EL ALCANCE DEL DERECHO AL RESPETO DE LA CORRESPONDENCIA DEL TRABAJADOR EN LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

Federico Navarro Nieto
Catedrático de Derecho del Trabajo y de la Seguridad Social
Universidad de Córdoba

EXTRACTO **Palabras Clave**: Respeto de la correspondencia, derecho del trabajador, poder de control empresarial, TEDH

El artículo tiene como objeto el estudio de la jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el respeto de la correspondencia recogido en el art. 8 del Convenio Europeo de Derechos Humanos. El estudio parte de la expansión del concepto de correspondencia de la mencionada norma en la jurisprudencia, hasta abarcar los medios telemáticos de comunicación en la empresa y aborda el estudio de la doctrina del TEDH sobre la privacidad de las comunicaciones en las relaciones laborales, centrándose en la STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*. La sentencia estima que la mera prohibición no justifica el sacrificio puro y duro de la privacidad de las comunicaciones del trabajador, pero entiende legitimas las injerencias empresariales en la medida en que su política al efecto supere el test de legitimidad que el propio Tribunal establece. Esta sentencia supone un avance en la clarificación de criterios a tener en cuenta en la aplicación del art. 8 CEDH, pero se trata de un avance que conviene relativizar teniendo en cuenta que, al margen de esta sentencia, el TEDH considera necesario valorar las decisiones impugnadas a la luz del conjunto de la causa y respetar el margen de apreciación del que disponen los tribunales nacionales, bastando al Tribunal con que la argumentación de los mismos sea pertinente y suficiente.

ABSTRACT **Key Words**: Respect of the correspondence, worker's right, power of corporate control, ECHR

The article aims to study the jurisprudence of the European Court of human rights on respect of the correspondence contained in article 8 of the European Convention on human rights. Study part of the expansion of the concept of the mentioned standard correspondence in jurisprudence, to encompass the telematic media company and deals with the study of the doctrine of the ECHR on the privacy of communications in the labour relations, focusing on the STEDH (Great Hall) 9-5-2017, Barbulescu affair. The statement estimated that the mere prohibition does not justify the pure sacrifice of worker communications privacy, but understands legitimate business meddling in so far as its policy to effect exceeds the test of legitimacy that the Court sets. This statement represents a breakthrough in the clarification of criteria to be considered in the application of article 8 ECHR, but it's a step forward that should be relative bearing in mind that, aside from this ruling, the ECHR considers it necessary to rating decisions challenged in the light of the whole of the cause and to respect the margin of appreciation which have national courts, sufficing to the Court with the same argumentation is relevant and sufficient.

 Recepción de original: 23.07.2018. Aceptación: 30.07.2018

ÍNDICE

1. INTRODUCCION

La capacidad que ofrece hoy día la tecnología para la monitorización empresarial de las comunicaciones del trabajador y el tratamiento de los datos personales deducibles de las mismas en el entorno laboral supone un evidente riesgo para los derechos fundamentales de aquel y la necesidad creciente de una regulación que reduzca o minimice tales riesgos. Como destaca el Considerando 6 del nuevo Reglamento de la UE 2016/679/UE, en materia de protección de datos (en adelante, RGPD), "la tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades". En el ámbito de la empresa estas nuevas tecnologías multiplican los riesgos de intrusiones en la vida privada del trabajador.

Una aproximación al uso de internet en el trabajo centrado en los derechos del hombre exige un marco regulador interno transparente, una política de puesta en marcha coherente y una estrategia de aplicación por los empleadores proporcionada a los objetivos pretendidos, pero lo cierto es que las regulaciones estatales son dispersas o inexistentes en la materia en estudio y las políticas y protocolos empresariales están en estado embrionario [1]. En este contexto, la problemática de la tutela de la privacidad del trabajador en el ámbito laboral, y en particular el

[1] Muy didáctico al respecto el acercamiento a las políticas de empresa de E. M. Blázquez Agudo, *Aplicación práctica de la protección de datos en las relaciones laborales*, Ed. W. Kluwer, 2018, pág. 169 y sigs.

respeto de su correspondencia, debe contemplarse hoy a partir del enfoque de la jurisprudencia del TEDH.

La relevancia de esta jurisprudencia referida al art. 8 CEDH se deduce claramente del eco que ha tenido en el derecho de la UE. Recuérdese que el art. 6.2 TUE indica que la UE respetará los derechos fundamentales tal como se garantizan en el CEDH, y téngase en cuanta también que el art. 7 de la CDFUE sigue las principales líneas trazadas por el concepto de secreto de las comunicaciones del art. 8 CEDH. La doctrina del TJUE sobre el derecho a la vida privada, por su parte, toma como referencia la doctrina del TEDH referente al art. 8 CEDH [2]. También aquella doctrina ha influido en la interpretación del alcance del art. 18.3 CE, a través de nuestra jurisprudencia interna, y ello debe ser resaltado en un sistema jurídico como el español, que, más allá de un marco genérico sobre los poderes de control y vigilancia empresarial (art. 20.3 ET), se encuentra entre los ámbitos jurídicos nacionales que no cuenta con una regulación legal específica de la materia y donde la interiorización en el contrato de trabajo de los derechos fundamentales es fruto de la jurisprudencia constitucional [3].

El enfoque del Tribunal Europeo es significativo teniendo en cuenta además, como he apuntado, la dispersión del tratamiento en los distintos sistemas nacionales y también que la existencia del RGPD aunque facilita una uniformidad básica entre los Estados miembros de la UE (véase el Considerando 10), no prevé una regulación en materia de protección de datos en las relaciones laborales, limitándose en su art. 88 a facultar a los Estados para establecer una regulación específica, dejándoles un amplio margen discrecional en la materia.

A la relevancia de la doctrina del TEDH para la fijación de criterios normativos básicos sobre los derechos a la privacidad del trabajador en el lugar de trabajo, hay que añadir la importancia también por su función uniformadora básica en este mismo terreno de la Recomendación CM/Rec(2015)5 del Comité de Ministros de los Estados miembros del Consejo de Europa, sobre el tratamiento de datos personales en el contexto del empleo, en interpretación del art. 8 CEDH (en adelante, Recomendación 2015, Ministros Consejo de Europa) y también con una función interpretativa complementaria en nuestra temática los documentos de trabajo y dictámenes del Grupo de Trabajo 29 (*art. 29 Working Party*) en interpretación de la derogada Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[2] J. L. Piñar Mañas y M. Recio Gallo, *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Ed. W. Kluwer, 2018, págs. 25-26.

[3] M. Rodríguez-Piñero y Bravo-Ferrer, *Contrato de trabajo e intimidad del trabajador*, Universidad de Huelva, 2004, pág. 7-8.

2. LA GARANTÍA DE LA PRIVACIDAD DE LAS COMUNICACIONES EN EL ART. 8 CEDH

El derecho al secreto de las comunicaciones, junto con la protección de la vida privada, constituye un bien jurídico de primer orden en el constitucionalismo moderno y en los instrumentos internacionales sobre derechos (DUDH de 1948, art. 12; PIDCP de 1966, art. 1; CEDH, art. 8), que, como derechos de libertad, aparecen vinculados a la dignidad de la persona. No en vano, la CDFUE agrupa estos derechos en el Capítulo II, sobre "Libertades". Aquellos bienes jurídicos protegidos confluyen en un bien jurídico más amplio, la llamada *privacy*, esto es, el derecho a la privacidad, que se configura como una macrocategoría que expresa "la voluntad de excluir a una generalidad de personas del conocimiento de determinadas informaciones", abarcando una constelación de derechos [4]. Esta confluencia es evidente hoy en el mundo de las comunicaciones telemáticas donde se produce una clara imbricación entre el derecho a la intimidad, a la protección de datos y al secreto de las comunicaciones. Pero estas consideraciones sobre la interrelación de derechos no permiten la indiferenciación entre ellos; de hecho, la mención normativa expresa de aspectos parciales inherentes a la *privacy* en el art. 8 CEDH subraya la relevancia de cada uno de esos bienes jurídicos particulares para una garantía efectiva y cualitativa de la vida privada [5].

El derecho al respeto de la correspondencia, amparado por el art. 8 CEDH, tutela la libertad de las comunicaciones y el secreto de las mismas. La configuración de este derecho en el constitucionalismo contemporáneo y en las normas internacionales se dirige a la protección de un objeto, la libertad individual de comunicación, cuya eficacia se tutela con una garantía, el secreto de las comunicaciones, que va acompañada de la regulación de excepciones; previsiones éstas que se dirigen a dar certeza y seguridad jurídica en el disfrute de aquella libertad individual, evitando injerencias arbitrarias en la misma [6]. El derecho protege la comunicación como "todo proceso de transmisión de mensajes entre personas determinadas a través de cualquier medio técnico" [7]. El principal rasgo característico del secreto de las comunicaciones, que lo distingue de otros derechos fundamentales (como el derecho a la intimidad), es su configuración como una garantía formal, de impenetrabilidad de las comunicaciones en cuanto tal para terceros, públicos o privados. La garantía del secreto no tiene nada que ver con su contenido ni con el hecho de que lo comunica-

[4] C. Colaprieto, "*Tutela della dignitá e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*", en GDLRI, nº 155, 2017, 3, págs. 445 y 448; X. Arzoz, "*Comentario al art. 8 CEDH*", en *Convenio Europeo de Derechos Humanos: comentario sistemático*, Iñaki Lasagabaster Herrarte (director), Civitas Thomson Reuters, 2015 pág. 339-340.

[5] X. Arzoz, "*Comentario al art. 8 CEDH*", cit. pág. 340.

[6] J. Jiménez Campos, "*La garantía constitucional del secreto de las comunicaciones*", REDC, nº 20, 1987, págs. 41-42.

[7] J. Jiménez Campos, "*La garantía constitucional del secreto de las comunicaciones*", cit. pág. 42.

do forme parte o no de la intimidad del individuo, y este dato es relevante dada la experiencia normativa, donde estos derechos aparecen enunciados conjuntamente por la norma, como es el caso del art. 8 CEDH [8].

En principio, la garantía de la privacidad de las comunicaciones se refiere al proceso mismo de comunicación, de forma que una vez cerrado éste la protección de la documentación del mensaje quedaría fuera del mismo y en su caso dentro del derecho a la intimidad o a la protección de datos [9]. Pero el ámbito objetivo de protección de la libertad de comunicación no es tan nítido. Conforme a la doctrina del TEDH, de la que se hace eco el TC español, se protege tanto el "soporte", como el "mensaje"; y también otros datos de la comunicación como el momento, la duración o la identidad de los comunicantes [10]. El derecho, pues, "puede resultar vulnerado tanto por la interceptación, en sentido estricto, consistente en la aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o la captación del proceso de comunicación, como por el simple conocimiento antijurídico de lo comunicado a través de la apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil, por ejemplo" (STC 241/2012, FJ 4) [11].

