VIGILANCIA Y CONTROL DE LOS TRABAJADORES Y DERECHO A LA INTIMIDAD EN EL CONTEXTO DE LAS NUEVAS TECNOLOGÍAS

Francisca M.ª Ferrando García

Profesora Titular de Derecho del Trabajo y de la Seguridad Social. Universidad de Murcia

Extracto

El presente trabajo analiza la compatibilidad del control de la actividad laboral que se desarrolla con medios informáticos o de comunicación institucional propiedad de la empresa con el derecho a la intimidad en sus diferentes manifestaciones, según la interpretación dada por la reciente doctrina constitucional y judicial, así como por el Tribunal Europeo de Derechos Humanos. Desde la misma perspectiva, se analizan los límites a la aplicación de los medios tecnológicos en la vigilancia del desempeño laboral e, incluso, de la actividad extralaboral.

Asimismo, se plantea la relevancia de la información obtenida a través de estas tecnologías como medio de prueba en el proceso laboral, a efectos, normalmente, de sustentar la imputación de comportamientos objeto de sanción disciplinaria.

Palabras claves: control empresarial, intimidad, nuevas tecnologías, redes sociales y medios de prueba.

Fecha de entrada: 14-04-2016 / Fecha de aceptación: 30-05-2016

EMPLOYEES SURVEILLANCE AND MONITORING AND RIGHT TO PRIVACY WITHIN THE CONTEXT OF NEW TECHNOLOGIES

Francisca M.ª Ferrando García

Abstract

This paper analyzes the compatibility of control of work developed using computerized or communication means owned by the company, with the right to privacy in its various manifestations, as interpreted by the recent constitutional and judicial doctrine, as well as the European Court of Human Rights. From the same perspective, this work deals with the limits on technological surveillance with regard to job performance and, even, activity outside work.

The study also raises the relevance of the information obtained through these technologies as evidence in labor proceedings, in order to support disciplinary measures.

Keywords: entrepreneur control, privacy, new technologies, social networks and evidence.

Sumario

1. Introducción
   1.1. Consideraciones iniciales: Importancia de las nuevas tecnologías en el desarrollo y control de la actividad laboral
   1.2. El derecho a la intimidad como límite a la facultad empresarial de vigilancia y control de la actividad laboral
      1.2.1. Proporcionalidad de la medida
      1.2.2. Ámbito objetivo de la facultad de control empresarial: Actividad laboral o extralaboral con trascendencia directa en las obligaciones laborales
      1.2.3. Información previa respecto de los medios de control

2. El uso de medios tecnológicos en el control de la actividad laboral
   2.1. Videovigilancia y grabaciones de sonido
   2.2. Geolocalización mediante GPS
   2.3. Registro de huellas dactilares
   2.4. Vigilancia por detectives privados

3. El control del uso de medios informáticos de titularidad empresarial
   3.1. Tolerancia empresarial y límites al control empresarial
   3.2. Particular referencia al control del correo electrónico y la mensajería
   3.3. Valor y eficacia de la prueba basada en el correo electrónico y la mensajería

4. La información reflejada en las redes sociales como base del ejercicio del poder disciplinario
   4.1. La red social, delatora
   4.2. El valor probatorio de la información obtenida en redes sociales
      4.2.1. Obtención lícita de la información vertida en redes sociales por parte de la empresa
      4.2.2. Fiabilidad, precisión temporal y autoría de la información

5. Incidencia de la ilicitud de la prueba en la calificación de la sanción

1. INTRODUCCIÓN

1.1. CONSIDERACIONES INICIALES: IMPORTANCIA DE LAS NUEVAS TECNOLOGÍAS EN EL DESARROLLO Y CONTROL DE LA ACTIVIDAD LABORAL

El desarrollo de la tecnología afecta profundamente a los procesos de trabajo y al modo en que se desarrollan las comunicaciones en el seno de la empresa. En la última década, el correo electrónico ha superado al correo postal y se recurre tanto o más al WhatsApp que a las llamadas telefónicas. Por otra parte, junto a la comunicación personal e individual se han introducido otras formas de comunicación, dirigidas a un grupo amplio de destinatarios, a través de las denominadas redes sociales. Las personas comparten información y opiniones a través de Facebook, Twitter, WhatsApp, Messenger o Instagram, con amigos, conocidos y compañeros de trabajo, información que finalmente se extiende a los amigos de todos ellos. También en el ámbito empresarial se utilizan estos medios para realizar gestiones relacionadas con la publicidad, anuncios, circulares, buzón de sugerencias, correo institucional, etc., destinando parte de los recursos al establecimiento, mantenimiento y actualización de nuevas tecnologías de comunicación. Ahora bien, la propia aplicación de estos medios en el desarrollo de la prestación laboral plantea a menudo la necesidad de delimitar qué se entiende por uso correcto de los mismos y hasta qué punto puede el empresario controlar las comunicaciones de sus trabajadores para determinar si su utilización ha sido adecuada.

Asimismo, estas nuevas tecnologías se aplican a los sistemas de supervisión y vigilancia de la actividad laboral, dentro y fuera del centro de trabajo, por medio de GPS, control de huellas dactilares, etc., permitiendo llegar a situaciones de tiempo y lugar que anteriormente escapaban de la capacidad de control empresarial. A la hora de elegir e implementar las medidas de control, el empresario puede, y así lo recuerda el artículo 20.3 del ET, acudir a aquellas que estime más oportunas para supervisar el desarrollo de la actividad laboral, pero –como advierte el mismo precepto– deberá respetar la dignidad humana, una de cuyas derivaciones más importantes es el derecho a la intimidad.

En definitiva, el derecho a la intimidad del trabajador constituye un límite a la facultad de control del empresario y su respeto marca la línea divisoria entre la prueba legal o ilegalmente obtenida y las posibilidades de hacer valer la información obtenida con dichas medidas en un eventual proceso judicial, en caso de impugnación de la decisión empresarial.

El objeto de este trabajo consiste en analizar la compatibilidad del control de la actividad laboral que recae sobre los medios informáticos o de comunicación institucional propiedad de la

empresa o que se implementa mediante las nuevas tecnologías con el derecho a la intimidad, así como la relevancia de la información obtenida a través de estas tecnologías como medio de prueba en el proceso laboral, a efectos, normalmente, de sustentar la imputación de comportamientos objeto de sanción disciplinaria.

1.2. EL DERECHO A LA INTIMIDAD COMO LÍMITE A LA FACULTAD EMPRESARIAL DE VIGILANCIA Y CONTROL DE LA ACTIVIDAD LABORAL

Conviene tener presente que, por su ubicación sistemática en el texto constitucional, el derecho a la intimidad personal, reconocido en el artículo 18.1 de la CE, tiene rango de derecho fundamental. Este derecho deriva, a su vez, del derecho a la dignidad de la persona (art. 10.1 CE) que implica «la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana» (STC 98/2000). El ámbito laboral no constituye una excepción a este principio, por lo que el artículo 4.2 c) del ET recoge expresamente el derecho de los trabajadores al respeto de su intimidad.

No obstante, el derecho a la intimidad del trabajador puede entrar en conflicto con el interés empresarial de controlar el cumplimiento de las obligaciones laborales, que llevará a cabo en virtud de las facultades directivas de que dispone al amparo de la libertad de empresa, reconocida en el artículo 38 de la CE. Dicho control empresarial se puede materializar a través de diversas medidas, genéricamente aludidas en el artículo 20.3 del ET, que en la actualidad se concretan bien mediante la supervisión personal de la actividad profesional desarrollada en el tiempo y lugar de trabajo, ya sea por el propio empresario o por trabajadores de la empresa, o fuera del mismo, por detectives privados, bien mediante diversas fórmulas de supervisión indirecta como la utilización de medios audiovisuales, el control del uso de internet o incluso a través de la información proveniente de las redes sociales.

En este contexto, y sin perjuicio del posterior análisis pormenorizado a que obliga la casuística, cabe adelantar siquiera de forma sucinta la existencia de ciertos presupuestos de validez del control empresarial, de cuyo cumplimiento se hace depender la licitud de la medida que afecta a la intimidad del trabajador, en los términos que se exponen a continuación.

1.2.1. Proporcionalidad de la medida

Como advierte el propio Tribunal Constitucional, «el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquel haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho» (por todas, SSTC 57/1994 y 143/1994).

Ahora bien, la doctrina constitucional no admite «el sacrificio de la intimidad de los trabajadores en aras de garantizar el correcto desenvolvimiento de la relación de trabajo, sino de una atemperación proporcional y recíproca de los derechos de ambas partes de la relación laboral»[1]. No en vano, el precitado artículo 20.3 del ET señala que en la adopción y aplicación de medidas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, el empresario deberá guardar «la consideración debida a su dignidad».

A fin de comprobar la compatibilidad del ejercicio de las facultades de control de la actividad laboral con la intimidad de los trabajadores afectados, es preciso valorar en cada caso específico si las medidas adoptadas por el empresario superan el denominado «juicio de proporcionalidad», integrado por un triple test, en virtud del cual se acredite que la medida sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad), que no exista otra medida más moderada para la consecución de tal propósito (juicio de necesidad) y, finalmente, que la misma sea equilibrada o proporcional de acuerdo con los bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)[2].

En la valoración de la medida de control se tiene especial consideración a la existencia de sospechas fundadas o indicios de incumplimiento por parte del trabajador, y a la posibilidad de contrastar su veracidad por otras vías. Se habla en este sentido de un «principio de intervención indiciaria», que justifica la adopción de medidas de control por parte del empresario cuando se acrediten indicios reveladores de una actuación irregular por parte del trabajador[3].

1.2.2. Ámbito objetivo de la facultad de control empresarial: Actividad laboral o extralaboral con trascendencia directa en las obligaciones laborales

En principio, el control debe ceñirse a la actividad laboral en el tiempo y lugar de trabajo[4]. Por ello, se entiende abusivo el control empresarial que sobrepase los límites de la prestación laboral de servicios para entrometerse ilícitamente en la vida íntima del trabajador. Por esta razón, aun encontrándose el trabajador en el lugar de trabajo, se rechazan los controles empresariales

[1] Selma Penalva, A.: «La información reflejada en las redes sociales y su valor como prueba en el proceso laboral. Análisis de los últimos criterios jurisprudenciales», *Revista General de Derecho del Trabajo y de la Seguridad Social,* núm. 39, 2014, pág. 362.

[2] En aplicación del citado juicio de proporcionalidad, véanse, por todas, las SSTC 57/1994, de 28 de febrero, y 143/1994, de 9 de mayo. Y más recientemente, las SSTC 96/2012, de 7 de mayo, 241/2012, de 17 de diciembre, 170/2013, de 7 de octubre y 39/2016, de 3 de marzo.

