EL CONTROL EMPRESARIAL DEL CORREO ELECTRÓNICO DEL TRABAJADOR

JOSÉ LUIS MONEREO PÉREZ
Catedrático de Derecho del Trabajo y de la Seguridad Social
Presidente de la Asociación Española de Salud y Seguridad Social (AESSS)
Universidad de Granada

POMPEYO GABRIEL ORTEGA LOZANO
Profesor Ayudante Doctor de Derecho del Trabajo y de la Seguridad Social
Universidad de Granada

"El interés por la libertad y la independencia sólo son concebibles en un ser que aún conserva la esperanza"
Albert Camus*

EXTRACTO **Palabras Clave:** Correo electrónico, control, monitorización, comunicaciones, videovigilancia

En este texto se estudia profundamente la doctrina jurisprudencial del control o monitorización del correo electrónico del trabajador por parte del empresario lo que plantea una fuerte tensión dialéctica entre varios derechos que disfrutan de dimensión constitucional. Es evidente que en este complejo tema se suscitan multitud de cuestiones conflictivas respecto al alcance y prevalencia de cada uno de los derechos, centrándonos en la parte práctica y la solución de casos conflictivos que han establecido criterios jurisprudenciales.

ABSTRACT **Key Words:** Email, control, monitoring, communications, video monitoring

This text studies deeply the jurisprudential doctrine of the control or monitoring of the email of the employee on the part of the employer, what presents a hard tension between several rights that have of constitutional dimension. It is evident that this complex issue causes multitude of conflictive questions about the scope and prevalence of each one of the rights, focussing on the practical part and the solution of problematic cases that have established jurisprudential criteria.

* CAMUS, A., *La mort heureuse,* París, Gallimard, Folio, 2010, pág. 38.

 Recepción de original: 20.09.2019. Aceptación: 22.10.2019

ÍNDICE

1. INTRODUCCIÓN

En el control del correo electrónico institucional del trabajador por parte del empresario se plantea una fuerte tensión dialéctica entre varios derechos que disfrutan de dimensión constitucional: por un lado, la propiedad privada y la tutela del patrimonio empresarial (art. 38 CE); y, por otro, los derechos fundamentales a la intimidad (art. 18.1 CE), al secreto de las comunicaciones (art. 18.3 CE) y a la libertad de expresión (art. 20.1 CE). Es evidente que en este complejo tema se suscitan multitud de cuestiones conflictivas respecto al alcance y prevalencia de cada uno de los derechos, centrándonos, en este texto, en la parte práctica y la solución de casos conflictivos que han sentado jurisprudencia. Pautas jurisprudenciales que vienen siendo aplicada, en mayor o menor medida, con interpretaciones diversas por los tribunales ordinarios españoles.

2. LA JURISPRUDENCIA DEL TEDH: CASO BARBULESCU II, CASO LÓPEZ RIBALDA Y CASO LIBERT

2.1. Sentencia del TEDH 5 de septiembre de 2017: Caso Barbulescu II contra Rumania

Es la Gran Sala del TEDH, en fecha de 5 de septiembre de 2017, cuando falla en el asunto *Barbulescu II*[1]. Anteriormente la Sección Cuarta del TEDH había dic-

[1] TEDH 5 de septiembre de 2017, Caso Barbulescu contra Rumania [TEDH\2017\61].

tado sentencia de fecha 12 de enero de 2016 declarando que no se había producido violación del art. 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950. Es por ello que, ante esta resolución negativa para el trabajador, el reclamante solicitó que el supuesto fuera remitido a la Gran Sala, lo que fue admitido y dio lugar a la citada sentencia que, como ya adelantamos, declaraba la vulneración de dicho precepto. De manera resumida, el TEDH condena que un empresario o superior controle y espíe el email del trabajador sin previo aviso: el empresario vulnera el derecho a la intimidad y al secreto de las comunicaciones al vigilar los mensajes enviados y recibidos en el correo del empleado cuando no ha sido previamente informado de esta posibilidad, aun cuando existan normas específicas en la empresa que prohíban su utilización con fines personales.

Esta sentencia versa sobre un ingeniero de ventas que trabaja para una empresa privada que, a petición de su empresario, creó una cuenta *Yahoo Messenger* –servicio de mensajería en línea que ofrece una trasmisión de texto en tiempo real en internet– con el fin de recibir y responder a preguntas de los clientes.

Asimismo, la empresa distribuyó a todos los empleados una nota informativa que decía: "*el tiempo que se pasa en la empresa debe ser tiempo de calidad para todo el mundo. Acudid al trabajo para ocuparos de los problemas de la empresa y profesionales, y no de los problemas privados. No paséis el tiempo en internet, hablando por teléfono o haciendo fotocopias de cuestiones que no competen a vuestro trabajo ni vuestras funciones. La empresa se ve en la obligación de verificar y vigilar el trabajo de los empleados y de tomar las medidas oportunas contra los trabajadores en falta*".

Igualmente, en la propia empresa existían estrictas reglas de uso de los ordenadores y medios informáticos que prohibían su utilización para fines personales de los trabajadores. Sin embargo, no se hacía referencia a la posibilidad de poder vigilar las comunicaciones de sus empleados. No obstante, posteriormente, la empresa decide despedir al ingeniero tras monitorizar el ordenador del trabajador y comprobar que mantenía conversaciones privadas en horario laboral. Por ello el empleado presenta demanda solicitando, entre otras cosas, la anulación de la decisión del despido. Sin embargo, el Tribunal del Condado de Bucarest desestima la queja del trabajador confirmando la legalidad de la decisión del despido. Posteriormente, el demandante interpone recurso contra esta sentencia ante el Tribunal de Apelación de Bucarest, el cual decide desestimar el recurso al considerar que "*internet es un instrumento que el empleador pone a disposición del empleado para su utilización con fines profesionales y que el empleador está en su derecho de establecer las reglas de utilización de dicho instrumento*".

Frente a tal decisión, se acude al Tribunal Europeo de Derechos Humanos (en adelante, TEDH) por considerar el demandante que ha existido violación del secreto de las comunicaciones en el despido por la utilización de mensajería ins-

tantánea para uso personal en el centro de trabajo. En efecto, el trabajador sostiene que la decisión de su empresa de despedirle se tomó basándose en una vulneración de su derecho al respeto de la vida privada y la correspondencia, y los tribunales nacionales no protegieron ese derecho.

Al respecto, para el TEDH sí existe violación del derecho a la intimidad. En estas circunstancias, parece que los órganos jurisdiccionales nacionales no consiguieron, por un lado, comprobar, concretamente, si el empleador había notificado previamente al demandante la posibilidad de que sus comunicaciones en *Yahoo Messenger* iban a ser controladas y, por otro, tener en cuenta que no se le había informado de la naturaleza y alcance de la vigilancia a que iba a ser sometido, así como del grado de intrusión en su vida privada y en su correspondencia. Por otra parte, no determinaron, en primer lugar, qué motivos concretos justificaban la introducción de las medidas de control, en segundo lugar, si el empresario pudo haber utilizado medidas menos intrusivas para la vida privada y la correspondencia del demandante y, en tercer lugar, si el acceso al contenido de las comunicaciones hubiera sido posible sin su conocimiento.

A la luz de todas las consideraciones anteriores, el TEDH considera que las autoridades nacionales no protegieron adecuadamente el derecho del trabajador respeto de su vida privada y su correspondencia y que, por lo tanto, no valoraron el justo equilibrio entre los intereses en juego. En consecuencia, para la Gran Sala (por nueve votos frente a seis) se había producido una violación de su derecho al respeto de la vida privada –derecho a la intimidad– y la correspondencia.