De esta forma, en el caso de la mensajería electrónica, los archivos o listado de correos enviados o recibidos están amparados por el derecho a la intimidad o a la protección de datos de carácter personal [12], pero en la medida en que permiten tener conocimiento de la comunicación en curso o realizada, de algunos de sus elementos externos o de los interlocutores, también están amparados por la privacidad de las comunicaciones [13]. De hecho, la injerencia en los archivos de las

[8] J. Jiménez Campos, op. cit. pág. 41-42; T. Martínez Montañez, "*Articulo 18.3. El secreto de las comunicaciones*", en *Comentarios a la Constitución Española*, Casas Baamonde y Rodríguez-Piñero y Bravo-Ferrer (Dirs.), Ed. Wolters Klumer, 2008, pág. 442-443.

[9] J. Jiménez Campos, op. cit., pág. 44.

[10] L. M. Díez-Picazo, *Sistema de derechos fundamentales*, Ed. Thomson Civitas, 4ª ed., 2013, pág. 306.

[11] Como recuerda la STS (Sala de lo Penal, Sección1ª) 10-12-2015, núm. 864/2015, es doctrina consolidada del TC y de la Sala del TS, acogiendo a su vez la doctrina del TEDH, que "el derecho al secreto de las comunicaciones (art. 18.3 CE) consagra la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado tanto por la interceptación en sentido estricto -aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación del proceso de comunicación- como por el simple conocimiento antijurídico de lo comunicado -apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil, por ejemplo-. Igualmente se ha destacado que el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores".

[12] Como se observa en la STC 241/2012, FJ 4, "la protección del derecho al secreto de las comunicaciones 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 otros derechos".

[13] De forma que "el concepto de secreto de la comunicación, cuando opera, cubre no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva

comunicaciones de los trabajadores mediante el acceso al ordenador en que están depositados es considerado por el TC como supuesto con relevancia constitucional al amparo del art. 18.3 CE en las SSTC 241/2012 y 170/2013.

El TEDH recuerda que la utilización de información relativa a la fecha y duración de las conversaciones telefónicas y en particular los números marcados, puede plantear un problema en relación con el artículo 8, ya que dicha información es «parte de las comunicaciones telefónicas» (STEDH 3-4-2007, *asunto Copland contra Reino Unido*, ap. 43). Más claramente en la sentencia STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu contra Rumani*a, como veremos, se subraya la relevancia, desde la perspectiva del respeto de las comunicaciones, de las injerencias en los contenidos de la mensajería electrónica. Esta orientación ampliatoria de la protección de las comunicaciones es avalada también en los documentos del Consejo de Europa interpretativos del alcance del art. 8 CEDH [14].

La garantía de no injerencia admite graduaciones dependiendo del soporte técnico empleado, de manera que interceptar un mensaje sin violentar o manipular el soporte no supone una injerencia [15]. En este sentido, la garantía de la privacidad de las comunicaciones requiere que se realicen en condiciones donde exista una expectativa razonable de privacidad, de ahí la exclusión de la protección para conversaciones orales en la vía pública o mediante comunicaciones telemáticas abiertas al público [16]. En el caso de la STC 241/2012, se estima que la pretensión de secreto carece de cobertura constitucional por la posibilidad de uso común del ordenador por todos los empleados, lo que permite considerar que la información archivada en el disco duro era accesible a todos los trabajadores (FJ 6) [17].

Como hemos indicado, el bien jurídico que da sentido al secreto de las comunicaciones es el de la *libertad para comunicarse*. Como apunta nuestro TC, en relación con el art. 18.3 CE, "el derecho fundamental consagra la libertad de las

de los interlocutores, por lo que este derecho queda afectado tanto por la entrega de los listados de llamadas telefónicas por las compañías telefónicas como también por el acceso al registro de llamadas entrantes y salientes grabadas en un teléfono móvil" (STC 241/2012, FJ 4).

[14] Así la Recomendación 2015, Ministros Consejo de Europa considera que del art. 8 CEDH cabe deducir el principio de que el secreto de las comunicaciones abarca las comunicaciones en el puesto de trabajo, tanto los correos electrónicos, como los archivos adjuntos a los mismos (pág. 9).

[15] L. M. Díez-Picazo, *Sistema de derechos fundamentales*, cit. págs. 306-307.

[16] F. Rivero Sánchez-Covisa, *Revisión del concepto constitucional del secreto de las comunicaciones*, Ed. Dykinson, 2017, pág. 186.

[17] Aunque es interesante la observación contenida en el voto particular a esta sentencia del magistrado Valdés Dal-Ré, que cuestiona esta aseveración, argumentando que "el proceso de reparto a domicilio de la correspondencia postal o su entrega mediante un sistema de casilleros abiertos —tan usual en ciertos ámbitos— no autoriza a nadie a abrir y leer las cartas que reparte o que encuentra depositadas en el casillero de otra persona, aunque sea perfectamente factible, nadie está tampoco autorizado a abrir los archivos de correo electrónico o de mensajería de otro, siempre que puedan ser identificados como tales, como era el caso, por más que el acceso sea posible al encontrarse los archivos desprotegidos y en un ordenador de uso común. Más allá de las precauciones que cada usuario pueda adoptar, debe afirmarse que quien abre un enlace o un archivo informático teniendo constancia de que contiene datos de las comunicaciones ajenas no hace nada diferente de quien abre una carta dirigida a otra persona" (FJ 4).

comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas" (STC 114/1984, FJ 7). Por otra parte, este bien jurídico no incluye *el derecho* al "medio" o al "soporte técnico" a través del que realizar la comunicación, que desde esta óptica podría concebirse como obligación o carga para terceros [18]. La libertad de comunicación tiene como principal destinatario a los poderes públicos, imponiendo tradicionalmente una obligación negativa de no injerencia, pero sin llegar a establecer obligaciones positivas de hacer, salvo en lo referente a la garantía misma de esa libertad individual. Este mismo planteamiento es trasladable a las relaciones interprivadas, como veremos.

Por otro lado, la expectativa de inmunidad frente a injerencias en la libertad de comunicación depende en su alcance de los términos de disfrute de la misma, que puede quedar condicionada, como hemos indicado, por los soportes de los que dispone el individuo y también por la existencia de otros bienes y derechos dignos de protección. El ámbito por tanto de garantía de la libertad de comunicación es una cuestión y otra distinta es que, existiendo dicha libertad en los términos que sean, se protege su disfrute mediante el derecho al secreto de las comunicaciones, salvo injerencias justificadas ex art. 8.2 CEDH.

Es importante subrayar, en el contexto de la llamada *privacy*, que las garantías del secreto de las comunicaciones del art. 8 CEDH se han enriquecido a partir de una normativa sobre protección de datos que amplía sus garantías a la protección de las comunicaciones electrónicas. Las normas y documentos internacionales y de la UE dedicados a la protección de datos, con un importante desarrollo en las últimas décadas, incluyen expresamente reglas o recomendaciones sobre protección de las comunicaciones electrónicas [19]. Muy significativa al respecto es la CDFUE. Con sus arts. 7 (respeto de la vida privada y familiar) y 8 (protección de datos personales) sigue las principales líneas trazadas por el concepto de secreto de las comunicaciones del art. 8 CEDH; pero se ha enriquecido de las orientaciones de la nueva generación de normas de secreto de las comunicaciones, incorporando las comunicaciones electrónicas con la misma protección que las comunicaciones tradicionales. De forma que el art. 8 CDFUE complementa sustancialmente la previsión del art. 7, con particular relevancia en la monitorización de la correspondencia electrónica [20].

[18] J. Jiménez Campos, "*La garantía constitucional del secreto de las comunicaciones*", cit. pág. 51.

[19] El Repertorio de recomendaciones prácticas de la OIT, sobre la protección de datos personales de los trabajadores, que la Oficina Internacional del Trabajo (OIT) elaboró en 1997, dedica su apartado 6.14 a la protección de los trabajadores en supuestos de medidas empresariales de vigilancia. La Recomendación 2015, Ministros Consejo de Europa, dedica su Parte II (Ap. 14) a la vigilancia empresarial de las comunicaciones electrónicas en el lugar de trabajo. El Documento de trabajo GT 29, 2002, formula una serie de conclusiones sobre la aplicación a las comunicaciones electrónicas de los principios aplicables a la protección de datos de la Directiva 95/46/CE.

[20] Véase, Documento de trabajo GT 29, 2002, pág. 10, También el Dictamen 2/2017 del GT29, sobre el tratamiento de datos en el trabajo, WP 249 (en adelante, Dictamen 2/2017 del GT29) adopta la misma perspectiva, adaptando las conclusiones de 2002.

Esta conexión del derecho al respeto de la libertad de las comunicaciones y la protección de datos es una nota destacable en la STEDH 5-9-2017, *asunto Barbulescu* [21]. Desde luego, es constatable en esta sentencia, como veremos, un trasvase de los criterios de la normativa de protección de datos a la protección de las comunicaciones del trabajador. Precisamente, en el *asunto Barbulescu* se utiliza como base jurídica el conjunto de normas y documentos internacionales y de la UE dedicados a la protección de datos en el asunto abordado [22]. En una sentencia posterior, el TEDH introduce una consideración muy importante a partir de la normativa sobre protección de datos y su conexión con el derecho a la privacidad del trabajador. Concretamente, la STEDH 9-1-2018, *asunto López Ribalda y otros contra España*, ap. 67, indica que "en una situación donde se hallaba claramente regulado y protegido por ley el derecho del sujeto de observación a ser informado de la existencia, objetivo y modo de la videovigilancia encubierta, las demandantes tenían una expectativa razonable de respeto a su privacidad". Es decir, la regulación de la *privacy* implica *ab initio* una garantía de la expectativa de privacidad. Y esta afirmación puede trasladarse sin especiales obstáculos jurídicos al derecho de no injerencia en las comunicaciones en el puesto de trabajo.