[3] Morales Vállez, C. E.: «El control de los medios tecnológicos por el empresario a la luz de la sentencia del TEDH de 12 de enero de 2016», *CEF.- Laboral Social*, febrero/2016 y Molina Navarrete, C.: «"Expectativa razonable de privacidad" y poder de vigilancia empresarial: ¿"*Quo vadis* justicia laboral"? Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos, de 12 de enero de 2016, asunto *Bărbulescu c. Rumanía*, demanda 61496/2008», *RTSS.CEF*, núm. 399, junio 2016.

[4] En este sentido, el Tribunal Constitucional ha declarado que la utilización por parte del empresario de medios de grabación dentro de la empresa, con la única finalidad de comprobar la conducta laboral del trabajador, no será, en principio, atentatorio de su derecho a la intimidad (STC 186/2000, 10 de julio).

sobre actividades del trabajador totalmente ajenas a su prestación laboral de servicios, como ocurre con los medios de grabación del sonido o de la imagen situados en zonas comunes o lugares de tránsito, como pasillos, aseos, comedores, etc.

No obstante, la supervisión y el control empresarial fuera de la jornada y el lugar de trabajo se admite en supuestos muy excepcionales, en los que se considera que la conducta seguida por el trabajador fuera de su jornada laboral, atendiendo a las específicas características de la prestación laboral contratada o de las concretas obligaciones a las que queda sujeto el trabajador, es también relevante en la relación laboral, bien por motivos de seguridad en las personas o en las cosas, bien porque puede repercutir negativamente en el rendimiento del trabajador o, en fin, porque su conducta privada puede considerarse atentatoria contra la buena fe contractual o implicar un abuso de la confianza empresarial.

A modo de ejemplo, se ha considerado legítima la intromisión de la empresa en la vida extralaboral del trabajador que desempeña actividades laborales que implican un gran nivel de responsabilidad sobre la vida de otras personas (pilotos de líneas aéreas, cirujanos, transportistas de mercancías peligrosas o trabajadores que en su empleo requieren una licencia de armas), «a fin de comprobar que, durante su tiempo libre, el trabajador sigue un tipo de vida ordenado». Se trata de supuestos en que la falta de sueño y el consumo de alcohol o sustancias tóxicas tienen trascendencia en la prestación laboral, en cuanto puede repercutir negativamente en el cumplimiento de las obligaciones laborales, pudiendo generar un riesgo para sí o para terceras personas (otros compañeros de trabajo, clientes o pacientes de la empresa, o incluso meros transeúntes)[5].

Pero además de la situación expuesta, la jurisprudencia viene admitiendo el control por parte del empresario de las situaciones de incapacidad temporal. En este caso, la intromisión del empresario en la vida privada del trabajador se halla legitimada por la vigencia de la relación laboral durante la baja y, con ella, de la obligación del trabajador de mantener escrupulosamente una conducta respetuosa con el deber de buena fe contractual (art. 20.2 ET), y la correlativa facultad de verificar el estado de salud del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo (art. 20.4 ET).

Sin ánimo exhaustivo, cabe citar asimismo otros supuestos en los que la actividad extralaboral del trabajador podría implicar un incumplimiento de sus obligaciones laborales, cual ocurriría en caso de competencia desleal o de incumplimiento de pactos de dedicación exclusiva, en los que, por tanto, se considera admisible el control por parte del empresario.

1.2.3. Información previa respecto de los medios de control

Dada la expectativa de intimidad que puede tener el trabajador en su vida diaria, la utilización de medios de control que pueden incidir en su derecho requiere que la empresa informe

[5] Selma Penalva, A.: «La información reflejada en las redes sociales…», *op. cit*., pág. 362.

previamente de su existencia. En este sentido, la STC 29/2013, de 11 de febrero, señalaba la necesidad de una «información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el 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 propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo» (FJ 8.º).

En coherencia con esta exigencia, aunque en el plano de la legalidad ordinaria, el artículo 64.5 del ET requiere que la empresa recabe informe, no vinculante, de los representantes de los trabajadores con carácter previo a la implantación y revisión del sistema de control del trabajo.

Con todo, según se expondrá posteriormente, el propio Tribunal Constitucional ha corregido la doctrina expresada en la precitada STC 29/2013. Así, la STC 39/2016, de 3 de marzo, ha concluido que las empresas pueden utilizar las imágenes captadas por cámaras de vigilancia, para verificar el cumplimiento de las obligaciones laborales, cuando los trabajadores tengan conocimiento de su instalación a través del correspondiente distintivo informativo situado en el escaparate del comercio. Por otra parte, la STC 170/2013, de 7 de octubre, considera que no es preciso informar a los trabajadores de que se procederá a controlar el uso del material informático propiedad de la empresa, cuando existan directrices sobre la prohibición de su uso que impidan generar una expectativa de confidencialidad en su utilización.

2. EL USO DE MEDIOS TECNOLÓGICOS EN EL CONTROL DE LA ACTIVIDAD LABORAL

2.1. VIDEOVIGILANCIA Y GRABACIONES DE SONIDO

La vídeo-vigilancia permite la captación y grabación en un soporte físico de la imagen mediante sistemas diversos como circuitos cerrados de televisión, grabación por dispositivos *webcam*, digitalización de imágenes o instalación de cámaras. Por consiguiente, esta medida de control incide directamente en el ámbito de los derechos a la propia imagen y a la intimidad. Más aún, como advierte la STC 29/2013, de 11 de febrero, las imágenes grabadas en soporte físico permiten la identificación de los sujetos, por lo que han de ser consideradas como datos de carácter personal incluidos en la cobertura del artículo 18.4 de la CE que consagra el derecho a la protección de datos de carácter personal. Así se deduce también del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), cuyo apartado a) define el concepto de «datos de carácter personal» como «cualquier información concerniente a personas físicas identificadas o identificables», y del artículo 5.1 f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, que define dicho

concepto como «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables»[6].

Por todo ello, si bien la doctrina constitucional admite la grabación de la imagen o el sonido como fórmula para supervisar el cumplimiento de las obligaciones laborales (STC 186/2000, de 10 de julio), establece las siguientes condiciones de validez, tanto de la medida como de la prueba obtenida:

a) Es preciso proporcionar información previa, tanto a los representantes de los trabajadores como a los trabajadores afectados, con relación a la existencia de los medios de vigilancia, así como del tratamiento que se va a dar a los datos obtenidos (STC 29/2013; art. 5 LOPD). Respecto de la necesidad de informar sobre la concreta ubicación de los medios de vigilancia, la doctrina de suplicación se ha pronunciado de forma contradictoria[7], habiendo entendido algún autor que no es necesario informar sobre su emplazamiento exacto siempre que se limiten a grabar los puestos de trabajo[8].

b) En lo que concierne a los fines para los que se puede utilizar la información obtenida a través de la videovigilancia, la doctrina constitucional ha evolucionado desde una tesis garantista de los derechos del trabajador a una posición destinada a asegurar el interés empresarial. En efecto, en un primer momento, se señaló que la empresa únicamente podía utilizar la información obtenida para los fines que expresamente hubiera comunicado al trabajador[9], de forma que si se había informado de que la videovigilancia se utilizaría precisamente para prevenir robos, no cabía utilizar las imágenes captadas para fines disciplinarios. En aplicación de esta doctrina, si la empresa deseaba servirse de las grabaciones con dicho propósito, debía comunicarlo previamente y de forma expresa a los trabajadores, pues de lo contrario la sanción impuesta se consideraba nula[10].

   Como se ha adelantado líneas arriba, la jurisprudencia constitucional ha experimentado un cambio sustancial a raíz de la STC 39/2016, de 3 de marzo, que avala la utilización para fines disciplinarios de las imágenes captadas por cámaras de vigilancia, bastando que los trabajadores tengan conocimiento genérico de su insta-

6 En sentido análogo, véase el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

7 A favor, STSJ de Madrid de 20 diciembre 2006. En contra, STSJ de Cataluña de 5 de julio de 2000.

8 En este sentido, Toscani Giménez, D.: «Vigilancia del trabajador mediante dispositivo GPS colocado en el vehículo de la empresa: límites y garantías. Comentario a la STSJ de Madrid núm. 260/2014, de 21 de marzo», *Revista Boliviana de Derecho*, núm. 19, pág. 755, basándose en la DTC 186/2000, cit.

9 STC 196/2004, de 15 de noviembre.

10 STC 29/2013, cit. STS de 13 de mayo de 2014 (rec. núm. 1685/2013).

lación a través del distintivo informativo situado en el escaparate del comercio[11]. La sentencia señala expresamente que es suficiente tal distintivo a efectos informativos sobre la utilización de la medida, «sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control».

En el caso enjuiciado, el tribunal justifica la medida de videovigilancia en la existencia de «razonables sospechas de que alguno de los trabajadores que prestaban servicios en dicha caja se estaba apropiando de dinero», después de detectar «múltiples irregularidades» tras la implementación de un nuevo sistema de control informático de los saldos de caja. De forma análoga, la existencia de sospechas de hurto de productos de la empresa por parte de los trabajadores justifica, según la doctrina de suplicación, utilizar como prueba las imágenes grabadas mediante cámaras de vigilancia instaladas temporalmente en cuatro puestos de trabajo tras informar al presidente del comité de empresa pero no a los trabajadores afectados[12]. En este sentido, el Repertorio de recomendaciones prácticas de la OIT en materia de protección de datos personales de los trabajadores[13] permite la ausencia de información a los trabajadores (aunque no a sus representantes) respecto de las medidas de vigilancia, cuando existan sospechas suficientes de actividad delictiva u otras infracciones.

Ahora bien, como advierte uno de los votos particulares con que cuenta la sentencia[14], esta nueva doctrina se basa en una premisa errónea, consistente en situar cualquier decisión empresarial en el ámbito de los artículos 33 y 38 de la CE, dotándoles, además, de una posición de paridad con los derechos fundamentales de los trabajadores, susceptible de aparentar una colisión de derechos de igual rango, que da pie a la aplicación del juicio de ponderación y proporcionalidad y finaliza, indefectiblemente, con el reconocimiento de la virtualidad de las facultades empresariales de limitar el contenido esencial de los derechos fundamentales de los trabajadores. Aún más censurable resulta el hecho –que subraya dicho voto particular– de que la sentencia avale esa capacidad de limitar los derechos fundamentales aun en el caso de que el empresario actúe con inobservancia del deber legal de informar a los trabajadores *ex* artículo 5 de la LOPD. A este respecto, el otro voto particular[15] de la sentencia niega que la información facilitada al público sea suficiente para cumplir con este requisito, puesto que el artículo 5 de la LOPD ordena específicamente que la información se dirija a los interesados (en este caso,

[11] Distintivo exigido a los efectos de cumplir con el deber de información previsto en el artículo 5 de la LOPD, por la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

[12] STSJ núm. 84/2015, de Madrid de 9 de febrero (rec. núm. 886 /2014).

