Revista de Estudios Europeos
n. 69, enero-junio, 2017, 5-16
ISSN: 2530-9854. http://www.ree-uva.es/

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? [1]

THE DOCTRINE OF THE EUROPEAN COURT OF HUMAN RIGHTS ON THE CONTROL OF ELECTRONIC COMMUNICATIONS AT WORK: THE END OF AN ETERNAL QUESTION?

Graciela LÓPEZ DE LA FUENTE
Universidad de Valladolid

Resumen: Los controles empresariales de la actividad laboral desarrollada a través de medios tecnológicos se transforman provocando conflictos de intereses con los derechos de los trabajadores como el derecho a la intimidad, al secreto de las comunicaciones e incluso, a la autodeterminación informativa. En ausencia de criterios legales claros, la vigilancia intencional del empresario y su confrontación con los derechos de los trabajadores sigue generando un intenso debate doctrinal y jurisprudencial sobre la determinación de sus límites. Sin duda, la Recomendación del Consejo de Europa para la protección de datos en el ámbito laboral de 1 de abril de 2015, el Reglamento (UE) 2016/679 de protección de datos, como la última sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Barbulescu contra Rumanía) resultan muy interesantes pues parecen poner un punto y final al eterno debate, obligando a nuestros tribunales a revisar su doctrina.

Abstract: The business controls of the labor activity developed through technological means are transformed causing conflicts of interest with the rights of workers as the right to privacy, the secrecy of communications and even, self-determination information. In the absence of clear legal criteria, the intentional monitoring of the employer and his confrontation with workers' rights continues to generate an intense doctrinal and jurisprudential debate about the determination of their limits. Undoubtedly, the Council of Europe Recommendation for data protection in the labor field of 1 April 2015, Regulation (EU) 2016/679 on data protection, such as the last judgment of the European Court of Human Rights of 5 of September 2017 (Barbulescu v. Romania) are very interesting because they seem to put an end to the eternal debate, forcing our courts to review its doctrine.

Palabras clave: Derecho a la intimidad, secreto de las comunicaciones, derecho a la autodeterminación informativa, vigilancia y control empresarial, juicio de proporcionalidad, expectativa razonable de intimidad.

Key-words: Right to privacy, secrecy of communications, right to self-determination information, supervision and employer control, proportionality judgment, reasonable expectation of privacy.

1. La digitalización del trabajo y nuevas formas de control empresarial: nuevas soluciones, viejos problemas.

La progresiva tendencia hacia una digitalización del trabajo en la que nos encontramos tiende a formar un tipo de "trabajador transparente estrechamente vigilado, conocido en gran parte de sus facetas gracias a la elaboración de su perfil completo, capaz de llevar en su manifestación extrema a un –intolerable –control total de los empleados en la empresa"[2]. El "Gran Hermano", como metafó-

1 El presente estudio se realiza en el marco del Proyecto de investigación DER2016-75993-P, sobre España ante Europa: retos nacionales en materia de derechos humanos, que se desarrolla entre el 30 de diciembre de 2016 y el 29 de diciembre 2020.

2 San Martín Mazzucconi, Carolina, Sempere Navarro, Antonio V., "Las TICS en el ámbito laboral", Francis Lefebre, Madrid, 2015, p. 39 citado por Alemán Páez, Francisco, "Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores", Derecho de las Relaciones Laborales, nº 6, 2016, p. 612.

ricamente denomina a las TICs el profesor Alemán Páez, "penetra abyectamente en 'la caja negra de cada individuo' y quiebra con facilidad el derecho a una 'razonable expectativa de intimidad'"[3]. Asistimos en la época actual, a una producción masiva de datos en la que los derechos de los trabajadores (intimidad, privacidad…) son altamente vulnerables. Sin negar las bondades que aportan los avances tecnológicos en la actividad empresarial, como son la mejora de su rentabilidad, la reducción de costes o incluso la conquista de nuevos mercados gracias al comercio electrónico, no es menos cierto también, que puedan producirse conflictos de intereses entre el empresario y los trabajadores derivados del uso de estas herramientas de trabajo. Dada la escasez de normas claras al respecto, surgen problemas derivados de la mayor información obtenida a través de nuevos medios.

En las relaciones laborales actuales la estricta separación entre la vida privada y la vida profesional se vuelve un terreno delicado fundamentalmente con la llegada de las nuevas tecnologías de la información y de la comunicación. Por una parte, resulta cada vez más extendida la práctica de responder a llamadas o contestar correos fuera del horario laboral, durante los períodos reconocidos de descanso para el trabajador, provocando un aumento de la tensión en el entorno laboral y del síndrome de burnout. Ante este fenómeno y a modo de ejemplo, el 1 de enero de 2017 entró en vigor en Francia el derecho a la desconexión digital del trabajador una vez finalizada la jornada laboral - droit à la déconnexion- introducido por la Ley 2016-1088, de 8 de agosto de 2016, conocida como Loi Travail o Loi El Khomri[4].

Por otra parte, fruto también del desarrollo de las TICs, se produce, en ocasiones, un manejo de los medios informáticos por los trabajadores durante la jornada laboral para fines particulares o en todo caso, extralaborales. Es el denominado "cyberslacking" que tanto preocupa a las empresas por el elevado coste que representa. Es comprensible que el empresario quiera asegurarse del rendimiento regular de sus empleados introduciendo medios de vigilancia directa o intencional. Ahora bien, es necesario buscar un punto de equilibrio entre el poder de control del empresario y los derechos de los trabajadores en la empresa que pueden resultar lesionados. Con frecuencia estos conflictos surgen, como bien afirma Aragón Gómez, "como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador o del teléfono de empresa y de la generalización de una cierta tolerancia a un uso moderado de los medios de la empresa"[5].

La realidad es que nos encontramos con una insuficiencia legislativa al respecto y la jurisprudencia ha venido solucionando la interminable problemática de la digitalización del trabajo y las conductas empresariales tendentes a vulnerar derechos fundamentales de los trabajadores. De acuerdo con Alemán Páez, "la no disposición de instrumentos jurídicos adecuados con los que atajar violaciones de derechos realizables mediante las TICS son factores que facilitan la dilución de responsabilidades en la gestión ilícita de dichas herramientas"[6].

