



FACULTAD DE DERECHO

EL CONTROL EMPRESARIAL SOBRE LOS MEDIOS INFORMÁTICOS Y CORREOS ELECTRÓNICOS

Análisis de la sentencia de la Gran Sala del Tribunal
Europeo de Derechos Humanos de 5 de septiembre de 2017
(Caso Barbulescu vs. Rumanía)

Autora: Alba López Juan
5ºE3C
Derecho Laboral
Tutora: María José López Álvarez

RESUMEN

El presente estudio trata de profundizar en el clásico conflicto entre los derechos fundamentales del trabajador y el poder de control del empresario, en el marco de una sociedad donde la irrupción de las tecnologías ha alcanzado el ámbito laboral. En concreto, se abordan las implicaciones legales de la inspección empresarial del correo corporativo y de los medios informáticos puestos a disposición del trabajador para el desarrollo de la prestación laboral. La ausencia de regulación específica acerca de esta materia en nuestro ordenamiento ha dado lugar a un creciente protagonismo de la labor interpretativa de los tribunales, que a través de sus resoluciones, tratan de resolver esta controversia. Precisamente por ello, este estudio analiza la reciente sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Barbulescu vs Rumania) y la influencia que ésta podría tener en los tribunales y empresas españolas. Si bien se trata de un caso contra Rumanía, lo cierto es que existen muchas expectativas de que la doctrina sentada por esta sentencia produzca un giro jurisprudencial en nuestro país, hacia posiciones más proteccionistas de los derechos de los trabajadores. En consecuencia, los empresarios españoles parecen estar abocados a un escenario en el que deberán extremar las precauciones y actuar más cautelosamente en el ejercicio de su derecho de control sobre los medios informáticos.

Palabras clave: control empresarial, expectativa de intimidad, derechos fundamentales, medios informáticos, correo electrónico, Tribunal Europeo de Derechos Humanos, Barbulescu.

ABSTRACT

The present study tries to look at the classic conflict of the fundamental rights of the employee and the power of control of the employer, in the framework of a society where the irruption of technologies has already reached the workplace. Specifically, the study addresses the legal implications of employer's inspection of the computer media and corporate mail made available to the personnel for their work performance. The lack of specific regulation on this matter in our legal system has given rise to a growing role of the interpretive work of the courts, which, through their resolutions, try to put an end to this controversy. Precisely for this reason, this study analyses the recent ruling of the European Court of Human Rights on September 5, 2017 (Barbulescu v. Romania case) and the influence that it could have on Spanish courts and companies. Although it is a case against Romania, the truth is that there are many expectations that the doctrine established by this ruling will produce a jurisprudential turn in our country, once again taking a more protectionist position in favour of the employee. As a result, Spanish companies seem to be heading to a scenario in which they must pay extreme attention and act more cautiously in the exercise of their right of corporate control over computer media.

Keywords: *employer control, privacy expectation, fundamental rights, computer media, e-mail account, European Court of Human Rights, Barbulescu.*

ÍNDICE

1. INTRODUCCIÓN	6
2. MARCO NORMATIVO	10
2.1 Normativa interna	10
2.2 Normativa comunitaria	14
2.3 Derecho comparado en Europa.....	17
3. JURISPRUDENCIA ESPAÑOLA	18
3.1. Doctrina del Tribunal Constitucional.....	18
3.2. Doctrina del Tribunal Supremo	20
4. LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES DEL TRABAJADOR EN EL ÁMBITO LABORAL	24
4.1. Teoría contractualista.....	24
4.2. Test de la tripe proporcionalidad	25
5. CONSECUENCIAS DE LA VULNERACIÓN DE LOS DERECHOS FUNDAMENTALES EN CASO DE DESPIDO	28
5.1 Teoría de la improcedencia.....	28
5.2. Teoría de la nulidad	30
6. SENTENCIA DE LA GRAN SALA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS DE 5 DE SEPTIEMBRE DE 2017 RELATIVA AL CASO BARBULESCU	33
6.1. Resumen de los hechos	33
6.2. Fallo de la Gran Sala.....	35
7. INFLUENCIA DE LA SENTENCIA BARBULESCU EN LOS TRIBUNALES ESPAÑOLES	38
8. PAUTAS DE ACTUACIÓN PARA LOS EMPRESARIOS ESPAÑOLES TRAS LA DOCTRINA BARBULESCU	42
8.1. Principio de transparencia informativa	42
8.2. Principio de causalidad	47
8.3. Principio de proporcionalidad.....	50
8.4. Principio de efectividad de la tutela.....	53
9. CONCLUSIONES	55
10. BIBLIOGRAFÍA	59

LISTADO DE ABREVIATURAS

BOE	Boletín Oficial del Estado
CE	Constitución Española de 1978
CEDH	Convenio Europeo para la Protección. de los Derechos Humanos y Libertades fundamentales, de 4 de noviembre de 1950
ET	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
LOPDCP	Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPJ	Ley orgánica 6/1985, de 1 de julio, del Poder Judicial
LRJS	Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social
LECrim	Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
STSJ	Sentencia del Tribunal Superior de Justicia
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia

1. INTRODUCCIÓN

En pleno siglo XXI, la tecnología está cada vez más presente en la sociedad, no sólo en su vertiente económica sino también social. Si bien las empresas están desarrollando sistemas productivos más eficientes de mano de las nuevas tecnologías, las personas, a su vez, en su dimensión privada, hacen uso de las mismas para relacionarse con lo demás. A medida que la tecnología va adoptando un papel cada vez más importante en nuestras vidas, se va introduciendo, de manera paralela, en el ámbito laboral, provocando profundos cambios en la relación entre empleados y empleadores, y dando lugar a múltiples litigios judiciales¹.

Las nuevas tecnologías presentan enormes posibilidades en el control del cumplimiento de las obligaciones de los empleados, de ahí su presencia cada vez mayor en el entorno laboral. Son múltiples las herramientas de fiscalización que la tecnología brinda, desde las más tradicionales cámaras de video vigilancia hasta mecanismos sofisticados de localización o identificación de los empleados (GPS, tarjetas de acceso), pasando por los registros de los ordenadores de uso empresarial y por la monitorización de los correos electrónicos y otras modalidades de mensajería instantánea². De hecho, la fiscalización por parte del empresario de estas últimas, se ha convertido en una de las más frecuentes manifestaciones del clásico conflicto entre el poder de control empresarial y los derechos fundamentales de los empleados³.

Dentro de las TIC's, el correo electrónico es la forma de mensajería más utilizada por las empresas como herramienta de comunicación. El fax, muy habitual en los años 80 del siglo

¹ MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B.M, “ El control empresarial del correo electrónico tras la STC 170/2013”, *Revista Doctrinal Aranzadi Social*, n.11, 2014 (disponible en <http://aranzadi.aranzadidigital.es/maf/app/document?docguid=I50f9e6308e1c11e3a97d01000000000&srguid=i0ad82d9a000001629c95754705e90db7&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificationMagazines=&fechacomun=&numeropub-tiponum> ; última consulta 04/04/2018)

² CUADROS GARRIDO, M. E., “La mensajería instantánea y la STEDH de 5 de septiembre de 2017”, *Revista Aranzadi Doctrinal*, n.11, 2017 (disponible en

³ PÉREZ DE LOS COBOS, 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 del trabajo*, n. 196, 2017, p.42.

XX, ha sido sustituido por el correo electrónico y ha quedado relegado al pasado por ser de poca utilidad en una sociedad cada vez más moderna⁴. Debido a infinitas ventajas brindadas por el correo electrónico en el ámbito laboral (como, por ejemplo, la inmediatez o facilidad de alcance), éste se ha convertido en una herramienta fundamental para las empresas del siglo XXI, por permitir un importante ahorro de tiempo en sus comunicaciones. Sin embargo, estas ventajas se pueden convertir en armas de doble filo, ya que pueden ser utilizadas para fines ajenos a la actividad laboral.

De hecho, el uso privado por parte de los empleados de los dispositivos electrónicos propiedad del empleador, ha evolucionado de forma más rápida que la capacidad de adaptación de muchas empresas⁵, que aún no han desarrollado un protocolo o política de uso relativa a los medios informáticos puestos a disposición del trabajador, ni tampoco han incorporado en sus convenios de manera expresa referencia alguna a esta materia. Precisamente es ahí, cuando nace el problema de la expectativa razonable de intimidad, y la posible vulneración de los derechos fundamentales por parte del empleador en el ejercicio de sus facultades de control.

A pesar de que el poder de dirección empresarial se fundamenta en el “principio de libertad de empresa” reconocido en el artículo 38 CE⁶, el empresario no debe pasar por alto la primacía de los derechos constitucionales del trabajador, que representan verdaderos límites formales y materiales de las facultades de control. Es decir, el poder del empleador que

⁴ RUBIO ALAMILLO, J., “El correo electrónico como prueba en los procedimientos judiciales”, *Diario la Ley*, n.8808, 2016 (disponible en http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAEAE2QTU DMAyGf01zqYT SbmPjkAPduCGEoHB3E9MasmTLR7f-e9yVA5EeJY5f2698zhimFq9JFbmWIX6ypfYhoC Rok6hyFJ-rRxpz_9HX55Cxcg5KdKX1kSOv0dCR0CUOv7MhTWAx3pqZotaliJPzbjqlitFgi6qSspiq2cqZsWsmQ2zZXb Mw5yTAnTKYA9eq2p-04gtdGofDAYmklJkXwC-4ZR1Q8iDv7yAiP1kMi7BsIykoxRh1byqVf31XonRgyRBeqTeraNYqB-eGbSoo8IQQ-v0KNqcjxnNHAH8XQV1v2wlfdbepGOHbDFzuB1D8E8OjMvUID8cGw1gv2vXdo2OSUe3SW35IS2fB8g4Z7X5syf6V-u9iN_lgEAAA==WKE; última consulta 05/04/2017).

⁵ MIRÓ MORROS, D., “El uso del correo electrónico en la empresa: protocolos internos”, *Actualidad jurídica Aranzadi*, n. 874, 2013 (disponible en <http://aranzadi.aranzadigital.es/maf/app/document?docguid=I57e7962057e111e39a4901000000000&srguid=i0ad82d9b000001629caa97e704e0e05c&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificacionMagazines=&fechacomun=&numeropub-tiponum=>; última consulta el 04/04/2018).

⁶ Constitución española (BOE 29 de diciembre de 1978).

emana del art 38 CE no se constituye como un derecho arbitrario⁷, en cuanto que ha de coordinarse con el respeto a los derechos fundamentales que el empleado, como cualquier ciudadano, posee, no sólo en el ámbito personal, sino también en el laboral.

El Estatuto de los trabajadores⁸, por su lado, reconoce en su art 20.3 la legitimidad del empresario para ejercer su derecho a tomar todas las medidas que estime oportunas para verificar el cumplimiento por parte del trabajador de sus obligaciones y deberes laborales. La crítica recurrente al mencionado artículo es su obsolescencia en el marco de una realidad tecnológica que se aleja mucho de aquella vigente en el momento de su redacción. Lo cierto es que nadie atisbó el desarrollo tan vertiginoso de las nuevas tecnologías y su influencia en el ámbito de las relaciones laborales, siendo prueba de ello las limitaciones del actual art 20.3 ET.

La referida ausencia de legislación específica sobre el control empresarial de las comunicaciones electrónicas ha multiplicado los litigios. En consecuencia, se está produciendo una progresiva judicialización de los conflictos, ya que son los jueces los que, a través de su interpretación, establecen los criterios limitativos del ejercicio del poder empresarial y de la subsecuente vulneración de los derechos fundamentales de los trabajadores. En consecuencia, la labor interpretativa realizada por los tribunales nacionales (Tribunal Constitucional y Tribunal Supremo) e internacionales (Tribunal Europeo de Derechos Humanos) ha adquirido un papel muy preponderante en los últimos tiempos.⁹

Precisamente por el mencionado protagonismo de la jurisprudencia en esta materia, el objetivo general del presente trabajo es analizar la influencia de la reciente sentencia “Barbulescu” de 5 de septiembre de 2017 de la Gran Sala del Tribunal Europeo de

⁷ FABREGAT MONFORT, G., “El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave”, *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, n. 5, 2015, p.76.

⁸ 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).

⁹ PÉREZ DE LOS COBOS, F. y GARCÍA RUBIO, M. A., “El control empresarial sobre las comunicaciones electrónicas del trabajador...”, *ob.cit.*, p. 43.

Derechos Humanos¹⁰ en la resoluciones judiciales de nuestros tribunales y en los protocolos o reglamentos internos de las empresas.

Este objetivo general se concreta en los siguientes objetivos específicos: a) describir el marco normativo; b) exponer la jurisprudencia española sobre el control de los medios informáticos; c) conocer el nivel de protección de los derechos fundamentales del trabajador en el ámbito laboral; d) analizar el despido como consecuencia de la inspección empresarial; e) estudiar en profundidad la reciente sentencia Barbulescu del TEDH; f) identificar posibles consecuencias de este fallo en los tribunales españoles y, g) extraer pautas de actuación para los empresarios de nuestro país.

Cada uno de estos objetivos se desarrolla en un capítulo independiente del trabajo que, además, consta de un apartado final de conclusiones y de otro de referencias bibliográficas.

Finalmente, la fuente de información fundamental será la jurisprudencia española y la sentencia del TEDH relativa al caso Barbulescu. Asimismo, se utilizarán publicaciones académicas, revistas doctrinales y manuales de derecho laboral.

¹⁰ Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, nº procedimiento 61496/08 (caso Barbulescu vs. Rumanía).

2. MARCO NORMATIVO

2.1 Normativa interna

El ordenamiento español no incluye normativa que aborde de manera específica los límites al ejercicio del control empresarial, pero sí reconoce tanto a nivel constitucional como legislativo los derechos de los trabajadores y del empresario.

- Constitución española

La Carta Magna recoge, en su art 38, la **libertad de empresa** dentro de una economía de mercado. Esta libertad, que en su sentido más amplio se refiere a las facultades de control empresarial, se concreta, a su vez, en una serie de poderes específicos. En primer lugar, el poder de dirección en sentido estricto, que permite al empresario organizar la actividad diaria de la empresa. En segundo lugar, la facultad del empleador de alterar las condiciones no esenciales del contrato (*“ius variandi”*), de acuerdo con los procedimientos establecidos en la ley y en el convenio. Por último, el poder disciplinario, que faculta al empresario a imponer sanciones a los empleados si éstos incumplen con las obligaciones contractuales.¹¹

Sin embargo, todas estas facultades no son, por su carácter y localización, derechos fundamentales, ya que, a pesar de estar la libertad de empresa recogida en el Título I de la Constitución, no se encuentra entre los artículos 10 y 30 de la Carta Magna. El ejercicio del derecho de control empresarial debe, por tanto, cohonestarse con el respeto de los derechos fundamentales constitucionalmente reconocidos, entre los que cabe mencionar el derecho a la protección de datos, el derecho a la intimidad, y el derecho al secreto de las comunicaciones. Cabe, no obstante, recalcar que estos derechos fundamentales no son derechos absolutos y, por ello, pueden ceder ante otros intereses relevantes, como el correcto desarrollo de la actividad productiva, siempre que su limitación sea proporcionada y esté dirigida a un fin constitucionalmente legítimo¹².

¹¹ FABREGAT MONFORT, G., “El control empresarial de los trabajadores a través ...”, *ob.cit.*, p. 76.

¹² RODRÍGUEZ ESCANCIANO, S, “El control empresarial de la mensajería electrónica como prueba de la transgresión de la buena fe contractual: A propósito de la STC de 7 de octubre de 2013, *Diario La Ley*, n.8195, 2013 (disponible en http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAE1RS08DIRD-NeVCYugr1QMHu-3BRI2xq_dZmG5RCivMtt1_76zsQZIP5vHNI_npMQ013kJP-oWam72XJgZK0Us8dwkzJAdeWpQe5BIDhi9Ms14ptCDRo6E_7bgMzgCHnqPsUo8NTCGUIOSW87iJNtm)

De hecho, en una sentencia de julio de 1993²³, el TC hace referencia al derecho de autodeterminación informática y lo define como el control que toda persona tiene sobre sus propios datos, pudiendo ésta oponerse a su uso ilícito, es decir, a su uso para fines distintos a aquel por el que fueron obtenidos²⁴.