[13] OIT, Ginebra, 1997, apartado 6.14.2.

[14] Firmado por el magistrado D. Fernando Valdés Dal-Ré, al que se adhiere la magistrada Dña. Adela Asúa Batarrita. Dicho voto se basa en las razones de fondo que se indican a continuación, así como de forma, en cuanto denuncia la ausencia de la motivación necesaria en caso de cambio de la doctrina precedente en la materia.

[15] Firmado por el magistrado D. Juan Antonio Xiol Ríos.

los trabajadores), información específica que, lejos de constituir un requisito de legalidad ordinaria, forma parte del contenido esencial del derecho. En fin, coinciden los votos discrepantes en observar que la medida empresarial no superaba el test de necesidad, toda vez que tanto en primera instancia como en suplicación se había hecho constar por los respectivos tribunales que existían otros elementos de prueba, independientes de la videovigilancia, suficientes para demostrar los hechos que dieron lugar al despido.

Pese a ello, la decisión mayoritaria del Pleno expresado en la STC 39/2016 concluye que no es necesario informar personalmente a los trabajadores, ni aludir al fin concreto que se dará a dichos medios. No obstante, es preciso plantearse si sería válida la utilización con fines disciplinarios de las imágenes grabadas, si se informó de que se utilizaría para otros propósitos, o se excluyó expresamente la posibilidad de su uso a efectos disciplinarios[16].

c) Aun realizándose en el propio centro de trabajo, no se admite la grabación en lugares pertenecientes a la esfera personal del trabajador, tales como pasillos, baños, vestuarios, comedores, cafeterías, habitaciones de recreo[17], aunque sí en las puertas de estas estancias, siempre que no se visualice el interior[18].

d) Las grabaciones deben ser genéricas no individualizadas respecto de un solo trabajador[19], salvo que existan sospechas razonables de incumplimientos contractuales por parte del trabajador (STC 186/2000, de 10 de julio), aunque habría que informar a los trabajadores y a sus representantes (siquiera en los términos genéricos establecidos en la STC de 3 de marzo de 2016) sobre la introducción de medios de control de la actividad en la empresa[20]. Por otra parte, no se admite, con carácter general, el denominado «test de honestidad», ni la provocación del incumplimiento para grabarlo, pues son medidas contrarias al deber de buena fe y comportan la ausencia de información sobre los medios de control.

e) Conforme al principio de proporcionalidad en el sacrificio del derecho a la intimidad e intervención mínima en dicho derecho (STC 98/2000, de 10 de abril), no se

16 El Informe jurídico 2009-0006: Legitimación para tratamiento de datos de los trabajadores, de la Agencia de Protección de Datos (cit. por Rodríguez Escanciano, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Valencia: Tirant lo Blanch, 2015, pág. 153), señala que no se pueden utilizar las cámaras de vídeo para fines distintos de los confesados, a no ser que no se trate de una finalidad compatible con la expresada en la información.

17 Por todas, SSTSJ de Andalucía de 17 de enero de 1994 (rec. núm. 3183/1993), Galicia de 21 de abril de 1995 (rec. núm. 1036/1995), Castilla y León/Valladolid de 18 de septiembre de 2006 (núm. rec. 1479 /2006), y Madrid 290/2009, de 17 de abril.

18 STS de 7 de julio de 1998 (Sentencia núm. 937/1998); STSJ de Cataluña núm. 3876/2007, de 24 de mayo.

19 STSJ de Castilla y León/Valladolid de 18 de septiembre de 2006 (núm. rec. 1479/2006), cit.

20 Toscani Giménez, D.: «La vulneración del derecho a la intimidad por delatores, detectives privados y medios tecnológicos», *Revista de Derecho Social*, núm. 71, 2015, pág. 71.

grabará audio cuando baste con la toma de imágenes. En consecuencia, por regla general, no se permite la grabación continuada de las conversaciones mediante micrófonos, o escuchas telefónicas. Excepcionalmente, se admite la grabación de las conversaciones telefónicas, sin que ello comporte vulneración del derecho al secreto de comunicaciones ni del derecho a la intimidad, cuando la actividad laboral se desarrolla precisamente de esta forma, en el caso de trabajadores de *telemarketing*, teleoperadores, banca *on-line*, bróker de bolsa, entre otros supuestos que para verificar su correcto desarrollo puede requerir el conocimiento de las comunicaciones con los clientes a través de las grabaciones.

La doctrina judicial indica ciertos límites en la aplicación de este medio de vigilancia: en principio, la grabación se efectuará de forma genérica y no personalizada en un concreto trabajador, de forma aleatoria. Ahora bien, en caso de sospecha de un comportamiento irregular (*v. gr*. por la existencia de quejas de los clientes) es posible incluso focalizar la medida en un concreto trabajador[21]. Por otra parte, el trabajador debe tener conocimiento previo de la posibilidad de que se grave la conversación. Sin embargo, no obsta el derecho al secreto de comunicaciones del cliente el no haber prestado su consentimiento a la grabación, si esta supera el juicio de proporcionalidad (equilibrada, necesaria e idónea)[22].

Conviene, por último, recordar que la grabación de conversaciones propias no atenta contra el secreto de las comunicaciones (art. 18.3 CE)[23] si se limita a aspectos profesionales o laborales[24], y a momentos de trascendencia contractual (negociaciones, despidos, contratación). Por el contrario, la grabación de conversaciones con los compañeros de trabajo traicionaría las expectativas de confidencialidad del trabajador, que se comporta en confianza en esos momentos[25].

2.2. GEOLOCALIZACIÓN MEDIANTE GPS

Como se sabe, el GPS (*Global Positioning System*) constituye un sistema de geolocalización que se puede insertar en vehículos de empresa, teléfonos inteligentes o *smartphones*, *tablets* y otros dispositivos, permitiendo determinar la ubicación de un vehículo y del trabajador en todo

21 STSJ de Andalucía/Granada de 4 de septiembre de 2014 (rec. núm. 1330/2014).

22 En el caso de la STSJ de Andalucía de 4 de septiembre de 2014, anteriormente citada, el medio resultaba idóneo, dado que era la única forma de constatar el tono y volumen de voz utilizado en el trato a los clientes.

23 SSTC 114/1984, de 29 de noviembre y 201/2004, de 15 de noviembre.

24 STS/Civil de 20 de noviembre de 2014 (rec. núm. 3402/2012), relativa a una trabajadora que grabó la conversación con su jefe mientras le despedía. Véase un análisis de la misma en Miñarro Yanini, M.: «Demanda civil contra la denunciante de acoso: La grabación al "jefe" mientras te sanciona no viola su intimidad. Comentario a la Sentencia del Tribunal Supremo, Sala 1.ª, de 20 de noviembre de 2014, rec. núm. 3402/2012», *RTSS.CEF*, núm. 383, febrero 2015.

25 Toscani Giménez, D.: «La vulneración del derecho a la intimidad por delatores, detectives privados y medios tecnológicos», *op. cit.*, pág. 70.

momento. Esta circunstancia implica su potencial incidencia en el derecho del trabajador a no estar localizado en todo momento, mediante dispositivos colocados en sus bienes contra su voluntad, derecho que constituye una manifestación del derecho a la intimidad[26].

En coherencia con la doctrina constitucional sobre información previa a los trabajadores respecto de los medios de control de la actividad laboral, la colocación de GPS con vistas a la supervisión del desempeño será lícita únicamente en la medida en que se haya informado al trabajador tanto de su colocación (en el vehículo[27] o en el móvil[28]), como de la finalidad con que se va a utilizar, aunque esta se exprese de forma genérica[29].

En este sentido, el artículo 5.1 de la LOPD dispone que el interesado debe ser informado previamente a recabar sus datos de carácter personal de modo expreso, preciso e inequívoco: de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información, de las consecuencias de la obtención de los datos, etc. Con relación a la posibilidad de utilizar el GPS para verificar el cumplimiento laboral, la Asociación Española de Protección de Datos, en su Informe 0193/2008, declaró que, si bien del artículo 20.3 del ET se deduce la facultad empresarial de adoptar medidas de vigilancia y control del cumplimiento de las obligaciones y deberes laborales, ello «no excluye el cumplimiento del deber de informar por parte del empresario previsto en el artículo 5.1 de la Ley Orgánica».

En lo que concierne a la proporcionalidad de la medida, la STSJ de Galicia de 6 de junio de 2014 analiza un supuesto en que se admiten como prueba los registros obtenidos con el GPS en un juicio por despido de trabajador vigilante durante el turno de noche. El tribunal concluye que no

---

26 En este sentido, Preciado Domènech, C.H. y Purcalla Bonilla, M. A.: *La prueba en el proceso social*, Cizur Menor: Lex Nova - Thomson Reuters, Aranzadi, 2015, pág. 137, citando la STEDH de 2 de septiembre de 2010, caso *Uzun contra Alemania.*

27 La doctrina judicial [STS 2194/2001, de 21 de junio de 2012 (aunque *obiter dicta*); STSJ de Madrid, núm. 739/2014, de 20 de septiembre de 2014; STSJ de Galicia, núm. 3031/2014, de 6 de junio de 2014 (rec. núm. 903/2014); STSJ del País Vasco, núm. 5122/2011, de 10 de mayo de 2011, rec. núm. 644/2011] se ha pronunciado en favor de tal exigencia, como condición de validez del registro de datos obtenido del GPS, de su utilización como medio de prueba y, en consecuencia, del despido impuesto con base en dichos datos. Asimismo, exigiendo la información por parte de la empresa respecto de la instalación del GPS, véase la STEDH de 2 de septiembre de 2010, cit.

28 STSJ de Castilla-La Mancha, núm. 715/2014, de 10 de junio 201; STSJ del País Vasco de 2 de julio de 2007 (rec. núm. 1175/2007).

