REGISTRO DE LAS COMUNICACIONES ELECTRÓNICAS DEL TRABAJADOR ¿ES NECESARIA LA AUTORIZACIÓN JUDICIAL?

MONITORING OF ELECTRONIC COMMUNICATIONS OF WORKERS. IS NECESSARY JUDICIAL AUTHORIZATION?

ARÁNZAZU ROLDÁN MARTÍNEZ
Universidad Europea de Madrid

Recibido: 18/01/2017
Aceptado: 06/04/2017

Resumen: La jurisprudencia de la Sala Cuarta del Tribunal Supremo ha admitido la monitorización de los correos electrónicos de los trabajadores por el empresario siempre que se cumplan determinados requisitos. Sin embargo, la Sala de lo Penal del mismo Tribunal en sentencia de 16 de junio de 2014, al valorar la eficacia en el proceso penal de una prueba que había sido previamente admitida en el proceso laboral, ha dejado claro que la doctrina contenida en aquellas sentencias sólo se aplica al ámbito laboral y en ningún caso al penal, donde por imperativo del artículo 18.3 de la Constitución se exige la autorización judicial previa para intervenir las comunicaciones. En este artículo se analiza si la interpretación que ha realizado la Sala de lo Penal supone una enmienda a la totalidad para la línea jurisprudencial emanada de la Sala de lo Social o si cabe realizar una interpretación que armonice ambas doctrinas, partiendo de la base de que los derechos fundamentales son únicos.

Palabras Clave: poder de vigilancia; correo electrónico; derecho a la intimidad; autodeterminación informativa; secreto de las comunicaciones

Abstract: *The case law of the Fourth Chamber of the Supreme Court has admitted monitoring emails of workers by the employer provided that certain conditions are met. However, the Criminal Chamber of the same Court in its ruling of June 16, 2014, when assessing the effectiveness in criminal proceedings of evidence that had previously been admitted in labor proceedings, has made it clear that the doctrine contained in those judgements only applies to labour proceedings but in no case in criminal proceedings, in which, in accordance to Article 18.3 of the Constitution, it is mandatory that a judicial authorization is requested prior to intervening communications. This paper examines whether the interpretation made by the Criminal Chamber involves an amendment in full of the case law emanating from the Social Chamber or whether it is an interpretation that harmonizes both doctrines, on the basis that fundamental rights are unique.*

Key Words: *surveillance at work; e-mail; right to privacy; personal data protection; secret of communications.*

privacidad". 2. PRONUNCIAMIENTOS DEL TRIBUNAL CONSTITUCIONAL SOBRE LAS SENTENCIAS RECAÍDAS EN EL ORDEN SOCIAL. 3. LA VALORACIÓN DE LA JURISPRUDENCIA LABORAL POR LA JURISDICCIÓN PENAL: LA STS DE 16 DE JUNIO DE 2014. 4. CONCLUSIONES FINALES: VÍAS DE ENCUENTRO ENTRE AMBAS JURISDICCIONES. 5. BIBLIOGRAFÍA.

INTRODUCCIÓN

La Sala de lo Social del Tribunal Supremo ha legitimado el control empresarial sobre las comunicaciones electrónicas realizadas por los trabajadores a través de los ordenadores de la empresa. El fundamento de esta fiscalización se situaría en el poder de dirección y vigilancia que el artículo 20.3 del Estatuto de los Trabajadores –en adelante ET– reconoce al empresario, argumento que ha sido avalado por el Tribunal Constitucional en las sentencias 241/2012 y 170/2013. Sin embargo, la Sala de lo Penal del mismo Tribunal Supremo en sentencia de 16 de junio de 2014, cuando ha tenido ocasión de valorar en el proceso penal la eficacia de una prueba que había sido previamente admitida en un proceso laboral, ha aclarado que la doctrina contenida en aquellas sentencias no se aplica al ámbito penal, donde por imperativo del artículo 18.3 de la Constitución se exige la autorización judicial previa para intervenir las comunicaciones. La sentencia recaída en sede penal causó preocupación a los empresarios y operadores jurídicos, por la posibilidad de que la monitorización del correo corporativo utilizado por los empleados, pese a ajustarse a los criterios marcados por la jurisprudencia social, pudiera ser constitutiva de delito, al haberse obtenido ilegalmente[1].

El objetivo de este estudio es analizar si la interpretación que ha realizado la Sala de lo Penal supone una enmienda a la totalidad para la línea jurisprudencial

[1] Prueba de ello son los comentarios realizados por los expertos en los medios de comunicación, así como por abogados especializados en Derecho informático, expresados en las salas de prensa o blogs de sus respectivos despachos, advirtiendo de la conveniencia de respetar los establecido en la STS de 16 de junio de 2014. *Vid,* por ejemplo el comentario de Javier Aparicio Salom - Socio de Cuatrecasas, Gonçalves Pereira "¿Hay delito en el control del email del empleado?, publicado el 4 de septiembre de 2014 en Expansion.com (disponible en *http://www.expansion.com/2014/09/04/juridico/1409857555.html*); el comentario de Raúl Rojas, socio de laboral del despacho Écija, "¿El correo electrónico corporativo está protegido por el secreto de las comunicaciones?", publicado el 6 de noviembre de 2014 en la Sala de Prensa del Despacho (disponible en *http://ecija.com/sala-de-prensa/el-correo-electronico-corporativo-esta-protegido-por-el-secreto-de-las-comunicaciones/*); el comentario de Jesús David García Sánchez y Marta García Bel, "El poder de control del empresario sobre el correo electrónico de sus trabajadores. A propósito de la sentencia de la Sala de lo Penal del Tribunal Supremo de 16 de junio de 2014", Foro de Actualidad, publicado en la página web del despacho (disponible en *http://www.uria.com/documentos/publicaciones/4623/documento/f08.pdf?id=5775*); o el comentario de Francisco Ramón González-Calero Manzanares, "Acceso al correo electrónico del trabajador ¿legal o ilegal?, publicado el 21 de diciembre de 2014 en El Derecho.com, de la editorial Lefèbvre-El Derecho, (disponible en *http://tecnologia.elderecho.com/tecnologia/privacidad/Acceso-correo-electronico-trabajador-ilegal_11_738055001.html*).

emanada de la Sala de lo Social o si cabe realizar una interpretación que armonice ambas doctrinas, partiendo de la base de que los derechos fundamentales son únicos. Nos preguntamos si existe una contradicción entre ambas jurisprudencias, que podrían estar teniendo una visión diferente del ámbito de protección del derecho fundamental al secreto de las comunicaciones y de las condiciones de legitimidad de su limitación, o si más bien la jurisprudencia penal vendría a complementar a la social.

La metodología a seguir será la siguiente: tras un imprescindible recordatorio sobre el contenido esencial de los derechos fundamentales que pueden resultar afectados por la monitorización de las comunicaciones electrónicas del trabajador, tal y como han sido interpretados por nuestro Tribunal Constitucional y por el Tribunal Europeo de Derechos Humanos, se estudiará la jurisprudencia recaída en la jurisdicción ordinaria social y en sede constitucional sobre el concreto problema analizado. El objetivo no es sólo sistematizar las condiciones que se han considerado necesarias para legitimar la interceptación de las comunicaciones, cuyo estudio crítico ha sido abordado ya en profundidad por la mejor doctrina[2], sino determinar si en los casos enjuiciados en las sentencias, realmente resultaba afectado el artículo 18.3 CE, o más bien el derecho a la intimidad con el que aquél tiende a confundirse. A continuación, se realizará un estudio del contenido de la STS de 16 de junio de 2014, complementándolo con pronunciamientos recientes de la Sala de lo Penal sobre el ámbito de protección del derecho al secreto de las comunicaciones. Estos estudios preliminares nos permitirán concluir si es posible una interpretación armonizadora entre ambas jurisprudencias o si, por el contrario, existe una separación absoluta entre la jurisdicción social y la penal.

1. UN VIEJO PROBLEMA: EL CONFLICTO ENTRE EL PODER DE DIRECCIÓN DEL EMPRESARIO Y LOS DERECHOS FUNDAMENTALES DE LOS TRABAJADORES

1.1. Bienes jurídicos del trabajador afectados por el control de las comunicaciones electrónicas

Lo característico del ordenador y de otros dispositivos de almacenamiento masivo es que en un único acto, como podría ser el registro del ordenador, pueden resultar afectados varios derechos fundamentales, el derecho a la intimidad, el derecho a la autodeterminación informativa y el secreto de las comunicaciones[3]. Estos derechos entran en tensión con el poder de dirección y control del empresario. El Tribunal Constitucional ha señalado en varios pronunciamientos que este poder es

[2] Además de las obras que se citarán en este artículo, *vid,* SEMPERE NAVARRO, A.V. SAN MARTÍN MAZZUCCONI, C., *Nuevas tecnologías y relaciones laborales*, Aranzadi, Cizur Menor, 2002; MARTÍN VALVERDE, "Uso extralaboral del correo electrónico empleando medios informáticos de la empresa. Control empresarial: requisitos", Actualidad Laboral, nº 2, 2014, (formato electrónico).

[3] *Vid,* STC 173/2011, que advirtió del significado de los tres derechos que convergen en la utilización del ordenador.

imprescindible para la buena marcha de la organización productiva –reflejo de los derechos proclamados en los arts. 33 y 38 CE– y se reconoce expresamente en el art. 20.3 ET, precepto que atribuye al empresario la facultad de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana (SSTC 98/2000, de 10 de abril; 186/2000, de 10 de julio; y 241/2012, de 17 de diciembre). A continuación, siguiendo la doctrina del TC y del TEDH, se delimitará el alcance y la cobertura de los derechos en juego. Por las limitaciones de espacio, se excluirá el derecho de autodeterminación informativa.

1.1.1. El derecho a la intimidad: ámbito protegido

El derecho a la intimidad es un concepto de carácter objetivo o material, mediante el cual el ordenamiento jurídico confiere a la persona el poder jurídico de imponer a terceros, ya sean éstos poderes públicos o simples particulares –por lo tanto, también el empresario– (STC 85/2003), el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido. La intimidad protegida por el art. 18.1 CE no se reduce a la que se desarrolla en un ámbito doméstico o privado, sino que también es aplicable en el ámbito de las relaciones laborales (STEDH de 16 de diciembre de 1992, Niemietz c. Alemania; doctrina reiterada en las SSTEDH de 4 de mayo de 2000, Rotaru c. Rumania, y de 27 de julio de 2004, Sidabras y Džiautas c. Lituania). Un criterio a tener en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas es el de las "expectativas razonables" que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observación o del escrutinio ajeno[4]. No pueden abrigarse expectativas razonables al respecto cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean, claramente pueden ser objeto de registro o de información pública (SSTEDH de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido y de 28 de enero de 2003, Peck c. Reino Unido 58; también, STC 12/2012, de 30 de enero y STC 170/2013, de 7 de octubre).