En esta línea, la Agencia Española de Protección de Datos ha considerado que el empresario puede controlar el contenido del correo electrónico de los trabajadores siempre que, por un lado, dicha cuenta sea de titularidad de la empresa y se haya puesto a disposición del empleado para el desempeño de sus funciones y, por otro lado, se haya informado al trabajador sobre la posible fiscalización, los medios de control empleados y las conductas no permitidas²⁵. Asimismo, el trabajador deberá tener siempre acceso a la información personal de la que dispone el empresario, para poder rebatirla en caso de considerarla perjudicial²⁶.

Por último, es posible que las medidas de control adoptadas por el empresario vulneren el derecho a la **libertad de información** reconocido en el art 20.1 CE. Recientemente, RTVE ha anunciado que implantará sistemas de control sobre los correos electrónicos de los periodistas, lo que ha disparado el debate de los derechos que se pueden ver afectados por el ejercicio del control empresarial. En empresas de este tipo, cabe incorporar a la lista un cuarto derecho: la libertad de información, que incluye el secreto profesional y el derecho a no desvelar las fuentes²⁷.

²³ Sentencia del Tribunal Constitucional de 20 de julio 254/1993.

²⁴ DESDENDATO BONETE, A. y MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, p.185.

²⁵ SAN MARTÍN MAZZUCCONI, C. , *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, Eolas, León, 2014, p. 224.

²⁶ CUADROS GARRIDO, M. E., “La mensajería instantánea y la STEDH de 5 de septiembre de 2017”, *ob.cit.*

²⁷ SÁNCHEZ, L. J. , “¿Pueden las empresas controlar el correo electrónico de sus trabajadores?”, *Confilegal*, 2018 (disponible en <https://confilegal.com/20180209-pueden-las-empresas-controlar-el-correo-electronico-de-sus-trabajadores/>; última consulta 02/04/2018).

- Estatuto de los trabajadores

En un nivel jerárquico inferior a la Constitución, el Estatuto de los Trabajadores recoge de manera genérica el poder de vigilancia y control en el art. 20.3, que dice así: “ El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por parte del trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana [.....]”²⁸.

Este artículo, no obstante, no establece los criterios limitativos del control empresarial, y recoge, únicamente, conceptos generales.

En este sentido, la ausencia de legislación que determine específicamente los casos en los que el empresario, en el ejercicio de su potestad fiscalizadora, atenta contra los derechos fundamentales del trabajador, refuerza la importancia de la labor interpretativa de los tribunales.

2.2 Normativa comunitaria

Más allá de la normativa interna, España es un Estado miembro de la Unión Europea y, como tal, está adherida a una serie de convenios que abordan, entre otras cosas, aspectos relativos a los derechos de los ciudadanos.

Con respecto al derecho a la intimidad y a las comunicaciones familiares, cabe destacar el Convenio europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales²⁹ que reconoce en su artículo 8 el derecho a que la vida privada, el domicilio y la correspondencia sean respetados. La autoridad no puede entrometerse en el ejercicio de este derecho salvo que existan razones de seguridad nacional, bienestar económico, orden público o protección de los derechos fundamentales, entre otras.

²⁸ 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).

²⁹ Convenio Europeo para la Protección. de los Derechos Humanos y Libertades fundamentales, de 4 de noviembre de 1950 (BOE 10 octubre de 1979).

De acuerdo con la jurisprudencia del TEDH³⁰, los controles ejercidos por el empresario pueden considerarse como un atentado contra su derecho a la vida privada, ya que el art.8 CEDH se interpreta de manera extensiva e incluye las restricciones que puedan imponerse en el ámbito profesional. De esta manera, se estará vulnerando el derecho a la vida privada si dichas restricciones repercuten en la identidad social del empleado y en su forma de relacionarse con los demás.

Por otro lado, a pesar de estar derogada por el Reglamento de Protección de Datos, la Directiva 96/45/CE³¹ reconocía una serie de principios que eran muy utilizados por los tribunales comunitarios, ya que regulaban el control del uso de internet y del correo electrónico en el ámbito laboral. Estos principios son los siguientes³²:

1. El principio de necesidad: la medida de control se considerará necesaria si es imprescindible para alcanzar el objetivo perseguido.
2. El principio de finalidad: El control empresarial debe estar dirigido a una finalidad legítima (principio de legitimidad), específica y explícita.
3. Principio de transparencia: se debe informar a los empleados sobre los sistemas de control utilizados como herramientas de fiscalización.
4. Principio de proporcionalidad: debe existir un equilibrio entre las medidas de control y datos personales sometidos a vigilancia, y la finalidad que se persigue con dicho control.
5. Principio de seguridad: el empresario deberá ofrecer cuantas garantías sean necesarias con el objeto de evitar que los datos personales del empleado sean accesibles para terceros.

³⁰ Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, n° procedimiento 61496/08 (caso Barbulescu vs. Rumanía).

³¹ Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE 23 de noviembre de 1995).

³² Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, n° procedimiento 61496/08 (caso Barbulescu vs. Rumanía).

Sin perjuicio de que muchos tribunales siguen inspirando su fallos en dichos principios, la Directiva fue derogada en 2016 por el Reglamento General de Protección de Datos³³, que contiene los siguientes principios sobre el tratamiento de los datos personales del empleado:

- Principio transparencia: el empleador debe tratar de manera lícita, real y transparente los datos personales, debiendo ser capaz de demostrarlo e incurriendo en responsabilidad si no lo hace (principio de responsabilidad proactiva).
- Principio de minimización: el empresario debe limitarse a acceder a aquellos datos personales que son necesarios para cumplir con la finalidad perseguida.
- Principio de seguridad: se debe garantizar la integridad y confidencialidad en el trato de los datos personales, ofreciendo protección frente a un tratamiento ilícito o desautorizado.
- Principio de exactitud: los datos deben estar actualizados, de manera que el empleado tendrá derecho a que se supriman aquellos que no sean exactos.
- Principio de limitación del plazo de conservación: los datos personales serán conservados durante un periodo limitado, de acuerdo con la finalidad perseguida.
- Principio de proporcionalidad: debe existir un equilibrio entre el derecho de protección de datos y los otros derechos e intereses en conflicto.

Por último, cabe destacar el convenio del Consejo de Europa³⁴ para la protección de personas físicas en lo relativo al tratamiento automatizado de datos de carácter personal, ratificado por España en 1984 y en vigor desde 1985, que recoge los requisitos de legitimidad, transparencia, finalidad, necesidad, exactitud y limitación en el plazo de conservación, así como garantías adicionales a la persona concernida.

³³ Reglamento 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOUE 4 de mayo de 2016).

³⁴ Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de datos de carácter personal (BOE 15 de noviembre de 1985).

2.3 Derecho comparado en Europa³⁵

La sentencia del TEDH de 5 de septiembre relativa al caso Barbulescu, incluye un estudio de la legislación comparada en materia de control empresarial del correo electrónico, cuyos aspectos más relevantes se exponen a continuación.

La mayor parte de los estados miembros reconocen, bien a nivel constitucional, o bien a nivel legislativo el derecho a la vida privada o intimidad, al secreto de las comunicaciones y a la protección de datos. No obstante, son muy pocos los que recogen una legislación específica de estas materias en el ámbito del derecho laboral. Al igual que España, países como Portugal Eslovaquia, Reino Unido, Finlandia o Luxemburgo no cuentan con normas relativas al derecho a la intimidad, secreto de las comunicaciones o protección de datos en el ámbito laboral (ni como parte de la legislación del trabajo, ni mediante leyes especiales).

Algunos países, no obstante, sí recogen normas específicas que regulan directamente requisitos para el ejercicio de la potestad de control empresarial y exigen al empresario la notificación al empleado con carácter previo al control o vigilancia. Ejemplo de ello son las leyes vigentes en Lituania, Grecia, Austria o Polonia.

En materia de control de la mensajería electrónica, son varios los países (Alemania, Francia o Italia, entre otros) que permiten la monitorización de los correos electrónicos marcados como “privados “sin que, sin embargo, se pueda acceder al contenido de los mismos. De hecho, resulta relativamente frecuente en los Estados Miembros que el derecho de control empresarial de los correos electrónicos varíe dependiendo de si éstos se dirigen a fines personales o profesionales.

³⁵ Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, nº procedimiento 61496/08 (caso Barbulescu vs. Rumanía).

3. JURISPRUDENCIA ESPAÑOLA

A pesar de la frecuencia con la que se producen conflictos entre los derechos fundamentales del trabajador y el derecho del empleador a ejercer control sobre la prestación laboral, no existe normativa específica sobre esta materia. De acuerdo con la doctrina constitucional, un contrato de trabajo no debe privar a los empleados de los derechos que, como cualquier ciudadano, poseen. No obstante, los derechos fundamentales no son absolutos y existe la posibilidad de limitarlos en favor de la consecución de un fin legítimo, como el desarrollo normal de la actividad productiva. La ausencia de regulación sobre estas posibles limitaciones ha conducido a una creciente importancia de la labor doctrinal y jurisprudencial, sobre todo en un contexto donde la irrupción de las tecnologías en el ámbito laboral ha multiplicado el número de casos de control empresarial.

3.1. Doctrina del Tribunal Constitucional

La primera sentencia en abordar la colisión entre los derechos fundamentales de los trabajadores y el poder de control del empresario sobre el uso de los ordenadores y medios informáticos de la compañía, fue la **sentencia del Tribunal Constitucional 241/2012**³⁶. En ella, el tribunal reconoce el carácter laboral de los sistemas informáticos entregados por el empresario y su subsecuente sujeción al control del mismo.

La sentencia trata un caso donde dos trabajadoras habían sido amonestadas por haberse descubierto de manera accidental que habían instalado en el equipo de la empresa, que era de uso compartido y no contaba con clave de acceso, un sistema de mensajería instantánea en el criticaban e incluso insultaban a compañeros y clientes. El Tribunal Constitucional entiende que es cada persona la encargada de determinar los límites de su propia intimidad, tanto personal como familiar. Por ello, en este supuesto, al haber instalado la aplicación de mensajería en un ordenador de uso común al que cualquier otro compañero o superior podría tener acceso, es la propia trabajadora, de manera voluntaria, quién limita el ámbito de su intimidad.

³⁶Sentencia del Tribunal Constitucional de 17 de diciembre 241/2012.

Por otro lado, y con respecto al secreto de las comunicaciones, el TC considera que los mensajes enviados por la empleada no quedan bajo la cobertura constitucional, no existiendo una “expectativa razonable de confidencialidad” de la comunicación, por haberse utilizado un canal abierto, es decir, un canal no secreto, y por existir la prohibición expresa de la instalación de aplicaciones de mensajería en los ordenadores propiedad de la empresa y de uso común.

Otra de las resoluciones más representativas de los conflictos que surgen entre los derechos del trabajador y del empresario, es la sentencia del **Tribunal Constitucional 170/2013**³⁷. Se trata de un caso donde un trabajador es despedido disciplinariamente en base al contenido de conversaciones telefónicas y correos electrónicos en los que el empleado proporcionaba información confidencial a la competencia. Los medios de transmisión eran titularidad de la compañía y el Convenio Colectivo tipificaba como falta leve el uso extralaboral de los dispositivos informáticos de la empresa.

En este caso, el tribunal considera que no puede haber expectativa razonable y fundada de intimidad, en cuanto que existe una prohibición convencional del uso extralaboral de los medios informáticos que lleva implícito el poder fiscalizador del empresario³⁸. De esta manera, se entiende que, siempre que exista una prohibición expresa en el convenio, es innecesario que el trabajador sea informado de la posibilidad de supervisión y vigilancia por parte del empleador.

En esta misma sentencia, el tribunal aplica el juicio de proporcionalidad, concluyendo que la medida es no sólo necesaria, idónea y estrictamente proporcionada, sino que está justificada. La medida es necesaria porque no había forma menos intrusiva de llegar al fin perseguido; es idónea porque cumplía con el objetivo para el cual ha sido creada, que no es otro que verificar que el trabajador había revelado información confidencial a la

³⁷ Sentencia del Tribunal Constitucional de 7 de octubre 170/2013.

³⁸ BAZ RODRÍGUEZ, J., "Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre [BOE n.º 267, de 7-XI-2013]: control empresarial de la utilización, por parte de los trabajadores, de los medios informáticos de la empresa (correo electrónico). Inexistencia de vulneración de los derechos a la intimidad personal y familiar (artículo 18.1 CE).", *Ars Iuris Salmanticensis (AIS): revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología*, vol.2, n.1, 2014, p.365.

competencia, y es estrictamente proporcionada porque el empresario únicamente había inspeccionado los mensajes relacionados con la actividad productiva de la empresa, que no revelaban información personal del trabajador.

En resumen, de la doctrina constitucional se pueden extraer cuatro grandes conclusiones:³⁹

1. El **derecho a la intimidad** y al secreto de las comunicaciones no queda reducido al ámbito doméstico sino que se extiende al ámbito laboral. No obstante, la utilización de canales abiertos para el envío de mensajes elimina la expectativa razonable de privacidad.
2. Los medios informáticos son herramientas de trabajo que pueden ser objeto de **control empresarial**, siempre que se respeten los derechos fundamentales y dignidad del empleado.
3. La **prohibición expresa** (tanto en Convenio Colectivo como reglamento interno) por parte del empresario del uso extralaboral de los medios informáticos, elimina la expectativa razonable de confidencialidad.
4. Para que una medida de control no suponga una vulneración de los derechos fundamentales del trabajador, debe estar justificada y cumplir con el test de la triple **proporcionalidad**.

3.2. Doctrina del Tribunal Supremo

La resolución del Tribunal Supremo más representativa en materia de colisión entre control empresarial y los derechos fundamentales del trabajador es la sentencia **del 26 de**

³⁹ANDERSEN TAX & LEGAL, “La Sentencia dictada por la Gran Sala del Tribunal Europeo de Derechos Humanos en fecha 5 de septiembre de 2017, sobre el control por el empresario del uso del correo electrónico”, *Publicaciones Derecho Laboral Andersen Tax & Legal*, 2017 (disponible en <http://www.andersentaxlegal.es/es/publicaciones-y-noticias/la-sentencia-dictada-por-la-gran-sala-del-tribunal-europeo-de-derechos-humanos-de-5-de-septiembre-de-2017-sobre-el-control-por-el-empresario-del-.html>; última consulta 25/03/2018).

septiembre de 2007⁴⁰, que trata de un caso en el que un trabajador es despedido disciplinariamente por haber accedido de manera recurrente a páginas pornográficas desde un dispositivo de la empresa.

Al igual que el Tribunal Constitucional, el Tribunal Supremo es consciente de la irrupción de las nuevas tecnologías en el ámbito laboral, así como de la tolerancia existente en el uso personal, aunque moderado, de los medios informáticos de la compañía. Por ello, esta sentencia reconoce que el ordenador es un instrumento de trabajo cuyo uso es susceptible de control, siempre que se respete la dignidad humana.

Sin embargo, la gran aportación de esta resolución es la introducción de un doble requisito para la eliminación de la expectativa razonable de intimidad del trabajador. Por un lado, la empresa debe informar a los trabajadores acerca de la posibilidad de control, indicando cuáles serán los sistemas o herramientas que se utilizarán para comprobar el cumplimiento de las obligaciones laborales. Por el otro, el empresario debe establecer unas pautas sobre el uso de los medios informáticos, pudiendo incluso imponer prohibiciones absolutas o parciales.

En consecuencia, la ausencia de reglas de uso de los medios informáticos o de una advertencia al empleado del posible acceso de la compañía a su contenido, puede generar en él una expectativa de confidencialidad. De hecho, en esta sentencia, el tribunal califica el despido como improcedente precisamente por existir la mencionada expectativa de privacidad, al no haberse informado debidamente a los trabajadores.

