

EL CONTROL DEL CORREO ELECTRÓNICO EN EL ÁMBITO LABORAL

THE CONTROL OF ELECTRONIC MAIL IN THE LABOR FIELD

Antonio Felipe Delgado Jiménez¹ – <https://orcid.org/0000-0002-1620-2737>

Resumen

DERECHO AL SECRETO DE LAS COMUNICACIONES Y A LA PROTECCIÓN DE DATOS PERSONALES: secreto de las comunicaciones y protección de datos personales en el ámbito laboral. Vigilancia en el marco de un proceso de despido: interceptación y transcripción de mensajes electrónicos personales en el lugar de trabajo constando prohibición por parte de la empresa. Falta de comprobación por los tribunales internos de si el empresario había notificado previamente al demandante de la posibilidad de que sus comunicaciones iban a ser controladas y de si había sido informado del alcance de la vigilancia y del grado de intrusión en su vida privada y correspondencia: falta de justificación de los motivos para la introducción de las medidas de control y de si hubiera sido posible utilizar otras medidas menos intrusivas: ausencia de justo equilibrio entre los intereses del empleador y el derecho del demandante al respeto de su vida privada: violación existente.

Palabras Clave: Protección de datos personales; secreto de las comunicaciones; obligaciones positivas de los Estados; deber de información previa; proporcionalidad.

Abstract

RIGHT TO THE SECRET OF COMMUNICATIONS AND THE PROTECTION OF PERSONAL DATA: secrecy of communications and protection of personal data in the workplace. Surveillance in the framework of a dismissal process: interception and transcription of personal electronic messages in the workplace, including prohibition by the company. Lack of verification by the domestic courts of whether the employer had previously notified the complainant of the possibility that his communications were to be controlled and of whether he had been informed of the scope of the surveillance and the degree of intrusion into his private life and correspondence: lack of justification of the reasons for the introduction of control measures and whether it would have been possible to use other less intrusive measures: lack of a fair balance between the employer's interests and the plaintiff's right to respect for his private life: existing violation.

¹ Abogado. Chief Executive Officer, CEO at CAIBEREC. Professor at Carlos III University of Madrid. *E-mail:* antdelga@ucm.es

Keywords: Protection of personal data; secrecy of communications; positive obligations of the States; duty of prior information; proportionality.

Sentencia objeto de comentario: STEDH, *Barbulescu c. Rumanía*, núm. 2017/61, 5.09.2017.

Sumario: 1. – Introducción. 2. – Resumen de la sentencia. 2.1. – La STEDH –Sección Cuarta – de 12.01.2016 (Barbulescu I). 2.2. – La STEDH de fecha 5.09.2017 (Barbulescu II). 2.2.1. – La aplicabilidad del art. 8 en los casos de control de la mensajería instantánea desde un ordenador de la empresa. 2.2.2. – Las obligaciones positivas requeridas a los Estados en orden a la protección de los derechos consagrados en el art. 8 CEDH. 2.2.3. – La proporcionalidad de la intervención: el Test Barbulescu de Garantía de la Privacidad (TBGP). 2.2.4. – La resolución del caso. 3. – Derecho español. 3.1. – El impacto de la STEDH en la doctrina sentada por el Tribunal Constitucional y el Tribunal Supremo. 3.1.1. – Los derechos fundamentales afectados. 3.1.2. – El criterio de la expectativa del derecho. 3.1.3. – La recuperación del test de proporcionalidad. 4. – Conclusiones. 5. – Referencias bibliográficas.

Recibido/Received 27.06.2019 – Aprobado/Approved 24.07.2019

1 INTRODUCCIÓN.

El objetivo de este artículo es el análisis de la doctrina sentada en la STEDH núm. 2017/61 de fecha 5.09.2017 (*caso Barbulescu c. Rumanía*, cuyos hechos son los siguientes:

El caso tiene su origen en una demanda (núm. 61496/08) dirigida contra Rumanía presentada ante el Tribunal el 15.12.2008 por un ciudadano rumano, el señor Bogdan Mihai Bărbulescu (“el demandante”), en virtud del artículo 34 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en adelante, “CEDH” o “el Convenio”).

El demandante trabajaba para una empresa privada (en adelante “la empresa empleadora”) como ingeniero de ventas. A petición de su empresa creó una cuenta *Yahoo Messenger* (servicio de mensajería en línea que ofrece una transmisión de texto en tiempo real en internet) con el fin de recibir y responder a preguntas de los clientes. El reglamento interno de la empresa prohibía la utilización por parte de los empleados de los recursos de la empresa en los siguientes términos: Artículo 50. – “*Está estrictamente prohibido perturbar el orden y la disciplina en el recinto de la empresa y particularmente (...) usar los ordenadores, fotocopiadoras, teléfonos, el télex y la máquina de fax con fines personales*”. No obstante, este reglamento no incluía ninguna mención sobre la posibilidad de la empresa de vigilar las comunicaciones de sus empleados. Se desprende de los documentos presentados al expediente por el Gobierno que el demandante había sido informado del reglamento interno de la empresa y lo había firmado tras haberlo leído.

El 13.06.2007 el demandante fue convocado por su director. La convocatoria le informaba de que se habían supervisado sus conversaciones en *Yahoo Messenger* y que ciertos elementos indicaban que había utilizado Internet con fines personales contrariamente al reglamento interno. A tal efecto se adjuntaban gráficas que indicaban

que su navegación por Internet era superior a la del resto de sus colegas y 45 páginas de transcripción de las comunicaciones que el demandante había mantenido con su hermano y su novia que trataban de temas privados, siendo algunas de ellas de carácter íntimo, motivo por el que fue despedido el día 1.08.2007.

El actor reclamó ante los tribunales nacionales rumanos, los cuales desestimaron su queja y confirmaron la legalidad de la decisión de despido por parte de la empresa. No conforme con esa decisión, el demandante eleva su queja ante el TEDH, siendo asignada la misma a la sección cuarta de este Tribunal, la cual emite un fallo el 12.01.2016 (seis votos a favor contra uno), siendo su respuesta negativa al considerar que no existió vulneración del derecho al secreto de comunicaciones, sino un mero ejercicio del poder empresarial de dirección y de control de la actividad de los trabajadores.

No conforme el demandante con esta decisión, este solicita la remisión del asunto a la Gran Sala del Tribunal, la cual dicta sentencia favorable a los intereses de aquel el día 5.09.2017 y revocando la resolución de la sección cuarta de fecha 12.01.2016.

2 RESUMEN DE LA SENTENCIA.

2.1 La STEDH –Sección Cuarta – de 12.01.2016 (Barbulescu I).

La primera de las sentencias del TEDH que integran el caso Barbulescu c. Rumanía data de fecha 12.01.2016, siendo dictada la misma por la Sección Cuarta de este Tribunal y, aunque en la misma se afirmaba –como se había establecido por los jueces rumanos–, que el empleador accedió a la cuenta profesional del trabajador creyendo que solo existían comunicaciones de índole profesional y sin voluntad de control, no obstante contiene una afirmación verdaderamente discutible, a saber: que si no existe una normativa nacional aplicable con reglas claras no resulta irrazonable que el empresario pueda controlar la efectiva prestación de trabajo por los asalariados a lo largo de la jornada laboral aunque, en principio, no existan elementos de afectación negativa para la productividad o el patrimonio empresarial.