El problema concreto de la privacidad de las herramientas tecnológicas empleadas por el trabajador ha sido abordado en varias sentencias del TEDH que se han pronunciado sobre la posible vulneración del artículo 8 del Convenio Europeo para la protección de los derechos humanos –CEPDH–, que reconoce el derecho de toda persona "al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". En la sentencia de 3 de abril de 2007 –asunto Copland– el TEDH conoció de la demanda presentada por una ciudadana británica contra el Reino Unido por el seguimiento de sus llamadas telefónicas, correo electrónico y navegación por internet realizado por su centro de trabajo para comprobar si se utilizaba con fines perso-

[4] *Vid,* sobre la expectativa razonable de intimidad o confidencialidad, ABRIL, P. y PIZARRO MORENO, E., "La intimidad europea frente a la privacidad americana", InDret, Revista para el análisis del Derecho, nº. 1, 2014, disponible en *WWW.INDRET.COM*.

nales. La sentencia considera que "los correos electrónicos enviados desde el lugar de trabajo estén protegidos en virtud del artículo 8, como debe estarlo la información derivada del seguimiento del uso personal de Internet". Da especial relevancia al hecho de que a la demandante no se le advirtiera de que sus llamadas podían ser objeto de seguimiento, por lo que el Tribunal considera que "ella podía razonablemente esperar que se reconociera el carácter privado de las llamadas efectuadas desde el teléfono del trabajo (Sentencia Halford [TEDH 1997, 37], ap. 45). La demandante podía esperar lo mismo en lo que respecta al correo electrónico y la navegación por Internet". En consecuencia, al haberse realizado sin su conocimiento, "la recogida y almacenamiento de información personal relativa a las llamadas telefónicas, correo electrónico y navegación por Internet de la demandante, (…), constituye una injerencia en su derecho al respeto de su vida privada y su correspondencia, en el sentido del artículo 8 del Convenio".

En el caso analizado por la sentencia Copland el empleador era un organismo público de cuyas actuaciones era responsable directamente el Estado en virtud del CEPDH. Por esa razón el Tribunal analiza si la inferencia en el derecho estaba "prevista por ley", tal como exige el artículo 8.2 para considerar legítimos determinados actos de injerencia de las autoridades públicas. Al respecto el Tribunal recuerda que esta expresión no sólo requiere que la medida impugnada tenga alguna base en la legislación interna, sino que también se refiere a la "calidad de la Ley en cuestión". Para cumplir con la "exigencia de la previsibilidad, la Ley debe emplear términos lo suficientemente claros para que todos puedan conocer en qué circunstancias y en qué condiciones pueden las autoridades recurrir a tales medidas". En el caso concreto, el Gobierno no argumentó que existiese alguna disposición en la legislación interna o en las normas que regían en el College, que regulase las circunstancias en las que se pudiese hacer un seguimiento del uso del teléfono, correo electrónico o Internet por parte de los trabajadores.

Para finalizar, si bien, a falta de consentimiento del afectado, el artículo 18.1 de la Constitución no exige autorización judicial, lo cierto es que en el ámbito penal la Sala segunda del Tribunal Supremo ha expresado que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual[5], como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante[6].

---

[5] Partiendo de la multifuncionalidad de los datos que se almacenan en un ordenador, la Sala de lo Penal del TS considera que "más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos", existe "un derecho al propio entorno virtual", en el que se integraría, "sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris* propio, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". *Vid,* por todas STS de 17 de abril de 2013 (Rec. 1461/2012).

[6] STS de 17 de abril de 2013 (Rec. 1461/2013).

1.1.2. El secreto de las comunicaciones: ámbito protegido

El derecho al secreto de las comunicaciones tiene carácter formal, "en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado" (STC 114/1984). La protección sólo alcanza a los procesos de comunicación que se realizan a través de medios o "canales cerrados", no gozando objetivamente de la tutela constitucional del art. 18.3 CE las comunicaciones a través de un "canal abierto" del que "no puede predicarse su confidencialidad" (STC 242/2012)[7]. La STC 114/1984 declara, además, que este derecho puede conculcarse por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje –con conocimiento o no del mismo– o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, o, como añadirá posteriormente la STC 142/2012, de un mensaje emitido por correo electrónico o a través de telefonía móvil, por ejemplo). El concepto de 'secreto', que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, "la identidad subjetiva de los interlocutores o de los corresponsales" (STC 142/2012, entre otras).

La protección del derecho alcanza al proceso de comunicación mismo, pero "finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos" (STC 70/2002). Al respecto recuerda la STS de 17 de abril de 2013 –Sala Segunda–[8] que: "los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones".

A diferencia del derecho a la intimidad, la configuración jurídica del derecho al secreto de las comunicaciones, precisamente por su carácter formal, no admite interpretaciones subjetivas "por parte de los titulares del derecho ni de terceros" respecto de "su naturaleza y alcance"[9]. La protección de las comunicaciones supo-

---

[7] Señala al respecto FERNÁNDEZ RODRÍGUEZ, J.J., (*Secreto de intervención de las comunicaciones en Internet,* Civitas, 2014, pp.99.100) que no están cubiertas por el art.18.3 CE las comunicaciones que se realicen por los canales abiertos de internet: WWW, grupos de discusión, televisión, radio y chat sin estar operativa la opción *vis a vis*. Tampoco resulta de aplicación a los servicios de acceso a la información y búsqueda de la misma, que no son procesos de comunicación.

[8] Rec.1461/2013.

[9] MARIN ALONSO, I., "El uso por los trabajadores de las comunicaciones electrónicas en la empresa: ¿se encuentran protegidas por el derecho al secreto de las comunicaciones?", Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad So-

ne que no podrá interferirse o intervenirse la comunicación de cualquier persona, salvo resolución judicial y con las garantías previstas en la ley, que en el caso del proceso penal se encuentran reguladas en el Título VIII de la Ley de Enjuiciamiento Criminal, bajo la rúbrica "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución", especialmente en los arts. 588 bis a) y siguientes. Resulta controvertido si el inciso del precepto constitucional relativo a la exigencia de autorización judicial tiene como destinatarios únicamente a los poderes públicos o también a "poderes" privados, como podrían ser un empresario, un sindicato o un partido político, (estos últimos, en la medida que ejercen también un poder disciplinario). Como recuerda MARÍN ALONSO, el derecho fundamental al secreto de las comunicaciones históricamente se reconoció como un "derecho de libertad" frente a los "poderes públicos" lo que "ha provocado una cierta crítica sobre la mala técnica jurídica utilizada en el texto constitucional que no previó en su momento la existencia de poderes privados sobre los que no resultara conveniente exigir, al menos en los mismos términos, dicha autorización judicial, pero ello no cambia la realidad actual del precepto constitucional"[10]. Ciertamente, una vez reconocida la eficacia horizontal de los derechos fundamentales (STC 18/1984) sería razonable interpretar que el artículo 18.3 se aplica sin excepciones, por lo que la autorización judicial sería también necesaria cuando el derecho fundamental al secreto de las comunicaciones de un particular pudiera resultar afectado por un poder privado.

1.2. La solución del conflicto en la jurisprudencia de la Sala Cuarta del Tribunal Supremo: no se vulneran los derechos fundamentales si no existe una "expectativa de privacidad"

En una primera etapa predominaron aquellas interpretaciones que legitimaban el control del ordenador desde una perspectiva "clásica", ya que buscaban la solución en normas o en doctrinas judiciales que respondían a problemas que se consideraban análogos. Una primera línea interpretativa incidía en el hecho de que el empresario era el propietario de los medios tecnológicos[11], por lo que no podía considerarse un tercero extraño al proceso de comunicación "de manera que no existe la penetración desde el exterior que la norma constitucional [art.18.3] impide"[12]. Una segunda línea interpretativa[13] acudió a la aplicación analógica de la regulación del registro de taquillas y efectos personales del trabajador, contenida en el art.18 ET, exigiendo la concurrencia de forma acumulada de todas las condiciones que prevé dicho pre-

---

cial, pág. 3, publicada en la obra colectiva *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social,* editorial Cinca, 2014, p. 3.

[10] MARIN ALONSO, I., "El uso por los trabajadores de las comunicaciones electrónicas en la empresa…", cit., p. 3.

[11] Representada, por ejemplo por la sentencia del TSJ Madrid de 13 de noviembre de 2001 (Rec.2899/2001).

[12] STSJ Andalucía de 9 de mayo de 2003 (Rec. 591/2003); STSJ Cataluña de 12 de diciembre de 2003 (Rec. 219/2003).

[13] STSJ Cantabria de 23 de febrero de 2004 (Rec. 46/2004).

cepto, para considerar legítima la monitorización. Una última línea interpretativa[14] encontró la legitimación de la actuación fiscalizadora del empresario en el artículo 20.3 ET, interpretado conforme a la doctrina del Tribunal Constitucional recaída en relación con las medidas de video vigilancia (especialmente las SSTC 98/2000 –caso Casino de La Toja– y la 186/2000). En dichas sentencias, el Alto Tribunal aplicó el test de proporcionalidad para valorar la legitimidad de la intromisión en el derecho a la intimidad de los trabajadores, siendo éste el canon que adopte la jurisdicción social ordinaria para valorar la licitud de las pruebas informáticas[15].

El cambio de orientación en la jurisprudencia se empieza a observar en diversas sentencias de suplicación, cuya interpretación fue confirmada por la STS de 28 de junio de 2006[16] que enjuició los hechos siguientes: la empresa, con el fin de controlar la actividad de un trabajador instaló un programa para capturar pantallas a intervalos de tiempo. Se recopiló la documentación aportada por la empresa como prueba documental. La empresa no accedió al contenido de los correos, simplemente identificó a la persona, fecha y duración de los contactos, y el acceso a Internet para actividades ajenas a la empresarial. El Tribunal Supremo no apreció contradicción entre la sentencia recurrida, que estimó la ilicitud de la prueba obtenida por vulnerar el derecho a la intimidad, y la referencial, ya que en la primera, la STSJ País Vasco de 21 de diciembre de 2004 había estimado que existía autorización para usar internet para fines particulares, tras constatar que no había sido expresamente prohibido por el empresario, mientras que en la referencial, del TSJ Galicia, no ocurrió así. Esta doctrina que atendía a la existencia de una prohibición de uso para fines particulares, se consolidó en la STS de 26 de septiembre de 2007[17]. En apretada síntesis los hechos que se enjuiciaron fueron los siguientes: el Director General de la empresa demandada, prestaba servicios en un despacho sin llave, en el que disponía de un ordenador, carente de clave de acceso y conectado a la red de la empresa que disponía de ADSL. Un técnico de una empresa de informática fue requerido para comprobar los fallos de un ordenador que la empresa señaló como del actor. En la comprobación se detectó la existencia de virus informáticos, como consecuencia de la navegación por páginas poco seguras de Internet. En presencia del administrador de la empresa se comprobó la existencia en la carpeta de archivos temporales de antiguos accesos a páginas pornográficas, que se almacenaron en un dispositivo de USB, que se entregó a un notario. Las operaciones llevadas a cabo en el ordenador se hicieron sin la presencia del actor, de representantes de los trabajadores ni de ningún trabajador de la empresa. El ordenador fue retirado de la empresa para su reparación y, una vez devuelto, se procedió a realizar la misma operación con la presencia de delegados de personal. La sentencia recurrida confirmó la decisión de instancia que había considerado que no era válida la prueba de la empresa, porque fue obtenida mediante un registro de un efecto personal que no cumplía las exigencias del artículo 18 ET. El Tribunal Supremo unifica la divergente doctrina de los Tribunales Superiores de

[14] Es exponente de esta doctrina la STSJ Galicia de 4 de octubre de 2001 (Rec. 4168/2001).
[15] A modo de ejemplo, STSJ Galicia de 4 de octubre de 2001antes citada.
[16] Rec. 605/2005.
[17] Rec. 966/2006.