Esta misma doctrina es seguida por el Tribunal Supremo en su posterior **sentencia del 8 de marzo de 2011**⁴¹, que trata de un despido disciplinario tras descubrir en un procedimiento de auditoría interna que el trabajador había realizado en horas de trabajo más de 5.566 visitas a páginas de contenido extralaboral. El tribunal califica ese despido como improcedente por considerar que el control llevado a cabo por la compañía era secreto , ya

⁴⁰ Sentencia del Tribunal Supremo, de 26 de septiembre del 2007 (RJ 2007\7514)

⁴¹ Sentencia del Tribunal Supremo de 8 de marzo de 2011 (RJ 2011\932).

que ésta no había establecido pautas sobre el uso de los medios informáticos de su propiedad, ni tampoco había informado a los trabajadores acerca de la realización de posibles controles dirigidos a garantizar el correcto uso de los dispositivos. De nuevo, el Tribunal Supremo hace referencia al doble requisito mencionado: la advertencia del control y el establecimiento de normas de utilización de las herramientas informáticas. Por tanto, en el caso de que los trabajadores tengan conocimiento de las normas de uso de los medios informáticos y de los eventuales controles, así como de los sistemas utilizados para llevarlos a cabo, el derecho a la intimidad recogido en el art. 18 CE no impedirá el ejercicio del derecho de control empresarial reconocido en el art. 20 ET.

Por último, cabe mencionar la sentencia del **Tribunal Supremo del 6 de octubre de 2011**⁴². Se trata un despido disciplinario por el uso indebido del ordenador de la empresa, que había sido detectado a través de sistemas de control pasivo. En este caso, la compañía había emitido previamente un comunicado a los trabajadores en el que se informaba sobre la prohibición de la utilización de los medios de la empresa para fines personales.

Esta sentencia unifica doctrina e incorpora ciertos matices a los criterios establecidos por las sentencias previamente mencionadas. El tribunal entiende que la existencia de una prohibición total del uso personal de los dispositivos titularidad de la empresa lleva implícita la advertencia a los empleados sobre posibles procedimientos de control. La prohibición elimina la expectativa razonable de intimidad, con independencia de la información ofrecida por la empresa sobre la fiscalización y su alcance. Por ello, en esta sentencia, el tribunal califica como procedente el despido, por considerar lícita la prueba aportada por la empresa.

Esta sentencia, como afirma Rodríguez Escanciano, matiza la doctrina anterior y supone un retroceso en la protección del derecho fundamental a la intimidad y al secreto de las comunicaciones del trabajador⁴³. Y es que, con la prohibición se “quiebra” la mencionada expectativa razonable de intimidad⁴⁴.

⁴² Sentencia del Tribunal Supremo de 6 de octubre de 2011 (RJ 2011\7699).

⁴³ RODRÍGUEZ ESCANCIANO, S., “Internet en el trabajo”, *Diario La Ley*, n. 8926, 2017. (disponible en <http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAC2PwU7DMAyGn4ZcKqF>)

En resumen, al igual que el Tribunal Constitucional, el Tribunal Supremo reconoce que los medios informáticos constituyen instrumentos productivos cuya utilización puede ser vigilada por el empresario. No obstante, la doctrina de este último incorpora nuevos requisitos para el ejercicio del control empresarial, destacando las siguientes cuestiones:

1. La expectativa razonable de confidencialidad es eliminada sólo si los trabajadores tienen **conocimiento** de las reglas de uso de las herramientas informáticas y de la posibilidad y alcance de las medidas de control.
2. En el caso de que exista una **prohibición expresa** sobre el uso privado de los medios informáticos, ésta se entenderá como advertencia implícita a los trabajadores sobre el control, cumpliéndose, por tanto, el requisito anterior de transparencia informativa.

[03TQ45NKWAxIgNAJ3t7XaQJaM2C3r2-MSIn1ybP-O_3zPmFaLVzYuMKaAXGAo0BecoIPPqGgNMaxnY9OMiqEjU2p9c-w3SqES9sJBOAp3wv3W0wp6nsG3sTfldncLWui2cRXTgKlejVYcGfwJyVSloin-vMDiRmAXQw0pL3XDYFqr5ez2O10d1IKJRGa-3IhiWk1unJ4EznogctTEwCn6x8E8dDF-2bbJdbte0DwjQ05PEEYUG4SQ-ukVJBG_8lnejbdAl6ty9B7EOYF_-9PkHVlfz8zio-QQe6r3EltgbMBjGP5_8AtkXkUKZAEAAA==WKE](https://www.boe.es/boe-2017-04-05/04501_001_001.htm) ; última consulta 05/04/2017).

⁴⁴ CARRIZOSA PRIETO, E., “El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores”, *Temas laborales: Revista andaluza de trabajo y bienestar social*, n.116, 2012, p. 265.

4. LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES DEL TRABAJADOR EN EL ÁMBITO LABORAL

En un primer momento, los tribunales españoles adoptaron la teoría contractualista, en virtud de la cual el contrato laboral prevalecía sobre los derechos del trabajador, que quedaban relegados a un segundo plano. No obstante, con el paso del tiempo, nuestros tribunales han adoptado una visión más proteccionista de los derechos del empleado, apoyándose en la teoría de la proporcionalidad.

4.1. Teoría contractualista

La tradicional teoría contractualista concede especial protagonismo al contrato, por ser una manifestación de la voluntad libre de las partes: empresario y empleado. En este sentido, si el trabajador acepta libremente tanto sus deberes como condiciones laborales, incluyendo aquellas que refuercen la posición del empresario, el vínculo contractual prevalecerá sobre cualquier posible vulneración de los derechos fundamentales del empleado. Es decir, esta teoría otorga al contrato de trabajo primacía sobre los derechos fundamentales, que deberán supeditarse a las facultades de control del empresario. Se entiende que la existencia de una relación contractual impide el ejercicio pleno de los derechos en el ámbito de trabajo.

Un claro ejemplo de la teoría contractualista es la sentencia del TC del 30 de octubre de 1987⁴⁵, que trataba una posible violación del derecho a la propia imagen por el despido de un camarero que se había negado a afeitarse. En este caso, el tribunal entiende que las obligaciones laborales recogidas en el contrato (en este caso, la de trabajar de cara al público) prevalecen sobre la vulneración del derecho a la propia imagen.

La principal crítica que recibe la lógica contractualista es que, si bien no existen obstáculos a la posible reglamentación de su uso, resulta cuestionable utilizar el contrato como una forma de obligar al empleado a dar su consentimiento para la inspección de su ordenador o correo electrónico.⁴⁶ En un mercado laboral competitivo como el actual, hacer uso del

⁴⁵ Sentencia del Tribunal Constitucional de 30 de octubre 170/1987.

⁴⁶ RODRÍGUEZ ESCANCIANO, S. El control empresarial de la mensajería electrónica..., *ob.cit.*

contrato como justificación de posibles vulneraciones de los derechos fundamentales constituye una práctica cuanto menos objetable, en la medida que los empresarios se pueden aprovechar de la posición débil de los empleados.

En este sentido, cabe destacar la sentencia del 21 de septiembre de 2015⁴⁷, que considera abusiva la cláusula de un contrato por la que se obliga al empleado a facilitar a la empresa su número de teléfono y su dirección de correo electrónico personales para que ésta pueda contactar con él por asuntos de naturaleza laboral. En este caso, el tribunal declara nula la cláusula por entender que ésta antepone la libertad de empresa recogida en el art. 38 de la CE al derecho del trabajador a la protección de sus datos personales⁴⁸.

4.2. Test de la tripe proporcionalidad

De manera progresiva, se ha abierto paso a la teoría de la proporcionalidad, que sostiene que el derecho fundamental del trabajador no se considera violado si la medida adoptada es idónea, necesaria y proporcionada en *stricto sensu*. La primera manifestación del abandono de la teoría contractualista es la sentencia del Tribunal Constitucional de 19 de julio de 1985⁴⁹, que estableció que la celebración de un contrato no supone la privación a las partes de sus derechos constitucionales. De esta manera, la libertad de empresa consagrada en el art. 38 no legitima situaciones en las que los derechos de los empleados se vean limitados injustificadamente.

Sin perjuicio de lo anterior, no se puede olvidar que la incorporación a una organización puede derivar en la imposición de limitaciones de los derechos fundamentales, con el objetivo legítimo de conseguir un normal desarrollo de la actividad empresarial⁵⁰.

⁴⁷ Sentencia del Tribunal Supremo de 21 de septiembre de 2015 (RJ 2015\4353).

⁴⁸ POQUET CATALÁ, R., “La protección del derecho a la intimidad del teletrabajador”, *Lex Social: Revista de Derechos Sociales*, vol. 8, n. 1, 2018, p. 113.

⁴⁹ Sentencia del Tribunal Constitucional de 19 de julio 88/1985.

⁵⁰ Sentencia del Tribunal Constitucional de 11 de abril 99/1994.

Como ya se ha mencionado anteriormente, los requisitos que una medida de control ha de cumplir para ser considerada una afectación legítima y no una vulneración de los derechos del trabajador son los siguientes⁵¹:

- a) **Idoneidad:** Se entiende que una medida de control es idónea cuando es apropiada para conseguir el objeto legítimo para el que va dirigida, que no es otro que la exclusión del uso privado de los medios provistos por la empresa para el desarrollo de la actividad productiva, y la comprobación de la comisión de presuntas irregularidades.

- b) **Necesidad:** Se considera que una medida de control es necesaria cuando es el único medio para comprobar el presunto incumplimiento de un trabajador. En otras palabras, se cumplirá con el requisito de necesidad cuando no existan medidas alternativas igualmente eficaces pero más moderadas, que permitan la consecución del objetivo perseguido. Esto implica que, cuando la afectación de los derechos fundamentales del trabajador sea imprescindible para verificar la presunta irregularidad, dicha afectación no será entendida como vulneración de los derechos fundamentales. En ese caso, la medida se entenderá como una manifestación del legítimo derecho del empresario de control y vigilancia.

- c) **Proporcionalidad o rigurosa adecuación:** Una medida es estrictamente proporcionada cuando es equilibrada, es decir, cuando los beneficios obtenidos para la colectividad son superiores a las posibles lesiones causadas a los derechos de los trabajadores. La contundencia de la medida de control debe corresponderse con la gravedad de la presunta falta ya que, de no ser así, se provocará una afectación desproporcionada a los derechos de los trabajadores, que no se verá compensada por los beneficios derivados del control. En este sentido, cabe recalcar que lo que no es proporcionado en una situación donde el trabajador cumple con todas sus

⁵¹ FORTEZA LAHERA, J., “Nueva vuelta de tuerca sobre el correo empresarial del correo electrónico corporativo de los trabajadores . Sentencia TEDH 5 de septiembre 2017 (asunto Barbulescu)”, *Relaciones Laborales*, n.128, 2017, p.70.

obligaciones y tiene un desempeño normal, puede serlo en aquellos casos en los que existan sospechas fundadas de incumplimiento.

Es importante tener en cuenta que no siempre son los mismos los derechos a considerar en el test de proporcionalidad. Si bien la intimidad y el derecho a las comunicaciones suelen ser un denominador común en los litigios sobre el control empresarial de los medios informáticos y del correo electrónico, las características de algunos casos obligan a tener en cuenta nuevos derechos, como el secreto profesional o la libertad de expresión..

A la hora de llevar a cabo el test de triple proporcionalidad, adquiere mucha importancia la finalidad con la que ha sido implementado el sistema de control por parte del empresario. En aquellos casos en los que el objetivo del control no es otro que garantizar el correcto funcionamiento diario de la empresa, se estará ante un supuesto de control ordinario. Sin embargo, cuando el objetivo del sistema de control es verificar el incumplimiento de un trabajador, por existir sospechas fundadas, entonces se tratará de un caso de control “extraordinario”. A este respecto, cabe recalcar que:

- a) Las medidas de control ordinario tienden a ser menos lesivas, en cuanto que únicamente buscan asegurar un normal cumplimiento de las obligaciones laborales. El tradicional fichaje o control de asistencia es un claro ejemplo de ello. Cuando las medidas de control ordinario son intrusivas y agresivas, no superarán el test de triple proporcionalidad, en cuanto que no son idóneas para el objetivo que persiguen⁵².
- b) Las medidas fiscalizadoras, tienden a ser más agresivas porque responden a la existencia de un presunto incumplimiento. En este sentido, deben existir fundadas sospechas de que se ha producido una irregularidad para que se puedan adoptar medidas de control tan intrusivas, y de no ser así, no se superará el test de triple proporcionalidad⁵³.

⁵² FABREGAT MONFORT, G., “El control empresarial de los trabajadores a través...”, *ob.cit.*, p.79.

⁵³ FABREGAT MONFORT, G., “El control empresarial de los trabajadores a través...”, *ob.cit.*, p.79.

5. CONSECUENCIAS DE LA VULNERACIÓN DE LOS DERECHOS FUNDAMENTALES EN CASO DE DESPIDO

Una vez realizado el test de triple proporcionalidad, en el caso de que la medida no sea considerada idónea, necesaria o equilibrada se determina la existencia de una violación de los derechos fundamentales del trabajador. Es entonces cuando surge la siguiente cuestión: ¿Es el despido fundado en la irregularidad conocida por medios ilegítimos improcedente o nulo? Si bien el despido no es la única consecuencia que se puede dar tras la investigación por parte de la empresa de la irregularidad cometida por el trabajador, la realidad es que es la más frecuente en la práctica. No obstante, podría ocurrir, aunque no es lo habitual, que el empleado acudiera a los tribunales para demandar al empresario por la intromisión en su derecho a la intimidad, a pesar de no haber sido despedido.

5.1 Teoría de la improcedencia

Parece consolidarse la tendencia jurisprudencial que considera que la prueba obtenida con intromisión a los derechos fundamentales es ilícita y provoca la calificación del despido como improcedente. Esto se manifestó en sentencia del TSJ de Cataluña de 9 de julio de 2002⁵⁴, que declaró un despido como improcedente por considerar que la prueba presentada era ilícita, ya que se había obtenido mediante el acceso ilegal al correo electrónico no laboral⁵⁵.

En virtud del art. 55 ET, la falta de acreditación de la causa que justifica un despido es motivo de improcedencia. El art.11 LOPJ⁵⁶ establece que la prueba obtenida de manera ilegítima vulnerando los derechos fundamentales no se tendrá en cuenta. En la línea con los

⁵⁴ Sentencia del Tribunal Superior de Justicia de Cataluña de 9 de julio de 2002 (AS 2002\2811).

⁵⁵ MOLERO MANGLANO, C., SÁNCHEZ- CERVERA VALDÉS, J. M., LÓPEZ ÁLVAREZ, M. J., y MATORRAS DÍAZ-CANEJA, A., *Manual de derecho del trabajo* Tirant lo Blanch, Valencia, 2017, p. 720.

⁵⁶ Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).

anteriores preceptos, el art.90 LRJS⁵⁷ declara la inadmisión de las pruebas que tengan su origen en procedimientos que impliquen la vulneración de los derechos fundamentales.⁵⁸

De la legislación vigente, por tanto, se puede deducir que la prueba ilícitamente obtenida no será admitida y, en consecuencia, un despido que se fundamente en la misma será declarado improcedente, por no haber sido probada justa causa.

Esta última cuestión es abordada por la STSJ de la Comunidad Valenciana de 16 de febrero de 2010, que sostiene :

[...]la prueba debe reputarse ilícitamente obtenida, con la consecuencia de que no sirve para probar la falta imputada en la carta de despido, que resulta no acreditada con la consecuencia de que proceda declarar improcedente el despido a tenor de lo dispuesto en los art. 55.4 y 56 del Estatuto de los Trabajadores⁵⁹ .

La idea fundamental sobre la que se apoyan todos los defensores de esta teoría es que la calificación de un despido debe depender de la causa que lo determina y no de la ilicitud de las pruebas aportadas al proceso. En otras palabras, esta teoría defiende que lo que es ilícito es la prueba, no la causa extintiva⁶⁰ . Es decir, si la causa de un despido es la transgresión de la buena fe contractual descubierta por medios ilícitos, éste nunca podrá ser declarado nulo, por no estar fundando en motivos discriminatorios contrarios a los derechos constitucionales.

