



JESÚS LAHERA FORTEZA

Consultor Abdón Pedrajas & Molero
Profesor Titular Dº del Trabajo UCM
jlf@abdonpedrajas.com

Nueva vuelta de tuerca sobre el control empresarial del correo electrónico corporativo de los trabajadores

Sentencia TEDH 5 septiembre 2017 (asunto barbulescu)

I. CRITERIOS DE LA JURISPRUDENCIA ESPAÑOLA]

La empresa tiene, dentro de su poder de dirección y vigilancia del art.20.3 ET, la capacidad de control del correo electrónico corporativo de los trabajadores, al ser un medio de producción de uso profesional. Pero este control debe respetar el derecho fundamental constitucional a la intimidad y al secreto de comunicaciones del art.18 CE, también reconocido, en el ámbito específicamente laboral, en el art.4.2.e ET.

La jurisprudencia española ha elaborado, al respecto, sólidos criterios que salvaguardan la intimidad y privacidad del trabajador en este tipo de control empresarial.

De inicio, son de aplicación al control de correos electrónicos corporativos, los criterios generales articulados por las **SSTC 98/2000** y **186/2000** en la salvaguarda del derecho a la intimidad del trabajador del art.18.1 CE desde la técnica clásica de la modulación de derechos personales en el contrato de trabajo. Son sentencias relacionadas con la videovigilancia pero exportables a este tipo de control. La medida empresarial de acceso al correo electrónico del trabajador debe ser:

- *"Adecuada o idónea"* para la consecución de una finalidad empresarial legítima como el control del cumplimiento del contrato de trabajo.
- *"Necesaria"*, no existiendo otra alternativa con menor riesgo de sacrificio

Hay que conseguir que los trabajadores se comprometan, que colaboren en la consecución de objetivos y que se queden •



de la intimidad personal del trabajador para la consecución de este fin legítimo.

- “Proporcionada” al fin perseguido, lo que exige contrastar la relevancia del beneficio obtenido por la empresa y el sacrificio de la intimidad personal del trabajo.

Este juicio de “*idoneidad, necesidad y proporcionalidad*” debe ser razonado en cada acceso empresarial al control electrónico corporativo de la plantilla.

Además, siguiendo las indicaciones de las **SSTS 26 Septiembre 2007, 8 Marzo 2011 y 6 Octubre 2011, 13 Septiembre 2016 y 17 Marzo 2017**, es imprescindible informar y advertir al trabajador previamente del uso y del control empresarial del correo electrónico. Sólo con esta información se puede crear una “*expectativa razonable de intimidad y confidencialidad*” del trabajador. La información debe ser clara y precisa.

Es viable que la empresa establezca reglas claras de uso del correo corporativo durante la jornada laboral, que pueden implicar la prohibición absoluta de una utilización personal,

El reclutamiento no solo se basa en el talento o la experiencia, también son importantes la actitud, la inteligencia emocional, la empatía, etc. ●

pero siempre que el trabajador sea informado de ello con claridad.

La jurisprudencia constitucional (**STC 170/2013**) ha terminado relajando este deber de advertencia, si el uso personal del correo corporativo está tipificado como infracción laboral en el convenio colectivo. Pero el TS ha seguido insistiendo en la necesidad de una información específica y clara al trabajador, que genere una expectativa de intimidad y confidencialidad.

El acceso al contenido del correo electrónico está sujeto al secreto de comunicaciones también garantizado en el art.18.3 CE. La **STC 241/2012** descarta que exista cobertura de secreto de comunicaciones en sistemas “*conocidos o asumidos*” por el trabajador. A partir de esta orden de la empresa y “*tolerancia del trabajador*” no cabe hablar de una “*expectativa razonable de confiden-*

cialidad” en los contenidos interceptados por estos medios conocidos o asumidos. Ello refuerza la necesidad de advertencia clara y previa al trabajador. Pero, como recuerda siempre el TS (recientemente en **STS 17 Marzo 2017**), el acceso al contenido de correos tampoco es ilimitado porque está protegido por el secreto de comunicaciones y sujeto, en consecuencia, al juicio de finalidad legítima y proporcionalidad, acreditado en cada caso.

