ASOCIACION DE JUECES Y MAGISTRADOS FRANCISCO DE VITORIA

BOLETÍN DIGITAL SOCIAL

NÚMERO 13. MARZO 2017

CORREO ELECTRÓNICO, PÁGINAS WEB, MENSAJERÍA MÓVIL Y REDES

RUBÉN LÓPEZ-TAMÉS IGLESIAS
Magistrado
Sala de lo Social del TSJ de Cantabria

Dirección
Natalia Velilla Antolín

Coordinación
Ramón Gimeno Lahoz

www.ajfv.es

CORREO ELECTRÓNICO, PÁGINAS WEB, MENSAJERÍA MÓVIL Y REDES

RUBÉN LÓPEZ-TAMÉZ IGLESIAS

Magistrado

VOCES: Prueba documental. Correo electrónico. Secreto de las comunicaciones. Derecho de defensa. Derecho a la intimidad. Página web. Redes sociales.

El presente trabajo monográfico analiza el valor probatorio en el proceso laboral de los mensajes de correo electrónico y la confrontación de los derechos al secreto de las comunicaciones y a la intimidad personal con el derecho a la defensa. Asimismo, se aborda la problemática del uso de internet en el centro de trabajo por los trabajadores y el control que el empresario puede tener sobre el adecuado uso de esta herramienta, siempre que advierta a los empleados de que pueden ser vigilados puesto que, de lo contrario, se estaría vulnerando el derecho a la intimidad de estos.

COMENTARIO

ÍNDICE: I. CORREO ELECTRÓNICO. 1. Naturaleza y aportación al proceso. 2. La intervención del correo electrónico en relación al secreto de las comunicaciones y al derecho a la intimidad. STC (Sala 1.ª) 170/2013, de 7 de octubre de 2013. A. Alegaciones del recurrente y doctrina del TS y del Tribunal Europeo de Derechos Humanos. B. Modulación de los derechos fundamentales en el ámbito laboral. C. Derecho al secreto de las comunicaciones. D. Derecho a la intimidad del demandante. II. PÁGINAS WEB Y DERECHOS FUNDAMENTALES. LA EVOLUCIÓN DE LA DOCTRINA JURISPRUDENCIAL. III. LA DOCTRINA

DE LA SALA PENAL SOBRE EL SECRETO DE LAS COMUNICACIONES Y LA NECESARIA INTERVENCIÓN JUDICIAL. IV. LA DOCTRINA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS. Asunto 61496/08, Barbulescu vs. Rumanía. Sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016. V. MENSAJERÍA MÓVIL (SMS, WHATSAPP, ETC) y REDES SOCIALES. Carga de la prueba. La demostración de la autenticidad. Primera sentencia sobre "pantallazos": Sentencia del Tribunal Supremo (Sala de Lo Penal) núm. 300/2015, de 19 mayo.

I.CORREO ELECTRÓNICO

1. Naturaleza y aportación al proceso

El correo electrónico encuentra encaje legal en la prueba de soportes o instrumentos (art. 90.1 y 384 LEC) si bien en algunos casos se le ha venido calificando como documento privado que ha de ser validado judicialmente y posibilitando así que quien afirmara su falsificación, pudiera acudir al orden penal (art. 86.2 LRJS)[1].

Esta calificación es más trascedente todavía a efectos de recurrir en suplicación, ya que la impresión de tales documentos produce una especie de "efecto taumatúrgico", lo que podemos definir como el "**fetichismo de lo impreso**" que convierte en documento lo que no lo es y se justifica que en algunos casos, partiendo de tal calificación documental, se defienda incluso la posibilidad, a su amparo, de revisar los hechos probados en suplicación[2].

Puede presentarse simplemente impreso, como decimos, lo más usual, o junto a una pericial. Normalmente, si la parte que aporta la prueba lo realiza en soporte papel y la contraparte no realiza alegaciones sobre la integridad o autenticidad de la prueba, ésta es aceptada sin más.