⁵⁷ Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social (BOE 11 de octubre de 2011).

⁵⁸ CARBONELL MURIO, J, “Efectos de la prueba ilícita en la calificación del despido”, *Foro Español de Laboristas*, 2013 (disponible en <http://fore3lab.com/home/premios-forelab/ii-premio-jovenes-laboralistas-2013-finalistas/>; última consulta 28/03/2018).

⁵⁹ Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 16 de febrero de 2010 (AS 2010\945). Fundamento Jurídico primero.

⁶⁰ DOCTOR, R. y VALENTÍN, G., “I jornadas de litigación laboral de Cuatrecasas: la video vigilancia y la prueba digital, a debate”, *Blog Cuatrecasas*, 2017 (disponible en <https://blog.cuatrecasas.com/laboral/i-jornadas-de-procesal-laboral-de-cuatrecasas-la-video-vigilancia-y-la-prueba-digital-a-debate/>; última consulta 08/4/2018).

Precisamente esta última idea queda reflejada en la STSJ de Castilla La Mancha del 10 de junio de 2014 ⁶¹ que concluye lo siguiente en lo relativo a la calificación del despido:

[...]lo que no ha sido admitido es el medio de prueba contaminado de donde derivaba la conclusión judicial de instancia, pero no se ha concluido que la decisión extintiva, en sí mismo considerada, pretendiera la vulneración de un derecho fundamental o libertad pública del trabajador, que llevara aparejada la calificación de nulidad del mismo ⁶².

El Tribunal Supremo, por su parte, también ha seguido en muchos casos esta teoría siendo prueba de ello la STS del 8 de marzo de 2011⁶³, donde un despido fue declarado improcedente, ya que las pruebas fueron consideradas ilícitas por haberse obtenido a través de una vulneración del derecho a la intimidad.

5.2. Teoría de la nulidad

Otra parte de la doctrina, no obstante, se posiciona a favor de la nulidad del despido, fundamentándose en la teoría del árbol envenenado. Así se pone de manifiesto en la sentencia del Tribunal Constitucional del 15 de noviembre de 2004, relativa al caso Iberia⁶⁴ en la que se afirma que “la reparación de la lesión de un derecho fundamental que hubiese sido causado por el despido laboral, debe determinar la eliminación absoluta de sus efectos, es decir, la nulidad del mismo, lo que implica la anulación de la Sentencia impugnada” ⁶⁵.

Se trata de una corriente garantista, que considera que la declaración de la ilicitud de una prueba debe producir iguales consecuencias en todo lo que derive de la misma, en este caso, el despido⁶⁶. De no ser así, la protección de los derechos fundamentales no sería real, ya que la declaración de la improcedencia del despido ofrece la posibilidad al empresario

⁶¹ Sentencia del Tribunal Superior de Justicia de Castilla La Mancha de 10 de junio de 2014 (AS 2014\1619).

⁶² Sentencia del Tribunal Superior de Justicia de Castilla La Mancha de 10 de junio de 2014 (AS 2014\1619). Fundamento Jurídico cuarto.

⁶³ Sentencia del Tribunal Supremo de 8 de marzo de 2011 (RJ 2011\932).

⁶⁴ CARBONELL MURIO, J., “Efectos de la prueba ilícita en la calificación del despido”, *ob.cit.*

⁶⁵ Sentencia del Tribunal Constitucional de 15 de noviembre 196/2004. Fundamento Jurídico décimo.

⁶⁶ PRADA BAUTISTA, A., “Nulidad del despido por ilicitud de los medios de prueba: análisis jurisprudencial”, *Repositorio institucional Universidad de Oviedo*, 2016 (disponible en <http://digibuo.uniovi.es/dspace/handle/10651/34556>; última consulta 13/04/18).

de elegir entre el pago de indemnización al empleador o la readmisión del mismo. De esta manera, se daría al empleador la facultad de vulnerar libremente los derechos fundamentales⁶⁷, en la obtención de la prueba, en la medida que siempre tendría posibilidad de alcanzar el objetivo final que perseguía, el despido del trabajador, aunque para ello tuviera que hacer frente a una indemnización. En esta línea, el 11 de febrero de 2013, el Tribunal Constitucional declara de nuevo, en un asunto relativo a la suspensión de pagos, que las sanciones que se fundamenten exclusivamente en pruebas lesivas de los derechos fundamentales, deberán calificarse como nulas⁶⁸.

De acuerdo con lo previamente expuesto, declarar la improcedencia del despido sería una flagrante conculcación de los derechos fundamentales del trabajador. Por ello, admitir el efecto reflejo de la prueba ilícita es una prueba evidente del papel predominante de los derechos fundamentales en nuestro ordenamiento⁶⁹. Se entiende que el espíritu y objetivo de la Constitución fue la protección de los derechos fundamentales y la única manera de que dicha protección sea real y efectiva, es declarando como nulos los despidos fundados en causas de las que se ha tenido conocimiento por medios ilícitos.

En el ámbito autonómico, también son varias las resoluciones que han abordado esta cuestión y se han decantado por la nulidad del despido. Destaca una sentencia del TSJ de Galicia del año 2001, que consideró que las grabaciones presentadas eran pruebas lesivas del derecho a la intimidad, lo que implicaba “conforme al artículo 55.5 y 6 ET, la nulidad del despido disciplinario”⁷⁰.

Y es que, en opinión de los defensores de esta teoría, la vulneración de un derecho fundamental en la obtención de la prueba y el inmediato despido del trabajador se subsume en el supuesto de hecho recogido en el art.55.5 ET que establece que “será nulo el despido que tenga por móvil alguna de las causas de discriminación prohibidas en la Constitución o

⁶⁷ Sentencia del Tribunal Constitucional de 15 de noviembre 196/2004.

⁶⁸ Sentencia del Tribunal Constitucional de 11 de febrero 29/2013.

⁶⁹ DÍAZ CABIALE, J. A. y MARTÍN MORALES, R., *La Garantía constitucional de la inadmisión de la prueba ilícitamente obtenida*, Civitas, Madrid, 2001, p. 71.

⁷⁰ Sentencia del Tribunal Superior de Justicia de Galicia de 30 de noviembre de 2001 (AS 2002\390). Fundamento Jurídico cuarto.

en la ley, o bien se produzca con violación de derechos fundamentales y libertades públicas del trabajador”⁷¹.

En relación con el control empresarial de los medios informáticos y de la mensajería electrónica propiedad del empleador, cabe mencionar la STSJ de Madrid de 13 de mayo de 2016, donde se abordaba el despido disciplinario de un empleado basado en correos electrónicos obtenidos desde una cuenta privada. El tribunal consideró que la prueba era ilícita en cuanto que había sido obtenida vulnerando los derechos fundamentales del trabajador y que, por tanto, no sólo la prueba sino también el despido debían declararse nulos: “no estamos solamente ante un supuesto de ineficacia absoluta de tal prueba, que es nula, sino de nulidad de cuantos actos y medidas traigan causa de ella, de modo que el despido ha de calificarse como nulo”⁷².

⁷¹ 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).

⁷² Sentencia del Tribunal Superior de Justicia de Madrid de 13 mayo de 2016 (AS 2016\1166). Fundamento trigesimoséptimo.

6. SENTENCIA DE LA GRAN SALA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS DE 5 DE SEPTIEMBRE DE 2017 RELATIVA AL CASO BARBULESCU⁷³

El caso Barbulescu sienta doctrina laboral sobre la fiscalización empresarial de las comunicaciones de los trabajadores. En esta sentencia, se analizan los límites de la vigilancia sobre los medios electrónicos y se refuerza la posición del empleado frente al derecho fiscalizador del empresario. Tal es la controversia en esta materia, que la resolución inicial del Tribunal Europeo de Derechos Humanos ha sido revocada por su Gran Sala, que ha dictado sentencia en sentido contrario.

6.1. Resumen de los hechos

El Sr. Barbulescu, ciudadano rumano, había trabajado como ingeniero de ventas desde agosto del 2004 a agosto de 2007 en una empresa privada. A petición de la misma, el empleado se creó una cuenta de Yahoo! Messenger para atender las dudas e incidencias de los clientes.

El reglamento interno de la compañía, que prohibía expresamente el uso de sus recursos informáticos para fines extralaborales, era conocido por el empleado, que lo había leído y firmado en diciembre de 2006. Asimismo, el 3 de julio de 2017 la empresa había enviado un comunicado a los trabajadores informándoles sobre el despido de una empleada por el uso extralaboral de las herramientas de la empresa. En esta nota informativa, se advertía, además, de que las faltas e irregularidades podrían ser objeto de investigación. El demandante no sólo había tenido conocimiento de este comunicado, sino que lo firmó entre el 3 y el 13 de julio de 2017.

El 5 de julio, apenas dos días después de circular la nota informativa, la empresa registró en tiempo real las conversaciones del empleado en Yahoo! Messenger. Finalizado el registro el día 13 de ese mes, el director citó al empleado para informarle de que se habían vigilado sus conversaciones y de que existían indicios para pensar que estaba haciendo un uso

⁷³ Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, nº procedimiento 61496/08 (caso Barbulescu vs. Rumanía).

extralaboral de internet. En esta reunión, el superior no hizo mención al contenido de los correos electrónicos y simplemente facilitó al trabajador gráficos que reflejaban que su uso de internet era mayor al de resto de los empleados. Ese mismo día, el demandante comunicó por escrito a su director que sólo había utilizado Yahoo! Messenger para fines meramente profesionales. Apenas unos minutos después, el trabajador fue llamado a dar una explicación de las 45 páginas de transcripción de su correspondencia que recogían conversaciones privadas con su pareja y su hermano.

El 1 de agosto de 2007 el trabajador fue despedido disciplinariamente, siendo esta decisión impugnada ante los tribunales nacionales rumanos. El demandante argumentó que, de acuerdo con el caso Copland contra Reino Unido⁷⁴, los correos enviados desde el lugar de trabajo quedan bajo la protección del art 8 del CEDH, que tutela el derecho a la vida privada.

El tribunal rumano confirmó la legalidad de la decisión del empresario y recordó que, antes de interponerse la sanción disciplinaria a los empleados, éstos habían sido advertidos mediante nota informativa sobre el control del uso de los medios de la empresa. Asimismo, el tribunal remarcó que los trabajadores habían sido informados de la normativa interna que prohibía expresamente el uso extralaboral de las herramientas informáticas. Esta resolución fue impugnada ante el Tribunal de Apelación de Bucarest, que se pronunció en el mismo sentido que la primera instancia y concluyó que, de acuerdo con los principios recogidos en la Directiva 95/46/ CE, la medida de control supuso una afectación necesaria, justificada, transparente y proporcionada para alcanzar el objetivo legítimo que perseguía.

De nuevo, esta decisión fue impugnada por el Sr. Barbulescu ante el TEDH, alegando, además de la vulneración del art. 8 CEDH, que los tribunales rumanos no habían llevado a cabo una justa ponderación de los intereses afectados.

⁷⁴ Sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007, nº procedimiento 62617/00 (caso Copland vs Reino Unido).

El TEDH reconoció en su sentencia del 12 de enero de 2016⁷⁵ que el empresario tenía un legítimo interés en comprobar el cumplimiento de las obligaciones laborales a través de la medida de control adoptada. Además, consideró que la medida no había sido invasiva por las siguientes razones⁷⁶:

- a) La prohibición expresa en el reglamento interno del uso de los ordenadores con fines personales eliminaba la expectativa razonable de intimidad.
- b) La empresa no había accedido al contenido de las conversaciones hasta que el demandante declaró que había utilizado los recursos para meros fines profesionales. La compañía, por tanto, confiaba en que la inspección de los mensajes no atentaría contra la privacidad del Sr. Barbulescu.
- c) El control se llevó a cabo con el objetivo legítimo de comprobar el supuesto incumplimiento laboral del Sr. Barbulescu.

Esta resolución fue nuevamente recurrida, esta vez ante la Gran Sala del TEDH, que dictó sentencia el 5 de septiembre de 2017.

6.2. Fallo de la Gran Sala

En esta sentencia, la Gran Sala se pronuncia por primera vez sobre la aplicabilidad del art. 8 CEDH en un caso en el que se discute la vulneración al derecho a la vida privada por un empleador privado y no público. Se afirma que, si bien el objetivo principal del artículo es proteger al individuo de la intromisión arbitraria de las instituciones públicas, el precepto también impone obligaciones positivas a los Estados, cuyos órganos jurisdiccionales deben velar por el cumplimiento de los derechos que el artículo tutela.

⁷⁵Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, nº procedimiento 61496/08 (caso Barbulescu vs. Rumanía).

⁷⁶ GARCÍA, L, “El caso Barbulescu y el control de las comunicaciones informáticas de los empleados”, *Newsletter Laboral Garrigues*, 2017,. (disponible en http://www.garrigues.com/sites/default/files/documents/newsletter-laboral-septiembre-2017_0.pdf; última consulta 03/04/2018).

En este sentido, la Gran Sala concluye que los Estados deben tener un margen de discrecionalidad amplio, pero no ilimitado, en la elaboración de un marco jurídico que regule las políticas de las empresas sobre el uso de las herramientas informáticas y los protocolos de control. Los tribunales nacionales deben garantizar que, en el ejercicio del control empresarial, los empleadores no incurran en abusos y, para ello, deben tener en cuenta los siguientes principios ⁷⁷:

- a) Principio de transparencia: La existencia de advertencias previas sobre la posibilidad de control por parte del empleador. Esta cuestión, no se debe confundir con la existencia de una prohibición expresa del uso extralaboral de los medios informáticos.

- b) Principio de proporcionalidad:
 - El alcance y extensión de la supervisión, en términos de intrusión en la vida privada del trabajador. Habrá que distinguir entre el control completo o parcial; permanente o temporal; general o individualizado.

 - La posibilidad de utilización de medidas alternativas menos intrusivas que el acceso directo al contenido de las comunicaciones, con las que se pudiera alcanzar el fin perseguido por el empresario.

 - Las consecuencias que la supervisión tiene sobre el empleado afectado. Concretamente, si el resultado de las medidas de vigilancia es utilizado para obtener el objetivo que las justifica.

- c) Principio de causalidad: La existencia de argumentos legítimos que justifiquen la vigilancia de las comunicaciones y el acceso al contenido de las mismas.

⁷⁷ MOLINA NAVARRETE, C. M., “El Poder empresarial de control digital: ¿ nueva doctrina” del TEDH o mayor rigor aplicativo?. A propósito de la STEDH de 5 de septiembre de 2017, caso Barbulescu c. Rumania”, *IusLabor*, n.3, 2017, p. 293.

- d) Principio de efectividad de la tutela: La protección del trabajador a través de las garantías pertinentes. En concreto, estas garantías deben asegurar que el empresario no pueda acceder al contenido de las comunicaciones del empleado si éste no ha sido notificado de ello.

En relación al principio de transparencia, la Sala entiende que los órganos jurisdiccionales no probaron que la advertencia fuera previa al control. El Sr. Barbulescu firmó el comunicado enviado por la empresa entre el 3 y 13 de julio, sin especificarse el día concreto en que dicha firma tuvo lugar. El control comenzó el día 5 de julio, por lo que no queda claro si en ese momento el demandante ya había firmado la nota informativa.

En términos de proporcionalidad, la Sala considera que los tribunales tampoco estudiaron el alcance y grado de intrusión de la supervisión, que se extendió a todas las comunicaciones enviadas en tiempo real por el Sr. Barbulescu durante el periodo de vigilancia. Además, la Sala cree que los tribunales nacionales no analizaron si se podría haber llegado a conocer el incumplimiento del trabajador por medio de medidas menos invasivas, ni tampoco si la consecuencia de la medida de control (que en este caso fue el despido) se adecuaba a la gravedad de la falta cometida por el trabajador.

Por otro lado, la Gran Sala defiende que los órganos jurisdiccionales rumanos no comprobaron la existencia de argumentos legítimos que justificaran el acceso al contenido de las comunicaciones del empleado.