Ante esta situación resulta sumamente interesante la Recomendación CM/Rec(2015)5 del Consejo de Europa para la protección de datos en el ámbito laboral adoptada por el Comité de Ministros el 1 de abril de 2015[7] que, como veremos, establece unas pautas divergentes respecto de nuestra doctrina judicial más reciente. Lo más relevante de la Recomendación es que en relación con el uso de los medios informáticos de la empresa por los trabajadores es necesario adoptar medidas preventi-

3 Alemán Páez, Francisco, "Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores", *Derecho de las Relaciones Laborales*, nº 6, 2016, p. 612 y San Martín Mazzucconi, Carolina, Sempere Navarro, Antonio V., "*Las TICS en el ámbito laboral*", Francis Lefebre, Madrid, 2015, pp. 39-167. Véase también al respecto: Marguénaud, Jean-Pierre; Mouly, Jean, "Big Boss is watching you – Alerte sur le contrôle des activités électroniques du salarié: (obs/s. Cour eur. Dr. H., Barbulescu c. Roumanie, 12 janvier 2016)" *Revue trimestrielle des droits de l'homme,* nº 108, 2016, pp. 1037-1048.

4 Loi nº 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels, Journal Officiel de la République Française nº 0184, 9 de agosto de 2016. Sobre esta novedosa cuestión véase: Alemán Páez, Francisco, "El derecho a la desconexión digital: una aproximación conceptual, crítica y contextualizadora al hilo de la 'Loi Travail Nº 2016-1088'", *Trabajo y derecho*, nº 30, 2017, pp. 12-33.

5 Argumentos similares que se recogen en las SSTS de 26 de septiembre de 2007, de 8 de marzo de 2011 y de 6 de octubre de 2011. Aragón Gómez, Cristina, "Artículo 20. Dirección y control de la actividad laboral", en: Cruz Villalón, Jesús, García-Perrote Escartín, Ignacio, Goerlich Peset, José María, Mercader Uguina, Jesús R. (Dirs.), *Comentarios al Estatuto de los Trabajadores*, Thomson Reuters, Pamplona, 2014, p. 288.

6 Alemán Páez, Francisco, "Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores", *Derecho de las Relaciones Laborales*, nº 6, 2016, p. 605.

7 En: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID= 09000016805c3f7a

vas evitando o limitando al máximo el control o la monitorización de la actividad para que no se produzcan los atentados a los derechos de los trabajadores. Asimismo, la Recomendación señala que hay que evitar la monitorización ininterrumpida y absoluta del trabajador durante la prestación de servicios. Y en su caso, de ser una medida necesaria, se deberán de respetar garantías adicionales y consultar con los representantes de los trabajadores. Igualmente, debemos destacar en el ámbito de la Unión Europea, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos[8] que entrará en vigor el 25 de mayo de 2018 y que está destinado a lograr una regulación más uniforme del derecho fundamental a la protección de datos[9]. Cabe por último añadir que, en virtud del Reglamento (UE) 2016/679 se ha impulsado un Anteproyecto de Ley Orgánica en nuestro país que derogará la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Esta revolución tecnológica ha influido inevitablemente en la prestación de servicios generando, a su vez, una serie de conflictos laborales de solución compleja. Así, el punto central de la cuestión se ubica en la fijación de los límites del uso de los medios tecnológicos de la empresa para fines privados y el posible control empresarial sobre los mismos. En definitiva, los medios de control se vuelven más sofisticados pero el problema que subyace sigue siendo el mismo: la problemática determinación de los límites al poder de control empresarial sobre el uso que hace el trabajador de los medios facilitados por la empresa. En palabras de San Martín Mazzuconi y Sempere Navarro, "se trata de conflictos a los que el ordenamiento laboral debe dar solución, y que replantean el debate sobre la esfera privada del trabajador en el seno de la empresa; o si se prefiere: estamos ante un nuevo episodio de la discusión sobre el alcance de los derechos fundamentales"[10]. Son viejos problemas a los que, debido a las nuevas herramientas digitales o tecnológicas, hay que aportar nuevas soluciones.

Se trata de saber si el empleador puede vigilar y bajo qué condiciones, los correos, sistemas de mensajería y de navegación por Internet, entre otros, que el trabajador utiliza durante su jornada laboral.

2. La evolución de la doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos sobre la fijación de los límites al poder de vigilancia y control.

La doctrina del Tribunal Europeo de Derechos Humanos es extensa en la materia, ya que existen diversos pronunciamientos en torno al derecho a la intimidad, y específicamente, como veremos, en relación al control empresarial sobre el uso de los equipos informáticos o telefónicos en el entorno laboral. La reciente solución adoptada por el Tribunal de Estrasburgo en el asunto Barbulescu contra Rumanía parece, sin embargo, dar una respuesta final aproximándose a una jurisprudencia anterior, favorable a una interpretación más conservadora o protectora de la noción de "vida privada" y de los derechos de los trabajadores (casos Copland y Halford).

2.1. La primera doctrina del Tribunal Europeo de Derechos Humanos: los casos Copland y Halford.

La doctrina anterior del Tribunal Europeo de Derechos Humanos al caso Barbulescu, favorable a una interpretación protectora derivada de una aplicación amplia del art. 8 del CEDH, se fundamenta en el criterio de la "expectativa razonable de intimidad o confidencialidad". Concretamente, este criterio, que posteriormente encontraremos en nuestra doctrina judicial, aparece en los pronunciamientos más importantes: la STEDH de 25 de junio de 1997 (caso Halford contra Reino Unido) y la STEDH de 3 de abril de 2007 (caso Copland contra Reino Unido). Los dos asuntos versan sobre la

8 En: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri= CELEX%3A32016R0679

9 Véase al respecto: Goñi Sein, José Luis, "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores. Análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016", *Revista de derecho social*, nº 78, 2017, pp. 15-42.

10 San Martín Mazzucconi, Carolina y Sempere Navarro, Antonio V., "Las TICS en el ámbito laboral", Francis Lefebre, 2015, p. 10

licitud de los controles realizados por el empleador en relación con el necesario respecto del art. 8 del Convenio Europeo de Derechos Humanos.

En el asunto Copland, el Tribunal de Estrasburgo considera que los trabajadores mantienen su derecho a la intimidad en la empresa, incluso cuando los dispositivos electrónicos pertenezcan a la misma y se utilicen durante las horas de trabajo. Afirmando en este sentido el TEDH que las llamadas telefónicas procedentes del ámbito laboral forman parte del concepto de "vida privada" y "de correspondencia" a los efectos del art. 8.1 del CEDH[11]. Del mismo modo, esta protección se hace extensible a los correos electrónicos enviados desde el lugar de trabajo y a la información derivada del seguimiento navegación en internet[12]. Así, la naturaleza privada prevalece al no haber advertido, en este caso, a la trabajadora de que sus llamadas iban a ser controladas, por lo que podía razonablemente confiar en el carácter privado de las comunicaciones[13].

