la realización del trabajo, se ha llevado a cabo un ejercicio de síntesis y análisis tanto doctrinal como jurisprudencial con el fin de obtener una conclusión acerca del modo en que debe ejercerse dicho control, que ha sido la siguiente: la manera más garantista y que aporta mayor seguridad jurídica tanto a los trabajadores como a las empresas del ejercicio de control, es otorgar información clara y expresa a los empleados tanto de las reglas de uso de los medios electrónicos como del ejercicio de control de los medios que puede llevar a cabo la empresa. Para la consecución del objetivo principal, el trabajo ha tratado de analizar determinados objetivos específicos, que han permitido concluir lo siguiente:

El medio informático primordial del que dispone un trabajador para llevar a cabo su prestación laboral es el ordenador, que se configura como un medio a través del cual el trabajador ejecuta su contrato de trabajo. Dicha configuración del ordenador como ejecutor del contrato laboral concede al empresario, en base al artículo 20 ET, a ejercer facultades de organización y control sobre el mismo, con el fin de verificar el correcto cumplimiento del desarrollo profesional del trabajador. En este contexto, el trabajador considerado como ciudadano, también cuenta con derechos fundamentales que se ponen en relación con las facultades de control del empresario. Asimismo, debido a la existencia de cierta tolerancia empresarial, el trabajador tiene la facultad de utilizar de forma moderada el ordenador para fines personales, lo que supone una expectativa razonable de intimidad y privacidad del trabajador. Por lo tanto, en el momento que el empresario ejerce el control sobre el ordenador, debe en todo caso respetar el derecho a la intimidad y el derecho al secreto de las comunicaciones del trabajador. Sin embargo, en aras del cumplimiento de la buena fe contractual, el empresario tiene la facultad de modular la eficacia de tales derechos con el fin de poder ejercer su potestad de control, siempre y cuando dicha modulación responda a un fin legítimo. Es decir, se permite que el empresario ejerza un poder de control sobre los medios informáticos puestos a disposición

del trabajador, limitando así sus derechos fundamentales, siempre que cumpla con unos determinados requisitos. A pesar de que los requisitos del ejercicio de control no estén legalmente determinados, la doctrina y jurisprudencia analizadas han permitido llegar a conclusiones válidas con el objeto de otorgar recomendaciones a las empresas acerca del modo en que deben actuar:

El empresario debe, primeramente, establecer previamente las reglas de uso de los dispositivos electrónicos, recogiendo claramente qué se le permite y qué se le prohíbe realizar al trabajador, con el fin de que este cuente con información clara tanto de sus posibilidades de actuación, como de las consecuencias que tiene llevar a cabo una conducta fraudulenta. Para ello, resulta conveniente recoger dichas medidas en códigos internos de conducta de la empresa, a los que tenga acceso todo trabajador. En segundo lugar, la empresa puede ejercer el control del cumplimiento de las directrices siempre que respete el juicio de proporcionalidad con el fin de evitar un grado de fiscalización excesivo; es decir, la medida ha de ser proporcional, necesaria e idónea, respondiendo siempre a un fin legítimo, evitando así la fiscalización gratuita. Por último, la empresa debe proporcionar a los trabajadores información acerca de la posibilidad de ejercer control sobre los medios electrónicos, con el fin de que el trabajador sea consciente del control ejercido, eliminando así la expectativa razonable de privacidad del trabajador. En suma, para evitar problemas de inseguridad jurídica, será conveniente que la empresa adopte la postura más garantista, y comunique a los trabajadores acerca del control existente de forma clara y expresa, sin erigirse la prohibición expresa del uso personal de los medios electrónicos como una facultad implícita de control.