Justicia, existente hasta el momento, y concluye que el supuesto de hecho del art. 18 ET es completamente distinto del que se produce con el control de los medios informáticos en el trabajo, por lo que no son aplicables las limitaciones que aquél impone. El problema es más amplio, porque, en realidad, lo que plantea el recurso, desde la perspectiva de ilicitud de la prueba obtenida vulnerando los derechos fundamentales, es la compatibilidad de ese control empresarial con el derecho del trabajador a su intimidad personal o, incluso, con el derecho al secreto de las comunicaciones, si se tratara del control del correo electrónico. Estamos en presencia de "medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario previsto en el artículo 20.3 ET", precepto que debe aplicarse con las siguientes matizaciones:

a) La primera se refiere a la necesidad de que las medidas de control guarden "en su adopción y aplicación la consideración debida" a la dignidad del trabajador, lo que también remite al respeto a la intimidad en los términos establecidos en las sentencias del Tribunal Constitucional 98/2000 y 186/2000. En este punto recuerda la Sala que en ocasiones existe un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. "Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio"**.** Por ello, "lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones". De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos –en los casos Halford y Copland– para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos.

b) La segunda precisión o matización se refiere al alcance de la protección de la intimidad, que es compatible, con el control lícito al que se ha hecho

> referencia. Esta matización permite a la Sala hacer una delimitación del ámbito de protección del derecho a la intimidad. Ve con claridad que las comunicaciones telefónicas y el correo electrónico están incluidos en este ámbito con la protección adicional que deriva de la garantía constitucional del secreto de las comunicaciones. La garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentran en el ordenador, así como a los archivos temporales. El Tribunal hace una importante afirmación cuando precisa que "tampoco es obstáculo para la protección de la intimidad el que el ordenador no tuviera clave de acceso. Este dato –unido a la localización del ordenador en un despacho sin llave– no supone por sí mismo una aceptación por parte del trabajador de un acceso abierto a la información contenida en su ordenador".

La aplicación de esta doctrina al caso analizado lleva a declarar la ilicitud de la prueba por vulneración del derecho a la intimidad de los trabajadores, pues no había existido previa advertencia sobre el uso y el control del ordenador. Por otro lado, aunque la entrada inicial en el ordenador podía justificarse por la existencia de un virus, no puede hablarse de que estemos ante lo que en el ámbito penal se califica como un "hallazgo casual"[18], pues se ha ido más allá de lo que la entrada regular para la reparación justificaba, ya que la actuación empresarial no se detuvo en las tareas de detección y reparación, sino que, se siguió con el examen del ordenador para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada.

Esta doctrina se reiteró posteriormente en la STS de 8 de marzo de 2011[19]. Nuevamente es la constatación de que en la empresa no existían reglas de uso del ordenador, ni se había advertido a los trabajadores de las posibilidades de control, lo que lleva a la Sala a deslegitimar las medidas de fiscalización sobre la navegación por internet, concluyendo que la prueba obtenida se había obtenido con vulneración del derecho a la intimidad. En ese mismo año tuvo ocasión de pronunciarse nuevamente el Tribunal Supremo en sentencia de 6 de octubre de 2011[20], dictada en Sala General. Los hechos analizados son los siguientes: para controlar el cumplimiento de las instrucciones sobre el uso de los medios de la empresa (correo electrónico, internet, teléfonos móviles…), que estaba prohibido para fines particulares, se procedió a la motorización de los ordenadores de la demandante y de otra trabajadora, instalándose un "software" al objeto de captar las pantallas a las que accedía la trabajadora para su posterior visualización. Se trataba de un sistema "pasivo", poco agresivo, que no permitía acceder a los archivos del ordenador que estaban protegidos por contraseñas de cada uno de los usuarios. Nuevamente el control afectó a la navegación por internet y se estudia la colisión con el derecho a la intimidad. En este caso existía una diferencia relevante respecto de la

[18] SSTS de la Sala de lo Penal de 20 de septiembre de 2006 (Rec. 10134/2006), 29 de noviembre de 2006 (Rec.1175/2005) y 1 de diciembre de 2006 (Rec.10381/2006).

[19] Rec.1826/2010.

[20] Rec. 4053/2010.

sentencia de 2007, ya que el uso extra laboral estaba prohibido expresamente por la empresa, razón por la cual, al no existir tolerancia del uso personal, no podía tampoco existir una expectativa razonable de confidencialidad. La sentencia da un paso más en la flexibilización del control de la legalidad de la actuación del empresario, ya que afirma que esto es así "con independencia de la información que la empresa haya podido proporcionar sobre el control y su alcance, control que, por otra parte, es inherente a la propia prestación de trabajo y a los medios que para ello se utilicen, y así está previsto legalmente", de lo que se desprende que al existir una prohibición de uso personal, no sería absolutamente necesario informar sobre la posibilidad de control y su alcance, como sí se indicaba en la STS de 2007. Si bien es cierto que el nuevo pronunciamiento parece contradecir el anterior del año 2007, como se afirma en el voto particular[21], el propio Tribunal Supremo aclara que las reflexiones que hizo cuatro años antes sobre el deber de informar a los trabajadores de la existencia de control y de los medios empleados para este fin, se presentaron "como matizaciones" y que la sentencia razonaba "obiter dicta" y "en el marco de la buena fe o de la legalidad ordinaria (art. 64.1.c) del ET)", tratándose de "matizaciones que operan ya fuera del marco estricto de la protección del derecho fundamental, como obligaciones complementarias de transparencia".

La doctrina del Tribunal Supremo fue confirmada en autos posteriores que inadmitieron los recursos de casación en unificación de doctrina por falta de contradicción entre la sentencia recurrida y la de contraste, al no existir en una de ellas una prohibición respecto del uso de los medios por la empresa[22]. Queremos destacar el Auto de 13 de septiembre de 2013[23], ya que niega la existencia de contradicción con la STS de 2007 con base no sólo en que existía una normativa que contenía las medidas para un buen uso de los recursos informáticos y se avisaba a los usuarios del correo electrónico de que la empresa se reservaba la facultad de chequear los mismos, sino que delimita también el ámbito de protección del secreto de las comunicaciones incidiendo en que "en ningún momento se interceptaron comunicaciones en curso", sino que únicamente se analizaron documentos contenidos en la base de datos donde se almacenaban los mensajes de correo una vez recibidos, o las copias que se guardan en el originador de los mensajes de correos enviados. "Se entiende que las comunicaciones en curso son objeto de una garantía mayor que no puede ser otra que la que otorga el secreto de las comunicaciones". Queremos destacar que en

[21] El voto particular, suscrito por cinco magistrados, discrepa de la decisión mayoritaria, por considerar que el criterio adoptado comportaba un retroceso en la protección de derecho a la intimidad, tal como había sido interpretado por la SSTS de 18 de enero de 2007 y de 8 de marzo de 2011. En su opinión, para dicha jurisprudencia no es suficiente la prohibición del uso del ordenador para actividades privadas, sino que dicha prohibición ha de ir acompañada de una información sobre la existencia de un control y de los medios que van a aplicarse.

[22] Autos de 27 de noviembre de 2008 (Rec. 3885/2007), de 29 de marzo de 2011 (Rec. 3570/2010), de 20 de marzo de 2012 (Rec. 3045/2011), de 9 de julio de 2013 (Rec. 354/2013), de 9 de enero de 2013 (Rec. 2000/2012), de 22 de octubre de 2014 (Rec. 251/2014), de 11 de noviembre de 2015 y de 5 de julio de 2016 (Rec. 2920/2015).

[23] Rec. 698/2012.

las sentencias del Tribunal Supremo estudiadas con anterioridad[24] se hacía mención a la posibilidad de que los correos electrónicos estuviesen protegidos también por el derecho fundamental al secreto de las comunicaciones, pero como evidencian los hechos, en ninguna de ellas se intervino en un proceso de comunicación en curso, sino que, *a posteriori* se leyeron correos enviados o recibidos almacenados en el servidor del ordenador[25]. Puede observarse, además, que la Sala Cuarta argumenta desde la perspectiva del derecho a la intimidad. En ningún caso, se hace una interpretación de las garantías del derecho al secreto de las comunicaciones en el ámbito de las relaciones laborales. MARÍN ALONSO ha explicado muy bien las razones de esta omisión y de la confusión entre ambos derechos que se observa en la jurisdicción social. Esta situación habría venido propiciada por el expreso y temprano reconocimiento del derecho a la intimidad en la relación laboral por el Tribunal Constitucional así como por la existencia de normativa de desarrollo del mismo entre particulares. Sin embargo, el derecho al secreto de las comunicaciones, no tiene un desarrollo normativo específico en las relaciones inter privados ni había sido analizado por el Tribunal Constitucional en el ámbito de la empresa hasta el año 2012, como veremos a continuación, siendo por tanto los Tribunales ordinarios los encargados de resolver los posibles conflictos sobre el mismo. "Esto último provocó que los tribunales resolvieran atendiendo a la doctrina ya asentada en nuestro ordenamiento sobre otros derechos de la personalidad en la empresa, en particular, respecto del derecho a la intimidad en tanto éste disfrutaba, por un lado, de una marcada flexibilidad o sub-

[24] Posteriores sentencias de los TSJ, han aplicado la doctrina del TS y atienden a la existencia de información previa sobre el uso de las herramientas tecnológicas para valorar si existe una expectativa razonable de confidencialidad. *Vid,* SSTSJ Madrid de 14 de julio de 2011 (Rec. 4654/2010) –se comprobaron correos enviados y recibidos desde las cuentas del dominio vinculado a la empresa–, Madrid de 20 de marzo de 2012 (Rec. 3045/2011), Madrid de 22 de abril de 2015 (Rec. 544/2014), Asturias de 30 de enero de 2015 (Rec. 28/2015) –se examinaron y recuperaron los correos enviados pero no eliminados–, Madrid de 20 de abril de 2015 (Rec. 57/2015), Andalucía/Sevilla de 25 de febrero de 2015 (Rec. 306/2014) –se controla por la empresa el cumplimiento de la normativa sobre el uso de internet–, Madrid de 26 de enero de 2015 (Rec. 679/2014) –se controla también la navegación por internet–, Valencia de 12 de mayo de 2015 (Rec. 977/2015) –se leyeron los correos personales enviados desde la cuenta de la empresa–, País Vasco de 29 de septiembre de 2015 (Rec. 1245/2015) –se valora que la prueba no se realizó entrando en el ordenador del trabajador, sino analizando las fotografías de la pantalla del ordenador del trabajador que, al igual que las de los ordenadores del resto de trabajadores de la empresa, eran remitidas mediante un programa instalado por la empleadora a través de un correo electrónico a una dirección; de esta forma se analizaban los correos y sus firmas digitalizadas, Asturias de 28 de febrero de 2017 (Rec. 129/2017).

[25] Sin embargo, en el caso analizado por la STSJ Canarias/Las Palmas de 8 de enero de 2016 (Rec. 877/2015) sí se realizó un control de los correos en tiempo real, lo que se justificó porque el trabajador había protegido el ordenador de tal forma que eliminaba los correos o no dejaba rastro de la utilidad que le daba ante la prohibición expresa de la empresa, lo que obligó a la empleadora a llevar a cabo con otros medios indagatorios y de investigación a través de programas informáticos que permitieran obtener esa información a tiempo real antes de su eliminación–. El Tribunal concluye que no se ha conculcado el derecho al secreto de las comunicaciones, ya que en la empresa existía una normativa que establecía la prohibición absoluta de uso del ordenador, correo electrónico e internet para asuntos particulares.

jetividad en su apreciación y, por otro, se presentaba como un límite no absoluto al poder de dirección del empresario"[26].