3. EL SUPUESTO AMPARADO POR EL ART. 8.1. UNA AMPLIACIÓN DEL CONCEPTO DE CORRESPONDENCIA

El artículo 8 CEDH, referido al "Derecho al respeto a la vida privada y familiar", prevé en su aparado 1º que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". El TEDH afronta la protección de la privacidad de las comunicaciones, amparada en el art. 8.1 CEDH, a partir de lo que podemos llamar el test del Convenio, que incluye dos momentos sucesivos de enjuiciamiento. En primer lugar, la aplicabilidad del art. 8 del Convenio al supuesto de hecho planteado; en segundo lugar, verificar la existencia de una injerencia en el derecho y la existencia o no de un fundamento al respecto; esencialmente, la existencia de una previsión legal, un fin legítimo, y el respeto del principio de proporcionalidad. Nuestro TC acoge esta metodología del TEDH de forma inequívoca y constante desde un primer momento. Señala con carácter general que las garantías de toda intervención de las comunicaciones requieren una previsión legal precisa, acompañada de una autorización judicial, que responda a un fin constitucionalmente legítimo y respete el principio de proporcionalidad (que la medida sea idónea e imprescindible para la finalidad pretendida) (SSTC 49/1999 y 184/2003) [23].

[21] J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador: la doctrina del Tribunal de Estrasburgo y la jurisprudencia constitucional*", en Revista *Trabajo y Derecho*, nº 40, abril, 2018, págs. 14-16.

[22] J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador…",* cit. pág. 15.

[23] L. M. Díez-Picazo, *Sistema de derechos fundamentales*, cit. págs. 299-300; T. Martínez Montañez, "*Articulo 18.3. El secreto de las comunicaciones*", cit. pág. 444 y sigs.

Por tanto, la primera cuestión a la que se enfrenta el TEDH es la delimitación del supuesto tutelado por el art. 8 CEDH. En este sentido, el Tribunal ha ido reforzando la efectividad de la norma en las relaciones laborales mediante una ampliación del concepto de vida privada y de correspondencia. Por lo que respecta al primer concepto, se puede decir sintéticamente que el TEDH evoluciona hacia una noción amplia de "vida privada" que "no se presta a una definición exhaustiva" (STEDH 5-9-2017, *asunto Barbulescu*, ap. 70). Este enfoque viene favorecido por la ausencia de una definición precisa del derecho al respeto de la vida privada, con la virtualidad expansiva de tutela que exige la creciente capacidad tecnológica de control social en la vida de los Estados contemporáneos [24].

El Tribunal reconoce que toda persona tiene derecho a una vida privada, lejos de la injerencia no deseada de otros y 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 círculo (STEDH 16-12-1992, *asunto Niemietz contra Alemania*). 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 (STEDH 5-9-2017, *asunto Barbulescu*, ap. 70). Esta identidad social puede incluir actividades de naturaleza comercial, profesional o laboral. El TEDH señala 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" (STEDH 16-12-1992, *asunto Niemietz contra Alemania*, ap. 29).

De forma que la vida laboral puede entenderse implícita en este concepto amplio de vida privada, y por tanto puede incluirse en el artículo 8 CEDH, porque repercute en la forma en que el trabajador forja su identidad social a través del desarrollo de relaciones con otros con motivo de su prestación laboral. Además, el Tribunal admite que, en el ámbito de las relaciones laborales y en determinadas circunstancias, sean considerados como contenido de "su vida privada" los datos no profesionales del trabajador, es decir, datos claramente identificados como privados y archivados por un empleado en un equipo puesto a su disposición por su empleador para el desempeño de sus funciones (STEDH 22-2-2018, *asunto Libert contra Francia*).

En lo que nos interesa, el TEDH también avanza hacia una interpretación amplia de la noción de "correspondencia" del art. 8. El Tribunal viene a afirmar un concepto funcional y no literal de la noción, que incluye la comunicación individual a través de cualquier soporte [25]. Por otra parte, con la STEDH 25-6-1997, *asunto Halford contra Reino Unido*, también se incluyen las comunicaciones realizadas desde el ámbito profesional o laboral. Se afirma en esta sentencia que «las

[24] X. Arzoz, "*Comentario al art. 8 CEDH*", cit. pág. 344.

[25] X. Arzoz, "*Comentario al art. 8 CEDH*", cit. págs. 425-427.

llamadas telefónicas realizadas desde establecimientos comerciales, así como desde el hogar pueden estar contempladas en los conceptos de "vida privada" y "correspondencia" en el sentido del artículo 8, apartado 1 [del Convenio]» (ap. 32). En la STEDH 3-4-2007, *asunto Copland contra Reino Unido*, ap. 41 y 45, el Tribunal afirma que los correos electrónicos enviados desde establecimientos comerciales y la información derivada del control del uso de Internet pueden formar parte de la vida privada y la correspondencia de un trabajador.

También la STEDH 5-9-2017, *asunto Barbulescu* (ap. 72), considera que esta doctrina es igualmente aplicable cuando tales comunicaciones se originan o se reciben en los puestos de trabajo. en particular mediante los correos electrónicos enviados desde el lugar de trabajo. Para el TEDH, en suma, 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 y la noción de "correspondencia" se aplica al envío y recepción de mensajes, incluso desde el ordenador de la empresa empleadora (STEDH 5-9-2017, *asunto Barbulescu*, ap. 74; STEDH 22-2-2018, *asunto Libert contra Francia*, ap. 24).

4. LA EXTENSIÓN DE LAS GARANTÍAS DEL ART. 8.1 AL AMBITO DE LAS RELACIONES LABORALES

Junto a este enfoque expansivo del concepto de correspondencia, que se extiende ahora a las comunicaciones electrónicas, la efectividad del CEDH en el ámbito laboral se refuerza a partir de la doctrina elaborada por el TEDH sobre el efecto horizontal de sus normas en la protección de derechos y libertades fundamentales.

La protección del secreto de las comunicaciones constituye un elemento central en la articulación normativa de la *libertad de los modernos*, garantizando un ámbito de inmunidad del individuo frente al Estado [26]. Desde esta óptica clásica, el CEDH identifica al Estado como destinatario del cumplimiento de sus prescripciones normativas, siendo directa su responsabilidad por los incumplimientos de entidades públicas del Estado. Pero ampliando esta perspectiva tradicional, la doctrina del TEDH también afirma una responsabilidad del mismo, aunque sea indirectamente, por las acciones de personas o entidades privadas. De manera que, junto a las obligaciones negativas de abstención del Estado (de no injerencia arbitraria en los derechos de los individuos) [27], cabe identificar también obligaciones positivas del mismo de cara a la efectividad de los derechos y libertades fundamentales en las relaciones interprivadas. Como sintetiza la STEDH 9-1-2018,

[26] J. Jiménez Campos, "*La garantía constitucional del secreto de las comunicaciones*", cit. pág. 35-36.

[27] Perspectiva adoptada en la STEDH 22-2-2018, *asunto Libert contra Francia*.

asunto López Ribalda y otros contra España: "a pesar de que el propósito del artículo 8 es esencialmente proteger al individuo contra las injerencias arbitrarias del poder público, el Estado no debe simplemente abstenerse de tal injerencia: además de este compromiso primordialmente negativo, pueden existir obligaciones positivas inherentes a un efectivo respeto por la vida privada. Estas obligaciones pueden implicar la adopción de medidas destinadas a respetar la vida privada incluso en el ámbito de las relaciones de los individuos entre sí" (ap. 60).

En el ámbito de las relaciones laborales, la STEDH 5-9-2017, *asunto Barbulescu*, llama la atención sobre el hecho de que pocos Estados miembros del Consejo de Europa se han manifestado explícitamente sobre el derecho de los trabajadores al respeto de su vida privada y de su correspondencia en su puesto de trabajo (apartado 52). Por otra parte, el Tribunal parte de la consideración de que se debe otorgar a los Estados miembros un amplio margen de discrecionalidad para valorar la necesidad de adoptar un marco jurídico que establezca las condiciones en las que una empresa puede adoptar una política que regule las comunicaciones no profesionales, electrónicas u otro, de sus empleados en su lugar de trabajo (ap. 118).

En este contexto de déficit regulatorio, el TEDH enfatiza que el derecho a la vida privada y al respeto de las comunicaciones se dirige, como derecho de protección, no sólo frente al legislador o la Administración, sino también frente a los jueces, que en la resolución judicial de un conflicto interprivados deben proteger de manera efectiva el interés del particular respecto de aquellos derechos [28]. De forma que, como observamos en la STEDH 5-9-2017, *asunto Barbulescu*, incurre en responsabilidad el Estado cuando sus tribunales aprecian la regularidad de un despido disciplinario del trabajador que, en opinión del Tribunal Europeo, ha tenido lugar con violación del secreto de las comunicaciones tutelado por el art. 8 CEDH (ap. 110).

5. ¿ES LEGÍTIMA UNA POLÍTICA DE GESTIÓN EMPRESARIAL QUE DISPONE DISCRECIONALMENTE LOS TÉRMINOS DE USO DE LOS DISPOSITIVOS ELECTRÓNICOS CON FINES PERSONALES?

Situándonos en el ámbito de nuestro derecho interno, conviene partir de la idea de que el poder de dirección del empresario, reflejo de los derechos proclamados en los arts. 33 y 38 CE, y amparado legalmente en el art. 20.3 ET, atribuye a aquel 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, debiendo salvaguardarse en su adopción y aplicación la consi-

[28] Sobre esta jurisprudencia, D. Sarmiento, *Las sentencias del Tribunal Europeo de Derechos Humanos*, Ed. Thomson Aranzadi, 2007, págs. 67-68.

deración debida a su dignidad humana. Esos poderes de vigilancia y control no se refieren a los resultados de la actividad laboral, sino al desarrollo de la actividad y a la conducta del trabajador [29]. Pero en la dogmática sobre derechos fundamentales y relación laboral se parte del axioma de la interpenetración entre los derechos fundamentales y la lógica contractual, que tiene como efecto el que la libertad de empresa, y su concreción en las facultades empresariales de organización del trabajo, deja de ser el único factor de legitimación de las decisiones empresariales [30]. Sobre tales premisas conceptuales, para el TC, "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" (STC 241/2012, FJ 5).

Ahora bien, nuestra jurisprudencia constitucional realiza esa ponderación de bienes constitucionalmente relevantes a partir de la 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 (STC 241/2012, FJ 5). De ahí que en supuestos donde la empresa sólo autoriza al trabajador el uso profesional del correo electrónico de titularidad empresarial, nuestra jurisprudencia constitucional entiende que no existe una expectativa razonable de privacidad, por lo que "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 LET, 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". Como se concluye en la STC 241/2012, FJ 6, la prohibición empresarial "en modo alguno aparece como arbitraria en tanto que se enmarca en el ámbito de las facultades organizativas del propio empresario". De este razonamiento, que comparto en lo esencial, se extrae como consecuencia, que no comparto, que la posible fiscalización de la comunicación del trabajador "quedaba fuera de la protección constitucional del art. 18.3 CE." (STC 170/2013, FJ 4 c); conclusión de la que se hace eco la STS 8-2-2018, rec. 1121/2015, FJ 4.5 a)). Aquí me parece que radica el error conceptual de nuestro TC, al mezclar las facultades empresariales de control con las expectativas de privacidad inherentes al art. 18.3 CE. Volveré sobre este punto.