Para llegar a tal conclusión, el TEDH se sustenta en una serie de puntos relevantes que deben destacarse. El primero de ellos hace referencia a la aplicación del artículo 8 del Convenio de Roma referido al derecho al respeto a la vida privada y familiar. En este sentido, el tribunal considera útil recordar que la noción de "vida privada" es un concepto amplio que no se presta a una definición exhaustiva[2]. El artículo 8 del Convenio protege el enriquecimiento personal[3], ya sea en forma de desarrollo personal[4] o de autonomía personal, que refleja un importante principio subyacente en la interpretación de las garantías del propio artículo 8[5]. El tribunal reconoce que toda persona tiene derecho a una vida privada, lejos de la injerencia no deseada de otros[6]. También considera que sería demasiado restrictivo limitar la noción de "vida privada" a un "círculo íntimo" en el que cada uno pueda vivir su vida personal como quiera y excluir completamente al mundo exterior de este

[2] TEDH 27 de julio de 2004, Caso Sidabras y Dziautas contra Lituania [TEDH 2004\55].

[3] TEDH 17 de febrero de 2005, Caso K. A. y A. D. contra Bélgica [TEDH 2005\15].

[4] TEDH 11 de julio de 2002, Caso Christine Goodwin contra Reino Unido [JUR 2002\181176].

[5] TEDH 29 de abril de 2002, Caso Pretty contra Reino Unido [TEDH 2002\23].

[6] TEDH 24 de julio de 2003, Caso Smirnova contra Rusia [JUR 2003\162895].

círculo[7]. Así, el artículo 8 garantiza un derecho a la "vida privada" en sentido amplio, que incluye el derecho a realizar una "vida privada social", es decir, la posibilidad de que el individuo desarrolle su identidad social. A este respecto, el mencionado derecho consagra la posibilidad de comunicarse con otros para establecer y desarrollar relaciones con sus semejantes[8].

Igualmente, el concepto de "vida privada" puede incluir actividades profesionales[9] o actividades que tengan lugar en un contexto público[10]. Las restricciones establecidas en la vida laboral pueden incluirse en el artículo 8 cuando repercuten en la forma en que el individuo forja su identidad social a través del desarrollo de relaciones con otros. Cabe señalar, en este punto, que es en el marco de la vida laboral donde la mayoría de la gente tiene muchas, si no la mayoría, de las oportunidades para fortalecer sus lazos con el mundo exterior[11].

Así, al igual que ocurre con las llamadas telefónicas, misma doctrina se aplica a los correos electrónicos enviados desde el lugar de trabajo: también están amparados por la protección del artículo 8 del Convenio de Roma, al igual que la información recogida mediante el seguimiento del uso que hace una persona de internet[12]. Igualmente, de la jurisprudencia del tribunal se desprende que las comunicaciones que se emiten desde el puesto de trabajo, así como las del domicilio, pueden incluirse en las nociones de "vida privada" y de "correspondencia" a que se refiere el artículo 8 del Convenio de Roma[13].

Aplicando estos principios, el tribunal no tiene más remedio que señalar, en primer lugar, que el tipo de mensajería instantánea en internet no es otra cosa que una forma de comunicación que forma parte del ejercicio de la intimidad social. Además, la noción de "correspondencia" se aplica al envío y recepción de mensajes, incluso desde el ordenador de la empresa empleadora. Sin embargo, el tribunal observa que el empleador esperaba que él y los otros empleados se abstuvieran de cualquier actividad personal en su lugar de trabajo. Este requisito del empleador incluía, de forma particular, la prohibición del uso de los recursos de la empresa para fines personales. Es para garantizar el cumplimiento de esta prohibición cuando la empresa decide establecer un sistema de control de la utilización de internet por sus empleados. A pesar de la prohibición de la empleadora, el trabajador intercambia comunicaciones de carácter personal con su novia y con

[7] TEDH 16 de diciembre de 1992, Caso Niemietz contra Alemania [TEDH 1992\77].

[8] TEDH 28 de mayo de 2009, Caso Bigaeva contra Grecia [TEDH 2009\61] y TEDH 19 de octubre de 2010, Caso Özpinar contra Turquía [TEDH 2010\103].

[9] TEDH 12 de junio de 2014, Caso Fernández Martínez contra España [TEDH 2014\35].

[10] TEDH 7 de febrero de 2012, Caso Von Hannover contra Alemania [TEDH 2012\10].

[11] TEDH 16 de diciembre de 1992, Caso Niemietz contra Alemania [TEDH 1992\77].

[12] TEDH 3 de abril de 2007, Caso Copland contra Reino Unido [TEDH 2007\23].

[13] TEDH 25 de junio de 1997, Caso Halford contra Reino Unido [TEDH 1997\37].

su hermano. De este contenido se desprende que el trabajador despedido había sido informado de la prohibición del uso de internet para fines personales establecida en las normas internas de la empresa empleadora. Sin embargo, no está tan claro que se le informara de que sus comunicaciones estaban siendo supervisadas antes de que se pusiera en marcha la actividad de vigilancia: por tanto, el TEDH parte de que el trabajador no fue informado con antelación del alcance y la naturaleza de la supervisión efectuada por su empleador o de la posibilidad de acceder al contenido de sus comunicaciones.

En suma, habida cuenta de todas estas consideraciones, para el TEHD las comunicaciones que el demandante realizó desde su lugar de trabajo estaban comprendidas en los conceptos de "vida privada" y "correspondencia". De ello se deduce que, dadas las circunstancias, el artículo 8 del Convenio es aplicable en el presente asunto.

Para resolver el caso planteado debe partirse de que el derecho laboral tiene características específicas que deben tenerse en cuenta. La relación entre una empresa y su empleado es una relación contractual, acompañada de derechos y obligaciones especiales, y caracterizada por una relación legal de subordinación. Se rige por su propio sistema jurídico, que es claramente distinto del sistema general de relaciones entre individuos[14]. Los tribunales nacionales deben velar porque el establecimiento por una empresa de medidas para vigilar la correspondencia y otras comunicaciones, sea cual sea su alcance y duración, vaya acompañado de garantías adecuadas y suficientes contra los abusos[15].

Para el tribunal, la proporcionalidad y las garantías procesales contra el carácter arbitrario son elementos esenciales. Por ello, y dado que la situación tecnológica está cambiando muy rápidamente, la Gran Sala considera que las autoridades nacionales deberían tener en cuenta los siguientes factores –denominado también como el *test Barbulescu*[16]–:

1. ¿El empleado ha sido informado de la posibilidad de que el empleador tome medidas para supervisar su correspondencia y otras comunicaciones, así como la aplicación de tales medidas? La comunicación de esta práctica debe ser, en principio, clara en cuanto a la naturaleza de la supervisión y antes del establecimiento de la misma.
2. ¿Cuál fue el alcance de la supervisión realizada del empleador y el grado de intrusión en la vida privada del empleado? A este respecto, debe ha-

[14] TEDH 12 de enero de 2017, Caso Saumier contra Francia [TEDH 2017\4].

[15] TEDH 4 de diciembre de 2015, Caso Roman Zakharov contra Rusia [JUR 2015\292490].

[16] Terradillo Ormaetxea, E., "El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional Español", en *Revista de Derecho Social*, núm. 80, 2017, pp. 139 y ss.

cerse una distinción entre el control del flujo de comunicaciones y el de su contenido. También se debería tener en cuenta si la supervisión de las comunicaciones se ha realizado sobre la totalidad o sólo una parte de ellas y si ha sido o no limitado en el tiempo y el número de personas que han tenido acceso a sus resultados.

3. ¿El empleador ha presentado argumentos legítimos para justificar la vigilancia de las comunicaciones y el acceso a su contenido? Dado que la vigilancia del contenido de las comunicaciones es por su naturaleza un método mucho más invasivo, requiere justificaciones más fundamentadas.
4. ¿Habría sido posible establecer un sistema de vigilancia basado en medios y medidas menos intrusivos que el acceso directo al contenido de comunicaciones del empleado? A este respecto, es necesario evaluar, en función de las circunstancias particulares de cada caso, si el objetivo perseguido por el empresario puede alcanzarse sin que éste tenga pleno y directo acceso al contenido de las comunicaciones del empleado.
5. ¿Cuáles fueron las consecuencias de la supervisión para el empleado afectado? ¿De qué modo utilizó el empresario los resultados de la medida de vigilancia, concretamente si los resultados se utilizaron para alcanzar el objetivo declarado de la medida?
6. ¿Al empleado se le ofrecieron garantías adecuadas, particularmente cuando las medidas de supervisión del empleador tenían carácter intrusivo? En particular, estas garantías debían impedir que el empleador tuviera acceso al contenido de las comunicaciones en cuestión sin que el empleado hubiera sido previamente notificado de tal eventualidad.