Por último, la Sala entiende que los órganos jurisdiccionales rumanos tampoco tuvieron en cuenta si el acceso al contenido de las comunicaciones hubiera podido tener lugar sin el conocimiento del trabajador.

En definitiva, la Gran Sala concluye que las autoridades nacionales no hicieron una correcta ponderación de los intereses afectados, al no proteger adecuadamente el derecho a la vida privada y secreto de correspondencia del Sr. Barbulescu.

7. INFLUENCIA DE LA SENTENCIA BARBULESCU EN LOS TRIBUNALES ESPAÑOLES

Las sentencias del TEDH sirven como criterio interpretativo en nuestros tribunales, y son de aplicación inmediata en el ordenamiento español, como se deduce del art 10 CE⁷⁸. Dado que la sentencia Barbulescu no se refiere a ciudadanos españoles, no afecta de manera directa a nuestros tribunales, pero sí lo hace de manera indirecta, en la medida que futuros litigios sobre control empresarial podrían ser recurridos ante este Tribunal. De ahí, que el caso Barbulescu anteceda un cambio importante en los criterios jurisprudenciales.

Si bien la sentencia de la Sala del TEDH no dista, en lo esencial, de la doctrina sentada por la jurisprudencia del Tribunal Constitucional y Tribunal Supremo, lo cierto es que el caso Barbulescu incorpora una serie de matizaciones que conviene tener en cuenta. En esta sentencia, se completan los requisitos fijados por nuestra jurisprudencia para que el empresario pueda ejercer su derecho de control sobre el correo electrónico de los trabajadores.

Parece que el test de triple proporcionalidad empleado por nuestros tribunales se asemeja mucho al filtro introducido por el TEDH. No obstante, en los últimos años, sobre todo de mano del TC, se había sentado en nuestro país una doctrina mucho más laxa, tendente a favorecer la facultad de control empresarial frente a los derechos fundamentales del trabajador⁷⁹.

La sentencia del TEDH del 5 de septiembre de 2017, se aproxima a una doctrina más garantista, que impone mayores limitaciones al control del uso que los trabajadores hacen de las herramientas informáticas. Con esta resolución, vuelve a cobrar relevancia la doctrina sentada hace una década por el TS en su sentencia del 26 de septiembre de 2007, que exigía a los empresarios, para eliminar la expectativa razonable de intimidad, informar

⁷⁸ BUJALDÓN TARRIDA, A., “Barbulescu II: cambio de criterio jurisprudencial”, *El jurista*, 2017 (disponible en <http://www.eljurista.eu/2017/10/09/barbulescu-ii-cambio-de-criterio-jurisprudencial/>; última consulta el 09/04/2018).

⁷⁹ LÓPEZ DE LA FUENTE, “La doctrina jurisprudencial del tribunal europeo de derechos humanos sobre el control de las comunicaciones electrónicas en el trabajo: ¿el fin de una eterna cuestión?”, *Revista de estudios europeos*, n.69, 2017, p.12.

a los trabajadores no sólo de las normas de uso de los medios informáticos, sino también de la posibilidad de su control. Sentencias más recientes del Tribunal Supremo, como la de **6 de octubre de 2011**⁸⁰ parecen, ahora, ser contrarias a la nueva doctrina Barbulescu.

Esta última resolución, consideraba que la prohibición expresa del uso personal de los dispositivos llevaba implícita la advertencia de control a los trabajadores, argumento que parece contrario al principio de transparencia sentado por la doctrina Barbulescu, que exige en todo caso la advertencia expresa a los empleados.

Si bien la doctrina Barbulescu incide sutilmente en la doctrina del TS, la sentencia del 5 de septiembre lo hace de manera más clara sobre la doctrina reciente del TC, mucho menos conservadora. Concretamente, se ha de revisar la doctrina sentada en las siguientes resoluciones⁸¹:

- a) **STC 241/2012**⁸². En esta sentencia se consideró que no se había vulnerado el derecho a la intimidad y al secreto de las comunicaciones del trabajador, por haber tenido lugar las comunicaciones intervenidas en un canal abierto. Con la doctrina Barbulescu, esto no podría ser motivo suficiente para considerar legítima la intromisión del empresario en los derechos del trabajador, ya que se exige advertir a los empleados del control, y esta advertencia nunca tuvo lugar en este supuesto. No podrá, por tanto, sostenerse la doctrina del TC que defendía la mayor o menor agresividad de las medidas de control, en función de las condiciones de disposición y uso de los medios informáticos⁸³.

⁸⁰ Sentencia del Tribunal Supremo de 6 de octubre de 2011 (RJ 2011\7699).

⁸¹ PRECIADO DOMENECH, C.H., “Nuevas formas de prueba basadas en las tecnologías de la información y la comunicación (TIC). Documento electrónico y prueba digital: Proposición y práctica. Ilicitud de estas pruebas por vulneración de derechos fundamentales”, *Actum social*, n.131, 2017, p. 34.

⁸² Sentencia del Tribunal Constitucional de 17 de diciembre 241/2012.

⁸³ PRECIADO DOMENECH, C.H., “Comentario de Urgencia a la STEDH 5 de septiembre de 2017. Caso Barbulescu contra Rumanía (Gran Sala). Recuperando la dignidad en el trabajo”, *Revista Jueces para la Democracia, Jurisdicción Social*, n.10, 2017 (disponible en <http://aranzadi.aranzadidigital.es/maf/app/document?docguid=177861700f80911e7b1a501000000000&srguid=i0ad82d9b000001629caf1fc7fde3afdb&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificacionMagazines=&fechacomun=&numeropub-tiponum=> última consulta 06/04/2018).

b) **STC 170/2013**⁸⁴. Esta sentencia supuso un paso hacia atrás en lo que seguridad jurídica y protección de los derechos de los trabajadores respecta. Se llegó a considerar que la prohibición expresa en un convenio colectivo del uso extralaboral de los medios informáticos eliminaba la expectativa razonable de intimidad, sin que fuera necesaria información adicional a los trabajadores. Por tanto, permitir que los empresarios accedan al correo electrónico de los empleados sin previo aviso amparados en la mera prohibición en un Convenio Colectivo o reglamento interno se opone frontalmente a la nueva doctrina del TEDH. En consecuencia, el empresario no podrá justificar un control intrusivo de las comunicaciones con este argumento.

Por último, es importante hacer mención al **STS del 8 de febrero de 2018**⁸⁵, en la que el Tribunal Supremo resuelve por primera vez desde la sentencia *Barbulescu* un recurso de casación de unificación de doctrina. En esta resolución, el tribunal afirma que, como se ha venido indicando, las pautas sentadas por el TEDH en su sentencia *Barbulescu* coinciden sustancialmente con el filtro establecido por la doctrina española en las sentencias anteriores del Tribunal Supremo y Tribunal Constitucional⁸⁶. Así, la comunicación previa al trabajador; la agresividad de la supervisión; la existencia de justificación legítima del control; la posibilidad de utilización de medios menos invasivos para la consecución de la finalidad perseguida; las consecuencias del resultado del control, y la previsión de garantías para el empleado parecen reconducirse al test de triple proporcionalidad utilizado por nuestros tribunales.

[...] Como es de observar, tales consideraciones del Tribunal Europeo nada sustancial añaden a la doctrina tradicional de esta propia Sala (SSTS 26/09/07 ; 08/03/11; y 06/10/11) pues sin lugar a dudas los factores que para el TEDH deben tenerse en cuenta en la obligada

⁸⁴ Sentencia del Tribunal Constitucional de 7 de octubre 170/2013

⁸⁵ Sentencia del Tribunal Supremo de 8 de febrero de 2018 (RJ 2018\666).

⁸⁶ Uría Menéndez, “ Pautas de revisión del correo electrónico tras *Barbulescu*: La sentencia del Tribunal Supremo del 8 de febrero de 2018”, *Noticias Uría Menéndez*, 2018 (disponible en <http://www.uria.com/es/actualidad/Noticias.html?id=1113> ; última consulta 20/03/2018).

ponderación de intereses, creemos que se reconducen básicamente a los tres sucesivos juicios de «idoneidad», «necesidad» y «proporcionalidad» requeridos por el TC.⁸⁷

Por otro lado, en esta sentencia, se analiza un despido disciplinario fundado en hechos conocidos gracias al acceso al correo electrónico corporativo del empleado. Cabe tener en cuenta las siguientes cuestiones:

- a) La empresa contaba con una política de uso de los medios informáticos basada en la utilización meramente profesional de los mismos.
- b) Las normas internas, aceptadas por el trabajador cada vez que accedía a su ordenador de empresa, informaban a los empleados de la posibilidad de control.
- c) La revisión de los correos se limitó a todos aquellos que pudieran ofrecer información importante a efectos de la investigación que se estaba llevando a cabo. Por ello, se filtraron los correos usando palabras clave.

A la vista de lo expuesto, el tribunal considera que la medida de control supera no sólo el test de la triple proporcionalidad (idoneidad, necesidad y proporcionalidad *stricto sensu*) sino también las pautas sentadas por el TEDH en su sentencia *Barbulescu*. Se exige, de nuevo, el conocimiento del empleado de las normas que regulan el uso de los medios informáticos y la advertencia previa a los trabajadores sobre el control, independientemente de la existencia de prohibiciones expresas del uso extralaboral de las herramientas de la empresa.

⁸⁷ Sentencia del Tribunal Supremo de 8 de febrero de 2018 (RJ 2018\666). Fundamento Jurídico sexto.

8. PAUTAS DE ACTUACIÓN PARA LOS EMPRESARIOS ESPAÑOLES TRAS LA DOCTRINA BARBULESCU

Las implicaciones de la doctrina Barbulescu, no sólo alcanzan a los Tribunales españoles, sino también a las empresas de nuestro país, que en su calidad de empleadores, deben actuar con cautela en el ejercicio del poder empresarial y atender a las siguientes cuestiones.

8.1.Principio de transparencia informativa

La doctrina Barbulescu presta especial atención al principio de transparencia, de manera que el trabajador debe de ser informado con carácter previo a la inspección, con independencia de la existencia de normas que, bien en el reglamento interno o bien en el convenio, prohíban el uso extralaboral de los medios informáticos o lo tipifiquen como falta.

En contraste con esta doctrina, existen voces autorizadas que consideran que el ordenador es un bien propiedad de la empresa, que puede ser objeto de registro sin necesidad de aviso previo, ya que su uso incorrecto supone un quebrantamiento de la buena fe contractual⁸⁸.

No obstante, la jurisprudencia española, en línea con lo establecido por el TEDH impone el deber de advertir de manera previa, expresa, precisa, clara e inequívoca sobre la finalidad del control y sobre su posible utilización⁸⁹.

- ¿Hay que informar siempre al trabajador sobre la fiscalización del correo electrónico?

Si bien la sentencia Barbulescu es clara con respecto a la necesidad de informar a los trabajadores, esta doctrina podría ser matizada con la aprobación de la nueva Ley Orgánica de Protección de Datos de carácter personal. En el artículo 22.5 del proyecto de Ley

⁸⁸SAN FULGENCIO GUTIÉRREZ, J.A. ,“¿Es privado el Email?”, *Boletín del Ilustre Colegio de Graduados Sociales de Madrid*, n.37, 2002, p. 33.

⁸⁹ COLÀS-NEILA, E, “La amenaza de los derechos del trabajador derivada de la innovación tecnológica en la empresa”, *Creatividad y sociedad*, n.26, 2016, p. 276.

aprobado en noviembre de 2017⁹⁰, se hace referencia a la videovigilancia en el ámbito del trabajo y se establece que, en los casos en los que las imágenes capten un delito flagrante, no es necesario haber informado a los trabajadores del control para que éstas tengan valor probatorio.

Aunque este artículo haga únicamente referencia al uso de cámaras de video, lo cierto es que podría ser objeto de aplicación analógica en los litigios sobre control empresarial del correo electrónico.

En este sentido, si el empresario monitorizara el correo electrónico de un trabajador y descubriera la comisión de un delito como, por ejemplo, la falsedad documental, entonces dicha prueba no sería calificada como nula y desplegaría todos sus efectos a pesar de haberse obtenido con una clara intromisión en el derecho de intimidad del trabajador.

La principal crítica que recae sobre este artículo es que, si bien no exige al empresario informar con carácter previo al control, sí exige cierto conocimiento de la legislación, en la medida que el empleador tiene que valorar si las sospechas que recaen sobre el trabajador se refieren a la comisión de un delito. El empresario, por tanto, debería analizar determinados preceptos jurídicos, antes de proceder al control del uso de los medios informáticos de un trabajador al que no se ha informado sobre dicha fiscalización.

En resumen, de acuerdo con la doctrina Barbulescu, el trabajador debe ser informado en todo caso sobre la posibilidad de inspección de los medios informáticos de la empresa. No obstante, por aplicación analógica del art 22.5 del Proyecto de Ley Orgánica de Protección de Datos, dicha información no es necesaria cuando el resultado de la investigación del empresario revele la comisión de un delito.

⁹⁰ Proyecto de Ley Orgánica 121/000013, de Protección de Datos de Carácter Personal (BOCG, de 24 de noviembre de 2017).

- ¿ Basta con advertir al trabajador o es necesaria la elaboración de un “protocolo tecnológico”?

La mera advertencia no resulta suficiente para que un empresario pueda quedar bajo la protección del art. 20 ET. Los empleadores deben, a su vez, establecer protocolos claros en los que recojan de manera precisa las pautas de uso de los medios informáticos propiedad de la empresa, con el objeto de evitar que el desconocimiento de los trabajadores pueda llevarles a tener una expectativa de intimidad equivocada. Asimismo, es importante informar sobre los procedimientos y sistemas utilizados en el ejercicio del control, y sobre el alcance del mismo, no siendo suficiente con el mero establecimiento de prohibiciones⁹¹.

En este sentido, el empresario debe comunicar sobre la existencia de este protocolo, y hacérselo llegar a sus trabajadores, solicitando la firma de los mismos. Además, es recomendable que el protocolo se publique en la plataforma de Intranet, de manera que todos los trabajadores puedan tener acceso al mismo, y que se haga referencia explícita a la existencia de dicho protocolo en el contrato de trabajo⁹².

En resumen, el empresario debe comunicar a los empleados las normas de uso de los medios informáticos, advertirles de posibles inspecciones e informarles de los medios que se utilizarán en el ejercicio de dicho control, así como de las medidas que se adoptarán y de su alcance. Dicha información debe estar siempre a su disposición y ser de fácil acceso.

Por último, es recomendable que esos protocolos incluyan los distintos niveles de gravedad de los incumplimientos y las sanciones que éstos llevan aparejados, en cuanto que esto favorece la seguridad jurídica⁹³.

⁹¹ LLUCH CORELL, F.J., “ El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador, *El Derecho*, 2017 (disponible en http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronico-trabajador_11_1045180003.html última consulta 25/03/18).

⁹² ÁLVAREZ DE LINERA GRANDA, P. Y SÁNCHEZ MOURIZ , N., “Regulación del uso de las herramientas tecnológicas en la empresa: El protocolo telemático”, *Jornada de 10 de marzo de uso y no abuso de los recursos tecnológicos en la empresa, organizada por Cámara Oficial de Comercio, Industria y Navegación de Gijón, Cobertura Informática y Garrigues*, 2011.

⁹³ ABAD BUSTILLO, A., “Tecnologías de la información y comunicación (TIC), control empresarial y derechos fundamentales”, *Repositorio de la Universidad de Cantabria*, 2015 (disponible en <https://repositorio.unican.es/xmlui/handle/10902/7014> ; última consulta 22/03/2018)

- ¿ Tiene que ser una advertencia individualizada o puede ser general?

En relación con el apartado anterior, surge la cuestión de si basta con una advertencia general dirigida al conjunto de los trabajadores o, de lo contrario, se requiere de una comunicación particular al empleado que es objeto de fundadas sospechas de incumplimiento. A este respecto, la jurisprudencia española y comunitaria, incluyendo la sentencia Barbulescu objeto de estudio, parecen apuntar a una advertencia general. De hecho, en esta última sentencia, la comunicación sobre el despido de una trabajadora y la advertencia sobre posibles medidas de control fue difundida entre todos los empleados. Esto tiene cierta lógica, en la medida que una advertencia individualizada a un empleado podría condicionar los resultados de la investigación: el trabajador corregiría su mala conducta, no pudiéndose nunca cumplir con el objetivo legítimo que se persigue con la medida de control.