Hay que señalar, incluso, que, en el orden penal, la **STS 16 Junio de 2014** aplica el secreto de comunicaciones al control de contenidos de mails corporativos de trabajadores, a los efectos de su valor probatorio en un procedimiento penal. En este ámbito, donde se dilucidan faltas o delitos del orden penal, es necesario solicitar la autorización judicial para acceder al contenido de los mails corporativos.



La nueva gestión del talento asociada a la digitalización y la tecnología dará lugar a que los RR.HH. asuman roles distintos de los de hoy •

II. CONFIRMACIÓN DE ESTOS CRITERIOS POR LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS]

La reciente sentencia del Tribunal Europeo de Derechos Humanos (TEDH) de **5 Septiembre 2017**, asunto *Barbulescu*, confirma los criterios que la jurisprudencia española viene manejando en el control de correos electrónicos corporativos de los trabajadores.

El TEDH aplica el art.8 del Convenio de Derechos Humanos, que reconoce la intimidad y privacidad, con los mismos parámetros y resultados al igual que efectuó en su sentencia de **3 Abril 2007**, asunto *Copland*. Esta sentencia matiza una anterior del propio TEDH de **12 Enero 2016**, sobre el mismo asunto, más restrictiva con la intimidad.

y advertencia previa al trabajador del posible control y su ámbito.

Esta exigencia coincide exactamente con la que viene siendo aplicada con rigor por nuestro TS y deja sin efecto la jurisprudencia menos protectora del TC, que parece avalar el control sólo con el convenio colectivo de referencia. La *“expectativa razonable de intimidad y confidencialidad”* que maneja la jurisprudencia española converge así con los requisitos marcados ahora por el TEDH.

III. PROTOCOLO DE ACTUACIÓN EN EL CONTROL DEL CORREO ELECTRÓNICO DE LOS TRABAJADORES]

Conforme a esta jurisprudencia española y del TEDH, se recomienda, por tanto, a las empresas, elaborar protocolos de actuación con estos criterios y tener cautelas en el acceso al contenido de los mails corporativos.

Es recomendable:

1. Establecer reglas empresariales de uso del correo corporativo, que puede implicar la prohibición absoluta de uso personal.
2. Información clara a los trabajadores de estas reglas empresariales de uso del correo corporativo.
3. Información a los trabajadores de los medios de control de uso del correo corporativo, con advertencia de posible acceso a su contenido si existen razones empresariales legítimas.
4. Justificación de la necesidad, adecuación y proporcionalidad del acceso empresarial al correo corporativo en cada caso.
5. Acceso al contenido de los correos de manera proporcionada al fin perseguido y de la manera menos intrusiva en la privacidad del trabajador.
6. Uso confidencial y restringido, en cualquier caso, del contenido de los correos a los que accede la empresa.
7. Solicitud de autorización judicial si existe una dimensión penal.]

La sentencia del TEDH de **5 Septiembre 2017** exige a la empresa *“razones legítimas”* que justifiquen el control del correo corporativo del trabajador y obliga a analizar si el objetivo empresarial podía lograrse con *“métodos menos intrusivos que el acceso a sus comunicaciones”*.

Estas exigencias se asemejan al *“juicio de idoneidad, necesidad y proporcionalidad”* de nuestra jurisprudencia en la salvaguarda de la intimidad y del secreto de comunicaciones, tanto en el propio acceso al correo, como en la lectura de sus contenidos.

Esta sentencia del TEDH impone a la empresa *“avisar con antelación”* al trabajador del *“control y de la amplitud”* de la vigilancia e intrusión en su vida privada. No resulta suficiente la presencia de una regla empresarial de prohibición de uso personal del correo corporativo, siendo imprescindible la información



RELACIONES
LABORALES