[1] STSJ Cataluña 11-11-2013 (JUR 2014, 2574).
[2] Por ejemplo, STSJ Aragón 17-11-2010 (AS 2011, 136)

Sin embargo, si la contraparte alega que la prueba no es íntegra o, incluso, que es falsa, la parte que aporta la prueba deberá practicar una prueba pericial que garantice tanto la integridad como la autenticidad de ésta, a fin de poder introducirla en el proceso. y siempre en soporte informático[3], lo que supone importantes dificultades[4]. Pese a ello, cuestionar en abstracto el alcance probatorio

[3] Extraordinario análisis el de J. RUBIO ALAMILLO, Ingeniero en Informática, Vocal de las Juntas de Gobierno del Colegio Profesional de Ingenieros en Informática de la CAM. Como expone: Debe ser siempre en soporte informático, ya que tanto el perito de la otra parte como el perito judicial, deben tener acceso al dictamen pericial del perito de la parte que aporta la prueba y, a la prueba misma o a una copia forense de ésta. Es, por tanto, absolutamente imposible determinar que un correo electrónico aportado exclusivamente en papel en un procedimiento, aún mediante informe pericial, es auténtico e íntegro, aunque para facilitar el trabajo del juzgador, además de presentar el correo electrónico en soporte informático, se puede aportar también en formato papel mediante impresión". J. RUBIO ALAMILLO, "el correo electrónico como prueba en procedimientos judiciales", *Diario La Ley*, Nº 8808, Sección Práctica Forense, 21 de Julio de 2016, Editorial LA LEY

[4] Como expone J. RUBIO ALAMILLO: "Un importante dilema que siempre planea sobre muchos profesionales jurídicos, tanto letrados, como fiscales o jueces, en este tipo de procedimientos en los que se aportan correos electrónicos, es si los mismos, aportados en soporte informático (evidentemente, se descartan los aportados únicamente en soporte papel), son originales o no. La respuesta, para la inmensa mayoría de los casos, es que no (...) Aportar un correo electrónico recibido original, es algo prácticamente impracticable desde el punto de vista técnico. Para ello, sería necesario adjuntar al procedimiento el disco duro del servidor al que llegó el correo electrónico, con su correspondiente código hash calculado ante fedatario público, suponiendo que la configuración del servidor conserve los correos electrónicos en el mismo una vez éstos han sido entregados a su destinatario. Salvo que se trate del ámbito penal, en un procedimiento en el que los ordenadores hayan sido intervenidos e incautados por las Fuerzas y Cuerpos de Seguridad del Estado recibiendo órdenes de un juez, no será posible realizar esta aportación, ya que ninguna empresa va a detener su servidor de correo electrónico motu proprio para aportar su disco duro a una causa, menos aún si se trata de una empresa de alojamiento web que preste servicios a varios clientes.

Por otra parte, para que un correo electrónico recibido, adjunto a un procedimiento judicial, fuese metafóricamente una fotocopia compulsada, tendría que aportarse una copia forense del disco duro del servidor de correo electrónico en el que se recibió el mismo antes de ser entregado a su destinatario. En la mayoría de los casos, debido a las configuraciones estándar de los clientes y servidores de correo electrónico, estos últimos siempre eliminan los correos electrónicos cuando los entregan, por lo que, casi nunca, se tendrá la posibilidad de aportar, a un procedimiento judicial, una metafórica fotocopia compulsada de un correo electrónico recibido. En la mayoría de las configuraciones estándar de clientes y servidores de correo electrónico, éstos entregan los correos electrónicos a los clientes, dejando en el servidor unas trazas o apuntes del origen y el destinatario, así como de los instantes de recepción y entrega, pero no almacenan el contenido del mensaje una vez éste ha sido entregado al cliente o destinatario(...).

Debido, como ya se ha indicado, a que la mayoría de los clientes y servidores de correo electrónico no están apropiadamente configurados para una eventualidad en la que deban aportarse, a un procedimiento judicial, uno o varios correos electrónicos recibidos, el perito informático únicamente podrá analizar el correo electrónico

del correo electrónico con fundamento en la **necesidad de soporte electrónico** que lo verifique, sería tanto como negar la evidencia de que este medio es la forma usual de transmisión de información en el ámbito laboral (el art. 27.3 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, dispone que la comunicación a través de medios electrónicos será válida siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifiquen fidedignamente al remitente y al destinatario)[5].

Resulta reseñable algún supuesto especial[6]. Por ejemplo, cuando lo cuestionado son los correos electrónicos enviados entre los letrados de las partes, admisible su aportación si se cuenta con la autorización de la Junta de Gobierno del correspondiente Colegio de Abogados"[7].

---

entregado en el cliente que, evidentemente, no es el original, sino una fotocopia no compulsada (suponiendo que el correo no esté firmado digitalmente) de éste. Puede que, incluso, con un poco de suerte, el perito pueda también analizar las trazas que dejaron tanto la recepción del correo electrónico en el servidor, como su entrega al cliente o destinatario.