Conviene recordar que la demanda debía examinarse desde el punto de vista de las obligaciones positivas de los Estado creadas por el CEDH ya que, por ser un empleador privado, no podía comprometer la responsabilidad del Estado. El TEDH debía pronunciarse sobre si el Estado rumano, como parte de sus obligaciones positivas, había llevado a cabo un justo equilibrio entre el derecho del demandante al respeto de su vida privada y de su correspondencia y los intereses del empleador. A tal efecto, el TEDH asumió íntegramente el planteamiento de los tribunales nacionales y concluyó que *“la monitorización ha sido razonable”*, por lo que, en atención a las circunstancias concretas, prevalece el derecho de la empresa a comprobar el cumplimiento de las obligaciones laborales frente al derecho a la intimidad y al secreto de las comunicaciones del empleado, entendiéndose razonable el Tribunal que un empresario quiera verificar que los empleados están realizando sus tareas profesionales durante las horas de trabajo.

No obstante, la sentencia contiene un extenso y acertado voto particular que formula el magistrado Paulo Pinto de Albuquerque. En él se destaca que el poder de control empresarial sobre el uso de los medios informáticos no es absoluto, discrecional y arbitrario, siendo necesario que concurra una justificación basada en la protección de otros derechos que no sean la mera productividad, así como un conocimiento previo por

parte de los asalariados de las medidas adoptadas al respecto por el empleador (lo que se descarta en este caso), entrando la misma en abierta contradicción con sus precedentes (*casos Halford y Copland c. Reino Unido*).

2.2 La STEDH de fecha 5.09.2017 (Barbulescu II).

Tras la Sentencia de la Sala Cuarta, el demandante solicitó que el asunto fuera conocido por la Gran Sala, siendo aceptada esa petición con fecha 6.06.2016 y dictándose finalmente Sentencia el 5.09.2017 en la que partiendo de los hechos probados en sede judicial nacional, la Gran Sala llega a una solución distinta de la de la sentencia de 2016 y concluye que los tribunales nacionales no realizaron una adecuada valoración entre los intereses del trabajador a la protección de su vida privada y correspondencia y el interés del empresario por controlar la actividad de su empleado.

Para apreciar en sus justos términos la radical ruptura de esta última sentencia con su precedente doctrinal es necesario revisar en detalle los argumentos ya que en este caso además de ser importante el resultado también resulta de gran interés el *iter* recorrido para llegar a dicha conclusión, el cual comienza con el examen de la aplicabilidad del art. 8 en el control de la mensajería instantánea a través de Internet desde un ordenador de la empresa; continúa señalando las obligaciones positivas que se requieren de un Estado miembro para cumplir con la protección de los derechos consagrados en el art. 8 y concluye con la valoración acerca de si los tribunales nacionales han ponderado previa y adecuadamente los intereses en conflicto.

2.2.1 La aplicabilidad del art. 8 en los casos de control de la mensajería instantánea desde un ordenador de la empresa.

Parte la Gran Sala del repaso de su dilatada y asentada jurisprudencia sobre la noción de “vida privada” recordando que dicho concepto debe ser interpretado de forma amplia no siendo el mismo susceptible de una definición exhaustiva y dejando claro que, en todo caso, la esfera de vida privada protegida en el art. 8 no se puede restringir al círculo más próximo de la persona ni excluir el mundo exterior, incluyéndose en el mismo las actividades profesionales de tal forma que restricciones que afecten a la vida profesional de una persona quedan protegidas por el art. 8 del Convenio “*cuando repercuten sobre la manera en que el individuo forja su identidad social por el desarrollo de relaciones con otros sujetos*”, enfatizando que es en el ámbito de las relaciones de trabajo donde tales relaciones se dan en mayor medida².

El TEDH parte, de este modo, de una noción amplia del concepto “vida privada”, la cual cubre no solo las injerencias de terceros en el círculo más íntimo de la persona, sino que incorpora también otros elementos tales como la esfera de

² GARCÍA VITORIA, I., “La protección de datos como eje de la jurisprudencia del Tribunal de Estambul sobre la privacidad del trabajador y el control empresarial”, en <http://eapc-rcdp.blog.gencat.cat/2018/02/28/la-proteccion-de-datos-como-eje-de-la-jurisprudencia-del-tribunal-de-estambul-sobre-la-privacidad-del-trabajador-y-el-control-empresarial-ignacio-garcia-vitoria/>

autodeterminación personal en el seno de las relaciones sociales, confirmando con ello que el art. 8 del Convenio protege el derecho de la persona a establecer y desarrollar relaciones con sus semejantes, siendo este un derecho que le acompaña y que no puede descartarse en un contexto público en el que se incluye, sin duda alguna, el ámbito laboral³. A tal efecto señala la Gran Sala que “*el ámbito de trabajo es una esfera donde las personas encuentran una mayor oportunidad para desarrollar relaciones con otros, de modo que las restricciones que afecten a la propia esfera de desenvolvimiento de su vida personal en el desempeño de sus tareas profesionales en el trabajo, quedan dentro de la protección del art. 8 CEDH*”⁴.

Y con respecto a la protección de la privacidad de la correspondencia, también se procede al repaso de la numerosa jurisprudencia del Tribunal, recordando, entre otras, la Sentencia *Copland c. Reino Unido* y la protección de los mensajes electrónicos enviados desde el lugar de trabajo. Para la Gran Sala, la comunicación electrónica es una forma de comunicación que debe ser protegida en cuanto forma parte del “*ejercicio de una vida privada social*”, siendo cuestión distinta la de los límites que pueden establecerse a su ejercicio, los cuales son abordados más adelante por la sentencia. Al amparo de los principios reseñados, y descendiendo al caso particular de la mensajería instantánea, confirma el Tribunal que “*este tipo de servicio de mensajes es tan solo una forma más de comunicación que permite al individuo tener una vida social, por lo que el envío y recepción de los mensajes está protegido por la noción de correspondencia incluso cuando se envía desde el ordenador de la empresa*”⁵, conduciendo esta doctrina a una noción de vida privada más acorde con la nueva realidad de la informática y de las telecomunicaciones y que conlleva proteger “lo privado” de manera diferente. Por lo demás, deja claro que vida privada y correspondencia son derechos con contornos diferentes pero que están estrechamente conectados por constituir ambas proyecciones de la dignidad humana⁶.

