Comentario Laboral

La Sentencia dictada por la Gran Sala del Tribunal Europeo de Derechos Humanos en fecha 5 de septiembre de 2017, sobre el control por el empresario del uso del correo electrónico

Septiembre 2017

Recientemente la mayoría de los medios de comunicación se hacían eco de una sentencia dictada por la Gran Sala del Tribunal Europeo de Derechos Humanos en fecha día 5 de septiembre de 2017, en el asunto Barbulescu vs Rumania (exp. 61496/08), que por once votos frente seis concluye que el Estado rumano violó el artículo 8 del Convenio Europeo de Derechos Humanos.

En concreto, la STEDH (cuyo contenido es accesible en la web del TEDH y disponible en francés e inglés) sienta que constituyó una vulneración del derecho a la intimidad y al secreto de las comunicaciones vigilar los mensajes enviados por un trabajador mediante medios propios de la empresa y acceder al contenido de los mismos, si no había sido previamente informado de esta posibilidad, incluso si existían normas en la empresa que prohibían su utilización con fines personales.

1.- Los **antecedentes** del caso enjuiciado eran:

El Sr. Barbulescu trabajaba como ingeniero encargado de compras. Por petición de sus jefes, creó una cuenta en Yahoo Messenger para responder las preguntas de sus clientes. Sin embargo, pasados tres años se le informó de que su cuenta había sido monitorizada y le mostraron las evidencias del uso de dicha cuenta para asuntos personales, y en consecuencia, le comunicaron el despido.

Inicialmente el trabajador negó la utilización de la cuenta para usos o fines personales, y entonces la empresa hizo pública una transcripción de mensajes que había intercambiado con su hermano y su novia y que guardaban relación con su vida personal, y también transcribió mensajes que el trabajador había intercambiado con su novia desde una cuenta personal de Yahoo.

El Sr. Barbulescu impugnó su despido antes los tribunales alegando que la misma era nula ya que se había violado su derecho a la privacidad. Su demanda fue denegada por el tribunal de Bucarest. El Sr. Barbulescu apeló la decisión, con resultado igualmente desestimatorio, al fundamentarse el órgano judicial en la **Directiva de la UE 95/46/CE**, explicando que la misma establece que los recursos de la empresa no deben ser utilizados para fines personales y que el seguimiento y monitorización de las comunicaciones era el único método disponible para determinar si se había producido un incumplimiento disciplinario.

Basándose en el artículo 8 de la CEDH (derecho al respeto de la vida privada y familiar, del hogar y de la correspondencia), el demandante recurrió ante el TEDH alegando que la decisión de rescindir su contrato después de controlar sus comunicaciones electrónicas y acceso a su contenido se basaba en una violación de su intimidad, y que los tribunales nacionales no habían protegido su derecho al respecto de su vida privada y correspondencia.

2.- ¿Qué doctrina ha sentado el TEDH?

La STEDH determina que para evaluar la legalidad de la monitorización de las comunicaciones de los empleados deben ponderarse los siguientes elementos:

> Si el trabajador ha sido notificado de la posibilidad de que su actividad puede ser monitorizada.
>
> El grado de intromisión del empresario (durante cuánto tiempo se prolonga, a qué archivos se accede y cuántas personas acceden al resultado de la monitorización).
>
> La existencia de una razón legítima empresarial que justifique la monitorización (al ser, por defecto, una medida intrusiva e invasiva).
>
> Si podrían haberse utilizado métodos de monitorización menos intrusivos que el acceso directo al contenido de las comunicaciones del trabajador.
>
> El uso que da la empresa al resultado de la actividad de monitorización y si el mismo se utiliza para alcanzar el objetivo que justificaba la misma.
>
> La existencia de mecanismos de salvaguarda para el empleado, garantizando que el empresario no acceda al contenido de las comunicaciones sin la previa notificación al trabajador.

Estos factores deben ser valorados por los tribunales nacionales para realizar la ponderación de los intereses en conflicto (poder disciplinario del empresario frente al derecho a la intimidad y al secreto de la correspondencia del trabajador) y determinar así si la monitorización es ajustada a derecho.

En el caso planteado el Tribunal le da la razón al trabajador Sr. Barbulescu toda vez que:

Las autoridades nacionales rumanas no habían protegido adecuadamente el derecho de Barbulescu al respeto de su vida privada y su correspondencia.

Los órganos jurisdiccionales no habían determinado si el demandante había recibido una notificación previa de su empleador sobre la posibilidad de que se supervisaran sus comunicaciones.

No se había tenido en cuenta el hecho de que no se le había informado de la naturaleza o el alcance de la vigilancia ni del grado de intrusión en su vida privada y en su correspondencia.

Los órganos nacionales jurisdiccionales no habían determinado, ni las razones específicas que justificaban la introducción de las medidas de control, ni tampoco si el empleador podía haber utilizado medidas que entrañaran menos intrusión en la vida privada y la correspondencia del Sr. Barbulescu, ni si se podía haber accedido a sus comunicaciones sin su conocimiento.

3.- ¿Qué consecuencias se derivan de esta sentencia con respecto a las empresas en España? ¿Asistiremos a un cambio en la doctrina de los Juzgados y Tribunales del orden social?