El Tribunal, a pesar de lo anterior, no excluye la posibilidad de que puedan realizarse determinados controles "necesarios en una sociedad democrática", y por tanto lícitos, sobre el uso que hacen los trabajadores del teléfono, del correo electrónico o de internet en la empresa. Sin embargo, las injerencias al derecho solo se encuentran amparadas si se realizan con consentimiento del titular o si están contempladas de forma expresa y clara en una ley. Sólo de este modo, según entiende el Tribunal, se cumple con la exigencia de previsibilidad y los ciudadanos pueden conocer con suficiente claridad las circunstancias y condiciones de la limitación[14].

2.2. La doctrina reciente del Tribunal Europeo de Derechos Humanos: el caso Barbulescu.

La reciente sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos, de 5 de septiembre de 2017, Barbulescu contra Rumanía (asunto 61496/08)[15] ha provocado múltiples reacciones dada la importante cuestión que aborda y que parece poner fin a un eterno debate. La sentencia, ya inapelable, se pronuncia con motivo de un recurso a una sentencia anterior del TEDH de 12 de enero de 2016[16] que pasamos a comentar.

2.2.1. Los antecedentes del caso y la sentencia del TEDH de 12 de enero de 2016.

Para analizar la argumentación del TEDH es necesario detenerse en los hechos y antecedentes del caso, concretamente, en la STEDH de 12 de enero de 2016, primer pronunciamiento en este asunto[17], que será corregido en la sentencia posterior de la Gran Sala del TEDH de 5 de septiembre de 2017.

Este concreto supuesto tiene como origen el despido de un trabajador por realizar un uso personal e indebido de la cuenta de mensajería instantánea puesta a disposición por la empresa para fines exclusivamente profesionales. Concretamente, el trabajador desempeñaba sus funciones como encargado de ventas para la empresa desde el año 2004. A petición de esta, el trabajador abrió una cuenta de Yahoo Messenger (cuenta de mensajería instantánea) para su uso profesional, fundamentalmente, para atender las peticiones y consultas de los clientes.

---

11 STEDH de 3 de abril de 2007, Copland contra Reino Unido, apartado 41; STEDH de 25 de junio de 1997, Halford contra Reino Unido, apartado 44.

12 STEDH de 3 de abril de 2007, Copland contra Reino Unido, apartado 42.

13 STEDH de 3 de abril de 2007, Copland contra Reino Unido, apartado 42; STEDH de 25 de junio de 1997, Halford contra Reino Unido, apartado 45.

14 STEDH de 3 de abril de 2007, Copland contra Reino Unido, apartados 45 a 47.

15 https://www.doctrine.fr/d/CEDH/HFJUD/GRANDCHAMBER/2017/CEDH001-177083

16 La sentencia se encuentra disponible en inglés en: http://hudoc.echr.coe.int/eng?i= 001-159906

17 Al respecto véase también: Goñi Sein, José Luis, "La vigilancia empresarial de la conversaciones electrónicas de los trabajadores: A propósito de la sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016, 'Barbulescu v. Rumanía'", *Trabajo y derecho*, nº 18, 2016, pp. 78-84; Bermejo Bosch, Reyes, Botella Vivó, Santiago, "La sentencia del TEDH sobre el control por el empleador del uso del correo electrónico (mensajería instantánea) por sus empleados (caso Barbulescu v. Rumanía Nº. 61496/08 de 12 de enero de 2016)", *Actualidad jurídica Uría Menéndez*, nº 43, 2016, pp. 90-94.

Es relevante decir que la empresa tenía una normativa interna conocida por el trabajador, en la que específicamente se establecía la prohibición del uso de los recursos y bienes de la empresa para fines personales.

El 13 de julio de 2007, el trabajador es informado de que las comunicaciones mantenidas a través de la cuenta Yahoo Messenger habían sido vigiladas durante 9 días (del 5 al 13 de julio) y que, por lo tanto, la empresa tenía conocimiento de que había estado utilizando la cuenta de mensajería profesional para fines personales en contra de lo establecido en la normativa interna.

El trabajador, ante estas acusaciones, negó haber realizado un uso privado de los instrumentos de la empresa. Tras lo cual, la empresa transcribió cuarenta y cinco páginas con las comunicaciones personales mantenidas entre el trabajador y otras personas, tales como su hermano y su pareja, en las que se hacía referencia a temas relacionados con su salud o su vida sexual.

El empleador procedió a la extinción del contrato con el trabajador alegando como causa del despido la infracción a la mencionada normativa interna de la empresa por los hechos narrados.

El trabajador, no conforme con la decisión de la empresa, decide impugnar el despido alegando que la monitorización de su cuenta de mensajería por parte del empleador supone una vulneración del derecho a la vida privada y al secreto de las comunicaciones al amparo de la Constitución y del Código penal de Rumanía. El tribunal de primera instancia resuelve declarando la procedencia del despido por entender que la empresa había informado adecuadamente de su normativa interna y de la prohibición de usar los instrumentos de la empresa para fines personales.

El trabajador recurre la sentencia invocando, esta vez, el artículo 8 del CEDH que reconoce el derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. El tribunal de apelación falla a favor de la empresa, confirmando nuevamente el despido, por considerar que la conducta del empleador fue razonable ya que la vigilancia de las comunicaciones era el único medio de probar la existencia de la infracción disciplinaria.

Tras agotar las vías internas, el trabajador decide recurrir ante el Tribunal Europeo de Derechos Humanos, siendo esta vez parte demandada el Estado de Rumanía. En esta ocasión, el Tribunal de Estrasburgo debe pronunciarse sobre la existencia o no de una vulneración del artículo 8 del CEDH y, concretamente, determinar si Rumanía ha respetado el correcto equilibrio entre los derechos de la empresa y los del trabajador.