Finalmente se plantea el Tribunal si la prohibición del empresario de utilizar los medios informáticos para fines personales deja al trabajador sin una expectativa de privacidad y, de ser así, hasta qué punto ello está permitido, sosteniendo que “*sea como fuere, las instrucciones de un empleador no pueden reducir la vida social privada del trabajador a cero. El respeto de la vida privada y de la confidencialidad de la correspondencia siguen existiendo aun cuando estas pudieran estar restringidas en la medida de lo necesario*”, afirmación esta que afecta de modo particular a nuestros tribunales como más adelante tenderemos ocasión de ver.

Para la mayoría de la Sala, de los hechos probados en sede judicial nacional no puede extraerse la conclusión de que la parte ahora recurrente fuera informada “*por anticipado de la extensión y de la naturaleza de la vigilancia llevada a cabo por su empleador*” ni tampoco de que este tuviera posibilidad de “*acceso al*

³ GALLARDO MOYA, R., “Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5.09.2017 en el caso *Barbulescu II c. Rumanía*”, en *RDS*, núm. 79, 2017, pág. 145.

⁴ Cfr. Ordinales 70-71 STEDH –Gran Sala – de 5.09.2017 (caso *Barbulescu c. Rumanía*).

⁵ Cfr. Ordinal 74.

⁶ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 146.

contenido de sus comunicaciones”. Tampoco considera debidamente acreditado que el trabajador hubiera tenido un conocimiento razonable de las limitaciones que iban a imponerse a su vida privada y a la confidencialidad de sus comunicaciones, limitaciones que ciertamente pueden establecerse solo “*en la medida necesaria*” y de las que ha de tener un conocimiento previo y preciso el trabajador, así como tampoco queda claro que las normas restrictivas de la empresa dejarán al demandante con la expectativa razonable de privacidad. De cualquier modo, lo verdaderamente relevante a los efectos que nos ocupa es que las instrucciones de una empresa no pueden anular en ningún caso el ejercicio de la privacidad social en el puesto de trabajo, sino que el respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario, aunque podrán modularse en la medida necesaria.

Todo ello lleva a la Gran Sala a considerar que el art. 8 del CEDH es aplicable al litigio enjuiciado en cuanto que las comunicaciones efectuadas desde el lugar de trabajo están protegidas por las nociones de “vida privada” y de “correspondencia”, habiendo sido violado el mismo.

2.2.2 Las obligaciones positivas requeridas a los Estados en orden a la protección de los derechos consagrados en el art. 8 CEDH.

¿Cuál es el parecer de la Gran Sala? En primer lugar se pronuncia, con un amplio y detallado análisis, sobre si el asunto en cuestión concierne a una obligación negativa o a una positiva por parte del Estado, concluyendo a favor de la segunda opción, recordando el margen de apreciación del que goza todo Estado para gestionar y encontrar un equilibrio entre los intereses en juego⁷, si bien llega a reconocer que hasta ahora han sido muy escasos los Estados que han abordado la problemática del ejercicio de los derechos a la vida privada y a la correspondencia en el lugar de trabajo aunque ello no sea reprochable a los Estados, los cuales gozan de un amplio margen de discrecionalidad para valorar la necesidad o no de un desarrollo legislativo en la materia basándose en las características particulares de la legislación laboral, la cual debe dejar margen de maniobra a la negociación colectiva, añadiéndose, además, que las medidas de tutela no se deben buscar únicamente en la legislación laboral, sino que son igualmente relevantes las garantías que establezca la legislación civil, penal y administrativa⁸, planteando el debate en torno a las obligaciones de las autoridades administrativas y judiciales para situar el foco sobre los jueces de lo laboral e incidir de modo especial en que los jueces nacionales deben examinar si el trabajador ha sido informado previamente de la posibilidad de que el empresario aplique medidas de control de las comunicaciones, al tiempo que precisa que la notificación debe ser clara y precisa

⁷ GARCÍA VITORIA, I., “La protección de datos como eje de la jurisprudencia...”, *op. cit.*

⁸ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 147.

acerca de la naturaleza de las medidas de control, adoptando el Tribunal⁹, como referencia principal, la normativa sobre protección de datos al objeto de exigir que el trabajador tenga información previa, clara y concreta sobre los sistemas de vigilancia, apoyándose para ello en el principio de transparencia que respaldan el Comité de Ministros del Consejo de Europa –Recomendación CM/REC (2015)– y el Grupo de Trabajo del art. 29 sobre Protección de Datos que existe en la Unión Europea. A tal efecto, dice literalmente la sentencia que “*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*”, al tiempo que hace un llamamiento expreso a que la proporcionalidad y las garantías procesales contra el carácter arbitrario sean elementos esenciales de valoración.

2.2.3 La proporcionalidad de la intervención: el Test Barbulescu de Garantía de la Privacidad (TBGP).

Las Sentencias de Sección y Gran Sala divergen, además, en el examen de la proporcionalidad de la intervención. La Sección Cuarta fue deferente con las autoridades nacionales adoptando un escrutinio basado en la determinación de si los tribunales internos habían ponderado adecuadamente el derecho a la vida privada del trabajador y los intereses del empresario, analizándose fundamentalmente la motivación de las sentencias nacionales. Por el contrario, la Gran Sala asume una posición más intervencionista y garantista estableciendo criterios detallados sobre cómo se deben valorar las medidas disciplinarias adoptadas por la empresa y revisando, además, de forma minuciosa la valoración de los hechos que hicieron los jueces nacionales¹⁰.

Señala la sentencia que el examen de la proporcionalidad debe modularse en función de la intensidad del control empresarial, para lo cual resulta determinante valorar si se accede al contenido de los mensajes, la amplitud de las comunicaciones sometidas a vigilancia, la duración del control o el número de personas que tienen acceso a los resultados. Al mismo tiempo, debe ponderarse la severidad de las medidas disciplinarias adoptadas por el empresario, especificando la Gran Sala que los controles que supongan un acceso por parte del empresario al contenido de las comunicaciones deben someterse a un control de proporcionalidad más intenso, para terminar señalando que los jueces nacionales debieron realizar un examen más estricto de la proporcionalidad del control empresarial, considerando insuficiente la motivación de las sentencias internas acerca de los fines que justificarían el acceso al contenido de los mensajes y sobre la existencia de medios alternativos de control menos restrictivos de la privacidad del trabajador¹¹.

⁹ GARCÍA VITORIA, I., “La protección de datos como eje de la jurisprudencia...”, *op. cit.*

¹⁰ ROJO TORRECILLA, E, De Barbulescu I a Barbulescu II. Notas a la importante sentencia de 5.09.2017, y amplio recordatorio de la sentencia de la Sala Cuarta de 12.01.2016, en www.Eduardorojotorrecilla.es

¹¹ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 149.