Para resolver el supuesto planteado el tribunal debe decidir el lado de la balanza que pesa más: por una parte, el derecho del trabajador al respeto de su vida privada y, por otro, el derecho de controlar y cumplir con las prerrogativas del empresario para garantizar el buen funcionamiento de la empresa. En suma, debe valorarse si la supervisión realizada por el empleador de las comunicaciones sobre las cuentas de *Yahoo Messenger* y el uso del contenido de estas comunicaciones en el contexto del procedimiento disciplinario en su contra, fueron o no lícitas.

De las pruebas aportadas se desprende que el trabajador había sido informado del reglamento interno de la empleadora que prohibía el uso de los recursos de la empresa para fines personales. Conocía el contenido de este documento y lo había firmado. Además, la empresa empleadora distribuyó una nota informativa entre todos los empleados, en la que recordaba la prohibición de uso de los recursos de la empresa para uso personal y precisó que una empleada había sido despedida por violar tal prohibición. Por último, el demandante fue citado dos veces por su empleador para explicar su uso personal de internet. Inicialmente, cuando le mostraron los gráficos que describían su tráfico de internet y el de sus colegas, afirmó

que había utilizado su cuenta de *Yahoo Messenger* sólo con fines profesionales. Después, cincuenta minutos más tarde, cuando se le presentó una transcripción de 45 páginas que contenían sus comunicaciones con su hermano y su novia, el trabajador informó a su empleador que éste era responsable de una infracción penal, a saber, la violación del secreto de la correspondencia.

El TEDH entiende que para ser considerada como previa, la advertencia del empleador debe darse antes de que comience la actividad de supervisión, y con mayor motivo, cuando la supervisión implica también el acceso al contenido de las comunicaciones de los empleados. Las normas internacionales y europeas van en esta dirección y exigen que la información se comunique al interesado antes de que sea objeto de control. En cuanto al alcance de la supervisión realizada y el grado de intrusión en la vida privada del demandante, el TEDH observa que esta cuestión no fue examinada por el Tribunal del Condado o el Tribunal de Apelación, mientras que parece que el empleador registró en tiempo real todas las comunicaciones hechas por el demandante durante el período de vigilancia, que tuvo acceso a ellas y que imprimió el contenido. Por otra parte, ni el Tribunal del Condado ni el Tribunal de Apelación examinaron suficientemente si el objetivo perseguido por el empleador podía haberse logrado mediante métodos menos intrusivos que el acceso al contenido mismo de las comunicaciones del demandante. Además, ninguno de los citados tribunales examinó la gravedad de las consecuencias de la medida de control y del procedimiento disciplinario que se siguió. A este respecto, el TEDH señala que el demandante había sido sometido a la medida disciplinaria más grave, a saber, el despido. Por último, el TEDH observa que los órganos jurisdiccionales nacionales no comprobaron si, cuando compareció el demandante para que explicara el uso que había hecho de los recursos de la empresa, el empresario había tenido ya acceso al contenido de las comunicaciones en cuestión. Observa que las autoridades nacionales no determinaron en qué momento del procedimiento disciplinario el empresario tuvo acceso a dicho contenido. Considera que admitir que el acceso al contenido de las comunicaciones pudo tener lugar en cualquier momento durante el procedimiento disciplinario, va en contra del principio de transparencia.

En estas circunstancias, parece que los órganos jurisdiccionales nacionales no consiguieron, por un lado, comprobar, concretamente, si el empleador había notificado previamente al demandante la posibilidad de que sus comunicaciones en *Yahoo Messenger* iban a ser controladas y, por otro, tener en cuenta que no se le había informado de la naturaleza y alcance de la vigilancia a que iba a ser sometido, así como del grado de intrusión en su vida privada y en su correspondencia. Por otra parte, no determinaron, en primer lugar, qué motivos concretos justificaban la introducción de las medidas de control, en segundo lugar, si el empresario pudo haber utilizado medidas menos intrusivas para la vida privada y la correspondencia del demandante y, en tercer lugar, si el acceso al contenido de las comunicaciones hubiera sido posible sin su conocimiento.

A la luz de todas las consideraciones anteriores, el TEDH considera que las autoridades nacionales no protegieron adecuadamente el derecho del trabajador respecto de su vida privada y su correspondencia y que, por lo tanto, no valoraron el justo equilibrio entre los intereses en juego. En consecuencia, para el TEDH se ha producido una violación del artículo 8 del Convenio de Roma.

2.2. Sentencia del TEDH 9 de enero de 2018: Caso López Ribalda y otros contra España

Relevante también es la reciente sentencia del TEDH (no de la Gran Sala), de fecha 9 de enero de 2018, en el asunto López Ribalda y otros contra España[17]. En este caso se trata la vulneración de la privacidad, no por control y monitorización del correo electrónico, sino por grabación con cámara oculta. En concreto, se avala por este tribunal la procedencia del despido por estimarse otras pruebas, pero se condena al Estado español a indemnizar a las cajeras que fueron despedidas por no haber sido previamente avisadas de la grabación de las cámaras ocultas, lo que puede transponerse también a los supuestos de control del correo electrónico (de ahí el interés en su análisis).

En el caso que se debate ahora debe analizarse si es lícita la vigilancia por vídeo en la cadena de supermercados donde trabajaban los empleados con la finalidad de investigar unos robos que habían venido produciéndose en el establecimiento. Concretamente el empresario instaló cámaras visibles y cámaras ocultas en cada caja. La empresa informó a sus trabajadoras sobre las primeras, pero no sobre las segundas.

Es por ello que las trabajadoras fueron grabadas robando junto a otros trabajadores y en connivencia con clientes. Además, los hechos fueron finalmente aceptados por las empleadas en una reunión privada con representante sindical, siendo despedidas por la empresa por razones disciplinarias.

Por otro lado, se llegó a un acuerdo entre las trabajadoras y el empresario en el que se reconocía, por parte de las trabajadoras, la participación en el robo y a no presentar demanda laboral y, por parte del empleador, a no iniciar un proceso penal contra ellas. Sin embargo, las trabajadoras impugnaron la legalidad del despido siendo considerados procedentes en primera instancia y en suplicación. Elemento fundamental de cara a su procedencia es que la prueba de vídeo fue aceptada como legalmente obtenida.

Ante los citados hechos, habiéndose declarado procedente el despido por el Juzgado de lo Social y, posteriormente, por el Tribunal Superior de Justicia, y previa inadmisión de los recursos interpuestos ante el Tribunal Supremo y el Tribunal

[17] TEDH 9 de enero de 2018, Caso López Ribalda y otros contra España [TEDH\2018\1].

Constitucional, las trabajadoras solicitan al TEDH que se declare la transgresión del artículo 8 –derecho al respeto de la vida privada– y artículo 6.1 –derecho a un proceso justo o equitativo– del Convenio Europeo de Derechos Humanos.

En efecto, las trabajadoras consideran que la toma de imágenes sin previa comunicación por las cámaras ocultas ha violado su derecho a la vida privada por lo que no pueden ser aceptadas como pruebas válidas. Sobre los acuerdos a los que habían llegado con la empresa en presencia del representante sindical, las trabajadoras consideran que no tendrían validez por haberse concluido bajo coacciones.