2. PRONUNCIAMIENTOS DEL TRIBUNAL CONSTITUCIONAL SOBRE LAS SENTENCIAS RECAÍDAS EN EL ORDEN SOCIAL

El Tribunal Constitucional se ha pronunciado en dos ocasiones sobre la legitimidad del control empresarial de las herramientas informáticas, situando de nuevo el canon de razonamiento en la existencia de una "expectativa de intimidad"[27]. La primera de ellas fue la STC 241/2012 de 17 de diciembre de 2012[28]. En esencia, los hechos que dieron lugar a la resolución del tribunal fueron los que siguen: la empresa Global Sales Solutions Line, S.L intervino las conversaciones mantenidas por dos trabajadoras mediante un programa de mensajería instantánea (Trillian) donde se habían vertido comentarios críticos, despectivos o insultantes en relación con compañeros de trabajo, superiores y clientes. Las dos trabajadoras implicadas habían instalado el programa contraviniendo la prohibición expresa del empresario, en un ordenador de uso común por todos los trabajadores. La empresa las amonestó verbalmente, procediendo ambas, pese a reconocer los hechos, a interponer demanda de tutela de derechos fundamentales, solicitando que se declarara la vulneración de su derecho a la intimidad y al secreto de las comunicaciones. Respecto del derecho a la intimidad, la Sala no aprecia afectación del mismo desde el momento en que fueron las propias trabajadoras quienes realizaron actos dispositivos que determinaron la eliminación de la privacidad de sus conversaciones. Respecto del secreto de las comunicaciones, concluye que por un lado, "las comunicaciones estaban 'abiertas' y no rodeadas de las condiciones que pudieran preservarlas". Por otro lado, admite que la empresa puede adoptar medidas empresariales de vigilancia y control y que éstas son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin. En el caso enjuiciado no existía tolerancia ni en la instalación de programas ni en el uso del ordenador, todo lo contrario, habían sido expresamente prohibido, por lo que "no existía expectativa razonable de confidencialidad". Realmente, el Tribunal Constitucional no hace sino aplicar la STC

---

[26] MARÍN ALONSO, I., "El uso por los trabajadores de las comunicaciones electrónicas en la empresa…", cit., pág. 4.

[27] Posteriores sentencias recaídas en suplicación aplican ambos pronunciamientos para valorar la legitimidad de la prueba aportada al juicio. En la STSJ Cataluña de 28 de mayo de 2015 (Rec. 1033/2015) la Sala, tras constatar que no existía ningún tipo de prohibición o restricción para que el trabajador utilizara para su uso personal el ordenador de la empresa que tenía asignado en exclusiva, entiende que la empresa no estaba facultada por sí y ante sí para abrir los correos personales del trabajador, que se encontraba de vacaciones y que, en consecuencia no podía dar consentimiento al respecto. *Vid,* también STSJ Madrid de 18 de diciembre de 2015 (Rec. 780/2015).

[28] *Vid,* un ponderado comentario sobre ambas sentencias en RODRÍGUEZ CARDO, I.A., "Política empresarial previa y supresión de la expectativa de privacidad: una reflexión crítica sobre las facultades de control del ordenador utilizado por el trabajador", Temas Laborales, nº. 126, 2014, pp. 167-197.

142/2012 y considerar que el canal de comunicación estaba abierto, de forma que no podía predicarse de él la confidencialidad, precisamente porque el empresario al prohibir su uso para asuntos particulares, se había reservado la posibilidad de fiscalizarlo[29]. Considera que esa ausencia de expectativa hace que su doctrina sea perfectamente compatible con las sentencias del Tribunal Europeo de Derechos Humanos Halford y Copland. Sin embargo, la sentencia se aparta de la interpretación realizada por la STS de 26 de septiembre de 2007 en la que se había afirmado que el hecho de que el ordenador no tuviera clave de acceso y se encontrara en un lugar común accesible a todos los trabajadores no impedía apreciar la existencia del derecho a la intimidad[30]. En sentido contrario, el Tribunal Constitucional concluye que el uso común del ordenador por todos los empleados hacía que la pretensión de secreto careciera de cobertura constitucional.

En el caso enjuiciado se leyeron los mensajes almacenados en el servidor del ordenador, es decir, el empresario no se apoderó de información vinculada a procesos de comunicación en marcha, argumento que podría haber servido por sí mismo para afirmar la inexistencia de afectación del secreto de las comunicaciones. Sin embargo, la sentencia omite por completo esta circunstancia, y concluye que la actuación de control de la empresa se ajustó a "un suficiente canon de razonabilidad" sin que se atisbe lesión de derechos fundamentales de las trabajadoras afectadas puesto que el acceso al contenido del programa de mensajería *Trillian* sólo se produjo cuando la empresa tuvo conocimiento de la instalación del programa a través de otro empleado. Además, la intervención empresarial se limitó a la comprobación de la instalación en el soporte informático de uso común, con la finalidad de constatar si había habido un incumplimiento por parte de las trabajadoras implicadas y su alcance, desarrollándose la actuación en un plazo razonable[31]. El juicio de proporcionalidad, no obstante,

---

[29] Utilizando una argumentación parecida, la doctrina de suplicación admite que no vulnera el derecho al secreto de las comunicaciones la prueba accediendo al Facebook del trabajador, siempre y cuando los contenidos aportados al juicio estuvieran abiertos al público y no reservadas a los "amigos". *Vid,* entre otras, SSTSJ Andalucía/Sevilla de 29 de octubre de 2015 (Rec. 2723/2014), Cantabria de 10 de noviembre de 2015 (Rec. 765/2015) y Canarias/Gran Canaria de 22 de enero de 2016 (Rec. 1167/2015).

[30] Compartimos la opinión crítica sobre este punto de RODRÍGUEZ ESCANCIANO, S., ("Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores", cit., 2015, pp. 56-57) y de DE LA QUADRA SALCEDO JANINI y SUÁREZ CORUJO, B., "¿Trabajadores incomunicados? La deriva de la doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones", Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, publicada en la obra colectiva *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social*, op.cit., p. 8. En el mismo sentido, *vid,* el voto particular de Valdés Dal-Ré a la sentencia.

[31] MARÍN ALONSO, I., ("El uso por los trabajadores de las comunicaciones electrónicas en la empresa…, cit., p. 8) es muy crítica con la STC 241/2012 ya que fundamenta su decisión en la existencia de una orden empresarial prohibitiva de instalar programas informáticos no autorizados por la empresa, pero sin entrar a "valorar convenientemente si la orden empresarial en sí misma se configura como un límite legítimo al ejercicio al secreto de las comunicaciones en la empresa y, sobre su alcance, en su caso". *Vid,* también comentarios críticos a la sentencia en CARDONA RUBERT, M.B., "Reinterpretación de los derechos de intimidad y secreto de las comunicaciones

se encuentra en nuestra opinión escasamente fundamentado, pues obvia el hecho de que si el fin era comprobar la falta cometida por las trabajadoras, se podría haber hecho, de forma menos invasiva identificando a los destinatarios de los mensajes, sin necesidad de entrar en el contenido[32]. En este sentido, el Tribunal Constitucional da un salto cualitativo muy importante, ya que legitima una interpretación jurisprudencial que configura la existencia expresa de prohibición como título habilitante suficiente para justificar la intromisión en derechos fundamentales del trabajador[33], sin necesidad de someter la actuación del empresario al test de proporcionalidad[34].

La sentencia tiene un voto discrepante de Valdés Dal-Ré quien, con cita en la STC 142/2012, reflexiona que, en atención al carácter formal del derecho y a sus contenidos, la protección que ofrece el art. 18.3 CE ha de incluir los supuestos en los que exista la trasgresión de una orden empresarial de prohibición de instalación de sistemas de mensajería electrónica o de empleo de los existentes para un fin ajeno a la actividad laboral, pues el incumplimiento de lo ordenado no habilita en modo alguno interferencias en el proceso o en el contenido de la comunicación, sin perjuicio de que pueda acarrear algún tipo de sanción. En otros términos, la infracción de las órdenes empresariales tolera la imposición de las sanciones previstas en el ordenamiento jurídico, pero ni consiente la vulneración directa de derechos fundamentales al amparo del incumplimiento de la orden empresarial, ni tampoco las intromisiones empresariales enderezada a verificar o comprobar la existencia de las comunicaciones, incluso cuando *ex post*, cometida la vulneración y gracias a esa ilegítima práctica, quede acreditado que aquellas sanciones eran ajustadas a Derecho. Para superar esos límites, Valdés Dal-Ré apunta que "cualquier intervención empresarial debe producirse con las prevenciones y cánones de la autorización judicial que cita el art. 18.3 CE, en cuya definición nuestra jurisprudencia incorpora la exigencia de una norma legal que habilite la injerencia –'una ley de singular precisión' (STC 49/1999,

---

en el modelo constitucional de relaciones laborales, un paso atrás. Comentario a la STC 241/2012, de 17 de septiembre", Revista de Derecho Social, nº. 60, 2012, pp. 169 y ss.

[32] De esta opinión es CARRILLO LÓPEZ, M., "El uso de internet en la empresa: a propósito de la STEDH de 13 de enero de 2016, caso Barbulescu C/ Rumanía", IUSLabor*,* nº. 1, 2016, pág.5 (disponible en *https://www.upf.edu/iuslabor/_pdf/2016-1/Carillo.pdf*). Última consulta 23 de junio de 2016.

[33] DE LA QUADRA SALCEDO JANINI y SUÁREZ CORUJO, B., "¿Trabajadores incomunicados?…", cit., p. 8.

[34] Destaca al respecto RODRÍGUEZ ESCANCIANO, S., ("Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores", cit., p. 55) que el TC ha sentado, respecto al secreto de las comunicaciones, una novedosa doctrina que "prescinde del juicio de proporcionalidad para adoptar el canon de expectativa de intimidad, lo que revela que el aspecto más significativo a tener en cuenta es el previo proceder de la empresa respecto a la determinación de las pautas de uso y control de los ordenadores". Para FERNÁNDEZ RODRÍGUEZ, J.J., (*Secreto e intervención de las comunicaciones en Internet*, cit., p. 162) el juicio de proporcionalidad es imprescindible. Admitir lo contrario sería una huida hacia delante en favor de los intereses del empresario "sin preocuparse de las exigencias constitucionales y de la autorización judicial que debe mediar para legitimar una intervención de las comunicaciones". Opina el autor que el hecho de que el trabajador conozca la política empresarial de control de las comunicaciones no supone una autorización para autorizar la revelación de su contenido (pág. 163).

FJ 4) – y dispone que los Jueces y Tribunales podrán adoptar la medida sólo cuando concurran los presupuestos materiales pertinentes (ibídem)".