El test Barbulescu de Garantía de la Privacidad (TBGP), como ha sido bautizado, es ya de obligada referencia en los casos de vigilancia de las comunicaciones, ya sea por correo electrónico o a través de la mensajería instantánea, cuando se use el ordenador de la empresa, pero considero que el mismo es también aplicable a cualquier supuesto de vigilancia electrónica o informática, video vigilancia¹², etc. de modo que para dilucidar, en cada caso concreto, si los actos de vigilancia respetan los derechos a la vida privada y a la correspondencia los órganos jurisdiccionales habrán de examinar los siguientes parámetros:

1. – En primer lugar se habrá de comprobar si la vigilancia se ha hecho con conocimiento del trabajador, lo cual exige indagar acerca de si este ha sido informado de la posibilidad de que el empresario fuese a adoptar medidas para controlar la correspondencia u otras comunicaciones, así como de la puesta en práctica de las medidas, debiendo ser la información previa, precisa, transparente y específica. Con ello deja claro que no es suficiente con que la empresa tenga protocolos o reglas internas que prohíban el uso de los medios técnicos para fines personales, sino que será necesario, además, que la empresa previamente avise sobre los controles que pudiera llevar a cabo, así como de los medios que piensa utilizar al efecto¹³.

Asimismo, habrá que determinar cuál ha sido el alcance de la vigilancia y su grado de intromisión en la vida privada del trabajador. En este sentido, el Tribunal identifica otros elementos de juicio que permiten valorar si hubo o no extralimitación en la vigilancia, como son: distinguir entre el control de las comunicaciones o frecuencia y su contenido; también si han estado sujetas a vigilancia todas las comunicaciones o solo parte de ellas; otro aspecto relevante es también si la fiscalización de las mismas fue o no por tiempo limitado y, por último, el número de personas que tuvieron conocimiento del resultado de la vigilancia.

2. – En segundo lugar, se impone la obligación de someter el control al test de proporcionalidad. En este sentido, señala la sentencia que hay que examinar si el empleador ha proporcionado previamente un motivo legítimo que justificara la vigilancia de las comunicaciones y el control de su contenido, teniendo en cuenta que el control del contenido de las comunicaciones requiere de una justificación más fuerte y más fundamentada, debiendo valorarse, asimismo, si hubiera sido posible utilizar un sistema de control menos invasivo que el hecho de acceder directamente al contenido de las comunicaciones¹⁴. O, dicho en otros términos, si el objetivo perseguido por el empresario hubiera podido alcanzarse sin necesidad de acceder al contenido de las comunicaciones. De igual modo, hay que analizar las consecuencias que ha tenido para el trabajador la medida de vigilancia y si la misma ha resultado

¹² GOÑI SEIN, J. L., “Nuevas tecnologías digitales, poderes empresariales y derecho de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016”, en *Revista de Derecho Social*, núm. 78, 2017.

¹³ MOLINA NAVARRETE, C., “De Barbulescu II a López Ribalda: ¿qué hay de nuevo en la protección de datos de los trabajadores?”, en *Revista de Trabajo y Seguridad Social del CEF*, núm. 419, febrero 2018.

¹⁴ PRECIADO DOMÉNECH, C. H., Comentario de urgencia a la Sentencia del Tribunal Europeo de Derechos Humanos de 5.09.2017. Caso Barbulescu contra Rumanía (Gran Sala). Recuperando la dignidad en el Trabajo. *Blog de la Comisión delo Social de juezas y jueces para la democracia*.

útil para alcanzar el objetivo perseguido con el control, así como también habrá de valorarse si el trabajador ha dispuesto de las debidas garantías al respecto¹⁵.

Por último, a modo de recordatorio, insiste el Tribunal en que las autoridades nacionales, de acuerdo con las obligaciones positivas de tutela del art. 8 del Convenio, deberían asegurar al trabajador, cuando sus comunicaciones han sido vigiladas, el derecho a un recurso ante un órgano jurisdiccional para que dictamine, al menos en esencia, según los criterios descritos anteriormente, acerca de la licitud de las medidas objeto de controversia.

2.2.4 La resolución del caso.

Concluida la operación de delimitación genérica de las obligaciones positivas, el siguiente paso consiste en la aplicación de los principios reseñados a la resolución del caso concreto, partiendo para ello la Gran Sala del examen que han realizado los Tribunales nacionales de primera instancia y apelación a fin de valorar si han conjugado adecuadamente los intereses y derechos en conflicto.

Sin negar en ningún momento que los tribunales nacionales identificaron correctamente los intereses en juego así como los principios legales aplicables, la sentencia señala que el Tribunal de apelación tuvo en consideración que la vigilancia del uso de Internet y de las comunicaciones electrónicas en el lugar de trabajo estaba gobernada por los principios establecidos en la Directiva 95/46/CE e hizo indicación expresa de los principios de finalidad, transparencia, legitimidad, proporcionalidad, exactitud de datos, seguridad y formación personal¹⁶. Sin embargo, parece que estos omitieron verificar otros elementos centrales que incidían directamente en el resultado de la valoración. En concreto, según se analiza en la sentencia, no se comprobó si el trabajador había sido informado previamente de la posibilidad de que el empresario podría vigilar y tampoco sobre el alcance y naturaleza de la misma, sino que todo parece indicar que los Tribunales nacionales no identificaron en qué momento el empleador había accedido a las comunicaciones, lo que a juicio del Tribunal es particularmente importante dado que el hecho de admitir que el acceso a las comunicaciones puede hacerse en cualquier momento del proceso disciplinario va en contra del principio de transparencia¹⁷.

De igual modo entiende que no se procedió a comprobar por los Tribunales nacionales el alcance de la vigilancia y el grado de intromisión en la vida privada del trabajador, ni se examinaron las razones justificadoras de la introducción de las medidas de vigilancia, así como tampoco valoraron suficientemente si el objeto perseguido por el empleador podría haberse logrado con métodos menos invasivos y sin necesidad que acceder al contenido de las comunicaciones y, por último, no se tuvieron en cuenta las consecuencias de la vigilancia para el trabajador, que recibió la máxima sanción al efecto con su despido¹⁸.

¹⁵ CABEZA PEREIRO. J., “La protección jurisdiccional de los derechos humanos y libertades fundamentales de los trabajadores ante el TEDH”, en *Revista de Derecho Social*, núm. 69, 2015.

¹⁶ Cfr. Ordinal 131.

¹⁷ Cfr. Ordinal 138.

¹⁸ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 149.

Teniendo en cuenta todas las circunstancias anteriores el Tribunal concluye que las autoridades nacionales no guardaron un equilibrio entre los intereses en juego y, por tanto, no otorgaron protección suficiente al derecho de respeto a la vida privada y correspondencia y, consecuentemente, existió una violación del art. 8 del Convenio.

3 DERECHO INTERNO.

La riqueza de los contenidos de la sentencia de la Gran Sala del TEDH y el papel que reserva el art. 10.2 CE a su doctrina deja claro que estamos ante un pronunciamiento que está llamado a asumir una notable relevancia o como ha dicho el Magistrado Carlos Hugo Preciado Domenech, ante “una resolución que marcará época”¹⁹.