Al respecto de todo lo comentado, el Tribunal Europeo de Derechos Humanos considera que: 1) Se ha producido la vulneración del artículo 8 del Convenio –derecho al respeto de la vida privada–, en la medida en que de acuerdo con la legislación de protección de datos española se debía haber informado previamente de la colocación de todas las cámaras. 2) En cuanto al artículo 6.1 del Convenio –derecho a un juicio justo–, el tribunal declara que no ha habido vulneración ya que, por un lado, a las demandantes se les ha permitido cuestionar la autenticidad de las grabaciones durante el proceso judicial y, por otro, las decisiones judiciales no se basaron únicamente en dichas grabaciones sino también en las declaraciones testificales, por lo que se avala la procedencia del despido. Además, considera el tribunal que los acuerdos o los finiquitos no se suscribieron bajo amenazas o coacciones por parte del empleador.

Respecto a la aplicación de los principios del presente asunto debemos destacar los siguientes. Lo primero de todo, el TEDH observa que el empresario decidió instalar videovigilancia consistente en cámaras tanto visibles como ocultas. Los empleados solo tenían conocimiento de la existencia de las cámaras visibles que enfocaban las salidas del supermercado, y no fueron informados de la instalación de cámaras enfocadas a las cajas.

El TEDH señala en primer lugar que la videovigilancia encubierta se llevó a efecto después de que el supervisor de la tienda detectara pérdidas, y se plantearan fundadas sospechas de la comisión de robos por parte de las demandadas, así como por otros empleados y clientes. El tribunal también observa que los datos visuales obtenidos implican el almacenamiento y procesamiento de datos de carácter personal, estrechamente vinculados a la esfera privada de las personas. Este material fue tratado y examinado por varias personas que trabajaban para el empresario de las demandantes (entre otros, el representante sindical y el representante legal de la empresa) antes de que las propias demandantes fueran informadas de la existencia de las grabaciones de vídeo.

El TEDH toma nota asimismo que la legislación vigente en el momento en causa contenía disposiciones específicas sobre protección de datos de carácter personal. De hecho, al amparo del artículo 5 de la Ley de Protección de Datos de Carácter Personal, las demandantes tenían derecho a ser informadas "*previamente de modo expreso, preciso e inequívoco*" de "*la existencia de un fichero o*

tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y de la identidad y dirección del responsable del tratamiento, o en su caso, de su representante". Además, el Gobierno ha reconocido expresamente que las empleadas no fueron informadas de la instalación de las cámaras de vigilancia ocultas que enfocaban a sus cajas registradoras o de sus derechos al amparo de la Ley de Protección de Datos de Carácter Personal. Por tanto, la legislación en vigor en el momento de los hechos de la causa establecía claramente que todo recolector de datos debía informar a los sujetos de la recogida de datos, de la existencia de medios de recogida y tratamiento de sus datos de carácter personal.

En consecuencia, el TEDH no puede compartir la opinión de los tribunales nacionales sobre la proporcionalidad de las medidas adoptadas por el empresario con el objetivo legítimo de proteger el interés del empresario en la protección de sus derechos propietarios. El tribunal observa que la videovigilancia llevada a cabo por el empresario, que se prolongó durante un largo periodo de tiempo, no cumplía con los requisitos establecidos en el artículo 5 de la Ley de Protección de Datos de Carácter Personal y, en particular, con la obligación mencionada anteriormente de informar previamente a los interesados de modo expreso, preciso e inequívoco sobre la existencia y características particulares de un sistema de recogida de datos de carácter personal. El tribunal observa que los derechos del empresario podrían haber sido protegidos, por lo menos hasta cierto grado, por otros medios, en especial, informando previamente a las demandantes, incluso de una manera general, sobre la instalación de un sistema de videovigilancia y dotándolos de la información establecida en la Ley de Protección de Datos de Carácter Personal.

Considerando lo anterior, el TEDH concluye en el presente caso que los tribunales internos no ponderaron un justo equilibrio entre el derecho de las demandantes al respeto de su vida privada al amparo del artículo 8 del Convenio y el interés del empresario en la protección de sus derechos propietarios.

2.3. Sentencia del TEDH 22 de febrero de 2018: Caso Libert contra Francia

Debemos también hacer referencia a la sentencia del TEDH, de fecha 22 de febrero de 2018[18], en el asunto *Libert* contra Francia. Para el TEDH, el presente asunto difiere del caso *Barbulescu II* porque, en este último, la vulneración del ejercicio del derecho al respeto a la vida privada y a la correspondencia denunciada por

[18] TEDH 22 de febrero de 2018, Caso Libert contra Francia [TEDH\2018\35].

un empleado era el hecho de un empleador que provenía estrictamente del sector privado, y no de la autoridad pública, que es lo que se analiza en el asunto *Libert*.

De acuerdo con la doctrina del TEHD, la proporcionalidad y las garantías procesales contra el carácter arbitrario son esenciales. Siendo así, el TEDH declara que el derecho positivo francés contiene un dispositivo dirigido a la protección de la privacidad. El principio es que, si bien el empleador puede abrir los archivos profesionales almacenados en el disco duro de los ordenadores que pone a disposición de sus empleados para el desempeño de sus funciones, no puede, "*excepto riesgo o acontecimiento especial*", abrir archivos subrepticiamente identificados como personales. Únicamente podrá proceder a la apertura de los archivos identificados como personales en presencia de los empleados afectados o después de que hayan sido debidamente informados.

El tribunal observa que los tribunales nacionales franceses han aplicado este principio en el presente caso. Tanto el Tribunal de apelación de Amiens como el Tribunal de casación lo señalaron explícitamente, habiendo confirmado el Tribunal de casación concretamente que "*los archivos creados por el empleado con la ayuda de la herramienta informática puesta a su disposición por el empleador para el desempeño de su trabajo se suponen de carácter profesional, por lo que el empleador tiene derecho a abrirlos en su ausencia, excepto si están identificados como personales*". En las circunstancias del caso, este principio no era obstáculo para que su empleador abriera los archivos en causa, dado que estos no habían sido debidamente identificados como de carácter privado.

El TEDH recuerda en primer lugar que corresponde ante todo a las autoridades nacionales y en particular a los tribunales interpretar el derecho interno. A reserva de una interpretación arbitraria o manifiestamente irrazonable, su papel se limita a comprobar la compatibilidad con el Convenio de los efectos de parecida interpretación. Observa a continuación que el Tribunal de apelación de Amiens se basó en la constatación de que las fotografías y vídeos pornográficos en cuestión figuraban en un archivo denominado "*risas*" contenido en un disco duro llamado "*D:/datos personales*" y en la explicación de la SNCF según la cual la unidad "*D*" se denominaba por defecto "*D:/ datos*" y tradicionalmente servía para que los agentes almacenaran sus documentos profesionales. Posteriormente consideró que un empleado no podía utilizar la totalidad de un disco duro, pensado para registrar datos profesionales, para un uso privado y que "*en cualquier caso, el término genérico de "datos personales" podía referirse a los expedientes profesionales gestionados personalmente por el trabajador y no designaba de manera explícita los elementos relativos a su vida privada*". Más concretamente, el tribunal de apelación sostuvo que el término "*risas*" no confería necesariamente al archivo así designado un carácter necesariamente personal, pudiendo esta designación referirse a intercambios entre colegas de trabajo o a documentos de trabajo conservados como "*tonterías*" por el empleado. Asimismo, el tribunal de apelación consideró

pertinente el argumento de la SNCF según el cual el manual del usuario establece que "*las informaciones de carácter privado deben estar claramente identificadas como tales (opción "privado" en los criterios de Outlook)*" y que es lo mismo en los "*soportes receptores de información (repertorio privado)*". Estimó asimismo que la medida en contra del demandante –la separación de los mandos– no era desproporcionada, dado que el demandante había incumplido gravemente el código deontológico y los referenciales internos, que recuerdan que los agentes deben utilizar los medios informáticos puestos a su disposición con fines meramente profesionales, siendo admitida una utilización de carácter privado. Según el tribunal de apelación, las actuaciones del demandante eran más graves si cabe debido a su condición de agente a cargo de la vigilancia general lo que le obligaba a mantener un comportamiento ejemplar.