En la segunda sentencia, la 170/2013 de 7 de octubre de 2013[35], se denegó el amparo a un trabajador cuyo despido había sido declarado procedente, basándose en que había cedido información confidencial de la empresa a la competencia, a través del correo electrónico y del teléfono móvil, ambos propiedad de la empresa. El Tribunal da un paso más en el fortalecimiento del poder de dirección y vigilancia del empresario, ya que admite que el requisito de la información previa queda suficientemente cumplido si el convenio colectivo tipifica el uso del ordenador para usos extra laborales como una falta sancionable; en el caso concreto, el convenio sectorial de la industria química lo tipificaba como falta leve[36]. En consecuencia, el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse, *ex* art. 20.3 ET, no sólo para vigilar el cumplimiento de la prestación laboral realizada a través del uso profesional de estos instrumentos, sino también para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo. Como en el supuesto enjuiciado en la STC 241/2012, estima que la remisión de mensajes se llevó a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, "se hallaba abierto al ejercicio del poder de inspección reconocido al empresario; sometido en consecuencia a su posible fiscalización" por lo que quedaba fuera de la protección constitucional del art. 18.3 CE. Dado que el trabajador no utilizó un "canal cerrado" para la comunicación, no podía tener "una expectativa fundada y razonable de confidencialidad

[35] *Vid,* un comentario a la sentencia en MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B.M., "El control empresarial del correo electrónico tras la STC 170/2013", Revista Doctrinal Aranzadi Social, nº. 11, 2014, versión digital (BIB 2014\122); también en SEPÚLVEDA GÓMEZ, M., "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites", Temas Laborales*,* nº. 122, 2013, pp. 197-214.

[36] En el caso enjuiciado por la sentencia recurrida, también se habían leído los SMS del teléfono móvil. La propia STSJ Madrid consideró ilegítimo este control, ya que el convenio colectivo no establecía nada sobre el uso exclusivamente profesional del teléfono móvil. En la STSJ Cataluña de 16 de diciembre de 2017 (Rec. 6194/2016) se aplica la doctrina contenida en la STC 170/2013, si bien, concluye que el trabajador sí tenía una expectativa razonable de confidencialidad, toda vez que la prohibición que se deriva de la calificación en el Convenio Colectivo de empresas siderometalúrgicas de la provincia de Tarragona, como falta grave del "empleo para usos propios de los útiles, herramientas, maquinaria o vehículos de la empresa", no puede considerarse como una prohibición absoluta de utilización del ordenador y teléfono móvil entregado al actor por la empresa. La sentencia hace una clara distinción entre el ordenador portátil y el teléfono móvil y otras herramientas que son propiedad de la empresa: "no puede perderse de vista la especial situación que respecto al uso de ordenadores y teléfonos móviles se produce, con situaciones y argumentaciones que no se dan con otros útiles que la empresa pone a disposición de los trabajadores para desarrollar su trabajo, como por ejemplo camiones, automóviles, martillos, taladradoras, etc, respecto de ninguna de las cuales se llega a afirmar la existencia de un 'hábito social generalizado de tolerancia con ciertos usos personales moderados', máxime en el caso de autos, en los que el ordenador no está en la empresa sino que es portátil y por lo tanto el trabajador lo lleva siempre consigo para el desarrollo de su trabajo".

respecto al conocimiento de las comunicaciones mantenidas" a través de la cuenta de correo proporcionada por la empresa. Es importante destacar que en el caso analizado se fiscalizaron comunicaciones que habían quedado registradas en el ordenador, es decir, la empresa no había interceptado el proceso de comunicación mientras los correos eran enviados y recibidos, sino que accedió a su contenido *a posteriori.* En este sentido, el Tribunal hace una importante precisión a efectos de nuestro estudio cuando añade que la conducta empresarial analizada se había realizado "además" cuando "el proceso de comunicación podía entenderse ya finalizado", y, en consecuencia no había supuesto "una interceptación o conocimiento antijurídicos de comunicaciones ajenas realizadas en canal cerrado", debiendo descartarse, en definitiva, la invocada lesión del derecho al secreto de las comunicaciones. Obsérvese, sin embargo, que este argumento no parece utilizarse como *ratio decidendi* para negar la existencia de la vulneración del secreto de las comunicaciones, sino que actúa como mero complemento de la razón fundamental: la inexistencia de expectativa razonable de confidencialidad[37].

El Tribunal analiza a continuación la posible vulneración del derecho a la intimidad. Partiendo de que en la empresa existía un régimen jurídico que prohibía el uso del correo electrónico para fines personales, concluye que tal circunstancia "impedía en este caso abrigar una expectativa razonable de privacidad que determinara la entrada en la esfera de protección del derecho a la intimidad". Es decir, utiliza el mismo razonamiento para excluir la intromisión ilegítima en ambos derechos fundamentales. Dentro del discurso sobre la posible afectación del derecho a la intimidad, estudia si el acceso por la empresa al contenido de los correos electrónicos había resultado excesivo o desproporcionado para la satisfacción de los objetivos e intereses empresariales. Aplicando similar razonamiento al seguido en la STC 186/2000, el Tribunal afirma que el acceso por la empresa a los correos electrónicos del trabajador reunía las exigencias requeridas por el juicio de proporcionalidad. Se trataba en primer lugar de una medida justificada, puesto que su práctica se fundó en la existencia de sospechas de un comportamiento irregular del trabajador. En segundo término, la medida era idónea para la finalidad pretendida por la empresa, consistente en verificar si el trabajador cometía efectivamente la irregularidad sospechada: la revelación a terceros de datos empresariales de reserva obligada, al objeto de adoptar las medidas disciplinarias correspondientes. En tercer lugar, la medida podía considerarse necesaria, dado que, como instrumento de transmisión de dicha información confidencial, el contenido o texto de los correos electrónicos serviría de prueba de la citada irregularidad ante la eventual impugnación judicial de la sanción empresarial; no era pues suficiente a tal fin el mero acceso a otros elementos de la comunicación como la identificación del remitente o destinatario, que por sí solos no permitían acreditar el ilícito indicado. Finalmente, la medida podía entenderse como ponde-

[37] Señala al respecto ABERASTURI GORRIÑO, U., ("Control empresarial del correo electrónico del empleado y relevancia de la información previa…",cit., p.5) que el TC podría haber alegado como argumento para concluir que el secreto a las comunicaciones no entraba en juego, que la comunicación ya se había consumado, siendo presumible que los mensajes remitidos por el trabajador en el caso concreto se habían abierto por el receptor.

rada y equilibrada, ya que, al margen de las garantías con que se realizó el control empresarial a través de la intervención de perito informático y notario, ha de partirse de que el control afectó sólo a los correos relativos a datos sobre la cosecha de 2007 y 2008, sin que conste que el contenido de estos mensajes reflejara aspectos específicos de la vida personal y familiar del trabajador, sino únicamente información relativa a la actividad empresarial. De ahí que, atendida la naturaleza de la infracción investigada y su relevancia para la entidad, no pueda apreciarse que la acción empresarial de fiscalización haya resultado desmedida respecto a la afectación sufrida por la privacidad del trabajador[38].

Entrando en el análisis crítico de la sentencia, creemos que se consolida la interpretación realizada en la STS de 2011, conforme a la cual la mera existencia de una prohibición de uso exonera a la empresa de la obligación de poner en conocimiento de los trabajadores las medidas de control y su alcance. Resulta muy discutible que un derecho fundamental, como es el secreto de las comunicaciones, sufra una restricción por parte de un Convenio Colectivo que se limita a tipificar como infracción leve la utilización de los medios informáticos de la empresa para fines distintos de los laborales, pero que no advierte de la posibilidad de fiscalización del empresario ni de la forma en qué está se llevaría a cabo. Todo ello unido al hecho de que el convenio fuera sectorial, no de empresa, no garantiza suficientemente, creemos, su conocimiento por parte de los trabajadores, lo que dificulta que pueda entenderse cumplido por parte del empresario su deber de información en los términos exigidos por la jurisprudencia del TEDH para valorar la "calidad" que debe tener la ley que permite la intromisión en el derecho a la intimidad y el secreto de las comunicaciones[39].

Tanto el Tribunal Supremo como el Tribunal Constitucional hacen especial énfasis en el hecho de que los medios utilizados por el trabajador que sirven de soporte para la comunicación, son de titularidad empresarial, de tal manera que con base en su derecho de propiedad el empresario podría llegar a limitar de forma absoluta su uso por parte de los trabajadores, olvidando la reflexión sobre la función social del derecho de propiedad que hizo el Tribunal Constitucional en su STC 281/2005, cuando tuvo oportunidad de pronunciarse sobre el derecho de los sindicatos a utilizar el correo electrónico de la empresa para comunicarse con los trabajadores[40].

---

[38] *Vid,* también la STS de 13 de septiembre de 2016 (Rec. 206/2015) que conoció de la demanda de conflicto colectivo contra unas Instrucciones de la Compañía de Radio Televisión de Galicia, relativas al uso del correo electrónico. La Sala considera que tales Instrucciones atendían cumplidamente a los tres juicios: idoneidad, necesidad y estricta proporcionalidad.

[39] De esta opinión es RODRÍGUEZ ESCANCIANO, S., "Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores", cit., p. 65. También, CARRASCO DURÁN, M., "El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería de la empresa", Revista Aranzadi Doctrinal, nº 9, 2014 (formato electrónico) p 7 pdf. Y ABERASTURI GORRIÑO, U., "Control empresarial del correo electrónico del empleado y relevancia de la información previa…", cit., pp.9-10. Considera el autor que el contenido de la información que hace decaer la existencia de una expectativa razonable de intimidad debe ajustarse a lo prevenido en la LOPD (pp-10-11).

[40] Sobre la función social que cumple la propiedad en el caso de los medios de comunicación de la empresa, *vid,* HERREROS LÓPEZ, J.M., "Las tecnologías de la información y comuni-

Consecuencia de lo anterior es que es la prohibición expresa de uso la que convierte el canal de comunicación en un canal abierto, y por lo tanto, fuera del ámbito de protección del art. 18.3 CE. Por otro lado, ambos tribunales pasan por alto un dato especialmente importante: en algunos de los casos enjuiciados existía un tercero interviniente en el proceso de comunicación, ajeno a la empresa y, por tanto, desconocedor de las condiciones de uso del correo electrónico por parte de ésta y al que no afectaba el convenio colectivo aplicable a sus trabajadores. Aplicando los criterios del propio Tribunal, este tercero sí podría tener una expectativa razonable de confidencialidad y, sin embargo, al calificarse como abierto el canal de comunicación, se ve sometido a la injerencia del empresario sobre su interlocutor[41]. Puede afirmarse también que el tratamiento que da el Tribunal Constitucional al secreto de las comunicaciones y al derecho a la intimidad es el mismo[42]. El hecho de que el proceso de comunicación hubiera finalizado no se toma como apoyo para justificar que el empresario no llegó a entrar en el ámbito de protección del secreto a las comunicaciones. Todo el razonamiento del Tribunal gira en torno a la existencia o no de la expectativa de confidencialidad que no existía en ambos casos analizados por haber tenido lugar las comunicaciones en un "canal abierto", siendo la política aplicable en la empresa la que configura en cada caso el canal como abierto o cerrado. Por otro lado, en ambas sentencias el Tribunal Constitucional niega que se produzca una colisión entre dos derechos fundamentales, ya que uno de los posibles derechos en juego (el de intimidad o el de secreto de las comunicaciones) no resultaba afectado dadas las circunstancias del caso. Negada la mayor, la existencia en el caso concreto de derechos fundamentales del trabajador que pudieran haber sido vulnerados, no es necesario realizar el juicio de proporcionalidad, pese a que el Tribunal, en la segunda de las sentencias analizadas sí lo realiza, pero obsérvese que lo hace "a mayor abundamiento" para fundamentar todavía más su doctrina, y ante la exigencia de contestar a las alegaciones del trabajador respecto al carácter desproporcionado de la fiscalización[43].