No cabe duda de que a partir de ahora los órganos jurisdiccionales deberán tener en cuenta la doctrina Barbuлесcu II y el conjunto de reglas o pautas que establece para orientarse en la valoración de la vigilancia informática y de las comunicaciones, lo cual dará cierto grado de certidumbre, tan necesaria en la tutela de los derechos fundamentales. Pero hay otra consecuencia igualmente importante, a saber: la necesidad de revisar la última doctrina del Tribunal Constitucional sobre el tema, a la que habría que añadir la concerniente a la Sala Cuarta del Tribunal Supremo, que será necesario corregir en no pocos aspectos²⁰. En efecto, es importante la brecha que se abre entre la doctrina del TEDH y nuestros Tribunales en el método y en la forma de enfocar el conflicto entre los derechos fundamentales y la potestad empresarial y que como veremos a continuación alcanza aspectos centrales.

3.1 El impacto de la STEDH en la doctrina sentada por el Tribunal Constitucional y el Tribunal Supremo.

3.1.1 Los derechos fundamentales afectados.

Para empezar, uno de los puntos de obligada referencia es su impacto en los derechos afectados por el control de las comunicaciones. Tanto la primera sentencia de la Sección Cuarta del TEDH como esta última de la Gran Sala confirman que el conflicto entre la potestad de vigilancia del empresario y los derechos fundamentales del trabajador no puede restringirse únicamente a los derechos a la intimidad, en su vertiente negativa, y al secreto de las comunicaciones, sino que a ellos hay que añadir la vertiente positiva de la intimidad o el derecho a mantener el control sobre los datos personales que le atañen al trabajador (derecho a la autodeterminación informativa), pues, como se subraya en ambos pronunciamientos, la vigilancia de las

¹⁹ PRECIADO DOMÉNECH, C. H., “Comentario de urgencia a la Sentencia...”, *op. cit.*

²⁰ ROJO TORRECILLA, E., “De Barbuлесcu I a Barbuлесcu II. Notas a la importante sentencia...”, *op. cit.*

comunicaciones electrónicas en el lugar de trabajo implican una recogida y tratamiento de datos del trabajador²¹.

Así, la Sentencia de 16.01.2016 ya señalaba como un requisito básico la información previa al trabajador sobre la prohibición de uso de los medios informáticos para asuntos personales²². Pero ahora la Gran Sala condiciona la legitimidad de la vigilancia a un requisito procedimental aún más fuerte como es que la vigilancia se haya hecho con conocimiento expreso del trabajador, lo cual requiere un aviso previo suficiente y transparente sobre la política interna en relación con el uso de los instrumentos informáticos. Pero no se conforma solo con la información, sino que requiere, además, que se haya avisado de la instalación de controles y del alcance de los mismos, esto es, de cómo se va a vigilar y con qué medios²³.

No cabe duda de que la incorporación del derecho fundamental a la protección de datos, como un derecho consagrado tanto en el art. 8 CEDH y en el art. 18.4 de nuestra Constitución, impone límites al poder de vigilancia empresarial dado que este derecho atribuye al titular un conjunto de poderes o facultades que se traducen en auténticos deberes para aquellos que utilizan sus datos, lo que supone un importante avance que esperemos acabe con la resistencia de nuestros tribunales a aplicarlo, salvo la excepción que hizo el Tribunal Constitucional en las Sentencias 29/2013 y 39/2016 que lo tuvieron en consideración, si bien limitado a la video vigilancia en el trabajo.

En la STC 29/2013, de 11 de febrero, se reconoce por primera vez el deber de información previa como condición necesaria para considerar la vigilancia empresarial respetuosa con el derecho reconocido en el art. 18.4 CE, concretando el TC el alcance de la información exigible, la cual debería ser *“expresa, precisa, clara e inequívoca a los trabajadores de la finalidad del control de la actividad laboral a la que esa captación podría ser dirigida”*, así como su contenido, el cual debía versar sobre *“las características y alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósito, explicando muy particularmente que podían utilizarse para imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”*.

Un deber de información que, sin embargo, fue banalizado y ninguneado hasta límites insospechados en la STC 39/2016 de 3 de marzo, que entendió cumplido el requisito de la información previa al trabajador simplemente con el hecho de que el empresario coloque en las zonas de video vigilancia un distintivo informativo ubicado en un lugar suficientemente visible, tanto en espacios abiertos como cerrados, y tener a disposición de los interesados impresos en los que se detalle la información prevista en el art.5.1 de la LOPD. No obstante, el contenido y el diseño del distintivo habrá de ajustarse a lo previsto en el Anexo de la Instrucción 1/2006 de la AEPD (faltaría más), según el cual, el distintivo deberá incluir una referencia a la Ley Orgánica 15/1999, de protección

²¹ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 150.

²² GARCÍA GONZÁLEZ, R. y PASTOR MERCHANT, J., “Límites a la necesaria flexibilización de los derechos a la intimidad y al secreto de las comunicaciones en el ámbito laboral: una reflexión tras la sentencia del TEDH de 12.01.2016 en el caso Barbulescu”, *Diario La Ley*, N. 8715, Sección Tribuna, 4.03.2016, Ref. D-95, Editorial LA LEY.

²³ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 151.

de datos; una mención a la finalidad para la que se trataran los datos (“Zona video vigilada”) y una mención expresa a la identificación del responsable ante quien pueden ejercitarse los derechos a los que se refieren los arts.15 y siguientes de la Ley Orgánica 15/1999.

En el viraje que supone la STC 39/2016, de 3 de marzo, se observa la incidencia, con invocación expresa, de la STEDH –sección cuarta – de 12.01.2016. El TC cuida en el discurso teórico de la sentencia – como hizo el TEDH – condicionar la legitimidad final al balance valorativo exigido por las concretas circunstancias del caso, pero en la práctica termina – también como el TEDH – sacrificando para el caso el sentido práctico del Derecho, como evidencian los votos particulares de esta sentencia, de modo que bastaría con el anuncio genérico hecho al público sobre la existencia de cámaras de seguridad en el local para satisfacer el deber de información previa, suficiente y adecuada en atención a cada colectivo de interesados (art. 5 LOPD), ignorando la STC 39/2016 deliberadamente, en el ámbito laboral, ese deber de información que exige la adaptación a las singularidades del mismo, en línea con la doctrina sentada por la STC 29/2013, la cual es abandonada, sin explicación alguna, para anclarse en otras muchas más antiguas –como acertadamente le reprocha el voto particular de los Magistrados Fernando Valdés Dal-Ré y Juan Antonio Xiol Rios, muy razonados y razonables-. Sorprendentemente, la fuerza prevalente del Derecho se diluirá con la sola constatación de una pegatina informativa que reúna, eso sí, *“los exigentes requerimientos de formato establecidos en el Anexo de la Instrucción 1/2006, de 8 de noviembre de la AEPD”* – como, con fina ironía, le reprocha el Magistrado Fernando Valdés Dal-Ré-. Consecuentemente, una vez existente la pegatina con el correspondiente distintivo, y constatada una fundada sospecha, el poder de control quedará plenamente legitimado para adentrarse en la vigilancia directa del trabajador. En definitiva, una construcción dogmática como la realizada por el TC en su sentencia 39/2016 que hace de una simple Instrucción de la AEPD un elemento decisivo del juicio de constitucionalidad, ya no será posible afortunadamente.