En ese sentido, parece que los tribunales aceptan cualquier advertencia al empleado bajo sospecha, aunque ésta no se dirija a él en particular sino al conjunto de los trabajadores. Por ejemplo, la colocación de una pegatina en todos los ordenadores de la compañía que advirtiera sobre la posible inspección en caso de uso indebido de los equipos informáticos sería suficiente, sin que fuera necesario que el empresario enviara una comunicación individualizada al trabajador objeto de investigación.

Existe, por tanto, discrecionalidad en la forma de advertir al trabajador sobre el eventual control del uso de los medios informáticos. Uno de los procedimientos más habituales en el cumplimiento de los requisitos de transparencia es incluir explícitamente en el contrato laboral, a través de cláusulas o anexos, todas aquellas conductas prohibidas en la utilización de los medios informáticos de la compañía, advirtiendo, además, de la posible realización de controles. No obstante, también se pueden divulgar códigos de conducta que incluyan las normas y advertencias pertinentes. Asimismo, los convenios, debido a su alcance, resultan una herramienta muy útil para recoger las pautas de uso de los medios informáticos de la compañía e informar sobre la posibilidad de realización de controles, sobre su alcance y sobre los medios que se van a emplear. Tampoco es infrecuente, que al acceder a los

ordenadores o correos electrónicos corporativos aparezca en la pantalla una advertencia sobre la obligación de utilizar de manera estrictamente laboral los equipos informáticos, requiriendo, en muchos casos, que el empleado pulse un botón para poder continuar.⁹⁴

Sin perjuicio de lo anteriormente expuesto, es indispensable que la advertencia sea previa, entendiendo La Gran Sala del TEDH que será previa si se produce antes de que comience la actividad de supervisión. De hecho, en el caso *Barbulescu*, no existe constancia de que el trabajador tuviera conocimiento de la comunicación con carácter previo al inicio del control y eso, entre otras cosas, fundamenta el fallo a favor del empleado. Por tanto, informar del control al trabajador una vez iniciado el periodo de vigilancia supondría un atentado contra el principio de transparencia defendido por el tribunal.

- ¿Debe ser la advertencia inmediatamente anterior al control?

Así como no se requiere la notificación individualizada de un posible control, tampoco es exigible una advertencia inmediatamente anterior al mismo, ya que, al igual que la advertencia individualizada, podría viciar los resultados de investigación. Y es que, la reacción inmediata del empleado tras recibir la advertencia podría ser la ocultación o el cese de las irregularidades de las que la compañía sospecha. Por eso, si se notificara al empleado la posibilidad de control justo antes de su inicio, esto podría provocar que éste rectificara su conducta. Por el contrario, si la notificación fuera previa al control pero no inmediatamente anterior a éste, entonces el trabajador tendería a volver a comportarse en su forma habitual, con lo que la investigación podría cumplir con los fines perseguidos.

Basta, por tanto, que se avise de cualquier forma con anterioridad al control, sin que se requiera cercanía temporal con la supervisión.

- ¿Cabe la prohibición absoluta del uso de los medios informáticos?

Es importante tener en cuenta que la existencia de una prohibición absoluta del uso extralaboral de los medios electrónicos no elimina el margen de tolerancia del uso personal

⁹⁴BARROS GARCÍA, M., “Problemas derivados de la utilización del correo electrónico e Internet en el ámbito laboral”, *Actualidad Jurídica Uría & Menéndez*, n.8, 2004, p.56.

razonable de los mismos. Y es que, parece estar generalizada cierta aceptación a que las personas en el puesto de trabajo utilicen para fines personales las herramientas de la empresa, siempre que lo hagan de manera moderada. Prueba de ello es la sentencia del Juzgado de lo Social de Madrid de 4 de marzo de 2002 que afirmaba que “la prestación de servicios en los locales de la empresa no puede significar un extrañamiento social del trabajador, que tiene derecho a una utilización personal razonable de los medios de comunicación puestos a su alcance como herramienta de trabajo”⁹⁵.

Además, es importante recalcar que, aun cuando existiera una prohibición expresa del uso extralaboral de medios de la compañía, una actitud posterior de tolerancia por parte del empresario dejaría sin efectos dicha prohibición⁹⁶. De esta manera, si el empresario ha venido permitiendo de manera manifiesta la utilización personal de las herramientas informáticas, un cambio repentino en su criterio con el objeto de castigar la conducta previamente permitida no podría ser admitido, a no ser que existiera una advertencia previa.

8.2. Principio de causalidad

La sentencia de Barbulescu exige la existencia de una causa legítima que justifique la aplicación de una medida de control para que ésta sea considerada una afectación de los derechos fundamentales del trabajador y no una vulneración de los mismos.

- ¿Deben existir indicios de incumplimiento para el ejercicio del derecho de control?

Una de las cuestiones más importantes a tener en cuenta por el empresario antes de ejercer su poder de control, es la existencia de indicios que evidencien una irregularidad cometida por el trabajador. En este sentido, cabe recordar que el control ordinario está dirigido únicamente a asegurar el normal desarrollo de la actividad productiva, y que el control

⁹⁵ Sentencia del Juzgado de lo Social de Madrid nº 33, de 4 de marzo de 2002 (JUR 2002\216228)

⁹⁶ TASCÓN LÓPEZ, R., “El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica”, *Aranzadi social*, n.17, 2007 (disponible en <http://aranzadi.aranzadidigital.es/maf/app/document?docguid=Ic29bae20bfe911dc95e301000000000&srguid=i0ad82d9a000001629cb142529c6b75d2&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificacionMagazines=&fechacomun=&numeropub-tiponum=>; última consulta 07/04/2018).

extraordinario o fiscalizador tiene como objetivo verificar el incumplimiento de una obligación laboral.

Mientras que una vigilancia realizada en una situación de normalidad no puede ser excesivamente invasiva, la realización de un control extraordinario permite un grado de intrusión mayor. Existen, por tanto, dos supuestos en los que se puede ejercer el poder empresarial: el primero se refiere a situaciones en las que hay indicios de que el trabajador ha producido un perjuicio a la compañía, y el segundo se refiere a situaciones donde el empresario no sospecha de una conducta irregular por parte del empleado⁹⁷. En este segundo supuesto, referido al control ordinario, las medidas tienen que ser muy poco agresivas, porque en caso de serlo, no existirá una ponderación adecuada entre el derecho a la intimidad del trabajador y el objetivo la medida de control.

El control ordinario, por tanto, trata de garantizar el correcto desempeño de la prestación laboral dentro de unos niveles de exigencia normales. Así, en una situación de normalidad laboral, resulta aceptable, por ejemplo, utilizar un programa informático que mida el número de páginas extra-laborales que se han visitado, pero resulta objetable, por ejemplo, la instalación de localizadores en el coche de empresa. En este sentido, cabe destacar la sentencia del TS de 21 de junio de 2012, que afirma que la instalación de un sistema de control GPS en el coche de un empleado en una situación en la que no existían indicios de incumplimiento y donde únicamente se pretendía llevar a cabo un control rutinario, era completamente desproporcionada. El TS fundamenta su decisión en “el carácter permanente del dispositivo de control (GPS) aplicado, su incorporación a un bien propiedad del trabajador, el exceso sobre las exigencias objetivas de control y la falta de proporcionalidad resultante”⁹⁸. En este caso, por tanto, no existía un fundamento legítimo de la medida de control, en cuanto que no había ninguna sospecha de irregularidad. Se trataba, pues, de una medida innecesaria que únicamente respondía a la mera conveniencia del empresario y que, en ningún caso, podía entenderse como ejercicio del poder de control ordinario reconocido en el art. 20 ET.

⁹⁷ MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, Consejo Económico y Social (CES), Madrid, 2002, P. 148.

⁹⁸ Sentencia del Tribunal Supremo de 21 de junio de 2012 (RJ 2012\7627). Fundamento Jurídico tercero.

Por tanto, cabe concluir que el empresario podrá imponer medidas de control permanente que no respondan a sospechas de incumplimiento, sólo si éstas son poco gravosas para el trabajador. En relación con la monitorización del correo electrónico, el control del volumen de mensajes enviados o de los dominios de destino podría considerarse normal en cuanto no es desproporcionado ni excesivamente intrusivo⁹⁹.

Distinto es, no obstante, el control ejercicio por el empresario cuando existen indicios de una mala actuación. En este caso, se podrán imponer medidas fiscalizadoras más agresivas, siempre que superen el test de proporcionalidad. En lo que el control de los correos electrónicos respecta, de la sentencia Barbulescu puede deducirse que, debido al carácter intrusivo de la medida, el acceso al contenido del correo electrónico sólo puede tener lugar cuando existan sospechas fundadas y graves de la comisión de una irregularidad por parte del empleado.

En este sentido, Fernández Villazón entiende que la inspección del contenido de la mensajería electrónica sólo puede darse en ocasiones excepcionales, cuando sea complementemente indispensable para el correcto desempeño de la actividad laboral¹⁰⁰. En el resto de los casos, el control debe limitarse a los “elementos externos” del mensaje, por considerarse que este tipo de registro es menos lesivo para el trabajador.

Sin perjuicio de lo anterior, existe la posibilidad de establecer medidas preventivas, como el filtrado de las páginas de internet a las que los trabajadores tienen acceso, que reducen el número de casos en los que se requiere de un control fiscalizador. De hecho, el Comité de miembros del Consejo de Europa adoptó en abril de 2015¹⁰¹ la Recomendación de Protección de Datos del ámbito laboral que decía, entre otras cosas, que las medidas

⁹⁹ GARCÍA ROPERO, J. y SAMPERE, P., “¿ Cuándo puede (y cuando no) la empresa espiar mis correos?”, *Cinco días-El país*, 2017 (disponible en https://cincodias.elpais.com/cincodias/2017/09/05/fortunas/1504637748_187161.html; última consulta 05/04/2018).

¹⁰⁰ FERNÁNDEZ VILLAZÓN, L. A, *Las facultades empresariales de control de la actividad laboral*, Ediciones Aranzadi, Pamplona, 2003, p.110.

¹⁰¹ Recomendación del Comité de Ministros del Consejo de Europa CM/Rec(2015)5, de 1 abril de 2015, sobre el tratamiento de datos personales en el ámbito laboral.

preventivas debían prevalecer sobre las de control o monitorización, con el objeto de minimizar las situaciones de vulneración de los derechos de los trabajadores¹⁰².

8.3. Principio de proporcionalidad

La doctrina Barbulescu es clara, y exige la proporcionalidad de la medida en términos de alcance, extensión y lesividad. Asimismo, el tribunal hace referencia a la proporcionalidad no sólo en el ámbito de las medidas de control sino también en el ámbito de sus consecuencias. En este sentido, se plantean las siguientes cuestiones.

- ¿ Se ha de tener en cuenta el perjuicio causado a la empresa para valorar la medida?

Un aspecto muy importante a la hora de elegir la medida de control que se va a aplicar, es el perjuicio que la presunta irregularidad del empleado ha causado a la empresa. Parece evidente que no es lo mismo que el trabajador intercambie mensajes puntuales con sus familiares, como ocurría en el caso Barbulescu, a que el empleado envíe datos confidenciales a la competencia, como se deducía de la sentencia del Tribunal Constitucional 170/2013¹⁰³. De hecho, en el primero de los casos, la Gran Sala del TEDH falló a favor del trabajador por considerar que se había producido una vulneración de su derecho a la intimidad y, en el segundo de los casos, el TC se pronunció a favor del empresario. A este respecto, cabe recordar que en los últimos tiempos se ha generalizado cierta tolerancia al uso moderado de los medios informáticos de la empresa¹⁰⁴.

- ¿ Se puede utilizar cualquier medida de control?

Es importante que en el ejercicio del poder empresarial se haga uso de la medida menos invasiva. Por ejemplo, en caso de tratarse de sospechas de un incumplimiento leve, parece mucho más razonable monitorizar únicamente la bandeja de entrada, sin llegar a acceder al contenido de los mensajes electrónicos. En este sentido, cabe recordar, que acceder al

¹⁰² SAN FULGENCIO, S, “ Recomendación del Consejo de Europa para la Protección de Datos el ámbito laboral: CM/rec (2015)5”, *Blog Cuatrecasas*, 2015 (disponible en <https://blog.cuatrecasas.com/propiedad-intelectual/recomendacion-del-consejo-de-europa-para-la-proteccion-de-datos-el-ambito-laboral-cmrec20155/>; última consulta 04/04/2015).

¹⁰³ Sentencia del Tribunal Constitucional de 7 de octubre 170/2013.

¹⁰⁴ ORTIZ DE SOLÓRZANO AURUSA, C., “Facultades empresariales de control, TICs y privacidad del trabajador”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n. 37, 2015, p.3.

contenido del correo electrónico del trabajador es una medida excepcional que sólo se ha de aplicar cuando sea estrictamente necesario y cuando se tengan evidencias de que los intereses de la compañía han sido gravemente perjudicados, como ocurría en la sentencia del Tribunal Constitucional 170/2013¹⁰⁵.

- ¿Se puede despedir al trabajador cuando la investigación revele un incumplimiento?

El empresario debe ponderar las consecuencias que el ejercicio de su poder de control tiene sobre el trabajador, de manera que las sanciones más severas deben estar reservadas a las faltas más graves. En la aplicación de estas sanciones se debe tener en cuenta, además, que los derechos del empleado tienen que interpretarse en todo caso de manera expansiva, nunca restrictiva¹⁰⁶.

Las consecuencias de la vigilancia deben, por tanto, adecuarse a la gravedad de los hechos descubiertos en el proceso de investigación, de manera que no todo incumplimiento del trabajador debe verse traducido en la sanción más grave, el despido. Por tanto, es fundamental que las acciones disciplinarias respondan a la infracción de manera ponderada¹⁰⁷.

Así, despedir a un empleado por usar ocasionalmente las herramientas informáticas para contactar con sus familiares resulta, cuanto menos objetable, sobre todo en el marco de una nueva realidad donde existe un margen de tolerancia al uso personal de los medios informáticos. En caso de que ese despido se hiciera efectivo, las consecuencias para la compañía serían mucho menos lesivas que para el trabajador y la medida sería, por ello, desproporcionada.

En contraposición, infracciones graves, como el envío de datos confidenciales a la competencia, sí pueden justificar sanciones más graves para el trabajador.

¹⁰⁵ Sentencia del Tribunal Constitucional de 7 de octubre 170/2013.

¹⁰⁶ MOLINA NAVARRETE, C. M., "El Poder empresarial de control digital...", *ob.cit.*, p.293.

¹⁰⁷ ABA-CATOIRA, A., "Los derechos de la generación electrónica en el ámbito laboral", *Revista de Derecho*, vol. 12, 2011, p. 264.

- ¿ Qué influencia tiene la posición jerárquica del infractor?

De lo previamente expuesto, parece deducirse que la severidad de la sanción por el incumplimiento descubierto tras el control empresarial, dependerá de la gravedad del mismo. Sin embargo, existen otros factores a tener en cuenta en el proceso sancionador, como el grado de responsabilidad de la persona que comete la falta.

Si el empleado que utiliza los medios electrónicos para fines extralaborales es una persona con una posición de responsabilidad, que deba de dar ejemplo a los demás, una medida fiscalizadora más invasiva, con repercusiones más graves, podría estar justificada.

Un claro ejemplo de la importancia de valorar la posición que ocupa el individuo que comete la irregularidad es la reciente sentencia del TEDH, del 22 de febrero de 2018¹⁰⁸. En este caso, una empresa pública ferroviaria decide despedir a un empleado cuando se descubren en su disco duro múltiples archivos pornográficos. El Tribunal Europeo de Derechos Humanos falla en contra del trabajador por considerarse sus acciones especialmente graves ya que, al ser el empleado un funcionario responsable de la vigilancia general, se esperaba de él un comportamiento ejemplarizante.