---

cación de la empresa al servicio de la libertad sindical", en AA.VV (Monterroso Casado, E., dir.), *Responsabilidad empresarial*, Tirant lo Blanch, Valencia, 2016, pp. 536-543.

[41] Como ha señalado destacada doctrina, en referencia al TC, se ha perdido la ocasión de matizar el alcance del control incondicionado por parte del empresario del correo electrónico empresarial en atención a la existencia de un tercero ajeno a la comunicación. Sería necesario exigir, para que el control fuera legítimo, que en los correos de la empresa constase la advertencia específica dirigida a los terceros de que se trata de un correo de la empresa y que puede ser sometido a fiscalización. *Vid,* DE LA QUADRA SALCEDO JANINI y SUÁREZ CORUJO, B., "¿Trabajadores incomunicados? …", cit., pp. 12-13.

[42] En este sentido, señalan MONEREO PÉREZ y LÓPEZ INSUA, que aunque el objetivo del TC era tratar de manera independiente ambos derechos, finalmente los relaciona, lo que para los autores es razonable ya que el secreto de las comunicaciones "constituye una categoría jurídica estrecha y funcionalmente asociada a la intimidad". *Vid,* MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B.M., "El control empresarial del correo electrónico tras la STC 170/2013", cit., p.7 (formato pdf).

[43] La STSJ Canarias/Las Palmas de 8 de enero de 2016 (Rec. 877/2015), tras concluir que en el caso analizado no existía expectativa razonable de confidencialidad y, por tanto, no había resultado afectado el secreto de las comunicaciones, precisa que "lo expuesto sería suficiente para

La doctrina del Tribunal Constitucional parecía haber sido avalada por el TEDH en sentencia de la Sala Cuarta, de 12 de enero de 2016 –asunto 61496/08 "Bărbulescu v. Rumanía"–[44], que abordó un supuesto muy similar a los enjuiciados por nuestro Alto Tribunal. En clara sintonía con él, declaró que la monitorización por parte de la empresa del uso de internet realizado por un empleado, concretamente de las comunicaciones realizadas a través de una cuenta de Yahoo Messenger creada a instancias de la compañía para comunicarse con los clientes de la empresa, no vulneraba su derecho a la intimidad ni a la inviolabilidad de la correspondencia (artículo 8 del Convenio Europeo de Derechos Humanos), teniendo en cuenta que existía una política interna de la empresa que prohibía expresamente el uso de los medios informáticos de la empresa para fines personales[45] y que la monitorización había sido proporcionada y razonable[46], prevaleciendo el derecho de la empresa a comprobar el cumplimiento de las obligaciones laborales frente al derecho a la intimidad y al secreto de las comunicaciones del empleado[47]. Recurrida la sentencia por el señor Barbulescu, la Gran Sala se pronunció en sentencia de 5 de septiembre de 2017, en la que revocó el pronunciamiento de la Sala Cuarta, declarando que había existido una violación del artículo 8 CEDH. Dicha sentencia, que obliga a revisar la doctrina del Tribunal Constitucional español, eleva los cánones de exigencia del deber de

---

el fracaso de esta impugnación jurídico sustantiva", esto es, no sería necesario realizar el test de proporcionalidad, pese a lo cual, "y, como corolario de ello, de la de naturaleza fáctica a ella subordinada, la Sala comparte plenamente la valoración judicial en cuanto a la idoneidad, necesidad y proporcionalidad de la medida de vigilancia y control instaurada por la empresa".

[44] *Vid,* un completo comentario a la sentencia en el blog de EDUARDO ROJO TORRECILLA, "No ha desaparecido el derecho a la privacidad del trabajador en la empresa, pero sí ha sido limitado (de momento). Una nota crítica a la sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero (caso Barbulescu v. Rumania) (I) y (II)" entradas del 18 de enero de 2016, disponible en *http://www.eduardorojotorrecilla.es/2016/01/no-ha-desaparecido-el-derecho-la.html* (última consulta 28 de marzo de 2016). *Vid,* también CARRILLO LÓPEZ, M., "El uso de internet en la empresa…",.cit.

[45] El Tribunal no aplicó la doctrina sentada en los asuntos Copland y Halford, por considerar que no son casos comparables, ya que en estas últimas el trabajador no había sido previamente informado.

[46] La sentencia tenía un voto particular parcialmente disidente, del magistrado portugués Paulo Pinto de Alburquerque En la misma línea que el voto particular, estima CARRILLO LÓPEZ, M., que la medida no fue proporcionada, ya que la empresa disponía de medios técnicos para comprobar el carácter personal de los correos enviados, sin necesidad de adentrarse en los contenidos, pudiendo haberse limitado a identificar a los destinatarios. CARRILLO LÓPEZ, M., "El uso de internet en la empresa…", cit, p.6.

[47] La sentencia del caso Barbulescu ha sido aplicada en un caso similar por las SSTSJ Madrid de 6 de mayo de 2016 (Rec. 187/2016) y 15 de julio de 2016 (Rec. 399/2016). De esta doctrina del TEDH se hizo también eco la STC 39/2016, de 3 de marzo de 2016 recaída en relación con el uso de cámaras de video vigilancia, manifestando que "esta facultad general de control prevista en la ley legitima el control empresarial del cumplimiento por los trabajadores de sus tareas profesionales (STC 170/2013, de 7 de octubre, y STEDH de 12 de enero de 2016, caso Barbulescu v. Rumania), sin perjuicio de que serán las circunstancias de cada caso las que finalmente determinen si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego ".

información, de modo que no es suficiente con que exista una prohibición del uso de las herramientas de la empresa, sino que es preciso, además, que el trabajador sea informado, con carácter previo a la monitorización, de la posibilidad de que sus comunicaciones van a ser supervisadas, así como de la naturaleza o el alcance de dicha supervisión y el grado de intrusión en la vida privada y la correspondencia[48]. Es decir, que lo que la STS de 6 de octubre de 2011 había considerado como meras "obligaciones complementarias de transparencia", integran el contenido esencial del deber de información y, por ende, del derecho fundamental a la intimidad y al secreto de las comunicaciones.

3. LA VALORACIÓN DE LA JURISPRUDENCIA LABORAL POR LA JURISDICCIÓN PENAL: LA STS DE 16 DE JUNIO DE 2014

La STS de 16 de junio de 2014 –Sala Segunda–[49] enjuició unos hechos de los que había tenido previamente conocimiento la jurisdicción social y que pasamos a referir: el trabajador de la empresa PARQUES REUNIDOS, S.A., fue despedido por el desvío de pagos a través de la manipulación y falsificación de facturas y por la anticipación de pagos a proveedores a cambio de comisiones ilícitas. Sostenía que la obtención de la prueba documental recogida de su puesto de trabajo, y la copia del disco duro de su ordenador, no se efectuó con todas las garantías, solicitando la nulidad de estos medios probatorios, al considerar vulnerado su derecho a la intimidad. En ningún momento se alegó vulneración del secreto de las comunicaciones. La STSJ Madrid de 13 de julio de 2009[50], aclarada por auto de 9 de septiembre de 2009, confirmó la procedencia del despido, rechazando la pretensión de nulidad de la prueba, con apoyo en la STS de 26 de septiembre de 2007. Recurrida en casación, el Auto de 7 de julio de 2010[51] denegó el recurso, ya que no apreció contradicción con la sentencia de referencia, pero explica que el fallo de esta última habría sido diferente si hubiera aplicado la STS 2007, que es la que –dice– contiene la doctrina del Tribunal Supremo sobre la cuestión, lo que no pudo hacer por razón de tiempo. En la vía penal, la empresa interpuso querella contra el trabajador quien fue condenado por el Tribunal de instancia, como autor de un delito continuado de falsedad documental en concurso medial con una estafa continuada. La sentencia fue recurrida en casación con apoyo en siete diferentes motivos. En lo que a este estudio interesa, el motivo Sexto alude a la vulneración del derecho a un proceso con garantías (art. 24.2 CE), por la forma en la que se obtuvo, sin intervención judicial, la información

[48] *Vid,* un comentario de la sentencia en PRECIADO DOMÈNECH, C.H., "Comentario de urgencia a la sentencia del TEDH de 5 de septiembre de 2017. Recuperando la dignidad en el trabajo", Blog de la Comisión de lo Social de Jueces y Juezas para la democracia, entrada del día 5 de septiembre de 2017.

[49] Rec.2229/2013. *Vid,* un comentario a la sentencia en MOLINA NAVARRETE, C., "Autotutela empresarial, secreto de comunicaciones y control judicial: la Sala Social pierde el paso con la Sala Penal", Revista de trabajo y seguridad social, nº.381, 2014, pp. 157-162.

[50] Rec.3247/2009.

[51] Rec. 265/2010.

contenida en el equipo informático utilizado por el recurrente para desempeñar sus tareas contables y la ausencia de garantías en la custodia del "disco duro" del mismo. Con base en la existencia de otras pruebas independientes de la memoria del ordenador y suficientes para sostener el "factum" y en la inexistencia de injerencia en el secreto de las comunicaciones del investigado, pues no constaba que se hubiera examinado ningún tipo de programa de correo electrónico privado, la Sala considera improcedentes o, en todo caso, irrelevantes, las alegaciones del recurso acerca de las dudas sobre la integridad y validez de la prueba informática. No obstante, a continuación y *obiter dicta,* el Tribunal Supremo estima conveniente, en aras a fijar una clara doctrina en materia de tanta trascendencia, salir al paso de ciertas afirmaciones rotundas, incluidas en la propia resolución de instancia, tales como las de que "...el ordenador registrado era una herramienta propiedad de la empresa y facilitada por la empresa a don (sic) Rodolfo exclusivamente para desarrollar su trabajo, por lo que entendemos que incluso en aquel supuesto en que pudiera utilizar el ordenador para emitir algún tipo de mensaje de carácter personal, entendemos que al utilizar precisamente un ordenador ajeno, de la empresa, y destinado exclusivamente para el trabajo a la empresa, estaba asumiendo –cediendo– la falta de confidencialidad –secreto– de las comunicaciones que pudiera tener el señor (sic) Rodolfo utilizando tal terminal informático". Estos argumentos, señala la sentencia del Tribunal Supremo, son los utilizados en el ámbito jurisdiccional de lo social, a partir de la importante sentencia de 26 de Septiembre de 2007, luego seguida y ampliada en sus efectos por otras de la misma Sala Cuarta de este mismo Tribunal, como las de 8 de Marzo y 6 de Octubre de 2011, e incluso la de 7 de Julio de 2010, referida precisamente a estos mismos hechos, aun cuando en su dimensión laboral a la hora de valorar la prueba informática y sus efectos para acreditar la procedencia del despido acordado respecto del recurrente por la empresa PARQUES REUNIDOS S.A. Estos criterios contenidos en dichas sentencias y que la Sala admite no desconocer que han sido posteriormente avalados por el propio Tribunal Constitucional, han de quedar restringidos, a su juicio, al ámbito de la Jurisdicción laboral, ante el que obviamente su actitud no puede ser otra más que la de un absoluto respeto, máxime cuando cuentan con la confirmación constitucional, pero que, en modo alguno, procede que se extiendan al enjuiciamiento penal, por mucho que en éste la gravedad de los hechos que son su objeto supere la de las infracciones laborales a partir de las que, ante su posible existencia, se justifica la injerencia en el derecho al secreto de las comunicaciones del sospechoso de cometerlas[52]. Los argumentos en los que apoya esta conclusión son los siguientes:

[52] GARCÍA-PERROTE ESCARTÍN, I., considera que aunque el pronunciamiento se limita al procedimiento penal, no parece razonable que una prueba sí valga (sea legal) en el orden social y no valga (sea ilegal) en el orden penal. *Vid,* "Control empresarial de la prestación de servicios y su utilización como prueba, en especial del uso por los trabajadores de los medios informáticos", Ponencia expuesta por D. Ignacio García Perrote Escartín, durante la Jornada Formativa "Actualidad Laboral" realizada el 6 de Mayo en el Salón de Actos del Ilustre Colegio de Abogados de Baleares. Disponible en *http://www.elaboralista.com/noticia/control-empresarial-de-la-prestacion-de-servicios-y-su-utilizacion-como-prueba-en-especial-del-uso-por-los-trabajadores-de-los-medios-informaticos/* martes 17 de mayo de 2016 (última consulta 3 de enero de 2017).