Resulta, pues, evidente que el Tribunal Constitucional tendrá que revisar su laxa doctrina sobre el contenido de la obligación de información previa y adaptarla a los criterios más exigentes que ha marcado el TEDH, a lo que hay que añadir que a partir de mayo de 2018 es de obligado cumplimiento para los Estados miembros el nuevo Reglamento 679/2016 del Parlamento Europeo y del Consejo.04.2016, con el que se pretende unificar la regulación de los 28 países en materia de protección de datos, cuyo art. 88, regulador del tratamiento de datos en el ámbito de las relaciones laborales, prevé que los Estados miembros podrán establecer por ley o por negociación colectiva *“normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de los trabajadores en el ámbito laboral”*, enumerando una larga lista de materias entre las que cabe mencionar la ejecución del contrato, incluidos los cumplimientos establecidos por ley o por convenio colectivo, la gestión, organización y planificación del trabajo, siendo de esperar que el legislador aborde por fin esta materia o, al menos, que los interlocutores sociales la incorporen los nuevos convenios colectivos que se vayan negociando guiados por las indicaciones que marca el art. 88.2 del Reglamento, a cuyo tenor *“dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como los intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro un grupo de*

empresarial o de una unión temporal de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo”.

Asimismo, la doctrina Barbulescu II supone un paso importante de garantía y respeto de los derechos fundamentales en el contrato de trabajo al tiempo que pone en evidencia, como se ha dicho, la doctrina del TC al respecto, la cual habrá de ser profundamente revisada, de modo que no puede considerarse – como lo hizo la STC 170/2013, de 7 de octubre – que la mera prohibición por convenio colectivo o por reglamento interior del uso del ordenador para fines personales suponga una supresión de la “expectativa de intimidad” del trabajador, por lo que ningún control del ordenador podrá ampararse en tales fundamentos, sin otro añadido, como tampoco podrá seguir sosteniéndose la doctrina del TC de la “variabilidad del alcance del poder de vigilancia”, afirmando que los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin.

3.1.2 El criterio de la expectativa del derecho.

Otra cuestión que debe destacarse de la sentencia Barbulescu es que el TEDH pone límites al uso (y abuso) que, del criterio de la expectativa de derecho, se ha venido haciendo al enjuiciar las medidas empresariales restrictivas de derechos fundamentales del trabajador. Esta técnica de enjuiciamiento coloca al intérprete en una situación previa al juicio de los intereses en conflicto y determina cuál es el ámbito constitucionalmente protegido del derecho fundamental²⁴.

Tanto el Tribunal Supremo como el Tribunal Constitucional han utilizado este criterio en orden a dilucidar cuándo se está ante manifestaciones del derecho a la intimidad y del secreto de la correspondencia protegibles, siendo de obligada cita a este respecto la sentencia del Tribunal Supremo de 26.09.2007 que abordó el tema por vez primera declarando que *“existe un hábito social de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa (...) esta tolerancia crea también una expectativa general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente de control empresarial”*, de forma que una vez que el empresario, cumpliendo con los requisitos de la buena fe, informa al trabajador de las reglas de uso de los medios informáticos y de los controles que se van a realizar para supervisar el cumplimiento de los mismos, el trabajador no puede albergar expectativa razonable alguna de intimidad.

Sin embargo, tanto uno como otro Tribunal han ido paulatinamente reduciendo la expectativa de ejercicio de los derechos fundamentales en el seno del contrato de trabajo como consecuencia de la sucesiva degradación de la obligación de preavisar por parte del empresario²⁵, llegando a declarar que los trabajadores podían prever la revisión de sus correos electrónicos cuando, según el tenor de la STS de 6.10.2011, el empresario

²⁴ CASAS BAAMONDE, M^a E., “La plena efectividad de los derechos fundamentales: juicio de ponderación (¿o de proporcionalidad?) y principio de buena fe”. *Relaciones Laborales*, núm. 12, 2004, pág. 3.

²⁵ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 153.

hubiere establecido reglas absolutas que prohibieran el uso de aquel para fines personales, desapareciendo en tal caso la eventual expectativa de intimidad o confidencialidad de aquellos en sus comunicaciones electrónicas y pudiendo la empresa vigilar el uso de los medios al objeto de comprobar el cumplimiento de las obligaciones y deberes laborales por parte del trabajador.

Por su parte, el Tribunal Constitucional continuó con esta línea de anulación de derechos fundamentales en el seno de la relación laboral primero en la Sentencia 241/2012, de 17 de diciembre, en la que sostiene que la prohibición expresa por parte de la empresa de instalar programas en un ordenador de uso común, como hicieron las trabajadoras que instalaron un programa de mensajería instantánea denominado “Trillian” impide albergar cualquier expectativa de intimidad en el uso de dicho programa. Y más tarde con la polémica y criticada Sentencia 170/2013, de 7 de octubre, en la que admite sin ambages que ni siquiera es necesario que la empresa informe directamente al trabajador para romper la expectativa de confidencialidad respecto a sus comunicaciones mantenidas a través de la cuenta de correo de la empresa y del teléfono, siendo suficiente a tal efecto con el hecho de que esté previsto en el convenio colectivo del sector la tipificación como falta leve del uso de los medios informáticos para fines privados²⁶.

Con arreglo a ello, el único criterio para que el trabajador albergue una fundada expectativa de intimidad en el empleo de los medios informáticos de la empresa es que exista tolerancia al respecto o, mejor dicho, que expresamente se permita su uso personal, pues incluso la tolerancia de la empresa, como hemos visto anteriormente, puede quedar truncada si el convenio aplicable sanciona la utilización de los mismos para fines extralaborales aunque sea como falta leve.

Esta última doctrina continúa la senda de lo que piadosamente se ha venido llamando “revocación suave”²⁷ de las garantías de los derechos fundamentales del trabajador tal como habían sido elaborados por la jurisprudencia constitucional. De este modo, en relación con el uso de los medios informáticos se ha ido rebajando paulatinamente la tutela de aquellos mediante una cada vez más exigua expectativa del ejercicio de los mismos hasta el punto de admitirse que los derechos a la intimidad y al secreto de las comunicaciones garantizados por la Constitución no se modulan frente al ejercicio del poder de dirección, sino que directamente ceden ante las pautas de uso que haya podido impartir el empresario, de forma que una vez constatado que el trabajador conoce, aunque solo fuere de forma vaga la prohibición, la empresa queda legitimada para fiscalizar el ordenador y supervisar las comunicaciones e incluso su contenido hasta donde fuese necesario al objeto de supervisar la actividad o para conseguir la prueba del incumplimiento de los deberes y obligaciones del trabajador²⁸.

²⁶ El XV Convenio Colectivo de la Industria Química (BOE de 29.08.2007) tipifica en su art. 59.11 como falta leve “la utilización de los medios informáticos propiedad de la empresa (correo electrónico, Internet, etc.) para fines distintos de los relacionados con el contenido de la prestación laboral...”.