El TEDH, que observa que los tribunales internos examinaron debidamente el motivo del demandante de una violación de su derecho al respeto de su vida privada, juzga estos motivos pertinentes y suficientes. Es cierto que al utilizar la palabra "*personal*" en vez de "*privado*", el demandante utilizó el mismo término que el que se encuentra en la jurisprudencia del tribunal de casación, según la cual, el empleador, en principio, no puede abrir los archivos identificados por el empleado como "*personales*". No obstante dada la valoración de la compatibilidad de las medidas en causa con el artículo 8 del Convenio, que ha efectuado el TEDH, no es suficiente para encausar la pertinencia o suficiencia de los motivos esgrimidos por los tribunales internos, considerando el hecho de que el manual del usuario para la utilización de los sistemas informativos de la SNCF indica específicamente que las "*informaciones de carácter privado deben estar claramente identificadas como tales (opción "privado" en los criterios de Outlook, concretamente) [y es lo mismo] para los receptores de estas informaciones (repertorio "privado")*". El tribunal concibe además que habiendo constatado que el demandante había utilizado una parte importante de la capacidad de su ordenador profesional para almacenar los archivos en causa (1.562 archivos representando un volumen de 787 Mb), la SNCF y los tribunales internos juzgaran necesario examinar su causa con rigor.

En suma, para el TEDH los tribunales internos no excedieron el margen de apreciación del que disponían, y que, por lo tanto, no ha habido violación del artículo 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950.

3. LA DOCTRINA DEL TRIBUNAL CONSTITUCIONAL SOBRE VIDEOVIGILANCIA Y CONTROL DE LAS COMUNICACIONES ELECTRÓNICAS DEL TRABAJADOR

En la STCo. 186/2000, de 10 de julio[19], el tribunal dictó un fallo importante sobre la legalidad de la videovigilancia encubierta en el lugar de trabajo relativa a la protección que ofrece el artículo 18.1 de la Constitución Española. En ella el tribunal analizó el uso de un sistema de cámara de vigilancia secreta instalado en el techo de la sección de ropa y calzado de una empresa, centrándose únicamente en tres cajas registradoras y en el mostrador de paso. En ese caso el Tribunal Constitucional sostuvo que la medida en cuestión debía de superar una triple prueba para considerarse aceptable: tenía que tener un objetivo legítimo ("un test de conveniencia"), necesario ("una prueba de necesidad") y proporcional ("una estricta prueba de proporcionalidad"), es decir, determinar si se había ponderado un justo equilibrio entre la injerencia en un derecho fundamental y la importancia del legítimo objetivo perseguido. En cuanto a la videovigilancia encubierta, el Tribunal Constitucional declaró que la medida de instalación de un circuito cerrado de televisión "*era una medida justificada (ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); idónea para la finalidad pretendida por la empresa (verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE*".

Por lo que se refiere específicamente a las comunicaciones electrónicas en el ámbito de las relaciones laborales, la STCo. 241/2012, de 17 de diciembre[20], ha tenido ya oportunidad de señalar que, en el marco de las facultades de autoorganización, dirección y control correspondientes a cada empresario, "*no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales*". Con relación a esta última limitación, aun cuando la atribución de espacios individualizados o exclusivos –como la asignación de cuentas personales de correo electrónico a los trabajadores– puede tener relevancia sobre la actuación

[19] STCo. 186/2000, de 10 de julio [RTC 2000\186].

[20] STCo. 241/2012, de 17 de diciembre [RTC 2012\241].

fiscalizadora de la empresa, ha de tenerse en cuenta que "*los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin*". Por tanto, la empresa había accedido a unos ficheros informáticos en los que habían quedado registradas las conversaciones electrónicas mantenidas por dos trabajadoras a través de un programa de mensajería que habían instalado en un ordenador de uso común a todos los trabajadores que no tenía clave de acceso; se incumplía pues la expresa prohibición de la entidad de instalar programas en el ordenador. En tales circunstancias, el Tribunal Constitucional concluyó que no existía una situación de tolerancia empresarial al uso personal del ordenador y que, por tanto, "*no podía existir una expectativa razonable de confidencialidad derivada de la utilización del programa instalado*"; en consecuencia, se rechazó la lesión del derecho al secreto de las comunicaciones porque las mantenidas no lo habían sido en un canal cerrado.

Posteriormente, en la STCo. 29/2013, de 11 de febrero[21], que se refería a hechos producidos después de la entrada en vigor de la Ley de Protección de Datos de Carácter Personal, el Tribunal Constitucional declaró que la instalación permanente de un sistema de videovigilancia como medida de seguridad y vigilancia requería que los representantes de los trabajadores y los empleados fueran informados previamente y la falta de ello implicaría una violación del artículo 18.4 de la Constitución Española. En este caso, un empleado de la Universidad de Sevilla fue suspendido sin paga por ausentarse y llegar tarde al trabajo, tras la evidencia obtenida de las cámaras de vídeo instaladas tras la aprobación administrativa. El Tribunal Constitucional declaró: "*en conclusión, no debe olvidarse que hemos establecido de forma invariable y constante que las facultades empresariales se encuentran limitadas por los derechos fundamentales*"[22]. Por ello, "*al igual que el interés público en sancionar infracciones administrativas resulta insuficiente para que la Administración pueda sustraer al interesado información relativa al fichero y sus datos, según dispone el art. 5.1 y 2 LOPD, tampoco el interés privado del empresario podrá justificar que el tratamiento de datos sea empleado en contra del trabajador sin una información previa sobre el control laboral puesto en práctica. No hay en el ámbito laboral, por expresarlo en otros términos, una razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del art. 18.4 CE[23]. Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la*

[21] STCo. 29/2013, de 11 de febrero [RTC 2013\29].

[22] Entre otras muchas, la STCo. 98/2000, de 10 de abril [RTC 2000\98] o STCo. 308/2000, de 18 de diciembre [RTC 2000\308].

[23] *Vid.* Monereo Pérez, J.L., *Los derechos de información de los representantes de los trabajadores,* Madrid, Ed. Civitas, 1992.

Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa".

En el caso enjuiciado, las cámaras de videovigilancia instaladas en el recinto universitario reprodujeron la imagen del recurrente y permitieron el control de su jornada de trabajo; captaron, por tanto, su imagen, que constituye un dato de carácter personal, y se emplearon para el seguimiento del cumplimiento de su contrato. De los hechos probados se desprende que la persona jurídica titular del establecimiento donde se encuentran instaladas las videocámaras es la Universidad de Sevilla y que ella fue quien utilizó al fin descrito las grabaciones, siendo la responsable del tratamiento de los datos sin haber informado al trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen. Vulneró de esa manera, el artículo 18.4 de la Constitución Española. No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

Por su parte, la STCo. 170/2013, de 7 de octubre[24], analiza si se ha producido la vulneración de los derechos a la intimidad y al secreto de las comunicaciones, al haberse considerado como prueba lícita en el proceso de despido la aportación por la empresa del contenido de determinados correos electrónicos del trabajador cuya obtención tuvo lugar mediante el acceso a un ordenador portátil propiedad de la empresa[25]. De acuerdo con los hechos probados, el contenido de los correos electrónicos reflejaba que, a través de la dirección electrónica facilitada por la entidad empresarial, el trabajador había mantenido contacto con terceros ajenos a ella a los que había remitido información detallada sobre las previsiones de cosecha. Esta conducta no estaba autorizada e implicaba la comisión de la falta laboral muy grave tipificada en el convenio colectivo de la industria química, consistente en la revelación a elementos extraños a la empresa de datos de reserva obligada.

En atención al carácter vinculante de esta regulación colectivamente pactada, el Tribunal Constitucional concluye que, "*en su relación laboral, sólo estaba*

[24] STCo. 170/2013, de 7 de octubre [RTC 2013\170].

[25] *Vid.* Monereo Pérez, J. L. y López Insua, B. M., "El control empresarial del correo electrónico tras las STC 170/2013", en *Revista Doctrinal Aranzadi Social*, núm. 11, 2014, versión electrónica.

permitido al trabajador el uso profesional del correo electrónico de titularidad empresarial; en tanto su utilización para fines ajenos al contenido de la prestación laboral se encontraba tipificada como infracción sancionable por el empresario, regía pues en la empresa una prohibición expresa de uso extralaboral, no constando que dicha prohibición hubiera sido atenuada por la entidad". Siendo este el régimen aplicable, el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse, ex art. 20.3 ET, tanto a efectos de vigilar el cumplimiento de la prestación laboral realizada a través del uso profesional de estos instrumentos, como para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo.