7. BIBLIOGRAFÍA, LEGISLACIÓN Y JURISPRUDENCIA

7.1. Bibliografía

1. AROLD LORENZ, N.-L; GROUSSOT, X. y PETURSSON, G. T., *The European Human Rights Culture - A Paradox of Human Rights Protection in Europe?*, Martinus Nijhoff Publishers, Leiden, 2013.
2. CARRASCO DURÁN, M., "El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa", *Revista Aranzadi Doctrinal*, núm. 9, 2014, (BIB 2013, 2695).
3. CUADROS GARRIDO, M.E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", *Revista Aranzadi Doctrinal*, núm. 10, 2017, (BIB 2017, 43157).
4. FALGUERA BARÓ, M. A., *Nuevas tecnologías y poderes empresariales: sus límites y su incidencia en el proceso social*, Gran Canaria, 2016.
5. FERNÁNDEZ AVILÉS, J.A. y RODRÍGUEZ-RICO ROLDÁN, V., "Nuevas tecnologías y control empresarial de la actividad laboral en España", *Labour & Law Issues,* vol. 8, núm. 1, 2016.
6. GARCÍA SALAS, A.I. "La adopción de medidas empresariales de vigilancia y control de la prestación de trabajo". En GARCÍA SALAS, A.I. "Necesidades empresariales de vigilancia y control de la prestación de trabajo", Madrid, 2016, pp. 1-10.
7. GARCÍA SALAS, A.I., "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018", *Revista de Información Laboral*, núm. 2, 2018, (BIB 2018/6596).
8. GARCÍA SÁNCHEZ, J.D. Y GARCÍA BEL, M., "El poder de control del empresario sobre el correo electrónico de sus trabajadores. A propósito de la Sentencia de la Sala de lo Penal del Tribunal Supremo de 16 de junio de 2014", *Revista de Actualidad Jurídica Uría Menéndez,* núm. 39, 2015.
9. GIL PLANA, J., "Control empresarial del uso personal por el trabajador de los medios tecnológicos del trabajo", *Revista Española de Derecho de Trabajo*, núm. 164, 2014, (BIB 2014, 1065).
10. LLUCH CORELL, F. J., "La prueba ilícita y sus efectos sobre la calificación del despido. Foro abierto", *Revista de Jurisprudencia El Derecho*, núm. 1, 2015.

11. MANTECA VALDELANDE, V., "Control del empresario sobre el uso del ordenador por los trabajadores: alcance, contenido y límites", *Actualidad Jurídica Aranzadi*, núm. 749, 2008 (BIB 2008, 456).
12. MIRÓ MORROS, D., "El uso del correo electrónico en la empresa: protocolos internos", *Actualidad Jurídica Aranzadi*, núm. 874, 2013, (BIB 2013, 2511).
13. MUÑOZ RUIZ, A.B., "Convergencia y divergencia entre los Tribunales del Orden Social y la Agencia Española de Protección de Datos en materia de control informático de la prestación de trabajo", *Revista española de Derecho del Trabajo*, núm. 156, 2012, (BIB 2012,3125).
14. PÉREZ DE LOS COBOS ORIHUEL, F. Y GARCÍA RUBIO, M. A., "El control empresarial sobre las comunicaciones electrónicos del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", *Nueva Revista Española de Derecho del Trabajo*, núm.196, 2017, (BIB 2017, 814).
15. PÉREZ DE LOS COBOS ORIHUEL, F., y GARCÍA RUBIO M.A., "El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", *Nueva Revista Española de Derecho de Trabajo*, núm. 196, 2017, (BIB 2017/84).
16. PONCE RODRÍGUEZ, S., "El poder de control empresarial sobre los medios informáticos puestos a disposición del trabajador. Sentencia del Tribunal Supremo de 26 de septiembre de 2007", *Actualidad Jurídica Uría Menéndez*, núm. 19, 2008.
17. PRECIADO DOMÈNECH, C.H., "Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalta y otras c. España", *Revista de Información Laboral*, núm. 1, 2018, (BIB 2018/6060).
18. SANMARTÑIN MAZZUCCONI, C., "Navegar por internet en horas de trabajo… ¿Quién? ¿Yo?", *Aranzadi Social*, parte Presentación, 2010, (BIB 2010/147).
19. TOSCANI GIMÉNEZ, D. y CALVO MORALES, D., "El uso de internet y el correo electrónico en la empresa: límites y garantías", *Revista Española de Derecho del Trabajo,* núm. 165, 2014 (BIB 2014/1659).
20. TRUJILLO PONS, F., "El uso del correo electrónico en el ambiente laboral y el modo en que éste puede afectar al derecho a la intimidad personal y al secreto de las comunicaciones", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2016, (BIB 2016/4123).

21. VIDAL, P., "El control del e-mail de los empleados y los frutos del árbol envenenado", *Actualidad Jurídica Aranzadi*, núm. 924, 2016, (BIB 2016, 9827).

7.2.Legislación

7.2.1. Legislación estatal y autonómica

1. Constitución Española (BOE 29 de diciembre de 1978).
2. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).
3. Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social (BOE 11 de octubre de 2011).
4. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE 24 de octubre de 2015).

7.2.2. Legislación comunitaria

5. Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma 4 de noviembre de 1950 (BOE 6 de mayo de 1999).
6. ECHR (2017, 5 de septiembre). Grand Chamber judgement in the case of Barbulescû v. Rumania. https://www.echr.coe.int/Documents/Press_Q_A_Barbulescu_ENG.PDF.

7.3.Jurisprudencia

7.3.1. Jurisprudencia Comunitaria

1. Sentencia del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (TEDH 1997/37).
2. Sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007 (TEDH 2007/23).
3. Sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016 (TEDH 2016/1).
4. Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (TEDH 2017/61).
5. Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018 (TEDH 2018/1).