²⁷ BAYLOS GRAU, A., “La protección de los derechos fundamentales por el Tribunal Constitucional español: auge y declive de la función de tutela”, *RDS*, núm. 69, pág. 28.

²⁸ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 154.

No obstante, no parece que esta doctrina case adecuadamente con la elaborada por el TEDH. Baste simplemente con recordar que en reiterados pronunciamientos tiene declarado este Tribunal que el hecho de que el trabajador no estuviese advertido de la posibilidad de que sus comunicaciones pudieran ser objeto de seguimiento por parte del empresario, ello determinaba que aquel podía confiar en el carácter privado de sus comunicaciones, ya fuesen las mismas del tipo de llamadas telefónicas, correo electrónico, chat u otras vía Internet²⁹. Por tanto, además de la prohibición de uso para temas personales, en orden a desvirtuar la expectativa razonable de privacidad, el TEDH exige la comunicación o advertencia previa de que aquellas van a ser controladas.

Y de nuevo se vuelve a pronunciar el TEDH a través de su Gran Sala para completar su tesis argumentando al efecto que la existencia de reglas internas en las empresas que prohíban el empleo de los medios informáticos con fines privados es un dato indicativo pero no necesariamente concluyente para romper la expectativa razonable de privacidad del trabajador, considerando además que *“las instrucciones de un empleador no pueden reducir la vida social privada en el lugar de trabajo a cero; el respeto de la vida privada y de la confidencialidad de la correspondencia siguen existiendo aun cuando pudieran estar restringidas en la medida de lo necesario”*³⁰, con lo que deja bien claro que los jueces y tribunales nacionales no pueden quedarse en la mera valoración de si la decisión de la empresa es legítima por estar amparada en una norma interna que prohíba el uso de los instrumentos informáticos de aquella para fines personales, sino que deberán adoptar en su canon de enjuiciamiento las pautas enumeradas anteriormente, las cuales imponen en primer lugar verificar que el trabajador fue informado con antelación y de manera transparente, concreta y precisa de la naturaleza y alcance de la vigilancia y, además, valorar la amplitud de la medida de control atendiendo al test de proporcionalidad.

3.1.3 La recuperación del test de proporcionalidad.

Otro importante efecto es, a mi juicio, que la doctrina Barbulescu recupera en sus verdaderos términos el principio de proporcionalidad³¹ en orden a la evaluación de la licitud del control empresarial y, con ello, un canon de enjuiciamiento más equilibrado al objeto de ponderar el conflicto entre los derechos fundamentales del trabajador y las facultades del poder empresarial.

De este, en orden a la valoración de la posible restricción del ejercicio del derecho fundamental del trabajador por la vigilancia del empresario es necesario en primer lugar que este *“proporcione previamente un motivo legítimo que justifique la vigilancia de las comunicaciones y el control de su contenido”*, esto es, que exista una verdadera adecuación entre el motivo de control y la limitación que sufre el derecho a la vida privada o a la correspondencia del trabajador. Condición que choca con la tesis del Tribunal Constitucional según la cual *“los grados de intensidad o de rigidez con que deben ser valoradas y aplicadas las medidas empresariales de vigilancia y control son*

²⁹ SSTEDH de 25.06.1997 (caso Halford c. Reino Unido) y de 3.04.2007 (caso Copland c. Reino Unido).

³⁰ Cfr. Ordinal 80.

³¹ RIBAS, X., “Matizaciones sobre la sentencia del Caso Barbulescu”, en <https://xribas.com/2017/09/06/matizaciones-sentencia-caso-barbulescu/>

*variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario para tal fin*³².

Por otro lado, exige que la vigilancia haya de ser idónea, es decir, obliga a determinar si hubiera sido posible utilizar un sistema de control menos invasivo para el derecho fundamental de que se trate, de modo que habrá de valorarse si es necesario e idóneo acceder al contenido de las comunicaciones o bastará con un mero informe de la frecuencia de las mismas, obviamente menos intrusivo. En todo caso, como insiste el TEDH, teniendo en cuenta que el acceso al contenido de las comunicaciones es siempre el acto más invasivo de los derechos de vida privada y correspondencia, se requiere en su caso una justificación más fuerte o más fundamentada, de donde cabe interpretar que la intensidad de la vigilancia permitida dependerá del carácter defensivo o preventivo de la misma³³. En suma, deberá tenerse en consideración cuáles han sido las consecuencias de la vigilancia para el trabajador a los efectos de valorar los sacrificios innecesarios o excesivos de los derechos fundamentales y descartar las conductas de vigilancia o control empresarial más agresivas a los derechos de vida privada y correspondencia.

De conformidad, pues, con la doctrina sentada por la Gran Sala, la expectativa del derecho a la intimidad y a la confidencialidad en las comunicaciones deja de depender exclusivamente de las órdenes impartidas por el empresario y de su prohibición para usos extralaborales para situar el centro de valoración en la previa información al trabajador, que requiere de un aviso suficiente y claro en relación con las políticas de uso³⁴, así como sobre los controles que se vayan a realizar y de los posibles medios que se emplearán en los mismos. Con ello, la sentencia enmarca la forma de enfocar el conflicto desde una metodología más equilibrada y racional en la valoración de los derechos fundamentales del trabajador que se aleja de la perspectiva contractual que viene utilizando hasta ahora el Tribunal Constitucional. Asimismo, en consonancia con lo anterior, marca las pautas a la hora de ponderar los intereses en conflicto que descansa en el test de proporcionalidad y que comporta un análisis detallado desde la perspectiva de la idoneidad, necesidad y proporcionalidad en sentido estricto en relación con el objetivo perseguido con la vigilancia³⁵.

A la vista de lo anterior, no cabe duda de que nuestro el Tribunal Constitucional tendrá que corregir en profundidad su doctrina para adaptarla a los estándares mínimos que impone el TEDH en el control de las comunicaciones en el seno de la empresa, ya sean llevadas a cabo estas mediante el ordenador de la empresa y utilizando el correo corporativo o mediante cualquier otro sistema de mensajería instantánea en el lugar y en el horario de trabajo.

³² STC 241/2012, de 17 de diciembre.

³³ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 155.

³⁴ RODRÍGUEZ MAGARIÑOS, F. G., “El derecho al respeto a la intimidad telemática versus la sentencia “Barbulescu”, del Tribunal Europeo de Derechos Humanos: consecuencias en el orbe penal”, *La Ley Penal*, N. 118, Sección Jurisprudencia aplicada a la práctica, Enero-Febrero 2016, Editorial Wolters Kluwer.

³⁵ GALLARDO MOYA, R., “Un límite a los límites de la vida privada...”, *op. cit.*, pág. 156.

Para concluir, señalar que son numerosos los méritos de esta sentencia, pero el más sobresaliente es, a mi juicio, que sitúa a los derechos fundamentales en el lugar que les corresponde, como freno a los excesos de vigilancia y control que permiten y favorecen, sin duda, el empleo de las nuevas tecnologías.