(...)Caso aparte es cuando se trata de un correo electrónico enviado en lugar de recibido. En estos casos sí es realmente posible aportar una metafórica fotocopia compulsada, siempre y cuando, evidentemente, se sigan los cauces procesales adecuados y ya explicados de clonación ante fedatario público del disco duro en el que se encuentre dicho correo electrónico, para posteriormente aportar dicha copia clónica al proceso (...). Los correos electrónicos enviados permanecen en la bandeja de correos enviados de la cuenta de correo electrónico desde la que se envían, aunque es necesario indicar que, si se desea certificar la recepción de un correo electrónico en destino, no podría garantizarse si éste realmente fue entregado a partir de, únicamente, un análisis del correo electrónico enviado, por lo que sería necesario efectuar también sendos análisis forenses de los servidores de salida y, si es posible, de destino, a fin de corroborar si el correo electrónico realmente llegó". J. RUBIO ALAMILLO, "el correo electrónico como prueba en procedimientos judiciales", *Diario La Ley*, Nº 8808, Sección Práctica Forense, 21 de Julio de 2016, Editorial LA LEY.

[5] STSJ Andalucía, Granada, de 7-1-2010 (JUR 2011\99047).

[6] STSJ Aragón 17-11-2010 (AS 2011, 136). En este caso la remisión de un correo electrónico al abogado de la parte ejecutante no podía sino interpretarse como un acto de reconocimiento de deuda que interrumpe la prescripción "ex" art. 1973 del Código Civil, por lo que a Sala debe concluye que la acción cuya ejecución se instó no estaba prescrita.

[7] El art. 34 del Estatuto General de la Abogacía, Real Decreto 658/2001, de 22-6, impone a los colegiados un deber consistente en "mantener como materia reservada las conversaciones y correspondencia habidas con el abogado contrario, con prohibición de revelarlos o presentarlos en juicio sin su previo consentimiento. No

2. La intervención del correo electrónico en relación al secreto de las comunicaciones y al derecho a la intimidad. STC (Sala 1.ª) 170/2013, de 7 de octubre de 2013.

El problema se plante en el siguiente **supuesto de hecho**: La sociedad Alcal, S.A. se dedica al cultivo y al tratamiento industrial de la planta adormidera para obtención de alcaloides (morfina y codeínas). Alcal tuvo noticia, por una empresa cliente, de que las previsiones de cosecha) de su actividad productiva eran puestas en conocimiento de otra empresa, a través (supuestamente) de alguno de sus empleados. Por ello, decidió adoptar determinadas medidas de control de los medios informáticos suministrados al personal; entre ellos, el ordenador del demandante de amparo .

Se depositó dicho ordenador en manos de un notario, para la práctica en la notaría de la copia de su disco duro, copia llevada a cabo "en presencia y por parte de un técnico" informático. El análisis de la copia del disco duro reveló que desde la dirección de correo electrónico del demandante se habían comunicado a otra sociedad mercantil datos sobre las cosechas previstas de planta adormidera en la empresa Alcal, en los años 2007 y 2008.

El trabajador fue despedido por transgresión de la buena fe contractual a que se refiere el art. 54.d) del Estatuto de los Trabajadores. Los preceptos del convenio colectivo aplicable (el XV Convenio Colectivo de la industria química) eran, de acuerdo con el propio relato de STC 170/2013. El primero de ellos tipifica como **falta leve "la utilización de los medios informáticos propiedad de la empresa** (correo electrónico, Internet, intranet, etc.) para fines distintos de los relacionados con la prestación laboral". El segundo califica como falta muy grave, y faculta para sancionar como tal, la inobservancia del deber de reserva de datos de la empresa.

---

obstante, por causa grave, la Junta de Gobierno del Colegio podrá discrecionalmente autorizar su revelación o presentación en juicio sin dicho consentimiento previo".

A. Alegaciones del recurrente y doctrina del TS y del Tribunal Europeo de Derechos Humanos

Defendido que el registro efectuado no se atemperaba a lo dispuesto en sentencia del Tribunal Supremo **de 26 de septiembre de 2007** (RCUD 966/2006), es decir, **la primera y más importante resolución de la jurisprudencia española** respecto del uso extralaboral del ordenador de trabajo. En ella se acoge y se aplica la doctrina sentada en la materia por el Tribunal Europeo de Derechos Humanos en dos importantes resoluciones: 1) sentencia TEDH de 27 de mayo de 1997, caso *Halford,* sobre requisitos del control empresarial de las comunicaciones telefónicas de sus empleados, y 2) sentencia TEDH de 3 de abril de 2007, caso *Copland*, sobre requisitos del control empresarial de las conversaciones telefónicas y del correo electrónico de sus empleados.