1º. El art. 18.3 CE es claro y tajante cuando afirma categóricamente que "se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial". Es decir que no contempla, ninguna posibilidad ni supuesto, "ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado (correo corporativo), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia".

2º. El art. 18.3 CE no admite una supuesta "tácita renuncia" al derecho que pudiera convalidar la ausencia de intervención judicial, por un lado porque obviamente dicha "renuncia" a la confidencialidad, o secreto de la comunicación, no se produce ni es querida por el comunicante que, de conocer sus consecuencias, resulta difícil imaginar que lleve a cabo la comunicación objeto de intervención y, de otra parte, porque ni aun cuando se entienda que la "renuncia-autorización" se haya producido, resultaría operativa ya que, a diferencia de lo que ocurre con la protección del derecho a la inviolabilidad domiciliaria (art. 18.2 CE), nuestra Constitución no prevé, por la lógica imposibilidad para ello, la autorización del propio interesado como argumento habilitante para la injerencia.

3º. Un régimen de protección tan estricto, en relación con el derecho al secreto de las comunicaciones, "sin duda el más enérgico de los que dentro del genérico derecho a la intimidad se contemplan en el repetido artículo 18 de la Constitución Española al excluir cualquier posible supuesto que no contemple la intervención del Juez como tutelador del derecho del investigado, encuentra un lógico fundamento en la gravedad y trascendencia de esta clase de injerencias, en tanto que se introducen y revelan toda clase de aspectos referentes a la privacidad del comunicante, tanto los de interés para la investigación como otros por completo ajenos a ese legítimo interés". En definitiva, lo que hace la Sala segunda es recordar que "los principios y garantías que caracterizan al proceso penal exigen la aplicación de criterios más rigurosos y estrictos para poder justificar la injerencia en el derecho al secreto de las comunicaciones de los imputados, y evitar una vulneración de los derechos que el imputado tiene reconocidos en el proceso penal[53]".

4º. Llama la atención sobre la existencia de un tercero ajeno a la empresa, que, como interlocutor en el proceso de comunicación, ve vulnerado su derecho al secreto de las comunicaciones[54].

---

[53] SÁNCHEZ, J.D y GARCÍA BEL, M., "El poder de control del empresario sobre el correo electrónico de sus trabajadores…", cit.

[54] La STS de 4 de diciembre de 2015 –Sala Segunda– (Rec. 10447/2015) llama la atención sobre algún posible destinatario de la comunicación que todavía no hubiera conocido el contenido del correo. En el caso concreto, concluye que no se produjo intromisión en el secreto de las comunicaciones, tras afirmar que "ningún proceso de comunicación fue interceptado. No existe constancia de que la Policía llegara a apoderarse de información vinculada a procesos de comunicación en marcha. Ni siquiera llegó a disponer de contenidos procedentes de comunicaciones ya concluidas, pero todavía desconocidas por alguno de sus destinatarios".

5º. Las anteriores afirmaciones no llevan a la Sala Segunda a impedir la utilización de estos medios de investigación, pero considera que deben cumplir con las previsiones constitucionales rectoras de un procedimiento tan invasivo en derecho de semejante trascendencia para los ciudadanos, resultando, a tal efecto, imprescindible, la autorización y el control que sólo el Juez puede dispensar en nuestro ordenamiento, incluso según la legislación laboral, que al menos aparentemente sigue el mismo criterio de clara vocación judicial, encontrando apoyo para la solicitud de dicha autorización en el artículo 76.4, en relación con el 90.2 y 4 de la Ley 36/2011, de 10 de Octubre, Reguladora de la Jurisdicción social –LRJS–. Recordemos que también en el orden social, el Tribunal Supremo, en sentencia de 13 de mayo de 2014[55] –caso Supermercados Champion– en un supuesto de fiscalización mediante sistemas de video vigilancia, había advertido de "las posibilidades de intervención judicial" a instancia de cualquiera de las partes que proporciona la nueva ley rituaria laboral, en orden a evitar posibles vulneraciones de derechos fundamentales, tanto en la fase de actos preparatorios y diligencias preliminares (art.76.4), como en la fase del juicio, incluso como prueba anticipada (art. 90.4). Obsérvese que la intervención del juez no estaba contemplada en la anterior Ley de Procedimiento Laboral, vigente en el momento de enjuiciar los casos que abordaron las sentencias del Tribunal Supremo y del Tribunal Constitucional. El silencio de la ley rituaria laboral condujo, por ejemplo, a la STSJ Andalucía de 9 de mayo de 2003[56] a afirmar que cuando la monitorización podía considerarse que vulneraba el derecho al secreto de las comunicaciones, el empresario no estaba facultado para la intromisión "sino sólo legitimado, si es perjudicado por conductas graves del trabajador, de relevancia penal, para su denuncia, siendo el proceso penal el marco adecuado para que se dicte resolución judicial motivada que permita la investigación del correo electrónico". La Sala de lo Penal remite ahora al proceso laboral para la solicitud de la autorización judicial.

Un sector de la doctrina laboralista ha puesto de relieve la novedad que supone la regulación sobre práctica de la prueba contenida en la LRJS en la materia que nos ocupa, de forma que el empresario sí debería solicitar autorización judicial en aquellos casos en los que conforme a la jurisprudencia del Tribunal Supremo y del Tribunal Constitucional el trabajador tuviera la "expectativa razonable de confidencialidad" [57], aunque lo cierto es que los nuevos preceptos suscitan serias dudas sobre su ámbito[58]. Otros autores rechazan que la solución venga de la mano de exigir au-

---

[55] Rec. 1685/2013.

[56] Rec. 591/2003.

[57] De esta opinión es CASTRO ARGÜELLES, M.A., "Los derechos fundamentales inespecíficos en el proceso laboral", en AA.VV., *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social,* cit., pp. 195-196; ABERASTURI GORRIÑO, U., "Control empresarial del correo electrónico del empleado y relevancia de la información previa…", cit., pp.13-14 pdf; PÉREZ DE LOS COBOS ORIHUEL, F., "Nuevas tecnologías y relaciones laborales", cit., pp. 351-354; TOSCANI GIMÉNEZ, D., "La vulneración del derecho a la intimidad por delatadores, detectives privados y medios tecnológicos", Revista de Derecho Social, nº 71, 2015, pág. 76.

[58] PÉREZ DE LOS COBOS ORIHUEL, F., "Nuevas tecnologías y relaciones laborales", cit., pp.351-352.

torización judicial y confían "en la especificidad de las soluciones laborales frente al tratamiento indiferenciado". Matizan, sin embargo, que si el poder de policía privada, a diferencia de la policía pública, no precisa autorización judicial "parece claro que el trabajador también requiere de tutela especial", razón por la cual, es razonable que la política empresarial sea realmente transparente y que la finalidad de control prime sobre la facilitación de la consecución de unas pruebas que aseguren al empresario el éxito en un posterior proceso sancionador. "De ahí la necesidad de una información específica, bien al trabajador y a los representantes laborales, bien solamente a estos"[59].

6º. Finalmente, la Sala afirma que la exigencia de autorización judicial operará tan sólo respecto a lo que estrictamente constituye ese "secreto de las comunicaciones", es decir, con exclusión de los denominados "datos de tráfico" –que el TEDH sí había incluido– o incluso de la posible utilización del equipo informático para acceder a otros servicios de la red como páginas web, etc., de los mensajes que, una vez recibidos y abiertos por su destinatario, no forman ya parte de la comunicación protección y conservación de datos (art. 18.4 CE) o a la intimidad documental en sentido genérico y sin la exigencia absoluta de la intervención judicial (art. 18.1 CE). Es decir, la apertura de correos que estuvieran en la bandeja de entrada, pero aun no hubiera sido leídos, exigiría autorización judicial, no así si habían sido leídos ya por su destinatario. Dos sentencias posteriores de la Sala Segunda del Tribunal Supremo, aplican los mismos criterios para deslindar las fronteras entre el derecho a la intimidad y el derecho al secreto de las comunicaciones. Nos referimos a las SSTS de 10 de diciembre de 2015[60] y a la STS de 26 de noviembre de 2014[61] En la primera de ellas se enjuició la licitud del acceso a la cuenta abierta por una menor en una red social por parte de su madre sin contar con su anuencia, ante la sospecha de que pudiera estar siendo víctima de un delito. La Sala, partiendo de que la menor era titular del derecho a la intimidad, concluye que no había ilicitud probatoria, siendo necesario precisar "que no estamos ante una incidencia en el derecho al secreto de las comunicaciones, sino ante una cuestión de intimidad. El derecho al secreto de las comunicaciones rige mientras se desarrolla el proceso de comunicación (…) Una vez cesado éste, llegado el mensaje al receptor, salimos del ámbito del art. 18.3 CE, sin perjuicio, en su caso, del derecho a la intimidad proclamado en el número 1 del mismo precepto, aunque en este segundo supuesto sin supeditación constitucional imperativa a la autorización judicial." En la segunda, se enjuiciaba un caso de inducción a la prostitución de una menor a cambio del suministro de drogas. Tras la muer-

[59] MOLINA NAVARRETE, C., "Expectativa razonable de privacidad y poder de vigilancia empresarial: ¿*Quo vadi*s justicia laboral? Comentario a la Sentencia del TEDH de 12 de enero de 2016, asunto Barbulescu c. Rumanía, demanda núm. 61496/2008*", Revista de Trabajo y Seguridad social*, nº. 399, 2016, p. 180. La opinión del autor, en cierto modo entronca con la de CASTRO ARGÜELLES Y ABERASTURI GORRIÑO (*supra* nota 38) ya que ambos autores para apreciar que no existe expectativa de intimidad exigen que la información al trabajador incluya no sólo la prohibición de uso, sino la advertencia sobre la posibilidad de control y el alcance del mismo.

[60] Rec. 912/2015.

[61] Rec.10269/2014.

te de la joven los padres extrajeron los mensajes de SMS recibidos por ésta en su terminal telefónico, sin autorización judicial, siendo a través de estos SMS como se obtuvo el número de teléfono del recurrente que fue intervenido con autorización judicial. Al margen de otras consideraciones, la Sala estima que no puede considerarse que los SMS aportados por los padres constituyan una prueba ilícita. "Las copias de los mensajes recibidos y transmitidos por la menor, que pueden ser borrados del terminal una vez leídos pero fueron guardados, equivalen a la correspondencia que pueda ser conservada por la menor entre sus papeles privados. Están obviamente amparados por su derecho constitucional a la intimidad, pero una vez fallecida no son inmunes al acceso por parte de sus herederos legítimos, que conforme a lo dispuesto en el art 661 del Código Civil suceden al fallecido, por el solo hecho de su muerte, en todos sus derechos y obligaciones"[62].