El TC por tanto aplica el principio de la expectativa de privacidad a partir de la política empresarial sobre uso de las TIC por los trabajadores (claramente en el caso de la STC 241/2012). Pero también hace entrar en juego el principio de proporcionalidad en la valoración de la injerencia empresarial en las comunicaciones de los

[29] M. Rodríguez-Piñero y Bravo-Ferrer, *Contrato de trabajo e intimidad del trabajador*, cit. pág. 37.

[30] M. Rodríguez-Piñero y Bravo-Ferrer, op. cit. pág. 10-13.

trabajadores en su actividad de vigilancia y control (es el caso de la STC 170/2013, donde al principio de la expectativa de privacidad, se añade la aplicación del test de proporcionalidad), aunque en este caso la ponderación debe tener lugar una vez se constata la existencia de una expectativa de privacidad para el trabajador [31].

Por su parte, el TS se ha pronunciado expresamente sobre la facultad empresarial para establecer una prohibición absoluta del uso personal de los medios de comunicación electrónicos. Para el TS, "la clara y previa prohibición de utilizar el ordenador de la empresa para cuestiones estrictamente personales" debe conducir 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» (STS 06-10-2011, rec. 4053/10, y STS 8-2-2018, rec. 1121/2015). Las cursivas son nuestras y subrayan como el TS incurre también en el error conceptual del TC. Sin embargo, el propio TS matiza esta tesis, considerado que es coherente con la jurisprudencia del TEDH, en el sentido de que las reglas de uso fijadas por la empresa (desde la prohibición absoluta a la admisión del uso personal condicionado) deben responder a un fin legítimo, deben respetar un principio de proporcionalidad y deben someterse a un principio de trasparencia.

En el ámbito de la UE, partimos de una lógica de ponderación de derechos e intereses en juego. A partir del art. 52.1 CDFUE, la jurisprudencia del TJUE viene afirmando que los derechos fundamentales (y se refiere concretamente al derecho a la vida privada y a la protección de datos) no son absolutos y pueden ser objeto de restricciones a partir de un criterio de ponderación de derechos [32]. La ponderación de intereses se subraya también en el RGPD, donde se admite la posibilidad de intereses legítimos que pueden justificar el tratamiento de datos personales [33]. El art. 88 del RGPD subraya intencionadamente esta necesidad de un equilibrio entre los intereses de la empresa y los derechos fundamentales de los trabajadores, que no pueden ser sacrificados [34].

[31] A. Desdentado Bonete y E. Desdentado Daroca, "*La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador*", en *Revista de Información Laboral*, nº 1/2018 (Base Aranzadi, BIB 2018, 6059), pág. 5 del documento electrónico.

[32] Sobre esta jurisprudencia, véase J. L. Piñar Mañas y M. Recio Gallo, *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, cit. págs. 29-31.

[33] Con carácter general, el art. 5.1 considera lícito el tratamiento de datos personales si se cumple al menos una de las condiciones que enumera, entre ellas, que "el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte" o que "el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento", pero "siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales".

[34] Dicho artículo dispone que los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer "normas más específicas para garantizar la protección de los

La cuestión que estamos abordando se suscita, en relación con la Directiva 95/46/CE, en el Documento de trabajo GT 29, 2002, en su comentario de la jurisprudencia del TEDH al respecto, donde se rechaza la interpretación conforme a la cual la mera advertencia inicial de prohibición de uso personal al trabajador sea suficiente para justificar una violación de sus derechos en materia de protección de datos (ap. 2.1). No obstante, a continuación, se indica que queda por ver (y de hecho el documento reconoce que cabe cierto margen de interpretación) en qué medida este principio puede estar sujeto a excepciones o limitaciones, en particular cuando es confrontado con los derechos y libertades de otros protegidos de forma similar por la Convención (por ejemplo, intereses legítimos del empleador). No obstante, este documento de trabajo GT 29, 2002 (págs. 20-21), así como el Dictamen 2/2017 GT29 (pág. 24), reiteran una idea central, que el hecho de que un empresario sea propietario de los medios electrónicos no excluye el derecho de los trabajadores a mantener en secreto sus comunicaciones, los datos de localización relacionados y la correspondencia, y las injerencias en el mismo sólo estaría justificada excepcionalmente [35].

En el ámbito del TEDH, el interrogante en cuestión lo suscita el juez Alburquerque en su voto discrepante en la STEDH (Sección 4ª) 12-1-2016, *asunto Barbulescu contra Rumanía.* Para este juez, "en nuestra época donde la tecnología ha desdibujado la frontera entre la vida profesional y la vida privada, y donde algunos empleadores autorizan a los trabajadores a utilizar el material de la empresa con fines personales, al mismo tiempo que otros les permiten utilizar su propio material con fines profesionales, y otros incluso permiten ambas posibilidades, el derecho para el empleador de hacer respetar ciertas reglas sobre el lugar de trabajo y la obligación del trabajador de cumplir correctamente sus tareas profesionales no justifica un control ilimitado de la expresión de los trabajadores a través de internet" (ap. 4). Concluye en este sentido que "los trabajadores no abandonan su derecho a la vida privada y a la protección de sus datos, cada mañana, al atravesar el umbral del lugar de trabajo" (ap. 22). De forma que "una prohibición general para los trabajadores de utilizar Internet con fines personales es inadmisible, de la misma forma que toda política de control generalizada, automática y continua del uso que los empleados hacen de Internet" (ap. 11).

Precisamente esta cuestión es planteada por el demandante en la STEDH 5-9-2017, *asunto Barbulescu* (ap. 84). Pero esta sentencia no permite extraer con-

derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral". Añade en su apartado 2 que dichas normas "incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales", prestando especial atención a la transparencia del tratamiento y los sistemas de supervisión en el lugar de trabajo.

[35] Así se nos indica, a modo de ejemplo en el primer documento, el supuesto de una actividad criminal por parte del trabajador que haga necesario para el empleador la injerencia en las comunicaciones para defender sus propios intereses cuando puede ser responsable de las acciones del trabajador, o cuando aquel es la víctima de la actividad criminal (pág. 21).

clusiones firmes [36]. El Tribunal se remite a las políticas fijadas por la empresa, lo que condiciona la expectativa de privacidad del trabajador. En el caso abordado el Tribunal concluye que no está claro que las normas restrictivas de la empresa empleadora dejaran al demandante con la expectativa razonable de privacidad; el nudo gordiano de la sentencia se centra en el hecho de que "no parece que el demandante hubiera sido 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" (ap. 78). Sin embargo, estas consideraciones se acompañan de la rotunda afirmación de que "las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo. El respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario…" (ap. 80). Pero ¿cómo se concreta este genérico reconocimiento si el trabajador hubiese sido informado con la antelación suficiente del alcance y naturaleza de la supervisión empresarial y de la posibilidad de acceder a los contenidos de las comunicaciones?, ¿en qué términos queda garantizada la expectativa de privacidad del trabajador en este supuesto?.

Recordemos que hay una significativa diferencia del asunto abordado en la STEDH 5-9-2017, *asunto Barbulescu*, con asuntos precedentes referidos al uso del teléfono profesional, cuyo uso con fines personales estaba permitido o, por lo menos, era tolerado, y por tanto permitía albergar una expectativa razonable de privacidad. En la STEDH 25-6-1997, *asunto Halford contra Reino Unido*, el Tribunal precisó que la demandante podía creer razonablemente en la privacidad de las llamadas telefónicas; para el Tribunal esta creencia se reforzaba por el hecho de que, por su puesto de trabajo, disponía de una oficina reservada para su uso, equipada con dos teléfonos, del que uno estaba destinado principalmente a sus conversaciones privadas. En STEDH 3-4-2007, *asunto Copland contra Reino Unido,* no existía ninguna política vigente en el centro de trabajo referente al seguimiento del uso del teléfono, correo electrónico o Internet por parte de los empleados. A diferencia de estos casos, en la STEDH 5-9-2017, *asunto Barbulescu*, existe una prohibición empresarial de uso personal de los medios electrónicos de comunicación. En esta última sentencia no se cuestiona la política empresarial de prohibición del uso personal de los medios electrónicos, sino que en su ejecución no se respetaron las reglas del test de legitimidad de las injerencias empresariales en las comunicaciones del trabajador, lo que permitía a éste mantener viva su expectativa de privacidad.

Éste es desde mi punto de vista el aspecto diferencial de la STEDH 5-9-2017, *asunto Barbulescu,* y la jurisprudencia española que hemos descrito. En la STC 170/2013, FJ 5 c), se parte de la diferenciación del supuesto de las sentencias *Halford* y *Copland* con el caso abordado en la STC (al igual que hemos visto en el

[36] En el mismo sentido, A. Desdentado Bonete y E. Desdentado Daroca, "*La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador*", cit. pág. 13 del documento electrónico

asunto Barbulescu), y se concluye que la mera prohibición "hacía factible y previsible la posibilidad de que el empresario ejerciera su facultad legal de vigilancia sobre los correos electrónicos del trabajador" (lo que, en tales términos, es negado en el *asunto Barbulescu*); con el agravante en el caso de la STC 170/2013 de que la prohibición procede de una cláusula del convenio colectivo, sin que se acredite información alguna de la empresa sobre reglas de uso de las TIC.

La STS 8-2-2018 (FJ 6.5) trata de salvar esta evidente contradicción al observar que "la lectura de los prolijos razonamientos utilizados por el TEDH en el asunto «Barbulescu», pone de manifiesto -entendemos- que el norte de su resolución estriba en la ponderación de los intereses en juego, al objeto de alcanzar un justo equilibrio entre el derecho del trabajador al respeto de su vida privada y de su correspondencia, y los intereses de la empresa empleadora….. tales consideraciones del Tribunal Europeo nada sustancial añaden a la doctrina tradicional de esta propia Sala… y a la expuesta por el Tribunal Constitucional en la sentencia de contraste [STC 170/2013], así como a las varias suyas que el Alto Tribunal cita…, pues sin lugar a dudas los factores que acabamos de relatar y que para el TEDH deben tenerse en cuenta en la obligada ponderación de intereses, creemos que se reconducen básicamente a los tres sucesivos juicios de «idoneidad», «necesidad» y «proporcionalidad» requeridos por el TC…".