29 A la vista de la última doctrina constitucional, el uso con fines disciplinarios de los datos registrados por el GPS no se halla condicionado a la previa información expresa de que existe esta posibilidad, ahora bien, la buena fe impide que se puedan hacer valer con este propósito cuando se especificó que se utilizarían para otros fines. Así, la STSJ de Madrid, núm. 260/2014, de 21 de marzo de 2014, declara ilícita la utilización de los datos obtenidos mediante el GPS para fines disciplinarios, pues en la comunicación de la empresa se informaba de la instalación de un dispositivo GPS «para mayor seguridad tanto del vehículo como del usuario», por tanto, para una finalidad distinta a la que se destinó. Véase un análisis de la misma en Rodríguez Crespo, M. J.: «El derecho a la intimidad informática del trabajador: Un límite más al poder de dirección del empresario», *Temas Laborales*, núm. 128, 2015, págs. 209-217.

ha existido intromisión en la intimidad del trabajador sino que el control a través de GPS es adecuado y proporcionado a la finalidad de controlar el cumplimiento del trabajador en la medida en que la actividad laboral se realizaba fuera de las dependencias de la empresa, por lo que el trabajador no estaba sometido a un control directo en cuanto a su jornada y horario. Es también relevante el hecho de que el sistema no tuviera por objeto captar imágenes íntimas de los trabajadores, sino facilitar el control de la actividad laboral e, incluso, favorecer la propia seguridad de estos. Por lo demás, el dispositivo únicamente registraba cuándo se arrancaba el vehículo y cuándo se detenía, permitiendo situarlo físicamente, y el control se realizaba exclusivamente durante la jornada laboral.

Las anteriores cautelas podrían resultar de aplicación, con las adaptaciones necesarias, a la utilización de las etiquetas de identificación por radiofrecuencia para controlar tanto el acceso de los trabajadores a la empresa como su actividad laboral, dado que permiten identificar de forma individualizada a los trabajadores, registrar datos y transmitir información a distancia[30].

2.3. REGISTRO DE HUELLAS DACTILARES

El reconocimiento de la huella dactilar, mediante un mecanismo de lectura biométrica de la mano por medio de un escáner que utiliza rayos infrarrojos, es un sistema utilizado de forma habitual para controlar el acceso y salida del puesto de trabajo. Sobre la validez de esta medida de control de la actividad laboral, se ha pronunciado la jurisprudencia concluyendo que no supone una intromisión de la intimidad del trabajador, en cuanto su finalidad es legítima y no constituye una medida desproporcionada[31].

Los conflictos planteados en la materia se han dirigido además a cuestionar la implantación del control horario mediante la huella dactilar sin consentimiento de los trabajadores afectados, si bien la doctrina de suplicación ha negado la necesidad de dicho consentimiento[32], con apoyo en el artículo 6.2 de la LOPD[33].

30 Para un análisis más detallado de este medio de control, véase Gala Durán, C. y Roig i Batalla, A.: «El uso de las etiquetas de identificación y radiofrecuencia en las empresas ¿un nuevo riesgo para los derechos de los trabajadores?», *Actualidad Laboral*, núm. 8, 2010, págs. 1 y ss.; Llamosas Trapaga, A.: *Relaciones laborales y nuevas tecnologías de la información y de la comunicación. Una relación fructífera no exenta de dificultades*, Madrid: Dykinson, 2015, págs. 157-163.

31 STS, Sala de lo Contencioso-Administrativo, de 2 de julio de 2007 (rec. núm. 5017/2003), relativa a la implantación de dicho sistema de control para el personal (tanto funcionario, como laboral) de la Comunidad Autónoma de Cantabria. Sobre la cuestión, véase Selma Penalva, A.: «El control de acceso por medio de huella digital y sus repercusiones sobre el derecho a la intimidad de los trabajadores», *Revista Doctrinal Aranzadi Social*, núm. 5, 2013.

32 STSJ de Canarias, núm. 914/2012, de 29 de mayo, con base en la mencionada STS, Sala de lo Contencioso-Administrativo, de 2 de julio de 2007.

33 Según el citado precepto: «No será preciso el consentimiento cuando los datos de carácter personal (…) se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento (…)».

2.4. VIGILANCIA POR DETECTIVES PRIVADOS

Uno de los recursos más comúnmente utilizados para el control de la conducta del trabajador fuera de la empresa con repercusión en su faceta laboral es la contratación de detectives privados. A sus servicios pueden acudir las empresas cuando existen sospechas de comportamientos extralaborales inadecuados, en especial con relación a las situaciones de competencia desleal, cumplimiento de pactos de dedicación exclusiva, control del rendimiento, uso del crédito horario por los representantes de los trabajadores y bajas por incapacidad temporal, que constituyen en la actualidad el grueso central de sus encargos. Si bien la necesidad de que existan previas sospechas fundadas no se establece de forma categórica por la normativa aplicable ni por la doctrina judicial, tal exigencia se puede deducir de los numerosos pronunciamientos que justifican la intromisión en la existencia de previas sospechas[34].

El valor probatorio del informe emitido por un detective privado, que precisa de ratificación en el acto de juicio, es el de una prueba testifical[35], no documental, ni pericial[36]. No obstante se trata de una prueba cualificada, habida cuenta la especial dedicación a dicha actividad en ejercicio de una profesión reglamentada[37]. Dicha consideración como mera prueba testifical determina que su valoración quede sometida a las reglas de la sana crítica, conforme al artículo 659 de la LEC, y no permita sustentar la revisión de hechos probados en suplicación ni en casación[38].

El Tribunal Supremo ha admitido expresamente la validez de la supervisión de la conducta extralaboral del trabajador para comprobar el estado de salud del trabajador de baja por incapacidad temporal o la actividad concurrente con la empresa, concluyendo que no implica una vulneración del derecho a la intimidad del trabajador la utilización de una agencia de investigación, cuyo informe se utiliza en el acto del juicio como medio de prueba de las actividades que dicho

34 Véase, en este sentido, Saiz de Marco, I.: «La "prueba de detectives" en la doctrina judicial», *Actualidad Laboral*, núm. 12, 2014. Por todas, ATC 99/1991, de 21 de marzo; STS de 13 de marzo de 2012 (rec. núm. 1498/2012); y SSTSJ de Madrid de 5 de julio de 2013 (rec. núm. 823/2013), Andalucía/Granada de 24 de mayo de 2012 (rec. núm. 738/2012) y País Vasco de 26 de enero de 2010 (rec. núm. 2607/2009).

35 STS de 17 de junio de 1996 (rec. núm. 1611/1995). Montoya Melgar, A.; Galiana Moreno, J. M.; Sempere Navarro, A. V.; Ríos Salmerón, B.; Cavas Martínez, F. y Luján Alcaráz, J.: *Curso de procedimiento laboral*, Madrid: Tecnos, 2014, pág. 180.

36 SSTSJ de Andalucía de 14 junio 2012, rec. núm. 2535/2011, y de Cataluña de 27 febrero 2013, rec. núm. 6343/2012.

37 STSJ de Madrid 603/2013, de 5 julio de 2013. Por esta razón, se ha propuesto *de lege ferenda* su consideración como prueba pericial (López Aniorte, M. C.: «Límites constitucionales al ejercicio del poder directivo empresarial mediante el uso de las TIC y otros medios de vigilancia y seguridad privada en el ordenamiento jurídico español», *Revista Policía y Seguridad Pública*, vol. 1, 2014, pág. 51).

38 Entre otras, STS de 25 de marzo de 2002 (RCUD 1292/2001), STSJ de Cataluña, núm. 9532/2001, de 4 de diciembre y STSJ de Madrid, núm. 578/2007, de 27 junio.

trabajador realizada durante su periodo de inactividad, ya que no existe la posibilidad de utilizar medios de vigilancia alternativos[39].

El seguimiento se ha de producir en espacios públicos, ya se trate de la vía pública, ya de establecimientos abiertos al público (locales, comercios, bares, etc.), en los que haya otras personas que también podrían haber visto u oído lo mismo[40], pero no se admite la vigilancia en domicilios o espacios privados[41]. En este sentido, el artículo 48.3 de la Ley 5/2014, de 4 de abril, de Seguridad Privada (LSP), establece expresamente que «(e)n ningún caso se podrá investigar la vida íntima de las personas que transcurra en sus domicilios u otros lugares reservados».

El interés de este medio de supervisión respecto del tema objeto de este estudio radica precisamente en que el informe del detective se apoya en otras pruebas como fotografías o reproducción de videos[42], que según la doctrina judicial serán válidos siempre que se trate de imágenes o grabaciones tomadas en un espacio público[43], y se hayan obtenido con medios materiales o técnicos que no atenten contra el derecho al honor, a la propia imagen, a la intimidad personal o familiar, al secreto de las comunicaciones o a la protección de datos [arts. 10.1 d) y 48.3 LSP].

Por el contrario, la obtención de datos mediante un GPS colocado por el detective privado en el vehículo del trabajador, sin informarle de este hecho, ha sido considerado un medio de prueba ilegítimo por vulnerar el derecho a la intimidad y a la protección de datos del afectado. La doctrina judicial considera que este medio de control no respeta el principio de proporcionalidad puesto que permite tener un conocimiento continuo y permanente, a lo largo del día y de la noche, del lugar donde se encuentra el trabajador, así como de otros datos complementarios (itinerarios, tiempos de utilización del vehículo, pausas, kilómetros recorridos y velocidad de circulación)[44].

En otro orden de consideraciones, la necesidad de que se informe previamente a los trabajadores sobre los medios de control utilizados con carácter habitual en la empresa impide el recurso a personal infiltrado, de plantilla o contratado *ad hoc*, cuya identidad desconocen los trabajadores. La utilización de tal figura iría contra las expectativas de confidencialidad del trabajador, que no

39 Por todas, véase la STS de 6 enero 1988. En la doctrina de suplicación, entre otras, STSJ del País Vasco de 10 de mayo de 2011, rec. núm. 644/2011.

40 STEDH de 27 de mayo de 2014, asunto *De La Flor Cabrera c. España*.

41 SSTS núm. 13116 /1989, de 19 de julio y núm. 17467/1990, de 6 de noviembre.

42 La doctrina judicial ha admitido la validez de este tipo de documentos digitales como medio de demostrar la realización de actividades laborales por parte de los trabajadores durante el periodo de incapacidad temporal [entre otras, STSJ de Galicia de 22 de noviembre de 2002 (rec. núm. 4211/2002) y STSJ de Murcia de 15 de julio de 2002].

43 Afectan a la intimidad y a la inviolabilidad del domicilio las fotografías tomadas en el interior del domicilio del trabajador, *v. gr*. en el garaje, como recuerda la STSJ de Cataluña núm. 2061/2005, de 8 marzo.

44 Así lo entiende la STSJ del País Vasco de 10 de mayo de 2011 (rec. núm. 644/2011). En sentido análogo, aunque *obiter dicta,* la STS 2194/2001, de 21 de junio de 2012.

se comportará de igual forma entre compañeros y amigos que en presencia de su jefe o empresario, o de persona en quien este delegue para supervisar la actividad laboral[45].