Esta resolución admite, en principio, como analizaremos después, los "**usos privados moderados**" de dichos medios informáticos ante las "dificultades prácticas» de excluir por completo la "utilización personalizada y no meramente laboral o profesional" de los mismos. y el control sobre utilización de estos instrumentos de trabajo –sigue la jurisprudencia sentada en la citada sentencias europeas– se ha de ajustar a las "reglas de uso" y a las medidas de vigilancia establecidas por la empresa.

Si el medio se **utiliza en contra de prohibiciones** (de **uso**) y **con conocimiento por parte de los afectados de los controles** y medidas aplicables, no podrá entenderse que, al realizarse el control por parte de la empresa, se haya vulnerado una expectativa razonable de intimidad del trabajador.

B. Modulación de los derechos fundamentales en el ámbito laboral

Se parte de la modulación de los derechos fundamentales en el contrato de trabajo, tal como se recoge en STC 170/2013, de forma que el

trabajador no pierde su condición y sus derechos constitucionales "por insertarse en el ámbito de una organización privada" como es la empresa (STC 88/1985) . Pero "la inserción en la organización laboral modula [el ejercicio de] aquellos derechos" constitucionales "en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva" (STC 99/1994), ya que el desenvolvimiento adecuado de la actividad productiva es "reflejo, a su vez, de derechos que han recibido consagración en el texto de nuestra norma fundamental (arts. 33 y 38 CE)", como lo son el derecho a la propiedad privada y el derecho a la libertad de empresa en el marco de la economía de mercado.

C. Derecho al secreto de las comunicaciones

El art. 18.3 CE menciona expresamente las comunicaciones "postales, telegráficas y telefónicas"; lo que pudiera plantear la duda de si comprende las comunicaciones por correo electrónico, que no son desde luego telegráficas o telefónicas, y que no son tampoco postales en el sentido estricto del término.

La sentencia considera el correo electrónico incluido dentro de las previsiones previstas para ese derecho porque la lista de comunicaciones incluida en el precepto constitucional no es exhaustiva y aquellos eran los tipos de medios de correspondencia o comunicación más importantes existentes en 1978 cuando el correo electrónico lo es, sin embargo, en la actualidad

Pero considera que la comunicación no es secreta o realizada "en canal cerrado" sino comunicación abierta porque establecida la prohibición del uso "extralaboral" del ordenador, a través de la sanción prevista en el convenio, la empresa está habilitada para el registro empresarial del ordenador de trabajo, que no supone la interferencia de un tercero en una comunicación secreta, sino el ejercicio del poder de dirección, en su vertiente de "vigilancia y control para verificar el

cumplimiento por el trabajador de sus obligaciones y deberes laborales" (art. 20.3 ET

D. Derecho a la intimidad del demandante

También se rechaza de la demanda de amparo en lo que respecta a la supuesta violación del derecho a la intimidad del demandante porque "el régimen jurídico aplicable en la empresa respecto al uso de las herramientas informáticas de su propiedad hacía factible y previsible que el empresario ejerciera su facultad legal de vigilancia sobre los correos electrónicos del trabajador … circunstancia [que] impedía en este caso abrigar una expectativa razonable de privacidad que determinara la entrada en la esfera de protección del derecho a la intimidad".

También se parte la aplicación del test de proporcionalidad es la valoración de la justificación del control, la cual arroja un resultado positivo, teniendo en cuenta «la existencia de sospechas de un comportamiento irregular del trabajador. El segundo elemento del test es la idoneidad de la medida de control adoptada, a la vista de la "finalidad pretendida por la empresa" de "verificar si el trabajador cometía efectivamente la irregularidad sospechada". En tercer lugar, la proporcionalidad "en sentido amplio" exige que "la medida" adoptada pueda considerarse «necesaria"; lo que también concurre en el caso, "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".

También la "proporcionalidad en sentido estricto". La medida adoptada de registro del disco duro del ordenador de trabajo del demandante se entiende en el caso "ponderada y equilibrada", ceñida a los «correos electrónicos aportados por la empresa como prueba en el proceso de despido», y sin abarcar "aspectos específicos de la vida personal o familiar del trabajador".

II. PÁGINAS WEB Y DERECHOS FUNDAMENTALES. LA EVOLUCIÓN DE LA DOCTRINA JURISPRUDENCIAL

Las páginas web encuentran su marco en el artículo 384 LEC pero pueden introducirse como páginas meramente impresas, como parte de una prueba pericial informática e incluso a través del la cibernavegación en el mismo acto del juicio.