En tales circunstancias, cabe entender también que "*no podía existir una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa y que habían quedado registradas en el ordenador de propiedad empresarial*". La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, incluida la adecuación de su prestación a las exigencias de la buena fe. En el supuesto analizado la remisión de mensajes enjuiciada se llevó pues 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, con lo que, de acuerdo con la doctrina del Tribunal Constitucional, quedaba fuera de la protección constitucional del art. 18.3 CE. En el contexto descrito concluye el tribunal que la conducta empresarial no ha supuesto una interceptación o conocimiento antijurídicos de comunicaciones ajenas realizadas en canal cerrado; en definitiva, debe descartarse la invocada lesión del derecho al secreto de las comunicaciones.

De forma similar a lo dicho respecto al derecho al secreto de las comunicaciones, tampoco en este caso el tribunal aprecia que el trabajador contara con una expectativa razonable de privacidad respecto a sus correos electrónicos registrados en el ordenador de la entidad empresarial. En este sentido, el acceso por la empresa al contenido de los correos electrónicos objeto de la controversia no ha resultado excesivo o desproporcionado para la satisfacción de los indicados objetivos e intereses empresariales. Al respecto, a la luz de la doctrina sobre el carácter no ilimitado del derecho a la intimidad en su colisión con otros intereses constitucionalmente relevantes, debemos recordar que "*para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria,*

en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"[26]. Para el Tribunal Constitucional ha de afirmarse aquí 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 ponderada y equilibrada; al margen de las garantías con que se realizó el control empresarial a través de la intervención de perito informático y notario, ha de partirse de que la controversia a dirimir en este recurso se ciñe a los correos electrónicos aportados por la empresa como prueba en el proceso de despido que fueron valorados en su decisión por la resolución judicial impugnada: en concreto, los relativos a datos sobre la cosecha. No consta en las actuaciones que el contenido de estos mensajes refleje aspectos específicos de la vida personal y familiar del trabajador, sino únicamente información relativa a la actividad empresarial, cuya remisión a terceros implicaba una transgresión de la buena fe contractual. 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. En consecuencia, una vez ponderados los derechos y bienes en conflicto en los términos vistos, el Tribunal Constitucional considera que la conducta empresarial de fiscalización ha sido conforme a las exigencias del principio de proporcionalidad. En atención, pues, a las consideraciones realizadas, se rechaza que se haya lesionado el derecho a la intimidad personal consagrado en el art. 18.1 CE.

En otra sentencia relativamente reciente, la STCo. 39/2016, de 3 de marzo[27], el

[26] STCo. 96/2012, de 7 de mayo [RTC 2012\96], STCo. 14/2003, de 28 de enero [RTC 2003\14] y STCo. 89/2006, de 27 de marzo [RTC 2006\89].

[27] STCo. 39/2016, de 3 de marzo [RTC 2016\39].

Tribunal Constitucional desarrolló su jurisprudencia relativa al uso de cámaras de vigilancia encubiertas. En este caso, la empresa había detectado ciertas irregularidades en la caja registradora presuntamente cometidas por uno de sus empleados. Instaló de forma temporal cámaras enfocadas al lugar donde se situaba el cajero. El empresario instaló una señal indicando de manera general la presencia de videovigilancia, así como un documento que contenía el texto del artículo 5 de la Ley de Protección de Datos de Carácter Personal, como requiere la Instrucción 1/2006 de 8 de noviembre dictada por la Agencia Española de Protección de Datos. Según el Tribunal Constitucional, una de las razones por las que no se violó el artículo 18.4 de la Constitución Española fue el hecho de que el empresario instaló una señal en la ventana de la tienda indicando la instalación de videovigilancia, de conformidad con el artículo 5 de la Ley de Protección de Datos de Carácter Personal, así como la Instrucción 1/2006. Según el Tribunal Constitucional, el empleado era conocedor de la instalación de un sistema de control y de su finalidad. Como resultado de la videovigilancia, el empleado fue captado robando dinero de la caja registradora y, por tanto, despedido. Por ello, el Tribunal Constitucional concluyó de la siguiente manera: la medida de instalación de un aparato de grabación de imágenes "*es una medida justificada –ya que existían sospechas razonables de la comisión por parte de los trabajadores de graves irregularidades– idónea para la finalidad pretendida por la empresa –verificar qué trabajador cometía efectivamente las irregularidades sospechadas y adoptar en su contra las medidas disciplinarias correspondientes– necesaria –ya que la grabación servía de prueba de tales irregularidades– y equilibrada –pues la grabación de imágenes se limitó a la zona de la caja–*".

4. LA RECIENTE DOCTRINA DEL TRIBUNAL SUPREMO SOBRE EL ACCESO DE LA EMPRESA A LAS COMUNICACIONES ELECTRÓNICAS DEL TRABAJADOR

Por parte del Tribunal Supremo debemos destacar la sentencia de fecha 8 de febrero de 2018[28]. En esta resolución el Tribunal Supremo confirma la posibilidad de controlar el correo del trabajador por la existencia de pruebas documentales. En concreto, se viene a declarar la procedencia del despido disciplinario del trabajador que acepta pagos de una empresa proveedora al que se le controla y examina los correos relativos a las transferencias bancarias. Más detalladamente, esta sentencia analiza un despido disciplinario procedente por transgresión de la buena fe contractual así como el abuso de confianza en el desempeño del trabajo. Como hecho a destacar debe señalarse que la apertura de la investigación que ha terminado con la extinción disciplinaria del trabajador se produjo a raíz de que

[28] STS 8 de febrero de 2018 [RJ\2018\666].

un tercer empleado de la empresa encontró, en la fotocopiadora general de la oficina, dos resguardos de transferencias bancarias efectuadas por un proveedor de la empresa en favor del trabajador demandante, resguardos que fueron puestos a disposición del superior jerárquico.

Para la resolución del caso, el Tribunal Supremo recuerda que en la empresa existe una concreta normativa empresarial que limita el uso de los ordenadores de la empresa a los estrictos fines laborales y que prohíbe su utilización para cuestiones personales. Igualmente los empleados de la empresa, cada vez que acceden con su ordenador a los sistemas informáticos de la compañía deben aceptar las directrices establecidas en la Política de Seguridad de la Información, en la que se señala que el acceso lo es para fines estrictamente profesionales, reservándose la empresa el derecho de adoptar las medidas de vigilancia y control necesarias para comprobar la correcta utilización de las herramientas que pone a disposición de sus empleados, por lo que el actor era conocedor de que no podía utilizar el correo para fines particulares y que la empresa podía controlar el cumplimiento de las directrices en el empleo de los medios informáticos por ella facilitados.

Específicamente, de esta sentencia del Tribunal Supremo, acerca de la inclusión del correo electrónico en el ámbito de protección del derecho a la intimidad, conviene resaltar lo siguiente: a) "*Aun cuando la atribución de espacios individualizados o exclusivos –como la asignación de cuentas personales de correo electrónico a los trabajadores– puede tener relevancia sobre la actuación fiscalizadora de la empresa, ha de tenerse en cuenta que los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin*"[29]. b) "*El uso del correo electrónico por los trabajadores en el ámbito laboral queda dentro del ámbito de protección del derecho a la intimidad; el cúmulo de información que se almacena por su titular en un ordenador personal –entre otros datos sobre su vida privada y profesional– forma parte del ámbito de la intimidad constitucionalmente protegido; también que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado el derecho a la intimidad personal en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado*"[30]. c) "*El ámbito de cobertura de este derecho fundamental viene determinado por la existencia en el caso de una expectativa razonable de privacidad o confidencialidad. En concreto, hemos afirmado que un criterio a tener en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente*

[29] STCo. 241/2012, de 17 de diciembre [RTC 2012\241].