La doctrina anterior (caso Copland), venía utilizando el criterio de la "expectativa razonable de confidencialidad" que puede tener el trabajador al desconocer la posibilidad de una intromisión del empresario en sus comunicaciones. En consecuencia, si el empleador pretende realizar un seguimiento debe destruir esa expectativa de confidencialidad del trabajador para que su intromisión sea legítima. Para ello, "debe establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones. De tal manera que si se cumplen tales exigencias (…) no podrá entenderse que, al realizarse el control se ha vulnerado "una expectativa razonable de intimidad[18]".

Sin embargo, el TEDH en la sentencia de 12 de enero de 2016 parece haber realizado un cambio de criterio. El TEDH considera que la normativa interna de la empresa era suficientemente conocida por el trabajador, lo que permitía destruir toda expectativa razonable de privacidad. Es decir, la información ofrecida con anterioridad al trabajador en la normativa interna de la empresa es fundamento suficiente para justificar la monitorización. Esta se entiende además proporcional y razonable ya que la empresa accedió a la mensajería "en la creencia de que el registro de comunicaciones contenía mensajes profesionales y no personales" por lo que la transcripción de las conversaciones se realizó con el único fin de constatar y acreditar el incumplimiento laboral del trabajador. Asimismo,

18 Lluch Corell, Francisco Javier, "El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador", 2017, p. 3, en: http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronico-trabajador_11_1045180003.html

el hecho de que no se hubiera accedido también al disco duro del ordenador fue considerado por el TEDH como un "elemento de mesura y ponderación"[19].

Añadir que la defensa, de entre sus argumentos, alegó que con su comportamiento no se había causado daño a la empresa. Este motivo que fue desestimado señalando que los efectos son indiferentes pues es legítimo que un empleador quiera comprobar el uso que hacen sus trabajadores del tiempo de trabajo con independencia del daño o repercusión para la empresa.

En definitiva, el TEDH hace prevalecer el derecho del empleador al control y vigilancia del cumplimiento de las obligaciones laborales frente al derecho a la intimidad del empleado. La "expectativa razonable de confidencialidad" queda destruida, a juicio del Tribunal, por la simple prohibición general "ex ante" de uso. Quizá lo más importante a extraer es que parece ser suficiente con una prohibición genérica incluida en una normativa interna, sin necesidad de firma ni comunicación expresa o directa al trabajador ni previo aviso de ningún tipo sobre la posibilidad de controles en la empresa. También es irrelevante que el comportamiento del trabajador no cause perjuicio o daño a la empresa ni que no sea reiterado ni abusivo. Este último argumento podía haber sido un elemento importante para valorar la proporcionalidad del despido respecto de la posibilidad de imponer otro tipo de sanción. Finalmente, añadir que a juicio del Tribunal, la intromisión del empleador se justifica en la creencia de que la información contenida estaba relacionada con actividades profesionales y que, por lo tanto era legítimo acceder a ella.

Así, el TEDH, tras revisar la normativa aplicable y valorar el fondo del asunto, declara (con seis votos a favor y uno en contra) [20] que no se ha producido una vulneración del artículo 8 del CEDH.

Tras el polémico pronunciamiento, la sentencia fue recurrida ante la Gran Sala del TEDH[21] que dictó sentencia en audiencia pública el pasado 5 de septiembre de 2017, sobre la cual nos detendremos a continuación. .

2.2.2. La sentencia del TEDH (Gran Sala) de 5 de septiembre de 2017 y la revisión de la doctrina del Tribunal Europeo de Derechos Humanos: la doctrina Barbulescu.

La Gran Sala del Tribunal Europeo de Derechos Humanos en su sentencia de 5 de septiembre de 2017 revisa el criterio vertido en la sentencia anterior de 12 de enero de 2016. En primer lugar analiza la normativa correspondiente teniendo en cuenta la 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 la libre circulación de esos datos[22]. Es necesario matizar que dicha Directiva va a quedar derogada a partir del 25 de mayo de 2018 con la entrada en vigor del citado Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos. Asimismo, la Gran Sala del TEDH retoma el análisis sobre la posible

19 Miranda Boto, José María, "Derecho a la intimidad de los trabajadores y uso del messenger corporativo ante el Tribunal Europeo de Derechos Humanos", *Derecho de las relaciones laborales*, nº 2, 2016, p. 104.

20 La STEDH de 12 de enero de 2016 cuenta con un voto particular del magistrado portugués Pinto de Albuquerque que resulta de gran relevancia. Entiende el magistrado que la política de uso de Internet en la empresa debe ser más precisa, siendo insuficiente una mera prohibición o aviso genérico del uso de los ordenadores para fines personales. Sería conveniente "recoger expresamente el conocimiento del trabajador de que está siendo controlado". Insiste el magistrado en la necesidad de "que las políticas de control sobre empleados establezcan reglas claras y transparentes sobre los usos permitidos, los controles que podían llevarse a cabo y su periodicidad o las medidas técnicas que serán implementadas a tales efectos". Por otro lado, el magistrado considera que la transcripción de los mensajes y su divulgación a otros empleados va más allá de lo estrictamente necesario. Desde luego parece razonable que una empresa no pueda divulgar la información obtenida del trabajador a través de los mecanismos de control utilizados, ya que la finalidad de la injerencia no puede ser otra que verificar el cumplimiento de las obligaciones laborales de los trabajadores.

21 Según establece el artículo 43 del CEDH: "1. En el plazo de tres meses a partir de la fecha de la sentencia de una Sala, cualquier parte en el asunto podrá solicitar, en casos excepcionales, la remisión del asunto ante la Gran Sala. 2. Un colegio de cinco jueces de la Gran Sala aceptará la solicitud si el asunto plantea una cuestión grave relativa a la interpretación o a la aplicación del Convenio o de sus Protocolos o una cuestión grave de carácter general. 3. Si el colegio acepta la solicitud, la Gran Sala se pronunciará sobre el asunto mediante sentencia".