La sentencia más trascendente, sin duda, es la dictada con fecha 27-6-2007 (Roj 6128/2007), antes referida.

En los hechos probados de la sentencia de instancia constar que el actor, Director General de la empresa demandada, prestaba servicios en un despacho sin llave, en el que disponía de un ordenador, carente de clave de acceso y conectado a la red de la empresa que dispone de ADSL.

Consta también que un técnico de una empresa de informática fue requerido para comprobar los fallos de un ordenador que "la empresa señaló como del actor". En la comprobación se detectó la existencia de virus informáticos, como consecuencia de «la navegación por páginas poco seguras de Internet". En presencia del administrador de la empresa se comprobó la existencia en la carpeta de archivos temporales de "antiguos accesos a páginas pornográficas", que se almacenaron en un dispositivo de USB, que se entregó a un notario.

La sentencia matiza que "las operaciones llevadas a cabo en el ordenador se hicieron sin la presencia del actor, de representantes de los trabajadores ni de ningún trabajador de la empresa». El ordenador fue retirado de la empresa para su reparación y, una vez devuelto, se procedió a realizar la misma operación con la presencia de delegados de personal.

La sentencia recurrida confirmó la decisión de instancia que aprecia la falta de validez la prueba de la empresa porque ha sido obtenida mediante un registro de un efecto personal que no cumple las exigencias del artículo 18 del Estatuto de los Trabajadores .

La sentencia de 26-9-2007 Tribunal Supremo establece diversos criterios:

- El control del uso del ordenador facilitado al trabajador, por el empresario, no se regula por el artículo 18 del Estatuto de los Trabajadores , sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse. Según el art. 20.3 ET, este ostenta la facultad de adoptar las medidas que considere oportunas para vigilar el cumplimento de las obligaciones laborales por los trabajadores, y eso es lo que sucede cuando se controla el uso de herramientas de trabajo de naturaleza informática. En cambio, los registros contemplados en el art. 18 ET constituyen una facultad "exorbitante y excepcional" del empresario, que excede del marco del art. 20 ET.

- La garantía de la intimidad también se extiende a los archivos personales del trabajador que se encuentran en el ordenador. La aplicación de la garantía podría ser más discutible en el presente caso, pues no se trata de comunicaciones, ni de archivos personales, sino de los denominados archivos temporales, que son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de Internet. Se trata más bien de rastros o huellas de la "navegación" en Internet y no de informaciones de carácter personal que se guardan con carácter reservado. Pero hay que entender que estos archivos también entran, en principio, dentro de la protección de la intimidad, sin perjuicio de lo ya dicho sobre las advertencias de la empresa.

No es obstáculo para la protección de la intimidad el que el ordenador **no tuviera clave de acceso**. Este dato –unido a la localización del ordenador **en un despacho sin llave**– no supone por sí mismo una aceptación por parte del trabajador de un acceso abierto a la información contenida en su ordenador.

- 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 crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida.

- Lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos. Por ello, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (TEDH 1997, 37) (caso Halford) y 3 de abril de 2007 (TEDH 2007, 23) (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos.

- No cabe entender que estemos ante lo que en el ámbito penal **se califica como un "hallazgo casual"** (sentencias de 20 de septiembre (RJ 2006, 6402), 20 de noviembre (RJ 2006, 9187) y 1 de diciembre de 2006 (RJ 2006, 9564), pues se ha ido más allá de lo que la entrada regular para la reparación justificaba.

La Sentencia de 8 marzo 2011[8](Roj 1323/2011) confirma referido criterio

La empresa Font Salem, perteneciente al Grupo Damm, realizó en los meses de enero y febrero de 2009 una **auditoría interna** en las redes de la información con el objeto de revisar la seguridad del sistema y detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados. Por lo que se refiere al ordenador utilizado por los jefes de turno, en el periodo de los dos meses indicados, se accedió a Internet en horas de trabajo con un total de 5.566 visitas a páginas referidas al mundo multimedia- vídeos, piratería informática, anuncios, televisión, contactos, etc. La gran mayoría de los accesos o visitas a Internet se produjeron en los turnos de trabajo de uno de los trabajadores. A su vez, casi la totalidad de visitas se realizaron en tramos horarios en que el trabajador estaba solo en el despacho, por el horario de trabajo del resto de usuarios.