Cabe advertir aquí que el TEDH subraya en su doctrina un elemento que considerará central en su test de legitimidad, el principio de trasparencia, que es un aspecto minimizado en nuestra jurisprudencia, al igual que ocurriera en la revocada STEDH (Sección 4ª) 12-1-2016, *asunto Barbulescu contra Rumanía.* La doctrina laboralista es coincidente, desde esta óptica, en que el canon de garantías fijado STEDH 5-9-2017, *asunto Barbulescu*, avoca a una rectificación de nuestra jurisprudencia interna [37].

En definitiva, la STEDH 5-9-2017, *asunto Barbulescu*, estima que la mera prohibición no justifica el sacrificio puro y duro de la privacidad de las comunicaciones del trabajador. Pero la sentencia no niega abiertamente la hipótesis de una política empresarial de prohibición del uso personal de los medios electrónicos, y en todo caso reconoce la legitimidad de las injerencias empresariales en el secreto de las comunicaciones, en la medida en que su política al efecto supere el test de legitimidad que el propio Tribunal elabora.

[37] M. E. Casas Baamonde, "*Informar antes que vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital?. La necesaria intervención del legislador*", *en Derecho de las Relaciones Laborales*, nº 2, 2018, págs. 117-118; C. Sáez Lara, "*Derechos fundamentales de los trabajadores y poderes de control del empleador a través de las tecnologías de la información y las comunicaciones*", en *Temas Laborales*, nº 138/2017, pág. 220-221; J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador…",* cit. págs. 24-25; A. Desdentado Bonete y E. Desdentado Daroca, "*La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador*",cit. pág. 12 del documento electrónico. C. San Martin y A. Sempere, "*Sobre el control empresarial de los ordenadores*", en AS nº 3, 2012, (Base Aranzadi, BIB 2012/984), págs. 33-34 del documento electrónico; C. Preciado Doménech, *El derecho a la protección de datos en el contrato de trabajo*, Th. Reuters Aranzadi, 2017, págs. 249-270.

En mi opinión, las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo, pero esto no significa que el empresario no pueda disponer unilateralmente el uso de los medios de comunicación de su propiedad y efectuar los controles pertinentes para garantizar ese uso [38]. De forma que, incluso, la empresa puede prohibir el uso del correo electrónico con fines personales, como podía hacerlo con el teléfono fijo o con el uso del vehículo de empresa puesto a disposición del trabajador para su actividad laboral [39]. Lo que ocurre es que en las medidas de control la empresa debe respetar la privacidad de las comunicaciones y su contenido, que es un derecho inherente a la persona ex art. 8.1 CEDH.

Como ya hemos indicado, en primer lugar, la *libertad para comunicarse*, no incluye *el derecho* al "medio" a través del que realizar la comunicación, de manera que no puede hablase de una obligación positiva para la empresa en relación con los soportes técnicos que son propiedad de la misma, a diferencia por ejemplo del derecho a la intimidad o a la protección de datos, donde existen obligaciones positivas para la empresa, de salvaguardar la intimidad del trabajador frente a terceros en la relación laboral, en el primer caso, o de ofrecer información previa al trabajador sobre tratamiento de datos, en el segundo caso. Tampoco es comparable el supuesto en estudio con el supuesto del derecho de uso sindical de las TIC existentes en la empresa, amparado en el derecho de libertad sindical, cuyo contenido esencial conlleva la obligación empresarial de hacer consistente en no impedir un uso sindical útil para la función representativa en la empresa una vez que las infraestructuras informáticas están creadas y en funcionamiento (STC

[38] En este sentido, no comparto la tesis del voto particular del magistrado Valdés Dal-Ré a la STC 241/2012, en el sentido de que "el derecho de libertad, que contiene el art. 18.3 CE, limita sus actos [los del empresario] de disposición y limitación de uso o prohibición, sin perjuicio de que quepa, obviamente, la reglamentación del mismo". En el mismo sentido que el voto particular, la STSJ Canarias 6-7-2017, rec. 12/2017, observa que el uso del correo electrónico y demás instrumentos de comunicación empresarial para fines particulares es lícito, aunque no haya sido pactado, siempre y cuando se cumplan las siguientes condiciones: 1) que se haya puesto a disposición del trabajador por la empresa el instrumento de comunicación informática por motivos laborales; 2) que no se perturbe la actividad normal de la empresa mediante el uso privado; 3) que no se vea perjudicado el uso específicamente productivo del instrumento; y 4) que no suponga un gravamen económico para la empresa por su uso. De forma que "la prohibición del uso para fines privados del instrumento de comunicación en tales condiciones podría vulnerar el derecho a la libertad individual de expresión y comunicación de los trabajadores, en los mismos términos que lo haría si se prohibiese a los trabajadores hablar entre sí". La tesis del Tribunal es llamativa, y de hecho, contradiciéndola añade más adelante la sentencia sorpresa se lle después en la sentencia, que "si la empresa prohíbe el uso de estos medios para fines particulares, la prohibición determina que ya no exista una situación de tolerancia con el uso personal del ordenador y que tampoco exista lógicamente una expectativa razonable de confidencialidad. En estas condiciones el trabajador afectado sabe que su acción de utilizar para fines personales el ordenador no es correcta y sabe también que está utilizando un medio que, al estar lícitamente sometido a la vigilancia de otro, ya no constituye un ámbito protegido para su intimidad. En otras palabras, existiendo prohibición expresa la conducta transgresora lo es desde el primer momento en que se produce".

[39] Otra cosa es que, como observa el Dictamen 2/2017 GT 29, una prohibición general de las comunicaciones por razones personales es poco práctica y su aplicación puede requerir un nivel de control desproporcionado (pág. 25).

281/2005, FJ 6º). Incluso en este caso, tratándose del empleo de "un medio de comunicación electrónico, creado como herramienta de la producción, no podrá perjudicarse el uso específico empresarial preordenado para el mismo, ni pretenderse que deba prevalecer el interés de uso sindical" (FJ 8).

En segundo lugar, la libertad de comunicación debe ser compatible con otros bienes y derechos dignos de protección. En este caso, la libertad de comunicación del trabajador no puede ignorar la propiedad empresarial de los medios electrónicos y el derecho del empleador a dirigir y controlar la actividad en la empresa. Como indica la STEDH 22-2-2018, *asunto Libert*, ap. 46, el empresario "legítimamente puede querer asegurarse de que sus empleados utilizan los equipos informáticos puestos a su disposición para el desempeño de sus funciones, conforme a sus obligaciones contractuales y a la reglamentación aplicable". Situándose en esta lógica de ponderación, señala la STEDH 5-9-2017, *asunto Barbulescu*, que, de conformidad con las obligaciones positivas del Estado en virtud del artículo 8 del Convenio, los órganos jurisdiccionales nacionales deben valorar la existencia de "intereses divergentes", de un lado, el derecho del demandante 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 este contexto 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 (ap. 119).

Con estos condicionantes, creemos posible llegar a tres conclusiones. En primer lugar, la libertad de comunicación del trabajador queda amparada en todo caso por el derecho al secreto de las comunicaciones. Independientemente del medio técnico empleado, las comunicaciones privadas del trabajador están amparadas por la garantía formal de su impenetrabilidad. En segundo lugar, el empresario en uso de sus facultades puede regular discrecionalmente las comunicaciones de los trabajadores a través de las TIC de la empresa (por ejemplo, prohibiendo o fijando condiciones para el uso personal); por ello, el empresario está facultado para vigilar que se cumplen sus prescripciones al efecto y, desde esta perspectiva, se condiciona la expectativa de privacidad del trabajador. En tercer lugar, el ejercicio de las facultades de control empresarial no permite justificar una injerencia en el secreto de las comunicaciones (por ejemplo, interferir las comunicaciones o acceder a sus contenidos para verificar el respeto de las reglas empresariales), salvo que pueda justificarse ex art. 8.2 CEDH y, en el marco jurídico español, con las exigencias que impone el art. 18.3 CE. Lo reconoce la STEDH 5-9-2017, *asunto Barbulescu*: "El respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario, *aunque pueden limitarse dentro de las medidas de necesidad*" (cursivas nuestras); y estas medidas se justifican por la existencia de intereses legítimos de la empresa amparados ex art. 8.2 CEDH, lo que nos remite al test de legitimidad elaborado por esta sentencia.

6. GARANTÍAS EN LA INTERVENCIÓN DE LAS COMUNICACIONES EN LA JURISPRUDENCIA DEL TEDH. EL TEST DE LEGITIMIDAD DE LA STEDH (GRAN SALA) 5-9-2017, *ASUNTO BARBULESCU*

La injerencia del empresario en las comunicaciones de los trabajadores dentro de la empresa debe respetar el marco jurídico del art. 8 CEDH. A este respecto, el TEDH centra el grueso de su doctrina sobre la privacidad de las comunicaciones en supuestos de injerencia de los poderes públicos, delimitando claramente determinadas garantías deducibles del art. 8 CEDH [40]. Pero también aborda las injerencias en las relaciones interprivadas trasladando los parámetros de su doctrina al contexto de las relaciones laborales. En este sentido, es particularmente relevante la doctrina de la STEDH 5-9-2017, *asunto Barbulescu* [41], que contiene un canon de garantías más acabado, recogiendo y sistematizando criterios de enjuiciamiento ya contemplados en+ la doctrina general del Tribunal y que son coincidentes con las directrices de organismos internacionales o europeos [42]. Como ya indicamos, una nota destacable en esta sentencia está en que hace entrar en juego el derecho a la protección de datos en la monitorización de las comunicaciones del trabajador [43].

[40] X. Arzoz, "*Comentario al art. 8 CEDH*", cit. págs. 342-343.

[41] Resumimos brevemente el caso de la STEDH 5-9-2017, *asunto Barbulescu*, a efectos de contextualizar las referencias a esta sentencia posteriormente. La síntesis se puede extraer del ap. 129 de la misma: "De las pruebas aportadas ante el Tribunal se desprende que el demandante había sido informado del reglamento interno de la empresa empleadora, que prohibía el uso de los recursos de la empresa para fines personales (ap. 12). Conocía el contenido de este documento y lo había firmado el 20 de diciembre de 2006 (ap. 14). Además, la empresa empleadora distribuyó una nota informativa de fecha 26 de junio de 2007 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 (apartado 15). El demandante tenía conocimiento de -+esa nota y la firmó en una fecha que no se especifica, pero que fue entre el 3 y el 13 de julio de 2007 (apartado 16 supra). Por último, el Tribunal recuerda que el 13 de julio de 2007 el demandante fue citado dos veces por su empleador para explicar su uso personal de Internet (apartados 18 y 20). 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 (apartados 18 y 19). 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 demandante informó a su empleador que éste era responsable de la una infracción penal, a saber, la violación del secreto de la correspondencia (apartado 22 supra)".