Puede verse la retransmisión de la audiencia de 30 de noviembre de 2016 ante la Gran Sala del TEDH en el siguiente enlace: http://www.echr.coe.int/Pages/home.aspx?p= hearings&w= 6149608_30112016&language= fr&c= fre&py= 2016

22 En: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri= OJ:L:1995:281:TOC

vulneración del artículo 8 del CEDH. Entiende además el Tribunal que el control empresarial de los medios informáticos tiene que ajustarse a las pautas establecidas en la Recomendación CM/Rec(2015)5 del Consejo de Europa para la protección de datos en el ámbito laboral adoptada por el Comité de Ministros el 1 de abril de 2015 y que, en consecuencia, el empresario no podía acceder al ordenador del trabajador porque existía una "expectativa razonable de confidencialidad no neutralizada". Seguramente lo más relevante de la sentencia sea que se considera necesaria la advertencia del empresario de la existencia de controles al trabajador así como de su naturaleza o alcance con carácter previo al establecimiento de las medidas de control. En definitiva, se exige para que los controles sean válidos, que vayan acompañados de las garantías adecuadas y suficientes. Existía a juicio del Tribunal, en definitiva, una expectativa razonable de confidencialidad no neutralizada pues el empleador debe de informar y advertir de la vigilancia a los trabajadores previamente a la implantación de las herramientas de control, sobre todo si afecta al contenido de las comunicaciones. Además la información debe ser clara en cuanto a la naturaleza de la vigilancia.

En el caso concreto no se había llevado a cabo la información con carácter previo al control y, por lo tanto, se vulnera el art. 8 CEDH.

La sentencia denominada ya por algunos como "doctrina Barbulescu" aporta un cambio fundamental pues somete cualquier medida de control al cumplimiento de una serie de requisitos. Se añade a la necesidad de información previa anteriormente señalada otros dos aspectos importantes, a saber, la necesidad de priorizar las medidas preventivas sobre las de control (como por ejemplo impedir o filtrar el acceso a determinadas páginas web) y la necesidad de garantizar la transparencia en el tratamiento de los datos de carácter personal.

3. Conexión de la doctrina jurisprudencial del Tribunal Europeo de Derechos Humanos con la jurisprudencia de los tribunales españoles.

Son muchos los pronunciamientos de nuestros tribunales sobre el uso de internet y de las TICs en el trabajo dando fruto a una doctrina judicial en evolución. Pero antes de referirnos a los asuntos más relevantes en la materia, es necesario señalar unas consideraciones previas.

No hay duda, pues así lo ha confirmado en reiteradas ocasiones nuestro Tribunal Constitucional, de que una relación laboral no implica en modo alguno la privación al trabajador de los derechos que tiene constitucionalmente reconocidos como ciudadano[23]. Podríamos, por ejemplo, mencionar el art. 18 ET relativo a la inviolabilidad de la persona del trabajador estableciendo que sólo se podrán realizar registros sobre el trabajador, su taquilla y efectos particulares, dentro del centro de trabajo y durante las horas de trabajo, cuando sean necesarios para la protección del patrimonio de la empresa y del de los demás trabajadores. Sin embargo, los derechos fundamentales no son absolutos. Muestra de ello es el art. 20.3 ET que atribuye al empresario la posibilidad de adoptar medidas de vigilancia y control sobre sus trabajadores estableciendo que "el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso". No obstante, a la hora de realizar dichos controles, especialmente sobre las comunicaciones y los medios tecnológicos, algunos derechos de los trabajadores pueden verse afectados como son el derecho a la intimidad personal (art. 18.1 CE) y el derecho al secreto de las comunicaciones (art. 18.3 CE).

3.1. La evolución de la doctrina del Tribunal Constitucional.

En un principio, los tribunales españoles venían aceptando cualquier medida de vigilancia y control en la empresa bajo el argumento de la dimensión pública que tiene el lugar de trabajo "minusvalorando" el alcance efectivo del respeto a la dignidad[24]. Posteriormente, esa postura fue modificada considerando que cualquier medida empresarial tendente a limitar derechos fundamentales de los trabajadores debe atender necesariamente a la observancia del triple juicio de proporcionalidad fijado

23 Doctrina reiterada en las SSTC 88/1985; 90/1997, 98/2000,186/2000, 196/2004, 125/2007.

24 Goñi Sein, José Luis, "El poder de control empresarial en la doctrina del Tribunal Supremo", en: García Murcia, Joaquín (Coord.), *El Estatuto de los Trabajadores en la jurisprudencia del Tribunal Supremo*, Tecnos, Madrid, 2015, p. 235.

en la STC 186/2000, convirtiéndose dicho parámetro en el "canon de enjuiciamiento" de los tribunales[25].

Posteriormente, tras la doctrina del Tribunal de Estrasburgo vertida en el citado caso Copland, nuestro Tribunal Constitucional en la sentencia 241/2012, de 17 de diciembre, se basa también en el criterio de la "expectativa razonable de confidencialidad" entendiendo que, en palabras de Baz Rodríguez, "es precisamente la tolerancia generalizada al uso moderado para fines personales de tales herramientas la que genera una expectativa, también general, de confidencialidad para el trabajador"[26].

Hasta una serie de pronunciamientos recientes, que veremos a continuación, podemos afirmar que la tesis generalizada se fundamentaba en la "no exigibilidad de información previa sobre el control cuando con ella se frustraría la finalidad pretendida sin que exista un medio más inocuo, siendo suficiente con el cumplimiento de los criterios de idoneidad, necesidad y proporcionalidad en sentido estricto. La doctrina judicial hacía hincapié en "la importancia de establecer previamente, de acuerdo con las exigencias de la buena fe, las reglas de uso de dichos medios"[27].

A pesar de lo expuesto, poco después, el Tribunal Constitucional sorprende con la aplicación del "derecho a la autodeterminación informativa" en la STC 29/2013, de 11 de febrero. En esta ocasión, el Tribunal no valora si la medida (una grabación con cámaras de video vigilancia) vulnera el derecho a la intimidad del trabajador, sino a la protección de datos de carácter personal. Es cierto que, en este asunto, el control empresarial no se centra en el ordenador o correspondencia electrónica del trabajador sino en un sistema de video vigilancia. En concreto, se sancionaba a un trabajador por faltas de asistencia y de puntualidad aportando la empresa como prueba imágenes obtenidas por las cámaras de video vigilancia. El Tribunal considera que la prueba aportada en forma de grabación, sin haber informado previamente a los trabajadores de su uso como mecanismo de control, resulta lesiva para el derecho a la protección de datos de carácter personal reconocido en el art. 18.4 CE. Es más, advierte el Tribunal que además era necesaria una información "previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo"[28].

A pesar de lo anterior, nuestro Tribunal Constitucional parece haber dado un nuevo giro en la STC 170/2013, de 7 de octubre, y en la STC 39/2016, de 3 de marzo, fortaleciendo el derecho a la propiedad de los instrumentos de trabajo y el poder de control empresarial.