Sin embargo, en el Caso de las Manteletas resuelto por **STS de 6 de octubre de 2011,** en Sala General, **se relajan referidos requisitos**. En este supuesto la empresa había entregado a todos los trabajadores una carta que los trabajadores recibieron y firmaron, en la que se le comunicaba que quedaba terminantemente prohibido el uso de medios de la empresa (ordenadores, móviles, Internet, etc.) para fines personales tanto dentro como fuera del horario de trabajo. La empresa decidió hacer una comprobación sobre el uso de sus medios de trabajo por los trabajadores, a cuyo fin procedió a finales del mes de enero de 2009 a la **monitorización de los ordenadores** de dos trabajadoras, encargándose de la instalación del "software" de monitorización, al objeto de captar las pantallas a las que se accedía para su posterior visualización. Se detectó que una de las trabajadoras realizaba visitas a Internet y, en definitiva, realizaba un uso del ordenador para asuntos

[8] RJ 2011\932

propios, ajenos a su tarea laboral, en horas de su jornada laboral. Como consecuencia de todo ello fue despedida.

Por lo tanto, se introduce una matización novedosa respecto de lo señalado por la Sentencia del Tribunal Supremo de 2007: en concreto, admite el control oculto (el realizado sin advertir de la posibilidad de la monitorización) cuando la empresa ha prohibido expresamente el uso personal de los medios telemáticos de su propiedad.

Es decir, l**as prohibiciones absolutas de uso personal** de las herramientas informáticas, p**or si mismas, ya implican una advertencia implícita** del posible control empresarial, incluyendo la instalación de sistemas de control del uso del ordenador por parte de los trabajadores, lo que descarta cualquier margen de tolerancia y elimina toda expectativa de intimidad y también la afectación del secreto de las comunicaciones de aquéllos. Confirma el criterio menos exigente, ya empleado por alguna resolución anterior.

Como expone, si bien es cierto que la STS de 26-09-2007 (RJ 2007, 7514) exigía informar a los trabajadores de la existencia de control empresarial y los medios utilizados., tal exigencia no es aplicable en supuestos de prohibición absoluta del uso de los medios tecnológicos en los que no concurre expectativa alguna de confidencialidad o intimidad por parte de los trabajadores.

La diferencia existente entre esta sentencias del Tribunal Supremo y la Sentencia del Tribunal Constitucional antes referida, la 170/2013, es que en la primera se considera que el trabajador está avisado sobre la normativa de uso con respecto a los sistemas informáticos que la empresa pone a su disposición por el mero hecho de que estas reglas están recogidas en el convenio colectivo al que están adscritos la empresa y los trabajadores.

III. LA DOCTRINA DE LA SALA PENAL SOBRE EL SECRETO DE LAS COMUNICACIONES Y LA NECESARIA INTERVENCIÓN JUDICIAL: STS 3ª DE 16-6-14 (Roj 2844/2014)

Sin embargo, la sentencia de la Sala de lo Penal del Tribunal Supremo de fecha 16 de junio de 2014 (Rº 2229/2013) pretende contribuir a "fijar una clara doctrina en materia de tanta trascendencia".

La sentencia censura los criterios de la Sala de lo Social del Tribunal Supremo y luego confirmados por el Tribunal Constitucional. En aquel caso "considera conveniente (...), **salir al paso de** ciertas afirmaciones rotundas como que "...el ordenador registrado era una herramienta propiedad de la empresa y facilitada por la empresa a don (sic) Rodolfo exclusivamente para desarrollar su trabajo, por lo que entendemos que incluso en aquel supuesto en que pudiera utilizar el ordenador para emitir algún tipo de mensaje de carácter personal, entendemos que al utilizar precisamente un ordenador ajeno, de la empresa, y destinado exclusivamente para el trabajo a la empresa, estaba asumiendo –cediendo– la falta de confidencialidad –secreto– de las comunicaciones que pudiera tener el señor (sic) Rodolfo utilizando tal terminal informático"».

Considera la Sala de lo Penal que los citados criterios **han de quedar restringidos al ámbito de la Jurisdicción laboral, incluso cuando cuentan con la confirmación constitucional**, pero que, en modo alguno, procede que se extiendan al enjuiciamiento penal, por mucho que en éste la gravedad de los hechos que son su objeto, delitos que en ocasiones incluso constituyen infracciones de una importante relevancia, supere la de las infracciones laborales a partir de las que, ante su posible existencia, se justifica la injerencia en el derecho al secreto de las comunicaciones del sospechoso de cometerlas".