A priori y en la práctica, ninguna consecuencia relevante se ha de producir. En efecto, como sienta la actual doctrina del Tribunal Constitucional (TC) y la jurisprudencia del Tribunal Supremo (TS), **las empresas deben informar al trabajador de sus políticas de control del uso de las herramientas informáticas antes de tomar medidas disciplinarias.**

Existe una línea jurisprudencial que parte de la protección de los derechos fundamentales y que ya establece la necesidad de que las restricciones al ejercicio de derechos esté debidamente justificada, sea proporcional al sacrificio de los trabajadores, y que la normativa que la imponga (sea convencional, sea de uso interno de la empresa) sea suficientemente conocida por el personal.

Más concretamente, en relación con la verificación del cumplimiento de sus deberes laborales por parte del empresario cuando se inspecciona el ordenador corporativo en el que realiza su actividad el trabajador, existen importantes pronunciamientos del TC y del TS (por todos, TC 241/2012; 170/2013; TS 20-9-07, Rec. 966/06; TS 8-3-11, Rec. 1826/10), cuya Doctrina puede resumirse del modo siguiente:

a.- Los sistemas informáticos de la empresa son un instrumento de trabajo sujeto a las facultades de control del empresario (TC 241/2012).

b.- El empresario ha de establecer unas pautas sobre el uso de los medios informáticos y advertir de la existencia de controles, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones (TC 241/2012). Si no existe advertencia sobre posibles límites de utilización y de posibilidad de realizar controles al efecto se vulnera el derecho intimidad del trabajador (TS 8-3-11, Rec. 1826/10).

c.- Cuando existe una prohibición absoluta de un uso personal, es posible su control y establecer mecanismos para controlar su uso exclusivamente laboral.

Si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no puede entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos establecidos en los siguientes pronunciamientos: TEDH 25-6-97, caso Halford; 3-4-07, caso Copland para valorar la existencia de una lesión del CEDH art.8.

d.- La misma regla rige cuando la prohibición del uso personal se contiene en el Convenio Colectivo de aplicación (TC 170/2013).

e.- El acceso empresarial a los correos del trabajador debe superar el juicio de proporcionalidad (TC 170/2013) siendo preciso que:

En primer lugar, se trate de una *medida* ***justificada*****,** que su práctica se funde en la existencia de sospechas de un comportamiento irregular del trabajador.

Que la medida sea ***idónea*** *para la finalidad* pretendida por la empresa, consistente en verificar si el trabajador cometía efectivamente la irregularidad sospechada (por ejemplo, la revelación a terceros de datos empresariales de reserva obligada y siempre con el objeto de adoptar las medidas disciplinarias correspondientes).

La medida de control debe considerarse también ***necesaria***, dado que, como instrumento de transmisión de dicha información confidencial, el contenido o texto de los correos electrónicos serviría de prueba de la citada irregularidad ante la eventual impugnación judicial de la sanción empresarial (así, en el ejemplo citado no sería suficiente a tal fin el mero acceso a otros elementos de la comunicación como la identificación del remitente o destinatario, que por sí solos no permitían acreditar el ilícito indicado).

Finalmente, la medida debe entenderse como ***ponderada y equilibrada.*** Así:

a) El control empresarial ha de realizarse con *garantías* **(**por ej.: a través de la intervención de perito informático y notario)

b) El contenido de los mensajes no ha reflejar aspectos específicos de la *vida personal y familiar del trabajador*, sino únicamente información relativa a la actividad empresarial, cuya remisión a terceros implique una transgresión de la buena fe contractual.

c) De tal forma que, atendida la naturaleza de la infracción investigada y su relevancia para la entidad, *no* pueda apreciarse que la acción empresarial de *fiscalización* haya resultado desmedida respecto a la afectación sufrida por la privacidad del trabajador.

Por contra, cuando no se establecen pautas claras en cuanto a la prohibición, existe un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores que crea una expectativa de confidencialidad en su uso, que aunque no se convierte en un impedimento del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio facilitado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio.

4.- A modo de conclusión

Desde la perspectiva de los derechos fundamentales, es esencial determinar si el acceso a los contenidos de los ordenadores u otros medios informáticos de titularidad empresarial puestos por la empresa a disposición de los trabajadores, vulnera el artículo 18.3 de la CE, para lo que habrá de estarse a las condiciones de la puesta a disposición.

El ejercicio de la potestad de vigilancia o control empresarial resulta limitado por la vigencia de los derechos fundamentales, si bien 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.

Las empresas pueden vigilar los correos internos y las redes sociales de sus trabajadores, utilizadas desde los dispositivos facilitados, pero teniendo en cuenta especialmente que aquellos deben ser conscientes, mediante un aviso o comunicación previa de que sus equipos pueden ser monitorizados. A su vez, el control debe ser proporcional, necesario y lo menos invasivo posible, evaluando el equilibrio entre el derecho del interés empresarial y la privacidad del trabajador**.**

En definitiva, lo primero que deberían delimitar las empresas, es establecer un una política, protocolo o similar regulando el uso de las citadas herramientas informáticas que haga disminuir, o incluso eliminar, lo que se ha denominado "*expectativa razonable de privacidad/intimidad*" e informar de los controles de los medios informáticos que van a existir, respetando siempre los derechos fundamentales y, particularmente, el derecho al secreto de en las comunicaciones, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

En las próximas semanas se publicarán numerosos estudios jurídicos de la sentencia del TEDH, que habrá que analizar para conocer las diferentes perspectivas de la misma. Y sobre todo esperar a próximos pronunciamientos judiciales que se hagan eco de la misma.

Para su información y conocimiento puede consultar la sentencia comentada aquí

Para más información, puede contactar con:

Alfredo Aspra
alfredo.aspra@AndersenTaxLegal.es

José Antonio Sanfulgencio
jantonio.sanfulgencio@AndersenTaxLegal.es