En el primer asunto, la STC 170/2013, se trataba de resolver un recurso de amparo interpuesto por un trabajador despedido disciplinariamente por revelación a terceros de información confidencial de la empresa. La empresa ante las sospechas de dicho comportamiento accedió al contenido de los correos electrónicos del trabajador con el fin de comprobar si, efectivamente, existía una irregularidad. Lo fundamental en este asunto es que el Convenio Colectivo aplicable tipificaba como infracción leve el uso de medios informáticos de la empresa para fines privados. Entiende el Tribunal Constitucional que el control de los correos realizado por la empresa no vulnera los derechos del trabajador y cumple con el principio de proporcionalidad. Para el Tribunal Constitucional, la previsión en el régimen convencional aplicable de que el uso particular de los medios informáticos de la empresa constituye una falta laboral leve, supone una prohibición absoluta de la utilización del correo electrónico o de Internet para fines privados. De modo que, no hay lugar en este caso para una expectativa fundada y

25 El Tribunal Constitucional ha elaborado una doctrina para valorar la constitucionalidad de cualquier medida restrictiva de derechos fundamentales bajo la observancia del conocido "principio de proporcionalidad". Así, para comprobar si una medida es restrictiva de un derecho fundamental es necesario realizar una adecuada ponderación de las circunstancias y constatar si supera el triple test gradualista o principio de proporcionalidad: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad), si la medida resulta de estricta necesidad por no existir otra más moderada (juicio de necesidad) y, por último, si la medida es adecuada y equilibrada por derivarse más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto (SSTC 66/1995,55/1996, 207/1996, 37/1998, 186/2000).

26 Baz Rodríguez, Jesús, "Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre [BOE n.º 267, de 7-XI-2013]", *Ars Iuris Salmanticensis*, Vol. 2, nº. 1, 2014, p. 365.

27 Id.

28 STC 29/2013, FJº 8

razonable de confidencialidad por parte del trabajador pues este debía conocer el convenio colectivo aplicable y la posibilidad de control del empresario.

Podemos extraer de lo anterior que "la mera tipificación, en el convenio colectivo aplicable (…), de infracciones sancionables relacionadas con el uso para fines personales de los medios informáticos de la empresa ha de considerarse, así pues, a partir de esta doctrina constitucional, como un régimen jurídico de uso de los mismos, sin necesidad de que existan propiamente (…) protocolos o instrumentos reguladores ad hoc de origen empresarial o convencional destinados a regular, normalizar, clarificar, detallar y publicar, para su debido conocimiento en profundidad por todos los trabajadores, las pautas de uso y control de los mismos en la empresa"[29].

En la misma línea de reforzar los poderes de vigilancia, se ha pronunciado más recientemente el Tribunal Constitucional en la sentencia 39/2016, de 3 de marzo (caso Bershka). Este asunto vuelve a tratar un conflicto entre el derecho a la intimidad y a la protección de datos de los trabajadores y un control efectuado mediante un sistema de video vigilancia. Esta vez, la grabación obtenida mediante una cámara de video vigilancia sin informar expresamente a la trabajadora de su colocación ni de su finalidad de control, resulta admitida como prueba justificativa de su despido. A juicio del Tribunal Constitucional, el deber empresarial de información se vio cumplido mediante la simple visualización del distintivo "zona videovigilada" en un lugar visible.

El asunto tiene su inicio en el despido disciplinario de una trabajadora por haberse apropiado de efectivo de la caja de la empresa. La empresa para constatar este comportamiento, instaló una cámara de videovigilancia. La instalación de la cámara se realizó sin comunicación a los trabajadores pero con la instalación, en un lugar visible, en el escaparate del establecimiento de un distintivo informativo. El Tribunal Constitucional tiene que pronunciarse sobre una posible vulneración del derecho a la protección de datos y el derecho a la intimidad de la trabajadora. No hay duda de que la imagen se considera un dato de carácter personal y el art. 6.1 de la LOPD establece que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa". Ahora bien, el apartado 2 del art. 6 LOPD reconoce como excepción a lo anterior que no será preciso el consentimiento cuando los datos de carácter personal se refieran a las partes de una relación laboral y sean necesarios para el mantenimiento y cumplimiento de las obligaciones derivadas del contrato de trabajo. En consecuencia, en el ámbito laboral no será necesario el consentimiento de los trabajadores afectados salvo que el tratamiento de los datos se utilice con una finalidad distinta al cumplimiento del contrato[30]. A pesar de lo anterior, añade el Tribunal, que aunque no sea necesario el consentimiento, el deber de información previa sigue existiendo. En el presente caso, el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes obtenidas a través de la cámara puesto que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral de conformidad con el art. 20.3 ET. Respecto de la obligación de información previa, entiende el Tribunal Constitucional que la empresa ha cumplido con este deber al haber colocado el distintivo en el escaparate por lo que la trabajadora podía conocer la existencia de la cámara y su finalidad[31].

Finalmente, sobre el genérico derecho a la intimidad personal de la trabajadora, el Tribunal Constitucional rechaza una vulneración del derecho al someter a la medida de control empresarial al juicio de proporcionalidad resultando ésta justificada, idónea, necesaria y equilibrada[32].

En definitiva, la STC 39/2016, de 3 de marzo, se aleja del criterio mantenido por la STC 29/2013, de 11 de febrero. De acuerdo con García Rubio, el Tribunal Constitucional "suaviza considerablemente las exigencias que el TCo 29/2013 estableció para entender cumplido el deber de información ínsito en el contenido del derecho de protección de datos personales. Para entender satisfecha la obligación empresarial, para el Tribunal basta ahora con el distintivo informativo general de

29 Baz Rodríguez, Jesús, "Sentencia del Tribunal Constitucional 170/2013…", *Ob. cit.*, p. 367.
30 STC 39/2016, FJº 3
31 STC 39/2016, FJº 4
32 STC 39/2016, FJº 5

"zona videovigilada", sin necesidad de comunicar a los trabajadores los ámbitos concretos de control de la prestación laboral a que pueden destinarse las grabaciones de las cámaras"[33].

Veamos, a continuación, cuál ha sido la evolución de la doctrina de nuestro Tribunal Supremo en la materia.