4 CONCLUSIONES

En definitiva, la nueva doctrina del TEDH impone a los órganos jurisdiccionales la obligación de observar los siguientes estándares mínimos en los casos de vigilancia de las comunicaciones por correo electrónico y, por ende, de video vigilancia en general:

– La intimidad ha de ser interpretada en sentido amplio. A tal efecto, el TEDH mantiene un concepto amplio de vida privada que va más allá del derecho a la intimidad en sentido estricto y que se proyecta en las relaciones sociales. A tal efecto, la sentencia utiliza el término “*private social life*”, lo cual es expresivo de cuanto decimos.

– La normativa interna de las empresas no pueden reducir la vida privada social en el marco de la relación laboral a cero, sino que subsiste en todo momento una expectativa razonable de privacidad a pesar de la existencia de una prohibición expresa y reiterada de uso de los medios informáticos de la empresa con fines personales.

– La mensajería electrónica enviada desde una cuenta profesional debe considerarse correspondencia a todos los efectos.

– El análisis de estos casos habrá de ser enfocado desde la perspectiva de las obligaciones positivas, en la medida en que se cuestiona la incapacidad de los poderes públicos nacionales de reparar la lesión supuestamente infringida por las empresas privadas.

– Las medidas de tutela no se han de buscar únicamente en la legislación laboral, siendo también igualmente relevantes las garantías que establezca el orden penal o civil (obviamente, debe entenderse incluido el orden administrativo).

– El debate ha de plantearse en torno a las obligaciones de las autoridades administrativas y judiciales, situando el foco la sentencia sobre los jueces de lo laboral, de modo que configura a estos como los garantes del respeto de los derechos fundamentales de los trabajadores en el marco del contrato de trabajo, imponiéndoles obligaciones positivas o de hacer a tales efectos.

– Se habrán de justificar expresamente los motivos para establecer medidas de vigilancia, los cuales habrán de ir más allá de la genérica alusión al poder de control empresarial del art. 20.3 ET, debiendo concretarse en motivos reales, concretos y precisos.

– Se establece la necesidad de información previa al trabajador acerca de la vigilancia de su correspondencia electrónica y otro tipo de comunicaciones, así como de la concreta puesta en marcha de las medidas al respecto. Ello implica la necesidad de que dicha información haya de ser previa a la efectiva implantación de las medidas de vigilancia y habrá de ser, por lo demás, expresa, precisa y concreta, debiendo los jueces nacionales examinar si el trabajador ha sido informado previamente de la posibilidad de que el empresario aplique medidas de control de las comunicaciones.

– La notificación ha de ser clara, concreta y específica tanto acerca de la prohibición de uso del correo electrónico como de la posibilidad de establecer

mecanismos de control del mismo y de la naturaleza de las medidas de control (“the notification should normally be clear about the nature of the monitoring and be given in advance”), adoptando el TEDH como referencia principal la normativa sobre protección de datos.

– Asimismo, se impone la obligación de ponderar la necesidad y el alcance efectivo de la vigilancia realizada por el empresario poniendo en relación la finalidad pretendida con los medios utilizados para alcanzarlos, de forma que será necesario determinar si hubiera sido posible el empleo de medidas menos intrusivas al efecto. De igual modo, se habrá de tener en cuenta cuáles han sido las consecuencias de la vigilancia para el trabajador.

– El control de proporcionalidad debe modularse en función de la intensidad del control empresarial. Para ello resulta determinante valorar si se accede al contenido de los mensajes, así como determinar la amplitud de las comunicaciones sometidas a vigilancia, la duración del control o el número de personas que tienen acceso a los resultados.

– Los controles que supongan un acceso por parte del empresario al contenido de las comunicaciones deberán ser sometidos a un control de proporcionalidad más intenso.

– Asimismo, habrá de someterse a ponderación la severidad de las medidas disciplinarias adoptadas por el empresario.

5 REFERENCIAS BIBLIOGRÁFICAS.

BAYLOS GRAU, A., “La protección de los derechos fundamentales por el Tribunal Constitucional español, auge y declive de la función de tutela”, *RDS*, núm. 69.

CABEZA PEREIRO, J., “La protección jurisdiccional de los derechos humanos y libertades fundamentales de los trabajadores ante el TEDH”, en *Revista de Derecho Social*, núm. 69, 2015.

CASAS BAAMONDE, M^a E., “La plena efectividad de los derechos fundamentales, juicio de ponderación (¿o de proporcionalidad?) y principio de buena fe”. *Relaciones Laborales*, núm. 12, 2004.

GALLARDO MOYA, R., “Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5.09.2017 en el caso Barbulescu II c. Rumanía”, en *Revista de Derecho Social*, Análisis Jurisprudencia, núm. 79, 2017.

GARCÍA GONZÁLEZ, R. y PASTOR MERCHANT, J., “Límites a la necesaria flexibilización de los derechos a la intimidad y al secreto de las comunicaciones en el ámbito laboral, una reflexión tras la sentencia del TEDH de 12.01.2016 en el caso Barbulescu”, *Diario La*

Ley, N. 8715, Sección Tribuna, 4.03.2016, Ref. D-95, Editorial LA LEY.

GARCÍA VITORIA, I., La protección de datos como eje de la jurisprudencia del Tribunal de Estrasburgo sobre la privacidad del trabajador y el control empresarial, en <http://eapc-rcdp.blog.gencat.cat>

GOÑI SEIN, J. L., “Nuevas tecnologías digitales, poderes empresariales y derecho de los trabajadores, análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016”, en *Revista de Derecho Social*, núm. 78, 2017.

MOLINA NAVARRETE, C., “De Barbulescu II a López Ribalda, ¿qué hay de nuevo en la protección de datos de los trabajadores?”, en *Revista de Trabajo y Seguridad Social del CEF*, núm. 419, febrero 2018.

PRECIADO DOMÉNECH, C. H., Comentario de urgencia a la Sentencia del Tribunal Europeo de Derechos Humanos de 5.09.2017. Caso Barbulescu contra Rumanía (Gran Sala). Recuperando la dignidad en el Trabajo. *Blog de la Comisión de lo Social de juezas y jueces para la democracia*.

RODRÍGUEZ MAGARIÑOS, F. G., “El derecho al respeto a la intimidad telemática versus la sentencia “Barbulescu”, del Tribunal Europeo de Derechos Humanos, consecuencias en el orbe penal”, *La Ley Penal*, N. 118, Sección Jurisprudencia aplicada a la práctica, Enero-Febrero 2016, Editorial Wolters Kluwer.

RIBAS, X., “Matizaciones sobre la sentencia del Caso Barbulescu”, en <https://xribas.com/2017/09/06/matizaciones-sentencia-caso-barbulescu/>

ROJO TORRECILLA, E., De Barbulescu I a Barbulescu II. Notas a la importante sentencia de 5.09.2017, y amplio recordatorio de la sentencia de la Sala Cuarta de 12.01.2016, en www.Eduardorojotorrecilla.es