3. EL CONTROL DEL USO DE MEDIOS INFORMÁTICOS DE TITULARIDAD EMPRESARIAL

3.1. TOLERANCIA EMPRESARIAL Y LÍMITES AL CONTROL EMPRESARIAL

Uno de los problemas más habituales relacionados con el uso del material informático facilitado por la empresa como herramienta de trabajo viene dado por los límites de la tolerancia de su utilización para fines personales durante la jornada (*v. gr*. el acceso a internet, el uso del correo electrónico), y las facultades de control de la actividad del trabajador en tiempo y lugar de trabajo.

A efectos de valorar su correcta utilización, el empresario precisa averiguar si se ha realizado durante el transcurso de la jornada en detrimento de su rendimiento laboral, lo que exige a su vez determinar si se ha tratado de una actuación puntual o abusiva, e incluso si el contenido de los archivos y mensajes está relacionado con la actividad laboral.

En lo que atañe al uso del ordenador facilitado al trabajador por el empresario, la STS de 26 de septiembre de 2007[46] ha señalado que el registro de dicho equipamiento no se regula por el artículo 18 del ET, sino por el artículo 20.3 del mismo texto legal, ya que la legitimidad de este control no se justifica en la necesidad de proteger el patrimonio empresarial, sino que deriva del carácter de instrumento de producción del objeto sobre el que recae. El citado pronunciamiento rechaza la equiparación entre las taquillas existentes en el lugar de trabajo para que el trabajador deposite sus objetos personales y las carpetas virtuales con información personal incluidas en la memoria de un equipo informático que se utiliza para el desarrollo de la actividad laboral. De ahí que la información contenida en carpetas de ficheros informáticos no se pueda beneficiar de las cautelas previstas en el artículo 18 del ET[47], que, como se sabe, exige que el registro se realice en el lugar y tiempo de trabajo, en presencia de un representante de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible.

No obstante, esta distinción se efectúa en el plano de la legalidad ordinaria, y, como ha precisado la mencionada sentencia, no obsta al respecto de la dignidad del trabajador (art. 20.3 ET)

[45] Toscani Giménez, D.: «La vulneración del derecho a la intimidad por delatores, detectives privados y medios tecnológicos», *op. cit*., pág. 66.

[46] Rec. núm. 966/2006.

[47] En este sentido, véase también la STSJ de Asturias, núm. 2144/2013 de 15 de noviembre.

y, por tanto, a la aplicación de las garantías del derecho a la intimidad (art. 18.1 CE) tanto a los archivos personales del trabajador que se hallen en el ordenador, como al historial de navegación por internet. Y es que esta labor de supervisión puede afectar a los derechos a la intimidad del trabajador (art. 18.1 CE), a la protección de datos de carácter personal (art. 18.4 CE), y al secreto de las comunicaciones (art. 18.3 CE)[48], cuando se trata de controlar los correos electrónicos y otras vías de mensajería instantánea (Skipe, Messenger, WhatsApp, Line, etc.)[49].

Con carácter general, la validez del registro y, por tanto, de la prueba obtenida con relación al uso del material informático y el acceso a internet, se halla en función de la existencia y contenido de directrices empresariales en la materia. Se trata de reglas que el empresario está facultado a dictar, en la medida en que se refieren al uso de equipamiento informático y medios de comunicación de los que es titular (teléfono, correo electrónico e internet), debiendo ser conocidas y respetadas por el asalariado. En este sentido, la precitada STS de 26 de septiembre de 2007 distingue dos supuestos:

a) La ausencia de normas o limitaciones expresas respecto al uso de los medios informáticos comporta una mayor tolerancia empresarial del uso extralaboral de estas herramientas, contribuyendo a generar expectativas de intimidad en el uso del material informático. Desde luego, ello no quiere decir que la empresa renuncie a sus facultades de control sobre el uso de dicho material[50], ahora bien, de conformidad con las exigencias de la buena fe, la empresa debe informar previamente a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos[51], sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

48 Según la STS, Sala Penal, núm. 2844/2014, de 16 de junio de 2014, el control de los denominados «datos de tráfico» o incluso de la posible utilización del equipo informático para acceder a otros servicios de la red como páginas web, etc., queda amparado por el derecho a la intimidad (art. 18.1 CE) pero no por el secreto de las comunicaciones (art. 18.3 CE), lo que excluye la necesidad de autorización judicial previa a su control. Con todo, el artículo 90.4 de la LRJS exige expresamente tal autorización para acceder a «documentos o archivos, en cualquier tipo de soporte, que pueda afectar a la intimidad personal u otro derecho fundamental».

49 La STEDH de 3 de abril de 2007, asunto *Copland contra Reino Unido,* concluye que la recogida y almacenamiento de información personal relativa al correo electrónico y la navegación por internet de una trabajadora, sin su conocimiento, vulnera su derecho al respeto de su vida privada y su correspondencia, de conformidad con el artículo 8 del Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales, por cuanto pueden contener datos sensibles que afecten a la intimidad y al respeto a la vida privada.

50 Por ejemplo, la STSJ de Cataluña, núm. 841/2011, de 3 de febrero, pese a existir en la empresa una tolerancia de un uso moderado de internet para fines personales, considera abusiva su utilización para entrar en determinadas páginas web altamente peligrosas, comprometiendo la seguridad de los equipos electrónicos de la empresa.

51 STS de 8 de marzo de 2011 (RCUD 1826/2010). A ello se suma la obligación de la empresa de recabar el informe previo de los representantes unitarios, según dispone el artículo 64.5 del ET, al que se ha hecho referencia anteriormente.

b) Por el contrario, si existen limitaciones expresas al uso extralaboral de los equipos o el acceso a internet, el quebrantamiento de dichas directrices constituye una conducta desobediente sancionable, salvo «que la empresa hubiera venido tolerando este tipo de incumplimientos, o que no se sancione a otros trabajadores por similar conducta»[52].

Cuando se establece una prohibición absoluta y tajante de su utilización para fines personales[53], expresamente advertida en el régimen disciplinario vigente o en directrices internas de la empresa sobre el uso lícito del material informático facilitado por la empresa, no existe una situación de tolerancia, por lo que la doctrina judicial entiende que tampoco se genera una expectativa razonable de confidencialidad. En consecuencia, si la empresa decide realizar un control de la correcta y diligente utilización de los medios informáticos puestos a disposición de sus empleados, no se produce vulneración del derecho de estos a la intimidad[54], y la eventual prueba del incumplimiento se considerará obtenida lícitamente, permitiendo justificar un despido disciplinario[55].

A diferencia de lo que ocurre en los supuestos de tolerancia del uso moderado para fines particulares o prohibición relativa, existiendo una prohibición absoluta, la STS de 6 de octubre de 2011 ha negado la exigencia de previa comunicación al trabajador de que se va a proceder a un control del ordenador[56], interpretación co-

52 Sempere Navarro, A. V., y Sanmartín Mazzucconi, C.: «¿Puede la empresa controlar el ordenador usado por su trabajador?», *Aranzadi Social*, núm. 7, 2007, pág. 369. Véase, también, Roqueta Buj, R.: «El despido por la utilización personal de los medios tecnológicos de información y comunicación de la empresa», *Actualidad Laboral*, núm. 2, 2005, págs. 2.246-2.257.

53 Aunque la prohibición absoluta ha sido admitida por la jurisprudencia [*v. gr.* STS de 6 octubre 2011 (RCUD 4053/2010)], deberá permitirse necesariamente el uso de internet y otros medios informáticos de la empresa para fines sindicales, toda vez que según la doctrina judicial (STSJ de Madrid, núm. 31/2001, de 26 de marzo) ha de considerarse como un uso profesional de la red, aunque no se vincule directamente a la concreta prestación laboral, por ser consustancial a la relación laboral (Sempere Navarro, A. V. y Sanmartín Mazzucconi, C.: *Nuevas Tecnologías y Relaciones Laborales*, Cizur Menor: Aranzadi, 2002, pág. 245). Es más, la doctrina constitucional ha reconocido que el derecho al uso del correo electrónico corporativo ya existente en la empresa para la distribución de información sindical forma parte del derecho a la libertad sindical, si bien al tratarse de medios de propiedad de la empresa, su utilización no podrá perjudicar el uso específico empresarial de dicho medio de comunicación, ni deberá imponer a la empresa gravámenes o costes adicionales (STC 281/2005, de 7 de noviembre). Precisando esta doctrina, la STS 2109/2015, de 24 marzo 2015, ha concluido que resulta constitucionalmente lícito que la empresa predetermine las condiciones de utilización para fines sindicales de las comunicaciones electrónicas, siempre que no las excluya en términos absolutos.

54 STS de 6 de octubre de 2011, cit. En la doctrina de suplicación, véanse las SSTSJ de Andalucía/Granada núm. 222/2012, de 26 enero, y de Murcia núm. 988/2013, de 14 octubre.

55 STSJ de Andalucía/Granada, núm. 2083/2013, de 14 noviembre.

56 RCUD 4053/2010. Esta sentencia corrige a la previa STS de 26 de septiembre de 2007 (RCUD 966/2006), según la cual, la exigencia de buena fe en el control empresarial requiere que la empresa establezca previamente las reglas de uso de los medios informáticos, e informe a los trabajadores de la existencia de control y de los medios empleados para este fin.

rroborada por la STC 170/2013, de 7 de octubre, en los términos que se analizarán en el siguiente epígrafe[57].

Se ha confirmado, incluso, la validez de la prueba obtenida y, por consiguiente, la procedencia del despido del trabajador que, pese a la radical prohibición de utilizar internet para fines personales en tiempo de trabajo, utilizó la clave *wifi* de la empresa para navegar por determinadas páginas web y visionar películas durante su jornada de trabajo, a través de un dispositivo de su propiedad[58].

3.2. PARTICULAR REFERENCIA AL CONTROL DEL CORREO ELECTRÓNICO Y LA MENSAJERÍA

Como se ha apuntado anteriormente, el control del correo puede vulnerar el derecho genérico a la intimidad del trabajador (STC 173/2011, de 7 de noviembre), así como su derecho al secreto de las comunicaciones (art. 18.3 CE), si bien este último derecho protege únicamente ciertas comunicaciones: las que se realizan a través de determinados medios o canales cerrados.

Por ello, el secreto de las comunicaciones no se ve afectado cuando el trabajador instala una aplicación de mensajería, sin clave, en un ordenador colectivo de la empresa, con lo que el acceso al contenido de los mensajes queda abierto a cualquier usuario de dicho ordenador (STC 241/2012, de 17 de diciembre), de forma que el trabajador no puede alegar una expectativa de secreto de su comunicación[59].