[42] Por ejemplo, en el ámbito de la UE Grupo de Trabajo del Artículo 29 (GT29), el *Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral* (WP48)1, Documento de trabajo GT 29, 2002, Dictamen 2/2017 GT 29. Estos documentos hacen referencia a principios como el de garantía de que los datos se tratan con fines específicos y legítimos, que sean proporcionados y necesarios; el de limitación de la finalidad y que los datos sean adecuados, pertinentes y no excesivos para la finalidad legítima; y el principio de trasparencia con los trabajadores sobre el uso y la finalidad de las tecnologías de control. La garantía de las comunicaciones del trabajador se ven reforzadas en el contexto de la protección de datos dentro de la UE, con la previsión del RGPD del principio de rendición de cuentas (art. 5.2), que viene a significar que el responsable de la protección de datos asume la obligación de adoptar una actuación diligente y proactiva para garantizar un tratamiento de datos conforme a los principios de tratamiento de datos ex art. 5.1 RGPD, lo que exige una previsión de qué datos van a ser objeto de tratamiento, con qué finalidad, con qué tipo de operaciones. Cfr. F. Gudín, *Nuevo reglamento europeo de protección de datos versus big data*, Ed. Tirant lo Blanch, 2018, pág. 84.

[43] J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador…",* cit. pág. 14.

La novedad del *asunto Barbulescu* está en la ordenación de unos principios generales aplicables a la valoración de la obligación positiva del Gobierno de velar por el respeto a la vida privada y a la correspondencia en el contexto de las relaciones laborales. Y estos principios se dirigen en particular a enjuiciar la conformidad de la actuación de los tribunales nacionales con el Convenio. Esos principios cristalizan en el test de legitimidad de la injerencia del empresario en las comunicaciones de los trabajadores, que contempla dos aspectos. De un lado, la regularidad de una política empresarial de uso de los medios electrónicos de comunicación. De otro lado, la posibilidad o previsión de controles o de monitorización del uso de tales medios y sus características.

Para la sentencia las autoridades nacionales "deberían tener en cuenta" una serie de criterios (seis) (ap. 120). Hablamos de criterios que integran el test de legitimidad, y que deberían considerarse de forma cumulativa. Los criterios de referencia para la sentencia se pueden ordenar siguiendo el siguiente esquema:

1) justificación para la injerencia (criterio iii);

2) principio de necesidad y proporcionalidad (criterio ii, criterio iv, criterio v);

3) garantías procedimentales (principio de trasparencia) (criterio i, criterio vi).

Antes de proceder a describir tales criterios convienen algunas consideraciones generales. En las políticas empresariales de control de las comunicaciones de los trabajadores hemos de tener en cuenta distintas situaciones. Es menester distinguir si el control se refiere a los aspectos exteriores (el control de flujos) o se refiere a los contenidos. En este último caso, las injerencias empresariales se consideran más excepcionales y se someten a exigencias más estrictas. La sentencia admite la posibilidad de una injerencia en el contenido de la correspondencia electrónica, pero subrayando que "la vigilancia del contenido de las comunicaciones … requiere justificaciones más fundamentadas" (criterio iii). Y vuelve a subrayar más adelante en el criterio iv) (principio de proporcionalidad), que ha de evaluarse "si el objetivo perseguido por el empresario puede alcanzarse sin que éste tenga pleno y directo acceso al contenido de las comunicaciones del empleado"; también el criterio i) (garantías procedimentales) prevé que la información previa al trabajador debe existir, con mayor motivo cuando la supervisión implica también el acceso al contenido de las comunicaciones de los empleados.

Por otro lado, la distinción entre las comunicaciones de carácter profesional o personal es relevante y condiciona el alcance de la finalidad que legitima la injerencia empresarial en las comunicaciones y el respecto a la proporcionalidad de la misma. La expectativa de privacidad tutela un posible uso personal de los medios de comunicación empresariales, que garantiza el art. 8.1 CEDH, admitiéndose injerencias únicamente conforme al test de legitimidad que vamos a describir [44].

[44] Sobre la cuestión, no hay consenso en las legislaciones nacionales, observa la STEDH 5-9-2017, *asunto Barbulescu* (Ap. 54), y nos recuerda que, en países como Alemania, Austria, Dinamarca, Finlandia, Francia, Grecia, Italia, Portugal y Suecia, los empleadores pueden vigilar los correos electrónicos marcados como privados, pero en ningún caso acceder a su contenido. La Recomendación 2015, Ministros Consejo

Siendo claro cuando los correos aparecen formalmente identificados como personales, el problema de las garantías del art. 8 CEDH frente a las injerencias empresariales surge allí donde esta diferenciación no es nítida (como ocurre en el *asunto Barbulescu*); por eso es fundamental una información clara sobre la política empresarial sobre las reglas de uso de las TIC en la empresa y sobre el tipo de controles que se reserva la empresa para su efectividad. La cuestión se pone de manifiesto claramente en la STEDH 22-2-2018, *asunto Libert contra Francia*, a la que nos referiremos brevemente al final del estudio, que, en relación con la privacidad de archivos en el ordenador, rechaza la tesis del Gobierno según la cual no hay injerencia porque no se trata de archivos personales sino profesionales, lo que según él deja la cuestión fuera del amparo del art. 8.1 CEDH. Sin embargo, en el supuesto de hecho la sentencia considerará legítima una regulación nacional donde se permite al empleador acceder a los archivos profesionales dentro de la herramienta informática, circunscribiéndose la cuestión a la legitimidad de la injerencia en los archivos privados.

En nuestra jurisprudencia constitucional, la STC 241/2012 admite la distinción entre comunicaciones profesionales y personales, quedando amparadas éstas por el secreto de las comunicaciones. Así, observa en su FJ 5, que "en pura hipótesis, pueden arbitrarse diferentes sistemas, siempre respetuosos con los derechos fundamentales, orientados todos ellos a que los datos profesionales o los efectos de la comunicación profesional llevada a cabo alcancen al conocimiento empresarial, *sin que se dé, en cambio, un acceso directo o cualquier otra intromisión del empresario o sus mandos en la empresa, en la mensajería o en los datos personales de los trabajadores, si este uso particular ha sido permitido*" (cursivas nuestras).

En nuestra opinión, cuando queda claro que los correos tienen carácter privado el empresario está condicionado por el secreto de las comunicaciones. De forma que el empleador podrá utilizar la información sobre el uso privado de los medios electrónicos con fines disciplinarios, si por ejemplo ha prohibido este uso, pero quedándole vedado el acceso a su contenido, porque es aquí donde juega la garantía formal en que consiste el secreto de las comunicaciones, salvo que existiese un fundamento ex art. 8.2 CEDH para acceder a su contenido. En nuestro ámbito jurídico, no existe unanimidad, argumentándose que no se puede realizar sin autorización judicial ex art. 18.3 CE [45] o que es posible sin la misma, siempre que la empresa respete en el control correspondiente el principio de proporcionalidad [46]. En mi opinión, si existe una política de trasparencia empresarial, y dentro

de Europa, señala que "En ningún caso deberán ser objeto de vigilancia el contenido, envío y recepción las comunicaciones electrónicas privadas en el marco del trabajo" (ap. 14.4).

[45] C. Zoco, *Nuevas tecnologías y control de las comunicaciones*, Thomson Reuters, 2015, pág. 241 y sigs.

[46] D. Martínez Fons, "*El control de la correspondencia electrónica personal en el lugar de trabajo*", en *Relaciones Laborales*, Tomo I, 2003, 809-810.

de ella la admisión del uso personal de las TIC de la empresa y una delimitación clara entre comunicaciones profesionales y personales, la intervención de las comunicaciones privadas, amparada en los fines legítimos ex art. 8.2 CEDH, requiere además por exigencia constitucional un requisito procedimental ineludible, la autorización judicial [47].

Por otra parte, hay que decir que los criterios que comentaremos presuponen una regla trazada en el art. 8.2 CEDH, conforme al cual "No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley….". Para el TEDH la existencia de una previsión legal que ampare la injerencia en el derecho debe proporcionar al individuo suficiente certeza y previsibilidad sobre el supuesto al que se liga la facultad de injerencia. Este es un requisito básico que se ve reforzado al venir exigido en toda política de tratamiento de datos personales en la normativa internacional (art. 5 del Convenio 108 del CE para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal), de la UE (art. 5.1 a) RGPD) y española (art. 4.7 LOPD). Precisamente, la falta de precisión del concepto de tratamiento lícito en el RGPD se mitiga con la remisión a la doctrina del TEDH sobre el art. 8.2 CEDH [48].

En el ámbito laboral no es usual la existencia de previsiones normativas, ni regulación de los casos y condiciones en que puede llevarse a cabo una injerencia en las comunicaciones de los trabajadores. La STEDH 5-9-2017, *asunto Barbulescu*, observa que, aunque los Estados miembros del Consejo de Europa reconocen con carácter general, a nivel constitucional o legislativo, el derecho al respeto de la privacidad y el secreto de la correspondencia, sin embargo, son escasos los que cuentan con una regulación específica sobre la cuestión del ejercicio de la vida privada en el lugar de trabajo de una manera explícita, ya sea como parte de la legislación laboral, ya sea mediante leyes especiales, siendo en general la regulación fragmentaria y referida a aspectos concretos (ap. 52 a 54). De ahí la relevancia de la jurisprudencia del TEDH, como referencia para los tribunales nacionales, y en particular la doctrina sentada por esta sentencia.

[47] En este sentido, comparto la tesis del voto particular del magistrado Valdés Dal-Ré a la STC 241/2012, en el sentido de que el incumplimiento de lo ordenado no habilita en modo alguno interferencias en el proceso o en el contenido de la comunicación, amparado por el derecho al secreto de las comunicaciones del art. 18.3 CE, sin perjuicio de que pueda acarrear algún tipo de sanción.

[48] F. Gudín, *Nuevo reglamento europeo de protección de datos versus big data*, cit. pág. 80. Esta doctrina del TEDH referida al art. 8 CEDH es acogida tempranamente por el TC español. Con base en esta doctrina el TC reclama una norma precisa y clara, que garantice las expectativas razonablemente fundadas del individuo en cuál ha de ser la actuación de los poderes públicos, es decir, en qué circunstancias y bajo qué condiciones se habilita a los poderes públicos para tomar tales medidas. Cfr. T. Martínez Montañez, "*Articulo 18.3. El secreto de las comunicaciones*", cit. pág. 444.