[30] STCo. 173/2011, de 7 de noviembre [RTC 2011\173].

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"[31].

También tiene en cuenta el Tribunal Supremo que la empresa solo ha examinado el contenido de ciertos correos electrónicos de la cuenta corporativa del empleado, pero no de modo genérico e indiscriminado, sino tratando de encontrar elementos que permitieran seleccionar qué correos examinar, utilizando para ello palabras clave que pudieran inferir en qué correos podría existir información relevante para la investigación y atendiendo a la proximidad con la fecha de las transferencias bancarias; y sin que deje ser relevante dos circunstancias: a) que el contenido extraído se limitó a los correos relativos a las transferencias bancarias que en favor del trabajador le había realizado un proveedor de la empresa; y b) que el control fue ejercido sobre el correo corporativo del trabajador, mediante el acceso al servidor alojado en las propias instalaciones de la empresa. Es decir, nunca se accedió a ningún aparato o dispositivo particular del empleado.

Concretamente, para resolver el caso concreto, el Tribunal Supremo tiene en cuenta que cada vez que los empleados acceden con su ordenador a los sistemas informáticos de la compañía, y de forma previa a dicho acceso, deben de aceptar las directrices establecidas en la Política de Seguridad de la Información, en la que se señala que el acceso lo es para fines estrictamente profesionales, reservándose la empresa el derecho de adoptar las medidas de vigilancia y control necesarias para comprobar la correcta utilización de las herramientas que pone a disposición de su empleados, respetando en todo caso la legislación laboral y convencional sobre la materia y garantizando la dignidad e intimidad del empleado, por lo que el trabajador era conocedor de que no podía utilizar el correo para fines particulares y que la empresa podía controlar el cumplimiento de las directrices en el empleo de los medios informáticos por ella facilitados. No olvidemos tampoco que el examen del ordenador utilizado por el trabajador accionante fue acordado tras el "hallazgo casual" de fotocopias de las transferencias bancarias efectuadas por un proveedor de la empresa en favor del trabajador demandante. Además, a lo que se accedió fue al servidor de la empresa en la que se encuentran alojados los correos remitidos y enviados desde las cuentas corporativas de todos y cada uno de los empleados.

Al hilo de lo anterior, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el

[31] STCo. 12/2012, de 30 de enero [RTC 2012\12].

interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

De acuerdo con lo anterior, para el Tribunal Supremo no cabe duda: a) Que el hallazgo casual de la referida prueba documental excluye la aplicación de la doctrina anglosajona del "fruto del árbol envenenado", en cuya virtud, al juez se le veda valorar no sólo las pruebas obtenidas con violación de un derecho fundamental sino también las que deriven de aquéllas. b) Que la clara y previa prohibición de utilizar el ordenador de la empresa para cuestiones estrictamente personales nos lleva a afirmar que si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo. c) Que el ponderado examen del correo electrónico utilizando el servidor de la empresa y parámetros de búsqueda informática orientados a limitar la invasión en la intimidad, evidencia que se han respetado escrupulosamente los requisitos exigidos por la jurisprudencia constitucional y se han superado los juicios de idoneidad, necesidad y proporcionalidad.

También se analiza en esta sentencia las condiciones del TEDH (caso *Barbulescu II*) estimándose que la conducta empresarial supera holgadamente el filtro de los requisitos que el Alto Tribunal europeo exige para atribuir legitimidad a la actividad de control enjuiciada. En este sentido, la sentencia analiza las diferencias entre el caso que ahora analiza el Tribunal Supremo y el caso que en su día analizó el TEDH (caso *Barbulescu II*), resaltando las siguientes disparidades: "*a) los mensajes monitorizados por la empresa no eran de correo electrónico, sino de chats que correspondían a cuenta privada del trabajador en Yahoo Messenger [uno que el empleado –sostuvo– que utilizaba para atender clientes de la empresa y otro estrictamente privada] y para cuyo acceso se precisaba una clave que sólo conocía él; b) aunque la empresa había prohibido el uso personal de los medios corporativos, no había advertido del alcance del control empresarial ni de la posibilidad de acceder a los chats sin consentimiento del interesado, y el trabajador consideraba que su cuenta era personal; c) la empresa accedió al contenido de los chats privados –con la novia y hermano del trabajador– y los imprimió; d) tampoco había mediado causa concreta que motivase el acceso a las comunicaciones privadas*". Todo lo anterior conlleva al Tribunal Supremo a estimar como correcta el comportamiento de la empresa, sin que haya vulnerado el derecho a la intimidad del trabajador.

5. CONCLUSIONES

Para controlar el correo electrónico del trabajador, parece evidente que con las últimas y recientes sentencias del TEDH, la doctrina que impera es aquella que confirma que no solo se requiere la prohibición expresa de uso personal del mismo sino que hace falta algo más: una advertencia clara y previa al control (principio de transparencia), que afecte a la intimidad o al secreto de la comunicación en la menor medida posible (principio de proporcionalidad), tanto en lo que respecta a la intensidad del control como a los medios técnicos utilizados para ello (principio de minimización)[32].

La jurisprudencia parte de la sentencia del TEDH de fecha 3 de abril de 2007, asunto *Copland*[33], y que, en suma, entiende que no se transgrede el derecho a la intimidad del trabajador cuando el control de los dispositivos electrónicos de la empresa (incluido el correo electrónico otorgado al trabajador) cuente con el conocimiento del empleado o se encuentre expresamente previsto en ley. Criterio completado con la sentencia del TEDH (Gran Sala) de fecha 5 de septiembre de 2017, Caso *Barbulescu II*[34], donde se reconoce que, a pesar de las instrucciones otorgadas por la empresa a los trabajadores sobre el uso y disfrute de los dispositivos electrónicos, se debe examinar si el empleado fue advertido antes de la vigilancia que iba a llevarse a cabo en las comunicaciones electrónicas de su correo institucional (es necesario un aviso previo antes del comienzo de la supervisión), sin que la empresa pueda provocar una intromisión importante en la vida privada del trabajador y valorando si existen vías menos invasivas para ello[35].

Así, el TEDH concreta que las autoridades nacionales deben de evaluar si la medida empresarial supera el siguiente test[36]: 1) Si existió información previa y clara a los trabajadores de las medidas de control que pueden utilizarse, de su alcance y de su puesta en práctica. 2) El grado de fiscalización empresarial y su extensión, tanto temporal como material (si se ha examinado la totalidad o solo parte de las comunicaciones). 3) Si existen argumentos legítimos que justifique el control, monitorización o la vigilancia de las comunicaciones y el acceso a las mismas por tratarse de una medida invasiva e intrusiva. 4) Si existen otras medidas y medios alternativos menos agresivos y más respetuosos con la vida privada del

[32] Rodríguez Escanciano, S., "Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos", en *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 16, 2019, p. 114.

[33] TEDH 3 de abril de 2007, Caso Copland contra Reino Unido [TEDH 2007\23].

[34] TEDH 5 de septiembre de 2017, Caso Barbulescu contra Rumania [TEDH\2017\61].

[35] *Vid.* Cuadros Garrido, M. E., "La mensajería instantánea y la STEDH de 5 de septiembre de 2017", en *Aranzadi Doctrinal*, núm. 11, 2007.

[36] Rodríguez Escanciano, S., "Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos", en *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 16, 2019, pp. 117 y 118.

trabajador y demás derechos fundamentales. 5) De qué modo utilizó el empresario los resultados de la medida de vigilancia, concretamente, si los resultados se utilizaron para alcanzar el objetivo declarado de la medida. 6) Si se respetan determinadas garantías para el trabajador de manera que, si se accede al contenido de sus comunicaciones, el mismo haya sido previamente notificado.