Considera la Sala que el texto constitucional es claro y tajante cuando afirma en su art. 18.3 CE categóricamente que: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, **salvo resolución judicial**".

Entiende el Tribunal que el citado precepto "n**o contempla, por tanto, ninguna posibilidad** ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado ("correo corporativo"), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia".

Tampoco admite la Sala de lo Penal, **una supuesta "tácita renuncia**" al derecho puede convalidar la ausencia de intervención judicial. Por dos tipos de razones. En primer lugar, "porque obviamente dicha "renuncia" a la confidencialidad, o secreto de la comunicación, no se produce ni es querida por el comunicante que, de conocer sus consecuencias, difícil es imaginar que lleve a cabo la comunicación objeto de intervención" y, por otra parte, "porque ni aun cuando se entienda que la "renuncia– autorización" se haya producido resultaría operativa ya que, a diferencia de lo que ocurre con la protección del derecho a la inviolabilidad domiciliaria (art. 18.2 CE), nuestra Carta Magna no prevé, por la lógica imposibilidad para ello, la autorización del propio interesado como argumento habilitante para la injerencia».

La sentencia recuerda que el régimen de protección del derecho al secreto de las comunicaciones es, sin duda, «**el más enérgico** de los que dentro del genérico derecho a la intimidad se contemplan en el repetido art. 18 CE al excluir cualquier posible supuesto que no

contemple la intervención del Juez como tutelador del derecho del investigado,

Por consiguiente, "bien claro ha de quedar que en el ámbito del procedimiento penal, el que a nosotros compete, para que pueda otorgarse valor y eficacia probatoria al resultado de la prueba consistente en la intervención de las comunicaciones protegidas por el derecho consagrado en el artículo 18.3 de la Constitución, r**esultará siempre necesaria la autorización e intervención judicial**, en los términos y con los requisitos y contenidos que tan ampliamente se han venido elaborando en multitud de Resoluciones por esta Sala, a partir del importante Auto de 18 de Junio de 1992 (**caso "Naseiro**"), cualquiera que fueren las circunstancias o personas, funcionarios policiales, empresarios, etc., que tales injerencias lleven a cabo».

Tal sentencia **se centra exclusivamente en el concepto de «comunicación», no «los denominados "datos de tráfico" o incluso de la posible utilización del equipo informáticopara acceder a otros servicios de la red como páginas web, etc., de los mensajes que, una vez recibidos y abiertos por su destinatario**, no forman ya parte de la comunicación propiamente dicha, respecto de los que rigen normas diferentes como las relativas a la protección y conservación de datos (art. 18.4 CE) o a la intimidad documental en sentido genérico y sin la exigencia absoluta de la intervención judicial (art. 18.1 CE)».

IV. LA DOCTRINA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS. ASUNTO 61496/08, BARBULESCU VS. RUMANÍA. SENTENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS DE 12 DE ENERO DE 2016

Según los hechos probados de esta resolución, el demandante, en su calidad de responsable de ventas de una empresa, creó una cuenta de Yahoo Messenger para atender las solicitudes de los clientes. El

empleador, tras comprobar que la cuenta de correo se había usado para fines particulares, despidió al trabajador, basándose en que la regulación interna de la **empresa prohibía expresamente** la utilización de ordenadores, teléfonos, fax y demás medios para fines personales, lo que el trabajador conocía.

El demandante, además de negar los hechos de que se le acusaba, señaló que se había **vulnerado su derecho al secreto de la correspondencia** al haber sido registrado su correo electrónico.

Ante el Tribunal Europeo de Derechos Humanos, el trabajador alegó una **vulneración del artículo 8 del Convenio** para la protección de los derechos y de las libertades fundamentales (Roma, 4 de noviembre de 1950), que establece que "toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".

Los tribunales de Rumanía declararon que el despido era procedente al haberse realizado conforme a la legislación aplicable, y que no se había violado el derecho a la intimidad del trabajador, pues éste había sido informado de la normativa interna de la empresa y el registro de su correo era el único modo de comprobar si había cumplido las normas.

El Tribunal señala que el empleador puede comprobar que sus empleados cumplen con sus obligaciones durante el horario de trabajo, y que en este caso había accedido a la cuenta de correo del trabajador **suponiendo que solo contenía comunicaciones con los clientes** de la empresa. Además, señala el Tribunal que **los órganos judiciales internos no desvelaron el contenido de las comunicaciones**, sino que éstas se utilizaron únicamente para probar que el trabajador utilizó el ordenador de la empresa con fines distintos a los estrictamente laborales durante la jornada de trabajo.