6.1. Justificación para la injerencia

El art. 8.2 prevé la posibilidad de injerencias legítimas en el derecho a la privacidad de las comunicaciones. Esta construcción es propia del reconocimiento del derecho en el constitucionalismo moderno, donde la estructura normativa se compone de un derecho de libertad con previsión de limitaciones [49]. Pues bien, conforme a aquella norma toda injerencia de la autoridad pública en el ejercicio de este derecho debe ser una medida "necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás". Este "inventario de indeterminaciones jurídicas", donde "no falta casi nada" [50], debe ser objeto de una interpretación estricta en tanto supone una excepción al derecho garantizado por el Convenio.

Desde la sentencia STEDH 3-4-2007, *asunto Copland contra Reino Unido*, se considera que el interés empresarial en el uso adecuado de los medios para garantizar el buen funcionamiento de la empresa puede considerarse un objetivo legítimo que justifique la injerencia empresarial en la privacidad del trabajador ex art. 8.2 CEDH. La garantía de la protección de "los derechos y las libertades de los demás" pueden referirse a los del empleador, "que legítimamente puede querer asegurarse de que sus empleados utilizan los equipos informáticos puestos a su disposición para el desempeño de sus funciones, conforme a sus obligaciones contractuales y a la reglamentación aplicable" (STEDH 22-2-2018, *asunto Libert*, ap. 46). Por tanto, garantizar el buen funcionamiento de la empresa y el cumplimiento por el trabajador de sus compromisos contractuales son motivos suficientes para justificar el interés legítimo de la empresa ex art. 8.2 CEDH.

Al mismo tiempo se reclama que dicho interés sea explícito y específico, en sintonía con la normativa internacional sobre protección de datos [51]. De esta forma no sería posible justificar la monitorización por el mero propósito de conocer el uso que el trabajador hace de los medios (control preventivo), sino que deben existir motivos fundados, por ejemplo, de un comportamiento irregular [52]. Los indicios deben ser algo más que simples sospechas, es decir, el secreto de las comunicaciones no se puede sacrificar a partir de hipótesis genéricas o prospectivas.

[49] J. Jiménez Campos, "*La garantía constitucional del secreto de las comunicaciones*", cit. pág. 38.

[50] J. Jiménez Campos, op. cit. pág. 60.

[51] Como indicaba la Directiva 95/46/CE, las operaciones de tratamiento de datos solo tendrán lugar con una finalidad legítima, que debía ser específica, explícita y legítima (art. 6). El art. 6.1 del vigente RGPD considera lícito el tratamiento de datos si se cumple al menos una de las condiciones que enumera, entre ellas, que "el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento". Puntualiza también el actual RGPD en su art. 5.1 que los datos personales serán recogidos "con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines".

[52] J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador…",* cit. pág. 20.

En la sentencia STEDH 5-9-2017, *asunto Barbulescu*, esta doctrina se plasma en el criterio iii) de la sentencia, conforme al cual el empleador debe presentar "argumentos legítimos para justificar la vigilancia de las comunicaciones y el acceso a su contenido". Y puntualiza que "dado que la vigilancia del contenido de las comunicaciones es por su naturaleza un método mucho más invasivo, requiere justificaciones más fundamentadas". Conforme a la doctrina del Tribunal que hemos expuesto, esta sentencia parte de la existencia de un interés empresarial que justifica la injerencia empresarial en la privacidad del trabajador ex art. 8.2 CEDH (ap. 127). En cuanto a los argumentos legítimos, la sentencia se remite a los ap. 38, 43 y 45 sobre textos normativos y documentos de la OIT, Consejo de Europa y UE, pero sin que de ellos se puedan extraer pautas claras sobre dichos argumentos legítimos. No obstante, de la sentencia cabe deducir que el Tribunal considera legítimos ciertos objetivos, aunque nunca en abstracto, como la necesidad de evitar una vulneración en los sistemas informáticos de la empresa, evitar el cuestionamiento de la responsabilidad de la empresa en caso de actividad ilegal en el espacio virtual, así como la divulgación de sus secretos comerciales (ap. 134). En el caso abordado el TEDH concluye que los tribunales nacionales mencionan estos objetivos en términos teóricos, ya que no se acusó concretamente al demandante de exponer a la empresa a ninguno de esos riesgos (ap. 134).

6.2. Respeto del principio de proporcionalidad

Conforme al art. 8.2, toda injerencia en el secreto de las comunicaciones debe constituir "una medida que, en una sociedad democrática, sea necesaria", lo que exige el respeto del principio de proporcionalidad, conforme al cual debe existir una correspondencia entre los fines pretendidos, el alcance de la vigilancia adoptada, y las características concretas de la vigilancia efectuada, que debe regirse por el principio de minimización (limitada a lo necesario para el fin pretendido). Existe una coincidencia en los instrumentos internacionales y de la UE sobre los parámetros que deben aplicarse [53]. En particular, el principio de proporcionalidad exige que la supervisión de las comunicaciones se adecue a los fines que la justifiquen, excluyendo vigilancias generalizadas o continuadas en el tiempo [54].

[53] La Directiva 95/46/CE establecía que la vigilancia debía ser necesaria para alcanzar un objetivo dado (principio de necesidad) y que la misma debía ser pertinente, adecuada y no excesiva respecto a la finalidad indicada (principio de proporcionalidad) (art. 6). El Dictamen 2/2017 del GT29, pág. 8, considera que el principio hace recomendable políticas preventivas con preferencia a las políticas de monitorización o control, y políticas que minimicen la injerencia en los derechos fundamentales del trabajador (conclusiones: 6.4, pág. 25). Puede concretarse esta política preventiva en la diferenciación de las comunicaciones profesionales y privadas, a través de la identificación de la correspondencia como privada o mediante la atribución al trabajador de cuentas de correo diferenciadas al efecto (Documento de trabajo GT 29, 2002, pág. 23; Dictamen 2/2017 GT 29, pág. 15). El actual RGPD en su art. 5.1 indica que los datos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)".

[54] Este aspecto es subrayado en algunos documentos recientes en la materia. El Informe 2/2017

La STEDH 5-9-2017, *asunto Barbulescu*, concreta este principio de proporcionalidad en distintos criterios. En primer lugar, conforme al criterio ii) de la sentencia, se requiere que exista una proporcionalidad entre el alcance de la supervisión realizada del empleador y el grado de intrusión en la vida privada del empleado. Para el TEDH, en el caso del control de las comunicaciones del trabajador, debe tomarse en consideración distintos aspectos. El principio de proporcionalidad será de distinta intensidad si el control se limita al flujo de comunicaciones o incluye también 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. En el caso abordado, el TEDH concluye que, en cuanto al alcance de la supervisión realizada y el grado de intrusión en la vida privada del demandante, 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 (ap. 133).

Conforme al criterio iv), el sistema de vigilancia debe estar basado "en medios y medidas menos intrusivos que el acceso directo al contenido de comunicaciones del empleado". En particular, debe evaluarse, 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". Aquí concluye la sentencia en el caso enjuiciado que 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 (ap. 135).

Conforme al criterio v), el respeto del principio de proporcionalidad requiere contemplar 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. En relación con este criterio, el TEDH considera que ninguno de los dos tribunales nacionales examinó la gravedad de las consecuencias de la medida de control y del procedimiento disciplinario que se siguió. A este respecto, el Tribunal señala que el demandante había sido sometido a la medida disciplinaria más grave, a saber, el despido (ap. 136).

6.3. Garantías procedimentales (principio de trasparencia)

Hay que subrayar que en la STEDH (Sección 4ª) 12-1-2016, *asunto Barbulescu contra Rumanía*, el TEDH se centró en el criterio de la proporcionali-

del GT29 indica que la monitorización continuada o el control sobre todas las actividades en línea de los trabajadores puede considerarse una respuesta desproporcionada y una injerencia en el derecho al secreto de las comunicaciones (pág. 14).

dad, marginando las garantías procedimentales, o al menos apoyándose en una interpretación que tuvo este efecto [55]. Pues bien, se indica en la STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, que, conforme al criterio i), el empleado ha debido ser informado de la posibilidad de que el empleador tome medidas para supervisar su correspondencia y otras comunicaciones, así como la aplicación de tales medidas. Puntualiza la sentencia que "la advertencia debe ser, en principio, clara en cuanto a la naturaleza de la supervisión y antes del establecimiento de la misma".

El Tribunal 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 (ap. 132). El TEDH concluye en el caso abordado que no parecía que el demandante hubiera sido informado con antelación del alcance y de la naturaleza del control efectuado por la empresa o de la posibilidad de que la empresa tuviera acceso al contenido de sus comunicaciones (ap. 132).

La doctrina insiste en que la exigencia de una información previa es un dato novedoso y diferencial con respecto a la STEDH (Sección 4ª) 12-1-2016 [56], aunque esta garantía de trasparencia ya es subrayada anteriormente en otros documentos relevantes [57]. Destaquemos que, actualmente, el RGPR sitúa como concepto clave la trasparencia de la información para asegurar la expectativa razonable de privacidad del afectado [58]. En este sentido, el art. 5.1 a) indica que los datos personales serán tratados "de manera lícita, leal y transparente en relación

[55] El Tribunal estimó que se examinaron las comunicaciones en su cuenta Yahoo Messenger, pero ningún otro dato o documento guardados en su ordenador. No constató que los tribunales nacionales otorgaran una importancia particular a las transcripciones o al mismo contenido de las comunicaciones. Por lo tanto, el Tribunal opinó que el contenido de las comunicaciones no fue un factor decisivo en las conclusiones de los tribunales nacionales (ap. 59). Por lo tanto, estimó que la vigilancia del empleador fue proporcionada y de alcance limitado (ap. 60). Una de las criticas principales que el juez Alburquerque subraya en su voto particular a la sentencia descansa precisamente en la inexistencia de una política de vigilancia del uso de internet por la empresa, lo que se remite a exigencias de carácter procedimental (ap. 2 y ap. 12).

[56] M. E. Casas Baamonde, "*Informar antes que vigilar…",* cit. pág. 114; J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador…",* cit. pág. 17.

[57] Así, Apartado 14.1 y apartado 21 a) Recomendación 2015, Ministros Consejo de Europa. El Informe 2/2017 GT29 recomienda que se comunique comunicarse efectivamente a los trabajadores cualquier control que se lleve a cabo, sus fines y circunstancias, y que las políticas y normas relativas al control legítimo sean claras y de fácil acceso. El Grupo de Trabajo recomienda que una muestra representativa de trabajadores participe en la elaboración y evaluación de dichas normas y políticas (conclusiones: 6.3, pág. 25). Ambos documentos subrayan la conveniencia de la consulta a los representantes de los trabajadores de los medios de vigilancia previstos por la empresa. En particular, el apartado 21 c) Recomendación 2015, Ministros Consejo de Europa aconseja que cuando se prevea alguna incidencia de estos medios de control sobre los derechos fundamentales de los trabajadores debe buscarse el acuerdo con los representantes.