Es más, a tenor de la STC 170/2013, de 7 de octubre, tampoco comporta una vulneración del derecho al secreto de las comunicaciones ni del derecho a la intimidad la supervisión de los correos electrónicos de los empleados, sin previa información por parte de la empresa, cuando el convenio colectivo prohíba o sancione el uso de las herramientas informáticas y el correo electrónico para uso particular. Este criterio ha sido, con razón, criticado por un sector doctrinal, en cuanto atribuye a la empresa el poder exorbitante de convertir el correo en un medio abierto de comunicación[60], mediante el establecimiento de directrices que prohíban su uso para fines particulares. Corolario de lo anterior es que dicha prohibición del uso del correo para fines particulares tiene la virtualidad de excepcionar la exigencia constitucional de autorización judicial respecto

57 Por razones análogas, las expectativas de intimidad se verán considerablemente reducidas de existir acuerdos o cláusulas pactadas en convenio colectivo, que prevean la posibilidad de auditorías periódicas de los sistemas informáticos y de comunicación del trabajador, ya sea mediante controles remotos o presenciales. Tal es el caso de los acuerdos en materia de teletrabajo en Telefónica España o en el BBVA. Para un estudio particularizado de la cuestión, véase García Romero, B.: *El Teletrabajo*, Madrid: Civitas, Thomson Reuters, 2012, págs. 116-122.

58 STSJ de Asturias, núm. 2144/2013, de 15 noviembre.

59 Ahora bien, en lo que concierne al respecto del derecho de intimidad, no es determinante que el ordenador no tuviera clave de acceso (STS de 26 de septiembre de 2007).

60 Rodríguez Escanciano, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op. cit*., págs. 98 y 99, con relación a la STSJ de Madrid de 29 de octubre de 2012 (rec. núm. 4309/2012).

de la injerencia en el correo (art. 18.3 CE)[61]. Conviene también recordar en este punto que en el ámbito laboral, el artículo 90.4 de la LRJS establece que «[c]uando sea necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que pueda afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existan medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto, previa ponderación de los intereses afectados a través de juicio de proporcionalidad y con el mínimo sacrificio»[62].

Aunque refiriéndose exclusivamente al ámbito penal, la Sala 2.ª del Tribunal Supremo, en su Sentencia de 16 de junio de 2014[63], ha insistido en la exigencia de autorización judicial previa, «cualquiera que fueren las circunstancias o personas, funcionarios policiales, empresarios, etc., que tales injerencias lleven a cabo», rechazando que la titularidad empresarial de la herramienta comunicativa, el carácter corporativo del medio de comunicación utilizado o su uso durante la jornada laboral implique una renuncia tácita a la confidencialidad o al derecho al secreto de la comunicación. No obstante, esta resolución ha precisado que los mensajes, «una vez recibidos y abiertos por su destinatario», pasan a ser considerados ficheros de datos, de suerte que no forman ya parte de la comunicación propiamente dicha, como tampoco los datos de tráfico (circunstancias de tiempo, líneas utilizadas, duración de la comunicación, etc.), por lo que no gozan de la tutela del derecho al secreto de las comunicaciones (art. 18.3 CE)[64], ni su lectura requiere autorización judicial previa[65]. Ahora bien, como ha advertido en esta misma sentencia, el hecho de que no se vean amparados por el secreto de las comunicaciones no impide que a los correos leídos se apliquen las garantías propias tanto del derecho a la protección de datos (art. 18.4 CE), lo que exige previa información al trabajador sobre la revisión y el tratamiento de los datos obtenidos (duración, fines, etc.), como del derecho a la intimidad de las personas (art. 18.1 CE).

Esta tesis de la Sala Segunda del Tribunal Supremo plantea una clara discrepancia en los ámbitos penal y laboral (a la vista de la doctrina expresada en el ámbito laboral por la STC 170/2013)[66], en lo que concierne a los límites al control empresarial de las comunicaciones por ordenador, y recuerda a la sentada por la STS de 26 de septiembre de 2007, según la cual, el hecho

61 Aberasturi Gorriño, U.: «Control empresarial del correo electrónico del empleado y relevancia de la información previa a los trabajadores como garantía mínima para ejercer ese control, a la luz de la STC de 7 de octubre de 2013», *Nueva Revista Española de Derecho del Trabajo*, núm. 180, 2015, pág. 217.

62 Toscani Giménez, D.: «La vulneración del derecho a la intimidad por delatores, detectives privados y medios tecnológicos», *op. cit*., pág. 87.

63 Rec. núm. 2229/2013.

64 En consecuencia, cuando la empresa, en ejercicio de sus facultades de vigilancia, procede a la lectura de los mensajes abiertos o al control de los datos de tráfico de las comunicaciones, no incurre en el delito contra el secreto de las comunicaciones tipificado en el artículo 197 del CP.

65 Ahora bien, esta doctrina se puede prestar a abusos, pues el trabajador podría marcar sus correos como no leídos. En tal caso, la empresa deberá valerse de un perito informático para destruir la presunción que se genera en favor del secreto de la comunicación.

66 Arbonés Lapena, H. I.: «Grabación de imagen o sonido y control de correo electrónico por el empresario», *Nueva Revista Española de Derecho del Trabajo*, núm. 178, 2015, pág. 216.

que el ordenador no tenga clave de acceso y esté localizado en un despacho sin llave, no supone una aceptación por parte del trabajador del acceso abierto a la información contenida en su ordenador, por lo que no es obstáculo para la protección de su intimidad. Pero, sobre todo, refleja un distinto y muy significativo posicionamiento respecto de la relación entre los derechos de propiedad (de los equipos y sistemas informáticos utilizados) y a la libertad de empresa, de un lado, y los derechos fundamentales de los trabajadores, como ciudadanos que son. De esta suerte, el orden penal de la jurisdicción asume hoy la posición garantista frente al ejercicio de los poderes empresariales de auto-tutela[67], que en otro tiempo fue el *leitmotiv* del orden social de la jurisdicción.

Por otra parte, algún autor ha criticado la doctrina constitucional en la medida que hace extensivo el criterio de control del correo electrónico corporativo a los sistemas de mensajería instantánea, instalados con fines particulares, pues no tienen vocación profesional, de ahí que el incumplimiento de las directrices que prohíben de forma absoluta el uso de material informático para fines particulares puedan justificar el ejercicio del poder disciplinario, pero no habiliten al empresario para fiscalizar su contenido, ni permitan fundar posibles sanciones con base en las afirmaciones contenidas en dichos mensajes, salvo que medie la necesaria autorización judicial[68]. Por el contrario, si se trata de una cuenta de mensajería instalada con fines laborales, sería posible sancionar al trabajador que la utilizara para fines privados. En este sentido, la STEDH de 12 de enero de 2016 ha concluido que no existe vulneración del derecho a la inviolabilidad de la correspondencia, ni del derecho a la intimidad (art. 8 Convenio Europeo de Derechos Humanos y Libertades Fundamentales), por el hecho de que la empresa supervise las comunicaciones mantenidas por el trabajador a través de una cuenta de Messenger, en un supuesto en que la cuenta de correo había sido creada por el trabajador a instancia de la empresa para exclusivos fines de comunicación con los clientes, y estaba terminantemente prohibido su uso para fines particulares[69].

La facultad así conferida al empresario plantea, en fin, serias dudas de compatibilidad con los derechos a la intimidad y al secreto de las comunicaciones de los terceros no vinculados mediante una relación laboral con el empresario, que reciben y envían correos o mensajes al trabajador a través del medio de comunicación corporativo. Por esta razón, se ha afirmado la necesidad de cumplir con las exigencias de transparencia en el referido control, recurriendo a elementos de

67 Molina Navarrete, C.: «Autotutela empresarial, secreto de comunicaciones y control judicial: La Sala Social pierde el paso con la Sala Penal. Comentario a la Sentencia del Tribunal Supremo, Sala 2.ª, de 16 de junio de 2014, rec. núm. 2229/2013», *RTSS.CEF*, núm. 381, 2014, págs. 158 y 162.

68 Goñi Sein, J. L., en «Los límites de las potestades empresariales vs. Derecho a la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral de las redes sociales», *Actum Social*, núm. 95, 2015.

69 En el supuesto enjuiciado por la STEDH de 12 de enero de 2016 (asunto *Bărbulescuv. Rumanía*, núm. 61496/08), el trabajador había sido despedido porque la empresa comprobó que había mantenido comunicaciones con familiares y amigos, a través de la cuenta creada en el programa informático Yahoo Messenger, puesto a disposición por la empresa para su trabajo profesional, pese a que había prohibido su uso privado. El Tribunal de Estrasburgo concluye que la empresa no pretendió en ningún momento comprobar o controlar aspectos de la vida privada del trabajador, sino controlar el cumplimiento de sus deberes laborales, por cuanto creía que la cuenta de correo solo contenía comunicaciones con los clientes de la empresa.

configuración del correo que permitan advertir a los comunicantes externos que se están relacionando con un correo corporativo que puede ser abierto por persona distinta de aquella a la que va dirigida[70], de forma análoga a los avisos que se utilizan en caso de grabación de las conversaciones telefónicas mantenidas con servicios de atención al cliente.

3.3. VALOR Y EFICACIA DE LA PRUEBA BASADA EN EL CORREO ELECTRÓNICO Y LA MENSAJERÍA

El ejercicio de la facultad empresarial de control de la actividad laboral en los términos anteriormente expuestos se puede traducir en la imposición de sanciones, cuya eventual impugnación requerirá la aportación al proceso laboral de las pruebas obtenidas mediante la revisión del ordenador, consistentes, en su caso, en mensajes de correo electrónico y mensajería móvil (SMS, WhatsApp, Messenger, Line, Tuenti, Twitter, etc.). Pese a su consideración técnica como prueba electrónica con base en el artículo 384 de la LEC, la doctrina de suplicación viene atribuyendo a este medio de prueba el valor de prueba documental en cuanto se aporta al juicio una copia impresa de la captura del contenido que se visualiza en la pantalla («pantallazo») o transcripción de los mensajes, de forma que permiten sustentar la revisión fáctica en suplicación[71].

No obstante, cuando se aporta como medio de prueba la mera transcripción escrita o la representación gráfica de la conversación o copia de la información que aparece en pantalla a modo de impresión fotográfica, la valoración de la información proporcionada a través de la mensajería instantánea debe realizarse con la máxima cautela, por el riesgo que existe de manipulación del contenido (mediante la creación o edición de un documento que imite la estructura lógica y presentación de mensajes) o de suplantación de identidad de su autor.