La jurisdicción social ya ha tenido ocasión de pronunciarse sobre el alcance de la STS de 16 de junio de 2014. La STSJ Madrid de 6 de mayo de 2016[63] ha considerado que dicho pronunciamiento se refiere exclusivamente al procedimiento penal y que la misma sentencia no descarta que en el ámbito laboral pueda resultar lícito y legítimo el control empresarial sin necesidad de autorización judicial[64]. Nuevamente, tenemos que decir que en el caso enjuiciado por el TSJ Madrid no se interfirió en un proceso de comunicación en curso, por lo que, de acuerdo con lo señalado por la Sala Segunda, no habría problema en admitir la prueba informática.

Pese a la preocupación que pudiera existir en el ámbito empresarial, lo cierto es que la Sala segunda no entra a valorar si la monitorización del correo electrónico podría ser constitutiva del delito tipificado en el artículo 197.1 del Código Penal. Creemos que en los casos analizados en las sentencias recaídas en la jurisdicción social, parece faltar el elemento subjetivo de los delitos, en la medida en que el empresario no realiza la monitorización "para" vulnerar la intimidad de otro. La Sala de lo Penal del Tribunal Supremo ya tuvo ocasión de pronunciarse sobre la existencia de un delito de descubrimiento y revelación de secretos, como consecuencia de la monitorización del ordenador de un empleado. En sentencia de 30 abril 2007[65] se absolvió a un alcalde y a dos ediles que accedieron al programa de correo electrónico instalado en el ordenador asignado a un funcionario. El Tribunal de instancia había negado el carácter típico de la conducta fundamentalmente sobre la base de la ausencia del elemento subjetivo. La Sala segunda del Tribunal Supremo entendió que tampoco concurría el elemento objetivo en su integridad: en primer lugar, porque el ordenador de trabajo, de titularidad pública, no "era el lugar idóneo para el archivo o alma-

---

[62] En el mismo sentido, SSTS de la Sala Segunda, de STS de 24 de febrero de 2015 (Rec. 1774/2014) y de 4 de diciembre de 2015 (Rec. 10447/2015).

[63] Rec. 187/2016.

[64] La empresa demandada interpuso una querella criminal frente al actor imputándole los delitos de estafa, corrupción entre particular, y la falsedad documental. Por tales hechos y tras admitirse la demanda se siguen diligencias previas por el Juzgado de Instrucción 50 de Madrid. Este caso nos dará la oportunidad de comprobar si el juez admite en el proceso penal la prueba aportada al juicio laboral.

[65] Rec. 1805/2006.

cenamiento de datos relativos a la intimidad personal del querellante"; en segundo lugar, porque al ordenador tenían acceso otras dos personas además del funcionario afectado, quienes conocían la clave de acceso por él empleada. Ciertamente la STS de 2014 no parece haber seguido esta senda.

4. CONCLUSIONES FINALES: VÍAS DE ENCUENTRO ENTRE AMBAS JURISDICCIONES

El examen de las sentencias recaídas en la jurisdicción social revela que, en definitiva, las cuestiones enjuiciadas no afectaban al secreto de las comunicaciones en los términos restringidos en que ha sido interpretado por la Sala Segunda del Tribunal Supremo en sentencia de 16 de junio de 2014. Ésta limita el proceso de comunicación a los correos que han sido enviados, pero todavía no han sido leídos por sus destinatarios, dejando al margen los correos electrónicos que se encuentran en la bandeja de entrada como leídos, la navegación por internet o los datos de tráfico. Hemos destacado varias sentencias del orden social que valoran que la monitorización no incluyera el correo electrónico ni las comunicaciones enviadas o recibidas por medio del ordenador, lo que evidencia que realmente se estaban enjuiciando casos que afectaban al derecho a la intimidad, no al secreto de las comunicaciones. La propia STC 170/2013 destaca que la monitorización se realizó cuando el proceso de comunicación podía entenderse ya finalizado, por lo que la medida de control no había supuesto una interceptación o conocimiento antijurídico de comunicaciones ajenas realizadas en canal cerrado.

Como puede observarse, la jurisdicción social destaca de forma especial un aspecto del ámbito de protección del secreto de las comunicaciones: la existencia de un "canal cerrado" de comunicación. En este sentido, la información que está obligado a aportar el empresario accede a un primer plano y se convierte en elemento central no sólo para valorar si ha resultado afectado el secreto de las comunicaciones, sino también el derecho a la intimidad. La ausencia de información provoca que el trabajador tenga una "expectativa razonable de intimidad" y que la comunicación se considere realizada en un "canal cerrado" protegido por el secreto de las comunicaciones.

Así pues, creemos que también en el orden social sería exigible la autorización judicial en los siguientes casos: cuando se interceptan correos en curso, cuando no exista la prohibición de uso del correo corporativo para fines particulares y cuando la monitorización se realiza sobre una cuenta particular del trabajador.

5. BIBLIOGRAFÍA

ABERASTURI GORRIÑO, U., "Control empresarial del correo electrónico del empleado y relevancia de la información previa a los trabajadores como garantía mínima para ejercer ese control, a la luz de la STC 7 de octubre de 2013", Revista española de Derecho del Trabajo, nº. 180, 2015 (formato electrónico)

ABRIL, P. y PIZARRO MORENO, E., "La intimidad europea frente a la privacidad americana", InDret, Revista para el análisis del Derecho, nº. 1, 2014, disponible en *WWW.INDRET.COM*.

ARBONÉS LA PENA, H.I., "Grabación de imagen o sonido y control del correo electrónico por el empresario", Nueva Revista española de Derecho del Trabajo, nº 178, 2015.

BELTRÁN DE HEREDIA RUIZ, I., "Facultad de control empresarial y el derecho a la libertad informática de los trabajadores: un derecho fundamental (inexplicablemente) olvidado", en, AA.VV., Internet, *Derecho y Política. Una década de transformaciones,* editorial Huygens, 2014.

CARDONA RUBERT, M.B., "Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales, un paso atrás. Comentario a la STC 241/2012, de 17 de septiembre", Revista de Derecho Social, nº. 60, 2012.

CARRASCO DURÁN, M., "El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería de la empresa", Revista Aranzadi Doctrinal, nº 9, 2014 (formato electrónico)

CARRILLO LÓPEZ, M., "El uso de internet en la empresa: a propósito de la STEDH de 13 de enero de 2016, caso Barbulescu C/ Rumanía", IUSLabor, nº. 1, 2016 (disponible en *https://www.upf.edu/iuslabor/_pdf/2016-1/Carillo.pdf*). Última consulta 23 de junio de 2016.

CASTRO ARGÜELLES, M.A., "Los derechos fundamentales inespecíficos en el proceso laboral", en AA.VV., *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social*, XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Ediciones Cinca, 2014.

DE LA QUADRA SALCEDO JANINI y SUÁREZ CORUJO, B., "¿Trabajadores incomunicados? La deriva de la doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones", Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, publicada en la obra colectiva *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social,* Ediciones Cinca, 2014.

PRECIADO DOMÈNECH, C.H., "Comentario de urgencia a la sentencia del TEDH de 5 de septiembre de 2017. Recuperando la dignidad en el trabajo", Blog de la Comisión de lo Social de Jueces y Juezas para la democracia, entrada del día 5 de septiembre de 2017.

FERNÁNDEZ RODRÍGUEZ, J.J., *Secreto e intervención de las comunicaciones en Internet,* Civitas, Madrid, 2004.

GARCÍA-PERROTE ESCARTÍN, I., "Control empresarial de la prestación de servicios y su utilización como prueba, en especial del uso por los trabajadores de los medios informáticos", Ponencia expuesta por D. Ignacio García Perrote Escartín, durante la Jornada Formativa "Actualidad Laboral" realizada el 6 de Mayo en el Salón de Actos del Ilustre Colegio de Abogados de Baleares. Disponible en *http://*

www.elaboralista.com/noticia/control-empresarial-de-la-prestacion-de-servicios-y-su-utilizacion-como-prueba-en-especial-del-uso-por-los-trabajadores-de-los-medios-informaticos/ martes 17 de mayo de 2016.

HERREROS LÓPEZ, J.M., "Las tecnologías de la información y comunicación de la empresa al servicio de la libertad sindical", en AA.VV (Monterroso Casado, E., dir.), *Responsabilidad empresarial,* Tirant lo Blanch, Valencia, 2016.

MARIN ALONSO, I., "El uso por los trabajadores de las comunicaciones electrónicas en la empresa: ¿se encuentran protegidas por el derecho al secreto de las comunicaciones?", Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, publicada en la obra colectiva *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social*, editorial Cinca, 2014.

MARTÍN VALVERDE, "Uso extralaboral del correo electrónico empleando medios informáticos de la empresa. Control empresarial: requisitos", Actualidad Laboral, nº 2, 2014, (formato electrónico).

MOLINA NAVARRETE, C., "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", Revista de Trabajo y Seguridad social, nº. 399, 2016.

— "Autotutela empresarial, secreto de comunicaciones y control judicial: la Sala Social pierde el paso con la Sala Penal (Comentario a la Sentencia del Tribunal Supremo, Sala 2.ª, de 16 de junio de 2014, rec. núm. 2229/2013)", Revista de Trabajo y Seguridad social*,* nº.381, 2014.

MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B.M., "El control empresarial del correo electrónico tras la STC 170/2013", Revista Doctrinal Aranzadi Social, nº. 11, 2014, versión digital (BIB 2014\122).

PÉREZ DE LOS COBOS ORIHUEL, F., "Nuevas tecnologías y relaciones laborales", en AA.VV (Teruel Lozano, G.M., Pérez Miras, A., Carlo Rafficta, E. dir.), *Desafíos para los derechos de la persona ante el siglo XXI: Internet y nuevas tecnologías,* Aranzadi, 2013.

RODRÍGUEZ CARDO, I.A., "Política empresarial previa y supresión de la expectativa de privacidad: una reflexión crítica sobre las facultades de control del ordenador utilizado por el trabajador", Temas Laborales*,* nº. 126, 2014.

RODRÍGUEZ ESCANCIANO, S., *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores,* Tirant monografías, núm. 1003, Valencia, 2015.

RODRÍGUEZ LAÍNZ, J.L., "En torno al concepto de comunicación protegida por el artículo 18.3 de la Constitución", Diario La Ley*,* sección Doctrina 5, nº. 8142, 2013.

ROJO TORRECILLA, E., "No ha desaparecido el derecho a la privacidad del trabajador en la empresa, pero sí ha sido limitado (de momento). Una nota crítica a la sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero (caso Barbulescu

v. Rumania) (I) y (II) entradas del 18 de enero de 2016 *http://www.eduardorojo-torrecilla.es/2016/01/no-ha-desaparecido-el-derecho-la.html* (última consulta 28 de marzo de 2016).

SEMPERE NAVARRO, A.V. SAN MARTÍN MAZZUCCONI, C., *Nuevas tecnologías y relaciones laborales,* Aranzadi, Cizur Menor, 2002.

SEPÚLVEDA GÓMEZ, M., "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites", Temas Laborales, nº. 122, 2013.

TOSCANI GIMÉNEZ, D., "La vulneración del derecho a la intimidad por delatadores, detectives privados y medios tecnológicos", Revista de Derecho Social, nº 71, 2015.