Por otro lado, siguiendo la estela del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD), extiende su ámbito de aplicación a las relaciones laborales y funcionariales en las cuales, aunque con alguna matización, rigen los principios y garantías de la protección de datos, que deben de ser respetados por la Administración como responsable del tratamiento: consentimiento, licitud, transparencia, finalidad, adecuación, pertinencia, exactitud y actualización, temporalidad, seguridad a través de la confidencialidad, seudonimización o cifrado, evaluación de impacto y responsabilidad proactiva. A los citados parámetros se le unen una serie de salvaguardas de la persona que se configuran como derechos subjetivos encaminados a hacer operativos los postulados genéricos: información, acceso, rectificación, supresión, bloqueo, limitación del tratamiento, portabilidad u oposición[37]. Asimismo, la citada ley establece límites en el ejercicio del poder de supervisión empresarial para proteger, entre otros aspectos: el derecho de la intimidad de los trabajadores y empleados públicos tanto en el uso de los dispositivos digitales puestos a disposición por su empresario (art. 87), como frente al recurso a los mecanismos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89) o también a raíz del establecimiento de sistemas de geolocalización en el ámbito laboral (art. 90), sin dejar de mencionar la posibilidad de desconexión del trabajador o empleado público para respetar sus tiempos de descanso (art. 88)[38]. No obstante, la norma no resuelve todos los problemas existentes, lo que obliga a seguir realizando una labor de integración entre, por un lado, el marco jurídico compuesto por la Ley y el Reglamento de aplicación directa y obligatoria, pudiendo ser invocado en todo tipo de relación pública o privada[39]; y, por otro, el propio EBEP (arts. 53.1 y 20.2 EBEP en relación con el art. 14 y 87.1 LOPDyGDD). En relación al correo electrónico u otras formas

[37] Rodríguez Escanciano, S., "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del reglamento europeo", en *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 423, 2018, pp. 19 y ss.

[38] Rodríguez Escanciano, S., "Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos", en *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 16, 2019, p. 113.

[39] Goñi Sein, J., *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018)*, Bomarzo, Albacete, 2018, p. 15.

de comunicación, de conformidad con la doctrina, ya no está implicado sólo el derecho fundamental a la intimidad o a la protección de datos, sino que también queda afectado el secreto a las comunicaciones, sin que pueda quedar explicado mediante las facultades que se le atribuyen a la Administración en relación con sus empleados[40].

De lo expuesto hasta ahora podemos extraer las siguientes consecuencias finales para el control de correo electrónico o comunicaciones[41]: a) El trabajador debe ser informado de las medidas que el empresario adopte a fin de controlar los medios de comunicación. b) Es necesario diferenciar los flujos de comunicación de su contenido. c) El control de los contenidos exige justificaciones claras y, de producirse, ha de instrumentarse mediante el establecimiento de unas efectivas garantías a favor del trabajador. d) La información facilitada al trabajador ha de ser clara y transparente. e) Debe realizarse con anterioridad a que se active y comience el control.

En suma, para que el control al trabajador por parte del empresario sea legítimo, primero, debe superarse el test de transparencia respecto a la información previa otorgada al afectado; segundo, debe superarse la cuestión relativa a la finalidad debiendo existir un motivo válido para su fiscalización; y, tercero, el principio de proporcionalidad en lo que se refiere a la preferencia de controles menos invasivos frente a los más intrusivos, siempre y cuando exista una opción real y no una mera comodidad o conveniencia empresarial[42]. Por tanto, no es suficiente prohibir la utilización personal del correo con la idea empresarial de destruir cualquier tipo de expectativa a la confidencialidad; sino que se requiere, además, la advertencia previa de control, que la misma sea clara, que existan motivos reales para la realización del control, y que con tal finalidad se utilicen aquellos medios que sean menos intrusivos para respetar la intimidad o el secreto de las comunicaciones del trabajador[43].

No obstante, después del caso *Barbulescu II*, y como también hemos analizado, se han dictado varias sentencias en las que se vuelve a poner el foco de atención en la solución otorgada. Nos referimos, primero, a la sentencia del TEDH, de fecha 22 de febrero de 2018[44], en el asunto *Libert* contra Francia. En esta sentencia, y

[40] Desdentado Bonete, A. y Desdentado Daroca, E., "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", en *Información Laboral*, núm. 1, 2018, pp. 19 y ss.

[41] Valdés Dal-Re, F., "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", en *Revista de Derecho Social*, núm. 79, pp. 15 y ss.

[42] Molina Navarrete, C., "El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente?", en *IusLabor*, núm. 3, 2017, pp. 287 y ss.

[43] Rodríguez Escanciano, S., "Posibilidades y límites en el control de los correos electrónicos de los empleados públicos a la luz de la normativa de protección de datos", en *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 16, 2019, p. 118.

[44] TEDH 22 de febrero de 2018 [TEDH\2018\35].

sustentándose en derecho francés, de manera dudosa, se confirma que en el control del ordenador del trabajador, al haberse localizado por el sustitutito del mismo material pornográfico y presuntas falsificaciones de documentos que no tenían que ver con la actividad laboral, la actuación empresarial fue legítima porque el derecho francés permite la compatibilidad entre la intimidad con la potestad empresarial de acceder a los ficheros profesionales del trabajador, aún en su ausencia, siempre y cuando este no identifique los ficheros como privados. En suma, en esta última sentencia, el TEDH (en comparación con el caso *Barbulescu II*) ya no se muestra igual de decidido en la protección del trabajador frente al control empresarial, sustentándose –con argumentos bastante débiles– en el derecho interno francés[45]. La valoración de este caso se hace desde un punto de vista crítico pues creemos que los argumentos jurídicos utilizados para fallar en tal sentido son algo débiles y contradictorios.

Nos referimos ahora, en segundo lugar, a la sentencia del Tribunal Supremo fecha 8 de febrero de 2018[46]. En la misma, y de manera resumida, se entiende que si no hay derecho a utilizar el ordenador para usos personales, no habrá derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, puesto que como no existe una situación de tolerancia de uso personal, tampoco puede existir una expectativa razonable de intimidad; y como el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que se abstenga del control del mismo[47]. En otros términos, impera en esta sentencia la doctrina de que puede utilizarse las facultades empresariales, incluida la prohibición absoluta del uso personal y la no exigencia de advertencia previa para realizar el control, cuando existan restricciones íntegras de ese uso, siendo suficiente para eliminar la expectativa de confidencialidad del trabajador, admitiéndose así la posibilidad de realizar controles extraordinarios en caso de sospecha[48].

Para terminar, vista la jurisprudencia del TEDH, la del Tribunal Constitucional y la del Tribunal Supremo (menos garantista), solo nos queda recomendar a las empresas que desarrollen un protocolo de actuación para el control del correo electrónico de los trabajadores[49], donde quede recogido, de manera clara, las reglas

[45] Mella Méndez, L., "El control empresarial de los correos y archivos electrónicos del trabajador: valoración crítica de la reciente jurisprudencia nacional y europea", en *Derecho de las Relaciones Laborales*, núm. 11, 2018, pp. 1198 y ss.

[46] STS 8 de febrero de 2018 [RJ\2018\666].

[47] Bartolomé Martín, A., "Control empresarial del uso de medios tecnológicos, ¿caso cerrado?", en *Revista de Información Laboral*, núm. 6, 2018.

[48] Desdentado Bonete, A. y Desdentado Daroca, E., "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", en *Información Laboral*, núm. 1, 2018, pp. 19 y ss.

[49] Lahera Forteza, J., "Nueva vuelta de tuerca sobre el control empresarial del correo electrónico corporativo de los trabajadores", en *Observatorio de recursos humanos y relaciones laborales*, núm. 128, 2017, p. 72.

y la prohibición del uso personal del correo electrónico institucional, así como la advertencia de la posibilidad de fiscalizar y monitorizar el correo electrónico por razones legítimas empresariales, por supuesto, de la manera menos intrusiva posible. Reglas o protocolos predeterminados en las que atenerse no solo trabajadores, sino también empresarios, evitando así cualquier tipo de abuso por alguna de las partes, dado que el trabajador conoce previamente que uso puede darle al correo electrónico institucional y el empresario evitaría así el control abusivo e inconstitucional de la propia monitorización.