A fin de dar valor de prueba de cargo o descargo a estas conversaciones, el artículo 382.2 de la LEC permite la aportación de elementos de convicción instrumentales, por lo que es posible acudir a otras fuentes probatorias como la prueba testifical o el interrogatorio de parte, siendo relevante la ratificación del contenido por parte de los interlocutores o la actitud silente de la parte a quien perjudican.

En caso de impugnación formal de la prueba, es conveniente la aportación de prueba pericial. En este sentido se ha manifestado una importante jurisprudencia en materia penal, de la que es claro exponente la STS de 19 de mayo de 2015[72], en la que se valora la impresión en papel de

70 Desdentado Bonete, A. y Muñoz Ruiz, A. B.: «Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia», *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 39, 2014, pág. 24.

71 Respecto del correo electrónico impreso, véase la STSJ de Aragón 822/2010, de 17 de noviembre. Con relación a los mensajes de texto SMS o WhatsApp, STSJ de Aragón, núm. 145/2015, de 16 de marzo.

72 Un interesantísimo comentario de la misma se puede encontrar en Rodríguez Laínz, J. L.: «Sobre el valor probatorio de conversaciones mantenidas a través de programas de mensajería instantánea (A propósito de la STS, Sala 2.ª, 300/2015, de 19 de mayo)», *Diario La Ley*, núm. 8569, 2015.

los pantallazos de conversaciones tipo mensajería instantánea mantenidas a través de la aplicación Tuenti móviles. Como sostiene la citada sentencia, en los supuestos de mera aportación del contenido de mensajes, la impugnación formal de su eficacia probatoria lleva inevitablemente a la necesidad de que la parte que aporta la prueba asuma la carga de realizar una prueba pericial que corrobore cuestiones referentes a su autenticidad e inalterabilidad[73].

4. LA INFORMACIÓN REFLEJADA EN LAS REDES SOCIALES COMO BASE DEL EJERCICIO DEL PODER DISCIPLINARIO

A diferencia de los medios de prueba que puede obtener el empresario en el ejercicio de su facultad de vigilancia y control del cumplimiento de la actividad laboral, mediante el recurso a detectives privados y grabaciones, la utilización de dispositivos GPS o mediante la inspección de los equipos de trabajo utilizados, en las redes sociales (Facebook, Twitter, etc.) se pueden encontrar, de forma sobrevenida, indicios de posibles incumplimientos contractuales del trabajador (fraude en bajas de incapacidad temporal, competencia desleal, comentarios peyorativos e insultos hacia compañeros o superiores, etc.).

El hallazgo, a menudo causal, de esta información publicada por el propio trabajador o por sus conocidos, puede desencadenar el ejercicio del poder disciplinario, lo que obliga a plantearse cuál es la naturaleza de este medio de prueba y hasta qué punto y con qué límites la información reflejada en una red social tiene fuerza probatoria.

4.1. LA RED SOCIAL, DELATORA

La casuística de los comportamientos reflejados en la red social es muy variada, como también lo es el soporte a través del cual se incluye la información incluida en la red social (fotografías, vídeos, comentarios, etc.), y la forma en que la empresa ha podido acceder a ella. Merece la pena efectuar un repaso sucinto de los supuestos que, normalmente como resultado de un hallazgo casual, pueden desencadenar el ejercicio del poder disciplinario[74].

a) En ocasiones, la información conseguida en las redes sociales ha permitido constatar la existencia de quebrantamiento del deber de buena fe contractual, consistente

[73] A tenor de la STS 342/2013, de 17 de abril, la valoración y análisis pericial de los datos analizados respecto de comunicaciones cuya realidad o autenticidad se cuestiona, es el pilar fundamental en el que se deberá asentar el juicio de valoración de estos medios de prueba.

[74] Para un estudio *in extenso* de la casuística en la materia, véase Rodríguez Escanciano, S.: Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores, *op. cit*., págs. 88-96.

en el desarrollo por el trabajador, fuera de su jornada y lugar de trabajo, de actividades incompatibles con la situación de incapacidad temporal, que evidencian una situación de fraude en el disfrute de la situación, porque presuponen la efectiva capacidad laboral del trabajador, o que perjudican o demoran su recuperación. En estos casos, la prueba electrónica (en forma de fotografías o comentarios) obtenida por la empresa a través de una red social, por sí sola[75] o, más habitualmente, valorada de forma conjunta con otro tipo de elementos probatorios (pericial, testifical por detective, etc.)[76], permite sustentar la procedencia de la sanción impuesta.

En la *praxis* judicial, se han detectado asimismo otros incumplimientos sancionables conforme al artículo 54.2 d) del ET, relacionados con la prohibición de competencia desleal con la propia empresa[77], o la utilización para fines personales de mercancías propiedad de la empresa[78].

b) Con relación al supuesto de hecho tipificado como causa de despido en el artículo 54.2 c) del ET, el citado precepto se refiere a «las ofensas verbales o físicas al empresario o a las personas que trabajan en la empresa o a los familiares que con ellos convivan», aunque no alude expresamente a las ofensas virtuales o divulgadas por escrito a través de Facebook. Por ello, la doctrina se ha planteado si cabe efectuar una interpretación extensiva del supuesto, para equiparar dichas ofensas virtuales a las puramente verbales, en virtud del artículo 3 del CC, dado que la ausencia de referencia a dicha forma de ofensas no proviene de un afán de exclusión de las mismas, sino de la imposibilidad de prever dicha situación en el momento en el que se promulgó el ET, concluyendo que esta subsunción es posible[79].

Asimismo, con relación a la valoración de los comentarios u opiniones vertidos en Facebook o en blogs personales de los trabajadores, parece claro que se deben emplear «las mismas reglas de modulación de la gravedad de la falta, utilizados tradicionalmente para valorar la gravedad de las expresiones verbales»[80]. De ahí que

75 *Cfr*. STSJ de Madrid, núm. 32/2012, de 23 de enero, y STSJ de Galicia, núm. 5601/2012, de 16 de noviembre.

76 De forma que la confirmación judicial de la procedencia del despido disciplinario se obtendrá gracias a la concurrencia de diversos medios de prueba conducentes a la misma conclusión (Selma Penalva, A.: «La información reflejada en las redes sociales…», *op. cit*., pág. 380). Para un ejemplo, véase el supuesto enjuiciado en la STSJ de Asturias, núm. 1333/2013, de 14 de junio.

77 En este sentido, véanse las SSTSJ de Murcia, núm. 582/2012, de 16 de julio, y de Madrid, núm. 475/2012, de 25 de junio.

78 *V. gr*. STSJ de Castilla y León/Valladolid de 28 de noviembre de 2013 (rec. núm. 1446/2013).

79 La STSJ de Castilla y León/Valladolid de 30 de abril de 2014 (rec. núm. 491/2014) considera procedente el despido de la trabajadora que subió a Facebook dos vídeos en los que se reflejaba cómo sus compañeras caían al suelo, lo que provocó comentarios jocosos de los usuarios.

80 Selma Penalva, A.: «La información reflejada en las redes sociales…», *op. cit*., pág. 384.

una expresión aislada de disgusto o irritación publicada en la cuenta de Facebook en un contexto de enfado por razón del trabajo no pueda justificar sin más el despido[81]. Sin embargo, según la doctrina judicial, las expresiones utilizadas en los blogs o *post* que se publican en el «muro» de Facebook se consideran publicadas con sosiego y meditación y no en el calor de un debate[82].

c) La utilización de las redes sociales puede poner de manifiesto otro tipo de incumplimientos laborales, como es el caso del acoso sexual, sancionable *ex* artículo 54.2 g) del ET, sufrido por una trabajadora por parte de su compañero, superior jerárquico en la empresa, que pudo ser demostrado merced a los comentarios incluidos por este en Facebook[83].

4.2. EL VALOR PROBATORIO DE LA INFORMACIÓN OBTENIDA EN REDES SOCIALES

Según el artículo 90.1 de la LRJS, las partes podrán servirse de cuantos medios de prueba se encuentren regulados en la ley[84], salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas. Entre ellos, el artículo 90.1 de la LRJS alude a «los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos», también denominada prueba por soporte informático o electrónica, calificación que cabe atribuir a los datos obtenidos a través de mensajería móvil e instantánea (SMS, WhatsApp, Line, Tuenti, etc.), de internet y las redes sociales (Facebook, Twitter, blogs, etc.), con independencia del formato en el que se presente la información (fotografías, vídeos, mensajes, conversaciones, etc.).

La prueba electrónica comprende los medios de prueba previstos en el artículo 299.2 de la LEC y regulados en los artículos 382 a 384 de la LEC, así como los medios de prueba innominados a que se refiere el artículo 299.3 de la LEC, al aludir a cualquier otro medio de prueba no enunciado expresamente en el artículo 299 de la LEC del que pueda obtenerse certeza sobre hechos relevantes. En atención a los citados preceptos, y pese a que en un primer momento se afirmó su consideración como prueba documental en sentido amplio, en la actualidad la jurisprudencia

81 STSJ del País Vasco, núm. 2326/2104, de 2 de diciembre.

82 STS, Sala 1.ª, de 12 de diciembre de 2013 (núm. 1333/2013).

83 STSJ de Cataluña, núm. 5376/2012, de 17 de julio.

84 Entendiendo por tal legislación, según se deduce de la disposición final cuarta de la LRJS, tanto los artículos 90 a 95 de la LRJS, como la regulación sobre los medios de prueba contenida en la LEC (arts. 281 y ss.), en lo que no se oponga a la normativa laboral precitada.

entiende que se trata de un medio de prueba autónomo y distinto de la prueba documental[85], por lo que no permitirá sustentar la revisión fáctica en suplicación[86].

Precisamente esta distinción impide que la prueba electrónica sea un medio de valoración legal, de suerte que la reproducción de palabras, imágenes y sonidos captadas mediante instrumentos de filmación, grabación, o grabadas en archivos de datos han de valorarse según las reglas de la sana crítica (art. 382.3 LEC).

Sin perjuicio de ello, en función de la modalidad de la prueba y de cómo se presente (exhibición del contenido de una página web mediante su impresión en papel o cibernavegación en el acto de la vista mediante *tablet* u ordenador portátil; exhibición o transcripción de mensaje SMS o conversación de WhatsApp; exhibición de un perfil de Facebook; exhibición o transcripción del contenido de discos duros de ordenadores o de dispositivos externos de almacenamiento de datos, de la información vertida en servicios de almacenamiento de datos *on-line* o «nubes» informáticas, etc.), la misma puede precisar el apoyo instrumental de otros medios de prueba (art. 382.2 LEC), como el reconocimiento judicial[87], la pericial informática, la testifical o el interrogatorio de parte, para acreditar la autenticidad de la información, la identidad del autor (si corresponde o no con el titular del perfil) o concretar el lugar y momento de los hechos relatados, o servir a su vez de apoyo a otros medios de prueba, como ocurre con la testifical prestada por detective.