El Tribunal Europeo de Derechos Humanos concluye que no se ha producido una vulneración del artículo 8 del Convenio, puesto que los tribunales rumanos mantuvieron un **equilibrio adecuado** entre el derecho del trabajador al respeto de su vida privada y su correspondencia y los intereses del empleador.

V. MENSAJERÍA MÓVIL (SMS, WHATSAPP, ETC). REDES SOCIALES. PRIMERA SENTENCIA SOBRE "PANTALLAZOS". STS TRIBUNAL SUPREMO (SALA DE LO PENAL) NÚM. 300/2015, DE 19 MAYO (Roj 2047/2015)

Constituyen medios del artículo 384 LEC, aunque, como sucede con los con las otras fuentes de prueba, se le ha reconocido, sin embargo, en algunas ocasiones carácter documental a efectos de recurso de suplicación y revisión de los hechos probados.

Su introducción en el proceso puede ser como tal aparente documental, a través de lo que se califica usualmente como pantallazo, en una prueba pericial.

Será necesaria la percepción directa por las partes y por el juez en el acto de la vista.

Respecto a este tipo de prueba, se han planteado básicamente **el problema de la Carga de la prueba, de la demostración de la autenticidad. Lo resuelve la primera sentencia sobre "pantallazos", la STS Tribunal Supremo (Sala de lo Penal) núm. 300/2015, de 19 mayo[9].**

Es lógico este problema. Se han apreciado en el año 2014 **errores de protección**, en el medio más utilizado,WHATSAPP,y **existen**

[9] RJ 2015\1920.

programas que permiten editar los mensajes, falsearlos como broma, etc. Por ejemplo WhatsAppToolbox o Fake SMS Sender (en este caso, para los SMS).

Además, **no existe ningún servidor externo** que conserve la información y los administradores se limitan a facilitar el tránsito de estas comunicaciones. La única información que pueden facilitar éstos es la constatación del tráfico de comunicaciones, origen y destino de las mismas, los datos conservados sobre identidades y nombres de usuario y clave, incluidos número de abonado telefónico asociado o IP de referencia.

La sentencia referida aborda un supuesto de abuso sexual continuado de una niña de apenas 13 años de edad por parte de la pareja sentimental de su madre, con quien convivía. Se aporta como prueba de cargo una impresión en papel de conversaciones tipo mensajería instantánea mantenidas por la menor a través de la red social Tuenti con un amigo, en las que bastante antes de que se iniciara le proceso penal, reconocía la realidad de dichos abusos sexuales

Respecto a la falta de autenticidad del diálogo mantenido, la Sala quiere puntualizar una idea básica. Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. **La posibilidad de una manipulación** de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, como expresa, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, **desplaza la**

carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria.

Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido.

En el presente caso, sin embargo, fueron dos razones son las que excluyen cualquier duda. La primera, el hecho de que fuera **la propia víctimala que pusiera a disposición del Juez de instrucción su contraseña de Tuenti** con el fin de que, si esa conversación llegara a ser cuestionada, pudiera asegurarse su autenticidad mediante el correspondiente informe pericial.

La segunda, el hecho de que el interlocutor con el que se relacionaba la acosada sexualmente **fuera propuesto como testigo** y acudiera al plenario. Allí pudo ser interrogado por las acusaciones y defensas acerca del contexto y los términos en que la víctima y el testigo mantuvieron aquel diálogo. En el plenario manifestaron que efectivamente mantuvieron esa conversación y en esos términos, sin que ninguno de los dos hiciera referencia a que se hubiera producido ninguna manipulación en la impresión de dicha conversación, que constaba no solamente aportada por la Acusación Particular sino también en las fotografías que del teléfono móvil de la menor adjuntó la Guardia Civil, ya que según consta en el oficio,

Con grandes dificultades probatorias ya el historial solo permitía retroceder hasta el 26 de Octubre de 2013, por lo que únicamente pudieron visualizarlo a través de la aplicación de Tuenti para teléfonos móviles, haciendo los agentes fotografías de las pantallas correspondientes a la conversación, que coincidían exactamente con las hojas impresas que fueron aportadas por la Acusación Particular. Además, la Acusación Particular facilitó las claves personales de Ana

María en Tuenti y solicitaba que, si había alguna duda técnica o probatoria, que se oficiara a "Tuenti España", indicando su dirección, para que se certificara el contenido de esa conversación, **sin que la defensa hiciera petición** alguna al respecto.