- ¿ Se puede controlar el correo electrónico personal?

Por último, resulta interesante recordar que el control ejercido sobre la mensajería electrónica debe reducirse a los correos corporativos. Si, por el contrario, el control recae sobre cuentas personales de correo electrónico, las comunicaciones quedan protegidas por el art.18 CE, que reconoce el derecho a la intimidad y al secreto de las comunicaciones.

Y es que, de forma generalizada, en aquellos supuestos en los que el empleado accede desde los dispositivos de la compañía a su cuenta personal, los tribunales tienden a inclinarse a favor de los derechos fundamentales del trabajador.

¹⁰⁸ Sentencia del Tribunal Europeo de Derechos Humanos de 22 de febrero de 2018, nº procedimiento 588/13 (caso Libert vs Francia).

En este sentido, destaca una sentencia del TSJ de Cataluña del año 2002¹⁰⁹, en la que se fallaba a favor de un empleado despedido, por considerar que los correos electrónicos aportados por la empresa habían sido obtenidos con una clara vulneración del derecho a la intimidad, ya que pertenecían a una cuenta personal de correo electrónico.

8.4. Principio de efectividad de la tutela

La sentencia Barbulescu exige, en el marco del control empresarial, que el trabajador sea protegido con las garantías pertinentes, poniendo especial hincapié en aquellas que impidan que el empleador aplique medidas de control sin el conocimiento previo de los empleados.

- ¿Qué garantías hay que ofrecer al trabajador?

La STS del 26 de septiembre de 2007¹¹⁰ determina que los medios electrónicos propiedad de la compañía no pueden ser considerados en ningún caso elementos personales, en la medida que se ponen a disposición del trabajador con el objeto de facilitar la prestación laboral¹¹¹. Esto significa que no será de aplicación el art 18 ET, que establece ciertos requisitos para llevar a cabo los registros de taquillas y efectos personales.

En consecuencia, el empresario puede ejercer su poder de control sobre los medios informáticos sin necesidad de que el trabajador esté presente, por considerarse que esto no atenta contra la dignidad del empleado. Asimismo, tampoco será necesario que el control se realice en el centro de trabajo y en horario laboral en cuanto que los dispositivos son de titularidad empresarial. Por último, tampoco se requerirá que esté presente un representante de los trabajadores, aunque esto, de acuerdo con el art 569 LECrim¹¹², reforzaría la validez de la prueba¹¹³.

¹⁰⁹ Sentencia del Tribunal Superior de Justicia de Cataluña de 9 de julio de 2002 (AS 2002\2811).

¹¹⁰ Sentencia del Tribunal Supremo de 26 de septiembre del 2007 (RJ 2007\7514).

¹¹¹ ABA-CATOIRA, A., “Los derechos de la generación electrónica ...”, *ob.cit.*, p. 274.

¹¹² Real decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (BOE 17 de septiembre de 1882).

¹¹³ ÁLVAREZ DE LINERA GRANDA, P. Y SÁNCHEZ MOURIZ, N., “Regulación del uso de las herramientas...”, *ob.cit.*

Por lo tanto, el correo electrónico corporativo no se debe equiparar a la taquilla del trabajador y, por ello, no es de aplicación el art 18 ET. En caso de ser así, se estaría reconociendo su carácter privado y la consecuente primacía del derecho a la intimidad, exigiéndose mayores garantías para el empleado.

Sin perjuicio de todo lo anterior, el empresario sí deberá garantizar al trabajador la transparencia en el uso y obtención de los datos personales¹¹⁴. En concreto, y en conformidad con la LOPDCP, el empleador deberá adoptar las medidas necesarias para proteger la seguridad de los datos y velar por que éstos se utilicen para el fin legítimo por el que fueron obtenidos.

Además, de acuerdo con la doctrina Barbulescu, el empresario debe ofrecer al trabajador todas las garantías necesarias que impidan inspeccionar el uso de los medios electrónicos sin la existencia de una advertencia previa a los empleados.

¹¹⁴ MARTÍNEZ FONS, D. *El poder de control del empresario en la relación laboral, ob.cit.*, p.220.

9. CONCLUSIONES

El desarrollo de las tecnologías tanto en el ámbito personal como en el profesional, ha dado lugar a situaciones en el entorno laboral en las que el uso o abuso por parte de los empleados de los recursos informáticos ha producido un aumento de las medidas de control de los sistemas y correos electrónicos corporativos. Si bien estas herramientas aumentan la productividad y rapidez de las tareas, también pueden propiciar el llamado absentismo presencial o, lo que es peor, ser utilizados en grave perjuicio de las empresas para, por ejemplo, enviar mensajes a la competencia. Por ello, en los últimos tiempos se han multiplicado los litigios relativos al control empresarial de los medios informáticos.

No obstante, a pesar de la frecuencia con la que se repiten estos casos, no existe regulación alguna que establezca los límites del poder de control empresarial, lo que aumenta la importancia de la jurisprudencia en esta materia. Tanto los tribunales internos como el Tribunal Europeo de Derechos Humanos se enfrentan habitualmente a litigios en los que tienen que ponderar el derecho a la intimidad, secreto de comunicaciones o protección de datos de los trabajadores frente al poder de vigilancia del empresario.

Esta ausencia de regulación, conduce a la **primera de las conclusiones** de este trabajo. La normativa constitucional y legislativa sobre los derechos a la intimidad, secreto de comunicaciones y protección de datos es insuficiente para dar respuesta a los litigios sobre el control del uso que los empleados hacen de las herramientas informáticas de la empresa. Por ello, es necesario el desarrollo legislativo de normas que regulen y modulen de manera específica el control de los empresarios sobre los medios informáticos corporativos.

En segundo lugar, se concluye que el contrato de trabajo no legitima en ningún caso al empresario a vulnerar los derechos que el trabajador, como cualquier ciudadano, posee. Es decir, la celebración de un contrato no priva a los empleados de los derechos que la Carta Magna les reconoce, aunque, en algunas circunstancias, se admite la imposición de ciertas limitaciones por parte del empleador.

La tercera conclusión, en línea con lo anteriormente expuesto, es que los derechos fundamentales no son absolutos, de manera que es posible su limitación a favor de otros intereses legítimos, siempre que ésta sea proporcionada. Esto no significa que el empresario pueda vulnerar arbitrariamente los derechos fundamentales del trabajador, sino que, en ocasiones, puede adoptar medidas de control que afecten a dichos derechos. Para que una actividad de inspección sea considerada una afectación legítima y no una vulneración de los derechos fundamentales, han de cumplirse tres requisitos: idoneidad, necesidad y proporcionalidad *stricto sensu*. Una medida de control será idónea si es adecuada para cumplir el objetivo que persigue; será necesaria si es la única manera de comprobar el incumplimiento del trabajador, y será estrictamente proporcionada cuando los beneficios para el interés general superen los perjuicios causados al resto de intereses en conflicto.

En cuarto lugar, este estudio confirma que, a pesar de que el despido suele ser la consecuencia más habitual del incumplimiento revelado por el control, también existen otro tipo de acciones disciplinarias. De hecho, puede ocurrir que empleados que no hayan sido despedidos acudan a los tribunales para demandar al empresario por la intromisión en sus derechos. Claro ejemplo de ello es la sentencia del Tribunal Constitucional 241/2012¹¹⁵, donde la trabajadora únicamente había sido amonestada. No obstante, en el caso de que la investigación efectivamente derivara en una medida extintiva de la relación laboral y el control no superara el test proporcionalidad, el despido podría declararse como improcedente o como nulo, en función de la doctrina aplicada. Por un lado, la teoría de la improcedencia considera que la ilicitud de la prueba no determina la nulidad de la medida extintiva. Por el otro, la teoría de la nulidad afirma que la ilicitud de la prueba debe llevarse a sus máximas consecuencias y determinar la nulidad del despido.

En quinto lugar, es importante recalcar que la mencionada ausencia de normativa específica propicia la creciente importancia de los tribunales en esta materia. Si bien en el pasado los tribunales tendían a favorecer más a los trabajadores, en los últimos años se ha producido una suavización de los requisitos que el empresario ha de cumplir para adoptar medidas intrusivas de los derechos fundamentales del empleado. Prueba de ello es la

¹¹⁵ Sentencia del Tribunal Constitucional de 17 de diciembre 241/2012.

sentencia del Tribunal Supremo del 6 de octubre de 2011¹¹⁶ y la del Tribunal Constitucional del 7 de octubre de 2013¹¹⁷, en las que se considera que la existencia de prohibiciones expresas de uso personal de los medios informáticos elimina la expectativa de intimidad del trabajador y legitima al empresario a adoptar medidas de control intrusivas sin que sea necesaria la previa advertencia al empleado.

La sexta conclusión se refiere a la posibilidad de que la doctrina sentada por los tribunales españoles pueda ser modificada por la sentencia Barbulescu, dictada el 5 de septiembre de 2017 por la Gran Sala del Tribunal Europeo de Derechos Humanos¹¹⁸. En esta sentencia se falla a favor del empleado y se establecen seis aspectos, desarrollados en este trabajo, que determinan si una medida de control empresarial, y concretamente la supervisión del correo electrónico, supone una vulneración de los derechos de los trabajadores. Sin perjuicio de otras consideraciones, lo cierto es que la sentencia de Barbulescu incorpora una peculiaridad: la exigencia de advertencia al trabajador independientemente de la existencia de prohibiciones expresas del uso personal de los medios electrónicos. Así, la nueva doctrina del TEDH se opone frontalmente, entre otras, a las mencionadas sentencias del Tribunal Supremo del 6 de octubre de 2011 y del Tribunal Constitucional del 7 de octubre de 2013.

Por último, **la séptima conclusión**, es la constatación de la nueva realidad que la doctrina Barbulescu parece confirmar: los empresarios deberían mostrarse más cautelosos con respecto a una serie de cuestiones, con el objeto de evitar intromisiones ilegítimas en los derechos de los empleados.

Por un lado, las empresas deben establecer normas claras sobre el uso de los medios informáticos, y advertir a los trabajadores sobre eventuales medidas de control, el alcance de las mismas y las herramientas empleadas para ello. Dicha advertencia debe ser en todo caso previa al control, pero no necesariamente tiene que ser individualizada para el

¹¹⁶ Sentencia del Tribunal Supremo de 6 de octubre de 2011 (RJ 2011\7699).

¹¹⁷ Sentencia del Tribunal Constitucional de 7 de octubre 170/2013.

¹¹⁸ Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, nº procedimiento 61496/08 (caso Barbulescu vs. Rumanía).

trabajador objeto de sospechas ni producirse inmediatamente antes del inicio de la inspección.

En segunda instancia, los empresarios deben diferenciar claramente entre el control ordinario o permanente y el control fiscalizador o excepcional. En el primero de los casos, el control debe ser mucho menos intrusivo, en cuanto que el fin que se persigue es el normal desarrollo de la actividad productiva. En el segundo caso, se permiten medidas más invasivas, ya que se fundamentan en la existencia de indicios de incumplimiento por parte de un trabajador. Así, el acceso al contenido de un correo electrónico sólo podría darse de manera excepcional como consecuencia de la existencia de graves sospechas o claras evidencias sobre el comportamiento irregular del empleado.

Por otro lado, las medidas tomadas por el empresario deben ser proporcionadas, teniendo en cuenta el perjuicio que el incumplimiento del trabajador podría estar causando en los intereses de la compañía, y la existencia de medidas alternativas menos lesivas para cumplir con el objetivo de la investigación. Así, el intercambio de mensajes de manera ocasional con familiares desde el correo corporativo de la empresa no justificaría medidas excesivamente intrusivas. En esta línea, las consecuencias del control deben adecuarse a la gravedad del incumplimiento descubierto, no siendo el despido la única solución. Asimismo, la posición del infractor en la organización y su eventual obligación de dar ejemplo, son factores a tener en cuenta a la hora de valorar las medidas de control y las consecuencias del mismo.

Finalmente, además de las cuestiones mencionadas, los empresarios deben ofrecer a los trabajadores garantías adicionales que aseguren la protección de los datos personales obtenidos en la investigación, y la existencia de normas que impidan la adopción de medidas de control sin la previa notificación a los empleados.

10. BIBLIOGRAFÍA

A) Referencias bibliográficas

ABA-CATOIRA, A., “Los derechos de la generación electrónica en el ámbito laboral”, *Revista de Derecho*, vol. 12, 2011, pp. 257-281.

ABAD BUSTILLO, A., “Tecnologías de la información y comunicación (TIC), control empresarial y derechos fundamentales”, *Repositorio de la Universidad de Cantabria*, 2015 (disponible en <https://repositorio.unican.es/xmlui/handle/10902/7014>.; última consulta 22/03/2018)

ÁLVAREZ DE LINERA GRANDA, P. y SÁNCHEZ MOURIZ, N., “Regulación del uso de las herramientas tecnológicas en la empresa: El protocolo telemático”, *Jornada de 10 de marzo de uso y no abuso de los recursos tecnológicos en la empresa, organizada por Cámara Oficial de Comercio, Industria y Navegación de Gijón, Cobertura Informática y Garrigues*, 2011.

ANDERSEN TAX & LEGAL, “La Sentencia dictada por la Gran Sala del Tribunal Europeo de Derechos Humanos en fecha 5 de septiembre de 2017, sobre el control por el empresario del uso del correo electrónico”, *Publicaciones Derecho Laboral Andersen Tax & Legal*, 2017 (disponible en <http://www.andersentaxlegal.es/es/publicaciones-y-noticias/la-sentencia-dictada-por-la-gran-sala-del-tribunal-europeo-de-derechos-humanos-de-5-de-septiembre-de-2017-sobre-el-control-por-el-empresario-del-.html>.; última consulta 25/03/2018).

BARROS GARCÍA, M., “Problemas derivados de la utilización del correo electrónico e Internet en el ámbito laboral”, *Actualidad Jurídica Uría & Menéndez*, n.8, 2004, pp. 51-63.

BAZ RODRÍGUEZ, J., "Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre [BOE n. ° 267, de 7-XI-2013]: control empresarial de la utilización, por parte de los trabajadores, de los medios informáticos de la empresa (correo electrónico). Inexistencia de vulneración de los derechos a la intimidad personal y familiar (artículo 18.1 CE).", *Ars*

Iuris Salmanticensis (AIS): revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología, vol.2, n.1, 2014, pp.364-367

BUJALDÓN TARRIDA, A., “Barbulescu II: cambio de criterio jurisprudencial”, *El jurista*, 2017 (disponible en <http://www.eljurista.eu/2017/10/09/barbulescu-ii-cambio-de-criterio-jurisprudencial/>; última consulta el 09/04/2018).

CARBONELL MURIO, J., “Efectos de la prueba ilícita en la calificación del despido”, *Foro Español de Laboristas*, 2013 (disponible en <http://forelab.com/home/premios-forelab/ii-premio-jovenes-laboralistas-2013-finalistas/>; última consulta 28/03/2018).

CARRIZOSA PRIETO, E., “El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores”, *Temas laborales: Revista andaluza de trabajo y bienestar social*”, n.116, 2012, pp. 251-268.

COLÀS-NEILA, E., “La amenaza de los derechos del trabajador derivada de la innovación tecnológica en la empresa”, *Creatividad y sociedad*, n.26, 2016, pp. 259-286.

CUADROS GARRIDO, M. E., “La mensajería instantánea y la STEDH de 5 de septiembre de 2017”, *Revista Aranzadi Doctrinal*, n.11, 2017 (disponible en <http://aranzadi.aranzadidigital.es/maf/app/document?docguid=Id21b2b50c68711e794c201000000000&srguid=i0ad82d9b000001629cb7ae0b2f624e15&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificacionMagazines=&fechacomun=&numeropub-tiponum=>; última consulta 15/03/2018).

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

DÍAZ CABIALE, J. A. y MARTÍN MORALES, R., *La Garantía constitucional de la inadmisión de la prueba ilícitamente obtenida*, Civitas, Madrid, 2001.