3.2. La evolución de la doctrina del Tribunal Supremo.

Sin duda, la sentencia más importante es la STS de 26 de septiembre de 2007. Este pronunciamiento clave se ubica en los mismos términos que establece el TEDH en los asuntos Halford y Copland en cuanto a la existencia de un hábito social generalizado de tolerancia con ciertos usos de los medios informáticos facilitados por la empresa, lo cual genera una "expectativa razonable de confidencialidad". No obstante, dicha expectativa puede ser desvirtuada por el empresario si cumple con un presupuesto básico, como es, en palabras de Goñi Sein, la transparencia informativa. Es decir, la "obligación de la empresa de informar sobre las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales para usos privados, y sobre la existencia del control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos"[34]. Esta doctrina de la Sala IV del Tribunal Supremo ha sido confirmada por dos sentencias posteriores, la STS de 8 de marzo de 2011 y la STS de 6 de octubre de 2011.

Sin embargo, cabe añadir que en la STS de 6 de octubre de 2011 el pronunciamiento del Tribunal se distancia algo de los anteriores. Es necesario recordar, tal y como explica Goñi Sein, que en la STS de 26 de septiembre de 2007 "se había establecido que la legitimidad del control requiere no sólo la advertencia de las reglas de uso de los medios informáticos, sino la previa comunicación sobre la existencia de los controles de uso del ordenador. El Tribunal, en la STS de 6 de octubre de 2011, realiza, sin embargo un juicio de fondo, consistente únicamente en valorar la primera de las dos condiciones; esto es, si hubo advertencia expresa de una prohibición absoluta de uso de los medios para fines personales"[35]. De esto modo, con la prohibición se quiebra toda "expectativa razonable de intimidad" o, lo que es lo mismo, la existencia de una prohibición empresarial delimita el contenido del derecho fundamental de modo que no puede hacerse efectivo a través de mecanismos empresariales ni durante el tiempo de trabajo[36].

Recordemos también que con un planteamiento similar se pronuncia el Tribunal Constitucional en la sentencia 170/2013, de 7 de octubre, comentada anteriormente. Así, la sentencia del Alto Tribunal de 6 de octubre de 2011, en palabras de Rodríguez Escanciano, "introduce una matización en la doctrina anterior, que supone una cierta marcha atrás en la protección del derecho fundamental a la intimidad y al secreto de las comunicaciones"[37].

A pesar de lo anterior, en una sentencia de 13 de mayo de 2014, el Tribunal Supremo parece retomar la línea argumental que venía siguiendo desde la STS de 26 de septiembre de 2007, considerando nuevamente que es necesario informar previamente a los trabajadores tanto sobre las reglas de uso de los ordenadores como sobre la existencia de mecanismos de control de la en la empresa para que la vigilancia empresarial sea legítima.

Más recientemente, el Tribunal Supremo en la sentencia de 7 de julio de 2016 sigue la última línea argumental del Tribunal Constitucional en torno a las grabaciones de cámaras de videovigilancia. Concretamente, el Tribunal Supremo admite como prueba en un juicio para justificar un despido, las grabaciones procedentes de cámaras de videovigilancia. El Alto Tribunal entiende en este asunto que las imágenes obtenidas no vulneran la protección de datos si el trabajador conoce la existencia de los dispositivos de grabación. Recuerda además la STC 39/2016 en cuanto a que no es necesario el consentimiento de los trabajadores cuando hay una relación laboral pero sí que es necesario informar

33 García Rubio, Mª. Amparo, "Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales", 2016, p. 5, en: http://www.elderecho.com/tribuna/laboral/doctrina-constitucional-videovigilancia-laboral-proteccion-personales_11_964930001.html

34 Goñi Sein, José Luis, "El poder de control empresarial….", *Ob. cit.*, p. 239.

35 *Id.*, p. 241.

36 Carrizosa Prieto, Esther, "El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores", *Temas Laborales*, nº 116, 2012, p. 266.

37 Rodríguez Escanciano, Susana, "Internet en el Trabajo", Diario La Ley, nº. 8926, 2017, p. 7.

de la existencia de cámaras de videovigilancia – siendo suficiente para cumplir con ese requisito la ubicación de un cartel indicativo en un lugar claro y visible - para no lesionar el derecho a la protección de datos.

Por último, la STS de 31 de enero de 2017 reitera la doctrina de la STC 39/2016, de 3 de marzo, y de la STS de 7 de julio de 2016 sobre la admisión de una prueba obtenida a través de una cámara de videovigilancia. Así, será lícita siempre que el trabajador tenga conocimiento de la instalación del sistema de videovigilancia y su ubicación por motivos de seguridad.

4. Consideraciones finales.

Hasta la reciente sentencia de 5 de septiembre de 2017, tanto en la jurisprudencia del Tribunal de Estrasburgo como en la de nuestros Tribunales internos, se constataba una evolución hacia la primacía del poder de dirección empresarial sobre los derechos fundamentales del trabajador. Por el contrario, la STEDH de 5 de septiembre de 2017 vuelve a aproximarse a los pronunciamientos que limitan las facultades de control del empresario y exigen mayores previsiones para acceder y controlar legítimamente las herramientas informáticas puestas a disposición del empleado.

Como hemos visto, en los últimos años, en la jurisprudencia de nuestros Tribunales, hay una reciente evolución hacia la primacía del poder de dirección empresarial sobre los derechos fundamentales del trabajador. Los planteamientos más recientes de nuestro Tribunal Constitucional se distancian de pronunciamientos jurisprudenciales más conservadores o proteccionistas para el trabajador. Hemos visto como los últimos pronunciamientos se alejan de aquellos que limitaban las facultades de control del empresario y exigían mayores previsiones para acceder y controlar legítimamente las herramientas informáticas puestas a disposición del empleado. Pues bien, la sentencia del TEDH de 5 de septiembre de 2017 cambia completamente toda la doctrina judicial más reciente del Tribunal Constitucional y Supremo. Desde luego, este último pronunciamiento parece obligar al Tribunal Constitucional a revisar su doctrina sobre la cuestión. Será interesante observar cuál será la tendencia de los tribunales españoles a partir de ahora en cuanto a la búsqueda del equilibro entre los derechos de los trabajadores y los poderes de control empresariales.