[58] J. Muñoz Ontier, "*Disposiciones generales (arts. 1-5*)", en *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, López Calvo (Coord.), Wolters Kluwer, 2018, pág. 348.

con el interesado («licitud, lealtad y transparencia»). El art. 12.1 dispone además que el responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información relativa al tratamiento de datos "en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo". Por su parte, el artículo 88 del RGPD prevé, para el campo de las relaciones laborales, que las normas del Estado o los convenios colectivos "incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales", prestando especial atención a determinados aspectos, el primero de los cuales es la transparencia del tratamiento de datos.

La información previa, además, no puede limitarse a ser una información genérica. Ha de incluir tanto las reglas sobre uso, como las reglas sobre controles y monitorización. Precisamente, el voto particular del Juez Alburquerque en la STEDH (Sección 4ª) 12-1-2016, *asunto Barbulescu contra Rumanía,* observa que la simple comunicación del empleador a los trabajadores indicándoles que "su actividad sería sometida a vigilancia" (como se recogía en el ap. 10 de la sentencia) no podía considerarse suficientemente clara en cuanto a la naturaleza, el alcance y las consecuencias del programa de vigilancia empresarial (ap. 18).

Dentro de las garantías procedimentales, conforme al criterio vi), se deben ofrecer al empleado garantías adecuadas, particularmente cuando las medidas de supervisión del empleador tienen carácter intrusivo. Se subraya que estas garantías deben impedir que el empleador tenga acceso al contenido de las comunicaciones en cuestión sin que el empleado hubiera sido previamente notificado de tal eventualidad. Se trata pues de que el trabajador pueda oponerse con antelación a la justificación del requisito de necesidad y proporcionalidad del control que efectúa la empresa.

En este punto, el Tribunal 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. 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 (ap. 137).

Una cuestión particular se suscita con los controles *ad hoc* del correo electrónico por existencia de sospechas. El problema es el de compatibilizar el secreto de la interceptación de las comunicaciones y las exigencias de previsibilidad deducibles de esta jurisprudencia. El asunto se ha planteado en relación con las injerencias de los poderes públicos en actividades de investigación y represión del delito o en la interceptación de la correspondencia de los internos en centros penitenciarios [59]. Esta jurisprudencia exige que exista una previsión normativa

[59] X. Arzoz, "*Comentario al art. 8 CEDH*", cit. págs. 428 y sigs.

que legitime la injerencia en el secreto de las comunicaciones, defina el alcance y las modalidades de ejercicio de un poder de injerencia semejante con suficiente claridad (teniendo en cuenta el fin legítimo pretendido) para proporcionar al individuo una protección adecuada contra las injerencias arbitrarias [60]. Trasladando esta doctrina al ámbito de las relaciones laborales la cuestión se remite a los mismos parámetros, es decir, a la existencia de la previsión de la posibilidad de estos controles y su conocimiento por el trabajador, y la verificación en el control *ad hoc* de una justificación específica y el respeto del principio de proporcionalidad en dichos controles[61]. La conclusión que cabe extraer de la STEDH 5-9-2017, *asunto Barbulescu*, es que el principio de trasparencia no permite amparar en genéricas prohibiciones absolutas iniciales la legitimidad de controles ocultos del correo electrónico por inexistencia de expectativa de privacidad, como admite nuestro TC (STC 170/2013) y el TS (STS 6-10-2011).

Al respecto resulta de interés la STEDH 9-1-2018, *asunto López Ribalda y otros contra España*, donde se plantea la legitimidad de una videovigilancia encubierta de la empresa. La videovigilancia 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. En el caso, los tribunales españoles constatan que las empleadas afectadas 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. Pero consideraron que la medida estuvo justificada (debido a las fundadas sospechas de robo), apropiada al objetivo legítimo perseguido, necesaria y proporcionada, dado que no existían otros medios igual de eficaces de proteger los derechos del empresario que interfirieran menos con el derecho de las demandantes al respeto de su vida privada.

Sin embargo, en este caso el TEDH entiende que la injerencia no es conforme con el art. 8 CEDH, por la falta de trasparencia y por violación del principio de proporcionalidad. Concretamente, estimará el Tribunal, en primer lugar, que en el asunto 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 (ap. 67). 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

[60] X. Arzoz, op. cit. págs. 427-428; D. Sarmiento, *Las sentencias del Tribunal Europeo de Derechos Humanos*, cit. pág. 69.

[61] A. Desdentado Bonete y E. Desdentado Daroca, "*La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador*", cit. págs. 14-15 del documento electrónico; J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador…",* cit. pág. 18-19. Ésta es la doctrina que viene manteniendo la AEPD, véase J. Mercader, *Protección de datos en las relaciones laborales*, Claves prácticas F. Lefebvre, 2018, pág. 115.

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 (ap. 69). En segundo lugar, la videovigilancia encubierta no era la consecuencia de una sospecha justificada contra las demandantes y, en consecuencia, no iba dirigida específicamente a ellas, sino a todo el personal que trabajaba en las cajas registradoras, durante semanas, sin límite de tiempo y durante todas las horas del trabajo (ap. 68).

Por último, subraya la sentencia STEDH 5-9-2017, *asunto Barbulescu*, que las autoridades internas deben velar para que los empleados, cuyas comunicaciones hayan sido objeto de seguimiento, puedan presentar un recurso ante un órgano judicial que tenga competencia para pronunciarse, al menos en esencia, sobre el cumplimiento de los criterios antes expuestos y la legalidad de las medidas impugnadas.

7. SOBRE LA OPERATIVIDAD DEL CANON O TEST DE LEGITIMIDAD DE LA SENTENCIA *BARBULESCU* Y EL MARGEN DE APRECIACIÓN DE LOS TRIBUNALES NACIONALES

En síntesis, la sentencia STEDH 5-9-2017 entiende que en el caso enjuiciado no se supera la aplicación del test de legitimidad de las medidas empresariales, porque 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 (apartados 120, 121 y 139).

La opinión disidente a la sentencia (emitida por seis jueces del Tribunal) discrepa en sus conclusiones de la mayoría. Conforme a esta opinión, las jurisdicciones nacionales juzgaron, sobre la base de los documentos en su posesión, que el trabajador demandante había sido suficientemente advertido de que sus actividades, incluido el uso del ordenador que el empleador puso a su disposición, podía ser objeto de vigilancia. En consecuencia, el demandante podía razonablemente esperar que sus actividades fuesen vigiladas (ap. 20).

Como ya he indicado, la novedad de la STEDH 5-9-2017, *asunto Barbulescu*, está sobre todo en la fijación de un canon de garantías más acabado, que básica-

mente ya tenía acogida en la normativa y documentos internacionales, así como en la jurisprudencia del TEDH (finalidad legítima, proporcionalidad, transparencia). La cuestión ahora es la operatividad de dicho canon o test de legitimidad. Recordemos que el Tribunal subraya que se trata de criterios que las autoridades nacionales "deberían tener en cuenta" (ap. 120), y por tanto que las autoridades judiciales nacionales gozan de cierta discrecionalidad en su valoración de conjunto, debiendo limitarse el Tribunal a valorar si la argumentación de los tribunales nacionales es pertinente y suficiente.

Es interesante comprobar como en la posterior STEDH 22-2-2018, *asunto Libert contra Francia*, el TEDH hace una interpretación menos estricta sobre la aplicación por los tribunales nacionales del test de legitimidad. En el caso, la empresa cuenta con un código deontológico conforme al cual los trabajadores deben utilizar los medios informáticos a su disposición con fines exclusivamente profesionales. No obstante, se tolera un uso personal puntual y razonable del correo electrónico y de Internet con el fin de facilitar la vida práctica o familiar siempre que no sea susceptible de afectar a la calidad del servicio asociado. La información privada debía identificarse claramente como tal (la opción "Privado"). Tras unos meses de suspensión de empleo por otro motivo, por tanto, en ausencia del trabajador, la empresa había analizado el disco duro de ese ordenador sin informar al mismo.

Para el TEDH existe un fin legítimo. El Tribunal se limita a considerar que la injerencia buscaba garantizar la protección de los derechos del empleador, "que legítimamente puede querer asegurarse de que sus empleados utilizan los equipos informáticos puestos a su disposición para el desempeño de sus funciones, conforme a sus obligaciones contractuales y a la reglamentación aplicable" (ap. 46). Además, el TEDH entiende que el derecho al respeto de su vida privada no era obstáculo para que su empleador abriera los archivos en causa, dado que éstos no habían sido debidamente identificados como de carácter "privado", sino como "personales" (ap. 50), confirmando la argumentación del Tribunal de Casación francés, 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" (ap. 49). El Tribunal recuerda 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 de la interpretación del órgano judicial nacional con el Convenio (ap. 51). Hay que recordar que esta argumentación está en la base del voto particular a la sentencia de la Gran Sala en el *asunto Barbulescu*.

El TEDH parece facilitar en este asunto un importante margen de valoración

a los tribunales nacionales en la aplicación del test de legitimidad de la injerencia empresarial en la privacidad del trabajador, al menos en contraposición al control estricto que el TEDH ejerce sobre la labor de los tribunales nacionales en la STEDH 5-9-2017, *asunto Barbulescu*. ¿El mero interés empresarial en el buen uso de las TIC es un fin concreto y específico para justificar la injerencia? ¿El dato formal de la calificación por el trabajador de los archivos como "personales" y no "privados", así como que el demandante había utilizado una parte importante de la capacidad de su ordenador profesional para almacenar los archivos en causa justifican la injerencia en dichos archivos "personales" y en el acceso a su contenido?. La gran novedad de la STEDH 5-9-2017, *asunto Barbulescu*, las garantías de transparencia de la política empresarial de vigilancia en el tratamiento de datos brillan por su ausencia: la notificación previa y clara al trabajador de la posibilidad de un control de los archivos del ordenador; la información previa sobre la naturaleza y alcance de la vigilancia a que podía a ser sometido, así como del grado de intrusión en su vida privada.

En definitiva, la STEDH 5-9-2017, *asunto Barbulescu*, supone un avance en la clarificación de criterios a tener en cuenta en la aplicación del art. 8 CEDH, pero se trata de un avance que conviene relativizar teniendo en cuenta que el TEDH considera necesario valorar las decisiones impugnadas a la luz del conjunto de la causa y respetar el margen de apreciación del que disponen los tribunales nacionales, bastando al Tribunal con que la argumentación de los mismos sea pertinente y suficiente.