DOCTOR, R. y VALENTÍN, G., “1 jornadas de litigación laboral de Cuatrecasas: la video vigilancia y la prueba digital, a debate”, *Blog Cuatrecasas*, 2017 (disponible en

<https://blog.cuatrecasas.com/laboral/i-jornadas-de-procesal-laboral-de-cuatrecasas-la-video-vigilancia-y-la-prueba-digital-a-debate/>; última consulta 08/04/2018).

FABREGAT MONFORT, G., “El control empresarial de los trabajadores a través de las nuevas tecnologías: algunas ideas clave”, *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, n. 5, 2015, pp.76-83.

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

FORTEZA LAHERA, J., “Nueva vuelta de tuerca sobre el correo empresarial del correo electrónico corporativo de los trabajadores. Sentencia TEDH 5 de septiembre 2017 (asunto Barbulescu)”, *Relaciones Laborales*, n.128, 2017, pp.70-72.

GARCÍA ROPERÓ, J. y SAMPERE, P., “¿ Cuándo puede (y cuando no) la empresa espiar mis correos?”, *Cinco días - El país*, 2017 (disponible en https://cincodias.elpais.com/cincodias/2017/09/05/fortunas/1504637748_187161.html; última consulta 05/04/2018).

GARCÍA, L, “El caso Barbulescu y el control de las comunicaciones informáticas de los empleados”, *Newsletter Laboral Garrigues*, 2017 (disponible en http://www.garrigues.com/sites/default/files/documents/newsletter-laboral-septiembre_2017_0.pdf; última consulta 03/04/2018).

LÓPEZ DE LA FUENTE, “La doctrina jurisprudencial del tribunal europeo de derechos humanos sobre el control de las comunicaciones electrónicas en el trabajo: ¿el fin de una eterna cuestión?”, *Revista de estudios europeos*, n.69, 2017, pp. 5-16.

LLUCH CORELL, F.J., “ El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador, *El Derecho*, 2017 (disponible

en http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronico-trabajador_11_1045180003.html ;última consulta 25/03/18).

MARTÍNEZ FONS, D., *El poder de control del empresario en la relación laboral*, Consejo Económico y Social (CES), Madrid, 2002.

MIRÓ MORROS, D., “ El uso del correo electrónico en la empresa: protocolos internos”, *Actualidad jurídica Aranzadi*, n. 874, 2013 (disponible en <http://aranzadi.aranzadidigital.es/maf/app/document?docguid=I57e7962057e111e39a4901000000000&sruid=i0ad82d9b000001629caa97e704e0e05c&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificationMagazines=&fechacomun=&numeropub-tiponum>; última consulta el 04/04/2018).

MOLERO MANGLANO, C., SÁNCHEZ- CERVERA VALDÉS, J. M., LÓPEZ ÁLVAREZ, M. J., y MATORRAS DÍAZ-CANEJA, A., *Manual de derecho del trabajo* Tirant lo Blanch, Valencia, 2017.

MOLINA NAVARRETE, C. M., “El Poder empresarial de control digital:¿ nueva doctrina del TEDH o mayor rigor aplicativo?. A propósito de la STEDH de 5 de septiembre de 2017, caso Barbulescu c. Rumania”, *IusLabor*, n.3, 2017, pp. 287-297.

MONEREO PÉREZ, J. L. y LÓPEZ INSUA B. M., “El control empresarial del correo electrónico tras la STC 170/2013”, *Aranzadi Social*, n. 11, 2014 (disponible en <http://aranzadi.aranzadidigital.es/maf/app/document?docguid=I50f9e6308e1c11e3a97d010000000000&sruid=i0ad82d9a000001629c95754705e90db7&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificationMagazines=&fechacomun=&numeropub-tiponum>; última consulta 04/04/2018).

ORTIZ DE SOLÓRZANO AURUSA, C., “Facultades empresariales de control, TICs y privacidad del trabajador”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n. 37, 2015, pp. 41-72.

PÉREZ DE LOS COBOS, 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 del trabajo*, n. 196, 2017, pp. 41-54.

POQUET CATALÁ, R., “La protección del derecho a la intimidad del teletrabajador”, *Lex Social: Revista de Derechos Sociales*, vol. 8, n. 1, 2018, pp. 113-135.

PRADA BAUTISTA, A., “Nulidad del despido por ilicitud de los medios de prueba: análisis jurisprudencial”, *Repositorio institucional Universidad de Oviedo*, 2016 (disponible en <http://digibuo.uniovi.es/dspace/handle/10651/34556>; última consulta 13/04/18).

PRECIADO DOMENECH, C.H., “Comentario de Urgencia a la STEDH de 5 de septiembre de 2017. Caso Barbulescu contra Rumanía (Gran Sala). Recuperando la dignidad en el trabajo”, *Revista Jueces para la Democracia, Jurisdicción Social*, n.10, 2017 (disponible en <http://aranzadi.aranzadidigital.es/maf/app/document?docguid=177861700f80911e7b1a501000000000&srcgu id=i0ad82d9b000001629caf1fc7fde3afdb&src=withinResuts&spos=1&epos=1&displayid=&publicacion=& clasificacionMagazines=&fechacomun=&numeropub-tiponum=>; última consulta 06/04/2018).

PRECIADO DOMENECH, C.H., “Nuevas formas de prueba basadas en las tecnologías de la información y la comunicación (TIC). Documento electrónico y prueba digital: Proposición y práctica. Ilicitud de estas pruebas por vulneración de derechos fundamentales”, *Actum social*, n.131, 2017, p. 11-34.

RODRÍGUEZ ESCANCIANO, S., “El control empresarial de la mensajería electrónica como prueba de la transgresión de la buena fe contractual: A propósito de la STC de 7 de octubre de 2013”, *Diario La Ley*, n. 8195, 2013 (disponible en http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAE1RS08DIRD-NeVCY ugr1QMHu-3BRI2xq dZmG5RCivMtt1 76zsQZIP5vHNI npMQ013kjP- oWam72XJgZK0Us8dwkzJAdeWpQe5BIDhi9Ms14ptCDRo6E_7bgMzgCHnqPsUo8NTCGUIOSW87iJNt mbHgPII5ZqYKgHP1uCfOTw2BVudhQn- qGuRmkzXpHJTcJR5I6Xlg8hhuGsa64rCJqs50rNNmbEnLFkrBhrxoZxz3gYfUqUurto9HyU3QVraPRaxG QxbQetBEUC 46cU- RTvL7CxbVALoYtpFLRWat3teKzUOv1aiEumDIT9KdrMRCKk2tPzwwqfMjZ5ar88ZPV-

ybG73pXFXs9dKhfkKCo7xBa5C4yQjKnN2CFm-15DxTvIHc34cM3Ww5_pL_4vCqXbB4qyDZx2DH7QqXPwKPI8H_55a8256I-20oFJ8wnt8dEFbgMdhp0l83BR0FKwIAAA==WKE ; última consulta 05/04/2017).

RODRÍGUEZ ESCANCIANO, S., “Internet en el trabajo”, *Diario La Ley*, n. 8926, 2017. (disponible en http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAC2PwU7DMAyGn4ZcKqF03TQ45NKWAXIgNAJ3t7XaQJaM2C3r2-MSIn1ybP-O_3zPmFaLVzYuMKaAXGAo0BecoIPPqGgNMMaxnY9OMiqEjU2p9c-w3SqES9sJBOAp3wv3W0wp6nsG3sTfldncLWui2cRXTgKlejVYcGfwJyVSloin-vMDiRmAXQw0pL3XDYFqr5ez2O10d1IKJRGa-3lhiWk1unJ4EznogctTEwCn6x8E8dDF-2bbJdbte0DwjQ05PEEYUG4SQ-ukVJBG_81nejbdAl6ty9B7EOYF_-9PkHVlfz8zio-OQe6r3EltgbMBjGP5_8AtkXkUKZAEAAA==WKE ; última consulta 05/04/2017).

RUBIO ALAMILLO, J., “El correo electrónico como prueba en los procedimientos judiciales”, *Diario la Ley*, n.8808, 2016 (disponible en http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAE2QTU_DMAyGf01zqYT_SbmPjkAPduCGEoHB3E9MasmTLR7f-e9yVA5EeJY5f2698zhimFq9JFbmWIX6ypfYhoC_Rok6hyFJ-rRxpz_9HX55Cyg5KdKX1kSOv0dCR0CUOv7MhTWAX3pqZotaliJPzbjqlitFgi6qSspiq2cqZsWsmQ2zZX_bMw5yTAnTKYA9eq2p-04gtdGojfDAYmklJkXwC-4ZR1Q8iDv7yAiP1kMi7BsIykoXrh1byqVf31XonRgyRBeqTeraNYqB-eGbSoo8IQQ-v0KNqejxnNHAH8XQV1v2wlfdbepGOhBdFzuB1D8E8OjMvUID8cGw1gv2vXdo2OSUe3SW35IS2fB8g4_Z7X5syf6V-u9lN_lgEAAA==WKE ; última consulta 05/04/2017).

SAN FULGENCIO GUTIÉRREZ, J.A. , “¿Es privado el Email?”, *Boletín del Ilustre Colegio de Graduados Sociales de Madrid*, n.37, 2002, p. 33.

SAN FULGENCIO, S, “ Recomendación del Consejo de Europa para la Protección de Datos el ámbito laboral: CM/rec (2015)5”, *Blog Cuatrecasas*, 2015 (disponible en <https://blog.cuatrecasas.com/propiedad-intelectual/recomendacion-del-consejo-de-europa-para-la-proteccion-de-datos-el-ambito-laboral-cmrec20155>; última consulta 04/04/2015).

SAN MARTÍN MAZZUCCONI, C. , *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, Eolas, León, 2014.

SÁNCHEZ, L. J. ,“¿Pueden las empresas controlar el correo electrónico de sus trabajadores?”, *Confilegal*, 2018 (disponible en <https://confilegal.com/20180209-pueden-las-empresas-controlar-el-correo-electronico-de-sus-trabajadores/>; última consulta 02/04/2018).

SEGOVIANO ASTABURUAGA, M. L., “El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores”, *Revista jurídica de Castilla y León*, n.2, 2004, pp- 147-190.

SUÁREZ ESPINO, M. L., “La intimidad de los trabajadores en el centro de trabajo y el poder de vigilancia del empresario”, *Diario La Ley*, n. 7906, 2012 (disponible en [TASCÓN LÓPEZ, R., “El lento \(pero firme\) proceso de decantación de los límites del poder de control empresarial en la era tecnológica”, *Aranzadi social*, n.17, 2007 \(disponible en \[; última consulta 07/04/2018\\).\]\(http://aranzadi.aranzadidigital.es/maf/app/document?docguid=Ic29bae20bfe911dc95e301000000000&srguid=i0ad82d9a000001629cb142529c6b75d2&src=withinResuts&spos=1&epos=1&displayid=&publicacion=&clasificationMagazines=&fechacomun=&numeropub-tiponum=\)](http://laleydigital.laley.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAE1RwU7EIBD9GrmQmNbdza4HDm7rwWQ1Rqv3aZm0uJSpQLv3cQD5K8wLx5DO-F7xn92uA1qhNI46IZjQYtNUpLQUYPLXyBjO9BopNoZYcuekqC3CS5JnoijT6xi-mNBdcZ4MpKHCE-C96QCKsjt46q8TOKCG1QZVHc7LuEkrFhbBk7xp5xYNynXiGgizPYmjpVprNZsIFW7QR5fvW4qkJEimDfMKi7nQgDXV6AjUA05I7g85NGa1U3Ba_ysD1stmJBH1igPk3PoVAMph9OjJ1EIIJFaW49kmrx5bo3NRV5pt1QvWMEXL5Bq5HthEQfDe8Ahfsdh55Lt1CmK7CujMz77_9PH8xeFHGabxW4PWD0-kbhAkfvMFsP-1ee5xjpH9ttHlnugs7zVErMCi039JfwCsCLhz1AEAAA==WKE; última consulta 05/04/2017)</p></div><div data-bbox=)

URÍA MENÉNDEZ, “ Pautas de revisión del correo electrónico tras Barbulescu: La sentencia del Tribunal Supremo del 8 de febrero de 2018”, *Noticias Uría Menéndez*, 2018 (disponible en <http://www.uria.com/es/actualidad/Noticias.html?id=1113>; última consulta 20/03/2018).

B) Fuentes legales

Normativa interna

- Constitución española (BOE 29 de diciembre de 1978).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE 14 de diciembre de 1999).
- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).
- Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social (BOE 11 de octubre de 2011).
- 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).
- Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. (BOE 17 de septiembre de 1882).
- Proyecto de Ley Orgánica 121/000013, de Protección de Datos de Carácter Personal (BOCG de 24 de noviembre de 2017).

Normativa europea

- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de datos de carácter personal (BOE 15 de noviembre de 1985).
- Convenio Europeo para la Protección de los Derechos Humanos y Libertades fundamentales, de 4 de noviembre de 1950 (BOE 10 octubre de 1979).

- Reglamento 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DOUE 4 de mayo de 2016).
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE 23 de noviembre de 1995).
- Recomendación del Comité de Ministros del Consejo de Europa CM/Rec(2015)5, de 1 abril de 2015, sobre el tratamiento de datos personales en el ámbito laboral.

C) Jurisprudencia

Tribunal Europeo de Derechos Humanos

- Sentencia del Tribunal Europeo de Derechos Humanos de 22 de febrero de 2018, nº procedimiento 588/13 (caso Libert vs Francia).
- Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, nº procedimiento 61496/08 (caso Barbulescu vs. Rumanía).
- Sentencia del Tribunal Europeo de Derechos Humanos de 3 de abril de 2007, nº procedimiento 62617/00 (caso Copland vs Reino Unido).
- Sentencia del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997, nº procedimiento 20605/92 (caso Halford vs. Reino Unido).

Tribunal Constitucional

- Sentencia del Tribunal Constitucional de 7 de octubre 170/2013.
- Sentencia del Tribunal Constitucional de 11 de febrero 29/2013.
- Sentencia del Tribunal Constitucional de 17 de diciembre 241/2012.
- Sentencia del Tribunal Constitucional de 2 de julio 142/2012.
- Sentencia del Tribunal Constitucional de 7 de noviembre 173/2011.
- Sentencia del Tribunal Constitucional de 15 de noviembre 196/2004.
- Sentencia del Tribunal Constitucional de 10 de abril 98/2000.
- Sentencia del Tribunal Constitucional de 11 de abril 99/1994.
- Sentencia del Tribunal Constitucional de 20 de julio 254/1993
- Sentencia del Tribunal Constitucional de 30 de octubre 170/1987.
- Sentencia del Tribunal Constitucional de 19 de julio 88/1985.

Tribunal Supremo

- Sentencia del Tribunal Supremo de 8 de febrero de 2018 (RJ 2018\666).
- Sentencia del Tribunal Supremo de 21 de septiembre de 2015 (RJ 2015\4353).
- Sentencia del Tribunal Supremo de 21 de junio de 2012 (RJ 2012\7627).

- Sentencia del Tribunal Supremo de 6 de octubre de 2011 (RJ 2011\7699).
- Sentencia del Tribunal Supremo de 8 de marzo de 2011 (RJ 2011\932).
- Sentencia del Tribunal Supremo de 26 de septiembre del 2007 (RJ 2007\7514).

Tribunales Superiores de Justicia

- Sentencia del Tribunal Superior de Justicia de Madrid de 13 mayo de 2016 (AS 2016\1166).
- Sentencia del Tribunal Superior de Justicia de Castilla La Mancha de 10 de junio de 2014 (AS 2014\1619).
- Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de 16 de febrero de 2010 (AS 2010\945).
- Sentencia del Tribunal Superior de Justicia de Cataluña de 9 de julio de 2002 (AS 2002\2811).
- Sentencia del Tribunal Superior de Justicia de Galicia, de 30 de noviembre de 2001 (AS 2002\390).

Juzgados

- Sentencia del Juzgado de lo Social de Madrid nº 33, de 4 de marzo de 2002 (JUR 2002\216228).