Respecto de los mecanismos de control, cierto es que cuanto mayor sea la incidencia de estos en la intimidad informática, mayores también tienen que ser las garantías. En consecuencia, la legitimidad de la medida de control no puede derivar del mero cumplimiento de la advertencia de las reglas de uso. Es decir, la exigencia de información sobre los controles o las grabaciones a los trabajadores debe de darse con carácter previo y de forma clara e inequívoca. Para lograr el complicado punto de equilibrio entre unos y otros derechos, son necesarias unas normas claras al respecto. Estas normas pueden concretarse bien en una normativa específica, a través de convenios colectivos o directamente por el empresario mediante la adopción, por ejemplo, de un protocolo o código de buenas prácticas negociado con los representantes de los trabajadores en la empresa, que refleje y clarifique aspectos tan esenciales como los límites al uso de los instrumentos de la empresa para fines privados y las prácticas y mecanismos de control previstos. De este modo, los trabajadores estarán indudablemente informados sobre las prohibiciones absolutas y parciales, los usos adecuados y permitidos de las herramientas de la empresa, los controles existentes y los medios que se van a utilizar para llevarlos a cabo, las posibles sanciones en caso de incumplimiento y el funcionamiento en general. Asimismo, y de acuerdo con las exigencias de buena fe, es necesario que la empresa establezca las reglas de uso de esos medios con carácter previo. Todo ello sin descartar la posibilidad de utilizar otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

Al margen de que a partir de un control empresarial puedan resultar vulnerados el derecho a la intimidad y al secreto de las comunicaciones de los trabajadores, no podemos descuidar el derecho a la protección de datos y todos los derechos y principios inherentes al mismo. En este sentido, "el conjunto de operaciones de recogida de los datos personales del trabajador que comporta un procedimiento de monitorización de lo que hace un trabajador en su ordenador, constituye tratamiento de datos personales y (que), por tanto, el canon interpretativo de obligada aplicación debe ser el derecho a la autotutela informativa. (…) La legitimidad del control empresarial requiere la observancia estricta

del principio de transparencia informativa, (…) lo que obliga a informar a los trabajadores también de los mecanismos de control dispuestos por el empresario"[38].

Es evidente que nuestro ordenamiento se ve excedido por una realidad tecnológica creciente e imparable que provoca situaciones que escapan al marco regulador hasta ahora establecido. El derecho del trabajo necesita crear normas que permitan ofrecer soluciones a nuevos escenarios en las relaciones laborales. En este sentido resulta muy pertinente la elaboración de un Anteproyecto de una nueva Ley Orgánica de Protección de Datos de Carácter Personal que dé cumplimiento al art. 88 del Reglamento (UE) 2016/679 que establece el mandato a los Estados de fijar normas específicas para el tratamiento de los datos personales de los trabajadores en el ámbito laboral con el fin de establecer normas más específicas para garantizar la protección de los derechos y libertades afectados, prestando especial atención a la transparencia del tratamiento.

5. Notas bibliográficas.

Alemán Páez, Francisco, "El derecho a la desconexión digital: una aproximación conceptual, crítica y contextualizadora al hilo de la 'Loi Travail Nº 2016-1088'", *Trabajo y derecho*, nº 30, 2017, pp. 12-33.

- "Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores", *Derecho de las Relaciones Laborales*, nº 6, 2016, pp. 602-618.

Aragón Gómez, Cristina, "Artículo 20. Dirección y control de la actividad laboral", en: Cruz Villalón, Jesús, García-Perrote Escartín, Ignacio, Goerlich Peset, José María, Mercader Uguina, Jesús R. (Dirs.), *Comentarios al Estatuto de los Trabajadores*, Thomson Reuters Lex Nova, Pamplona, 2014, pp. 281-291.

Baz Rodríguez, Jesús, "Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre [BOE nº 267, de 7-XI-2013]", *Ars Iuris Salmanticensis*, Vol. 2, nº. 1, 2014, pp. 364-367.

Bermejo Bosch, Reyes, Botella Vivó, Santiago, "La sentencia del TEDH sobre el control por el empleador del uso del correo electrónico (mensajería instantánea) por sus empleados (caso Barbulescu v. Rumanía Nº. 61496/08 de 12 de enero de 2016)", *Actualidad jurídica Uría Menéndez*, nº 43, 2016, pp. 90-94.

Carrizosa Prieto, Esther, "El control empresarial sobre el uso de los equipos informáticos y la protección del derecho a la intimidad de los trabajadores", *Temas Laborales*, nº 116, 2012, pp. 251-267.

García Rubio, Mª. Amparo, "Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales", 2016, en: http://www.elderecho.com/tribuna/laboral/doctrina-constitucional-videovigilancia-laboral-proteccion-personales_11_964930001.html

Goñi Sein, José Luis, "El poder de control empresarial en la doctrina del Tribunal Supremo", en: García Murcia, Joaquín (Coord.), *El Estatuto de los Trabajadores en la jurisprudencia del Tribunal Supremo*, Tecnos, Madrid, 2015, pp. 235-251.

- "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores. Análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016", *Revista de derecho social*, nº 78, 2017, pp. 15-42.
- "La vigilancia empresarial de la conversaciones electrónicas de los trabajadores: A propósito de la sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016, 'Barbulescu v. Rumanía'", *Trabajo y derecho*, nº 18, 2016, pp. 78-84.

Lluch Corell, Francisco Javier, "El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador", 2017, en: http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronico-trabajador_11_1045180003.html

Marguénaud, Jean-Pierre; Mouly, Jean, "Big Boss is watching you – Alerte sur le contrôle des activités électroniques du salarié: (obs/s. Cour eur. Dr. H., Barbulescu c. Roumanie, 12 janvier 2016)" *Revue trimestrielle des droits de l'homme,* nº 108, 2016, pp. 1037-1048.

Miranda Boto, José María, "Derecho a la intimidad de los trabajadores y uso del messenger corporativo ante el Tribunal Europeo de Derechos Humanos", Derecho de las relaciones laborales, nº 2, 2016, pp. 102-105.

Molina Navarrete, Cristóbal, "'Expectativa razonable de privacidad' y poder de vigilancia empresarial: '¿Quo vadis justicia laboral?' (Comentario a la Sentencia del TEDH de 12 de enero de 2016, asunto 'Barbulescu c. Rumanía', demanda núm. 61496/2008", Estudios financieros. Revista de trabajo y seguridad social, nº 399, 2016, pp. 171-180.

Rodríguez Escanciano, Susana, "Internet en el Trabajo", Diario La Ley, nº. 8926, 2017, pp. 1-13.

San Martín Mazzucconi, Carolina, Sempere Navarro, Antonio V., "*Las TICS en el ámbito laboral*", Francis Lefebre, Madrid, 2015.

38 Goñi Sein, José Luis, "El poder de control empresarial…", *Ob. cit.*, p. 242.