7.3.2. Jurisprudencia Española

6. Sentencia del Tribunal Constitucional de 29 de noviembre de 1984 (RTC 1984/2014).

7. Sentencia del Tribunal Constitucional de 11 de abril de 1994 (RTC 1994/99).
8. Sentencia del Tribunal Constitucional de 10 de enero de 1995 (RTC 1995/6).
9. Sentencia del Tribunal Constitucional de 26 de marzo de 1996 (RTC 1996/54).
10. Sentencia del Tribunal Constitucional de 12 de junio de 1996 (RTC 1996/106).
11. Sentencia del Tribunal Constitucional de 23 de julio de 1996 (RTC 1996/136).
12. Sentencia del Tribunal Constitucional de 2 de abril de 1998 (RTC 1998/81).
13. Sentencia del Tribunal Constitucional de 10 de abril de 2000 (RTC 2000/98).
14. Sentencia del Tribunal Constitucional de 10 de julio de 2000 (RTC 2000/186).
15. Sentencia del Tribunal Constitucional de 17 de diciembre de 2012 (RTC 2012/241).
16. Sentencia del Tribunal Constitucional de 7 de octubre de 2013 (RTC 2013/170).
17. Sentencia del Tribunal Constitucional de 11 de febrero de 2013 (RTC 2013/29).
18. Sentencia del Tribunal Constitucional de 3 de marzo de 2016 (RTC 2016/39).
19. Sentencia del Tribunal Supremo de 26 de septiembre de 2007 (RJ 2007/7541).
20. Sentencia del Tribunal Supremo de 6 de octubre de 2011 (RJ 2011/7699).
21. Sentencia del Tribunal Supremo de 21 de septiembre de 2017 (RJ 2017/4310).
22. Sentencia del Tribunal Supremo de 8 de febrero de 2018 (JUR 2018/58399).
23. Sentencia del Tribunal Superior de Justicia de Cantabria de 20 de febrero de 2004 (REC 47/2004).
24. Sentencia del Tribunal Superior de Justicia de Castilla La Mancha de 17 de mayo de 2006 (REC 2005/1282).
25. Sentencia del Tribunal Superior de Justicia de la C. Valenciana de 19 de julio de 2005 (AS 2005/3205).
26. Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 22 de diciembre de 2005 (REC 2005/3503).
27. Sentencia del Tribunal Superior de Justicia de Castilla La Mancha de 17 de mayo de 2006 (REC 2005/1282).
28. Sentencia del Tribunal Superior de Justicia del País Vasco de 2 de julio de 2007 (JUR 2007/95052).

29. Sentencia del Tribunal Superior de Justicia del País Vasco de 6 de noviembre de 2007 (AS 2008/1556).
30. Sentencia del Tribunal Superior de Justicia de Madrid de 5 de mayo de 2008 (REC 2008/4747).
31. Sentencia del Tribunal Superior de Justicia de Castilla La Mancha de 24 de marzo de 2009 (REC 2008/1356).
32. Sentencia del Tribunal Superior de Justicia de Cantabria de 24 de junio de 2009 (REC 381/2009).
33. Sentencia del Tribunal Superior de Justicia de Madrid 15 de enero de 2010 (REC 2009/4921).
34. Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 5 de octubre de 2010 (REC 2010/2195).
35. Sentencia del Tribunal Superior de Justicia del País Vasco de 10 de mayo de 2011 (REC 2011/644).
36. Sentencia del Tribunal Superior de Justicia del País Vasco de 27 de septiembre de 2011 (REC 1973/2011).
37. Sentencia del Tribunal Superior de Justicia del País Vasco de 18 de octubre de 2011 (REC 2011/2081).
38. Sentencia del Tribunal Superior de Justicia de Islas Baleares de 14 de diciembre de 2011 (REC 2011/503).
39. Sentencia del Tribunal Superior de Justicia de Asturias de 26 de julio de 2013 (REC 1293/2013).
40. Sentencia del Tribunal Superior de Justicia de Madrid de 21 de marzo de 2014 (EDJ 2014/50774).
41. Sentencia del Tribunal Superior de Justicia de Andalucía, Granada de 17 de julio de 2014 (REC 2014/1136).
42. Sentencia del Tribunal Superior de Justicia de Extremadura de 30 de julio de 2014 (RC 2014/284)
43. Sentencia del Tribunal Superior de Justicia de Andalucía de 4 de septiembre de 2014 (AS 2014/3148).
44. Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 16 de diciembre de 2014 (REC 2014/2422).
45. Sentencia del Tribunal Superior de Justicia de Asturias de 30 de enero de 2015 (REC 2015/20).

46. Sentencia del Tribunal Superior de Justicia de Cataluña de 13 de junio de 2016 (JUR 2016/188647).