Ahora bien, la virtualidad probatoria de los datos, hechos, fotografías o consideraciones manifestadas en una red social tiene como presupuesto que dicha información se haya obtenido sin vulneración del derecho a la intimidad del trabajador, así como que se pueda acreditar que la misma reproduce con exactitud los hechos acaecidos en la realidad y que su autoría corresponde al trabajador.

4.2.1. Obtención lícita de la información vertida en redes sociales por parte de la empresa

Puesto que opera como condición de la admisión de la prueba, es preciso acreditar en primer término que el manejo por parte de la empresa de este tipo de información personal del trabajador no ha vulnerado el derecho a la intimidad del trabajador. Son distintas las situaciones que pueden plantearse al respecto:

---

85 SSTS de 16 de junio de 2011 (RCUD 3983/2010) y 26 de noviembre de 2012 (RCUD 786/2012); STSJ de Madrid, núm. 165/2012, de 12 de marzo. Sin embargo, alguna doctrina de suplicación ha admitido el correo electrónico impreso como prueba documental [*v. gr.* STSJ de Aragón, núm. 822/2010, de 17 de noviembre y los mensajes de texto SMS o WhatsApp, con virtualidad para fundar la revisión de hechos en suplicación cuando están debidamente transcritos en autos (STSJ de Aragón, núm. 145/2015, de 16 de marzo)].

86 SSTS de 16 de junio de 2011 (RCUD 3983/2010) y 26 de noviembre de 2012 (RCUD 786/2012), cits.

87 STSJ del País Vasco de 23 de septiembre de 2014 (rec. núm. 1667/2014).

a) Por una parte, puede tratarse de información privada a la que se accede a través de maquinaciones informáticas que alteran la configuración de privacidad de la cuenta de otra persona con el único fin de acceder subrepticiamente a la información allí reflejada. En este punto, conviene recordar que el artículo 90.2 de la LRJS establece que «no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas».

b) Respecto de la información obtenida por parte de la empresa utilizando el icono de acceso directo al perfil personal del trabajador que pudiera existir en el ordenador de la empresa cuyo uso personal tuviese asignado el trabajador, parece conveniente aplicar criterios análogos a los utilizados para valorar los posibles usos abusivos de los medios informáticos propiedad de la empresa para fines personales. En síntesis, se entenderá que «no hay vulneración de la intimidad del trabajador si la empresa había emitido instrucciones expresas, prohibiendo tajantemente toda utilización personal de este tipo de instrumentos de trabajo o si advirtió su intención de realizar controles tendentes a garantizar la utilización adecuada de estos, admitiendo una razonable expectativa de intimidad en caso contrario»[88].

c) Distinto es el caso en que las imágenes o comentarios han sido incluidos «en abierto» en la citada red social o en espacios abiertos a los que se accede sin necesidad de utilizar clave ni contraseña[89], como ocurre en los blogs, bien por el propio trabajador, bien por uno de sus contactos[90]. En estos supuestos, la doctrina judicial niega la existencia de lesión del derecho a la intimidad del trabajador, en la medida en que él mismo ha compartido la información en su perfil de Facebook, renunciando al posible carácter íntimo que pudiera habérsele atribuido[91].

   En estos casos, es irrelevante que las fotografías compartidas se hayan capturado en un entorno público o privado, ya que la voluntaria difusión por parte del trabajador resta privacidad a las imágenes reflejadas en ella, lo que lleva a estimar que no hay una intromisión en la intimidad del trabajador por parte de la empresa que las aporta como prueba[92].

---

88 Selma Penalva, A.: «La información reflejada en las redes sociales y su valor como prueba en el proceso laboral. Análisis de los últimos criterios jurisprudenciales», *op. cit*., pág. 368.

89 En el caso de la STSJ de Asturias, núm. 1333/2013, de 14 de junio, se entiende que no existió vulneración del derecho a la intimidad de la trabajadora, puesto que el acceso a las fotografías no estaba limitado al público, y se obtuvieron libremente, sin necesidad de utilizar clave ni contraseña alguna.

90 STSJ de Castilla y León/Valladolid de 28 noviembre 2013 (rec. núm. 1446/2013).

91 STSJ de Asturias, núm. 1333/2013, de 14 de junio, cit.

92 En este sentido, *cfr*. la STSJ de Madrid, núm. 524/2012, de 28 de mayo.

En fin, ni la LOPD, ni la Ley Orgánica 1/1982, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, establecen limitaciones a la hora de emplear la información voluntariamente expuesta y difundida por el propio titular, quedando sus indicaciones y prohibiciones solo referidas a la utilización de los datos personales cedidos a terceras personas para un fin determinado[93].

d) Alguna doctrina de suplicación ha entendido lícitamente obtenida la información del trabajador colgada en Facebook pese a que su perfil esté configurado en acceso restringido cuando dicha información llega al empresario a través de contactos comunes con el trabajador[94]. Análoga conclusión cabría establecer en el supuesto de información que llega a la empresa a través de *retweets* de mensajes o fotos de Instagram. Con todo, no faltan voces discrepantes que sostienen que el trabajador tendría derecho a que se considerara el carácter restringido de la información en virtud de los patrones de privacidad que el mismo fijó para su cuenta de Facebook, por más que luego la información se haya hecho pública por terceros[95].

4.2.2. Fiabilidad, precisión temporal y autoría de la información

Al tratar sobre las conversaciones de mensajería instantánea, se aludió al efecto negativo que las dudas sobre la fiabilidad de la información obtenida podían tener en su valoración en el conjunto de la prueba aportada al proceso. Algo similar ocurre con los datos obtenidos a través de una red social; de hecho, muchas de las formas de mensajería instantánea se articulan en el marco de una red social.

Entre los factores que restan eficacia probatoria a este medio de prueba se encuentra, en primer lugar, la ausencia de garantías de veracidad de la información obtenida en las redes respecto de los hechos aludidos por el usuario. Es más, cabe cuestionar la propia autenticidad de las conversaciones, pues existe la posibilidad de una manipulación de los archivos digitales mediante los que se materializa el intercambio de ideas[96]. Aun tratándose de información real, no siempre es fácil precisar el momento en que se han producido los hechos aludidos, o se han captado las imágenes o fotografías de las que se quiere deducir un incumplimiento[97].

93 STSJ de Castilla y León/Valladolid de 30 de abril de 2014 (rec. núm. 491/2014). Selma Penalva, A.: «La información reflejada en las redes sociales…», cit., pág. 370.

94 Cfr. STSJ de Madrid, núm. 32/2012, de 23 de enero.

95 Goñi Sein, J. L.: «Los límites de las potestades empresariales vs. Derecho a la intimidad de las personas trabajadoras en el entorno de las TIC», cit.

96 La STS, Sala 2.ª, núm. 300/2015, de 19 de mayo, recoge un ejemplo de impugnación de la autenticidad de las conversaciones mantenidas en Tuenti.

97 STSJ de Asturias, núm. 926/2013, de 19 abril de 2013.

Cabría incluso cuestionar la identidad del autor de los comentarios, pudiendo darse supuestos de suplantación de identidad, de identidad fingida o de hechos publicados en un blog sin identificación nominal reconocible. En principio, se presume que provienen del titular del perfil y corresponden a la persona bajo cuya entidad se publican, pero el trabajador al que se imputan los hechos puede cuestionar su autoría mediante la impugnación formal del documento en el que se reflejan las manifestaciones, argumentando que se trata de un perfil de Facebook creado por persona distinta[98], o que los comentarios han sido introducidos por otras personas que han accedido a su cuenta sin permiso, al haber obtenido la contraseña del titular por medio de aplicaciones que permiten el control remoto del ordenador o, sencillamente, a través del acceso directo a su perfil creado por el propio trabajador bien en el ordenador de la empresa, bien en su dispositivo móvil.

Como ha observado la doctrina, la impugnación de estos medios de prueba presenta en el proceso laboral el inconveniente de que, puesto que no existe la obligación de aportarlos con la demanda ni con carácter previo al acto de juicio, puede ocurrir que el trabajador desconozca su existencia hasta el mismo acto de juicio, en cuyo caso no podrá preparar los medios de prueba adecuados (normalmente, de carácter pericial) para cuestionar su veracidad, autoría, fecha, etc. En estos casos, sería pertinente la petición de diligencias finales conforme al artículo 88 de la LRJS, a fin de garantizar el principio de contradicción[99].

En detrimento de la virtualidad probatoria de esta información juega, además, su volatilidad o falta de permanencia, pues el titular del perfil puede eliminar u ocultar la información (fotos, manifestaciones realizadas por él o por otras personas) reflejada, de forma que en el momento de aportarla como prueba a un proceso, puede haber desaparecido de la red social[100]. En consecuencia, la aportación de fotografías o capturas de pantalla como medio de prueba plantea la necesidad de demostrar que dicha información se corresponde exactamente con la publicada en una fecha concreta en un determinado perfil, para lo cual puede resultar útil un acta notarial[101]. En su defecto, la aportación de fotografías, impresiones de pantalla o archivos de datos en DVD[102] no puede tener más que un valor indiciario respecto de la información ya retirada.

Por las razones expuestas, los tribunales otorgan a este tipo de datos un valor relativo, que precisa del apoyo instrumental de otros medios de prueba (art. 382.2 LEC). En todo caso, corresponderá al juez, conforme a las reglas de la sana crítica (art. 382.3 LEC), ponderar los diversos elementos de juicio que se hayan aportado en el proceso, teniendo en cuenta que este tipo de información no siempre se ajusta a la realidad.

98 SJS núm. 1 de Cartagena (Región de Murcia), núm. 517/2011, de 6 de julio.

99 Preciado Domènech, C. H. y Purcalla Bonilla, M. A.: *La prueba en el proceso social*, *op. cit*., pág. 499.

100 Selma Penalva, A.: «La información reflejada en las redes sociales…», *op. cit*., págs. 391 y 392.

101 Así se procede en el caso de la STSJ de Cataluña, núm. 1197/2012, de 14 de febrero.

102 STSJ de Galicia, núm. 977/2012, de 23 de febrero.

5. INCIDENCIA DE LA ILICITUD DE LA PRUEBA EN LA CALIFICACIÓN DE LA SANCIÓN

Por último, es preciso analizar los efectos de la obtención de la prueba con vulneración de los derechos fundamentales del trabajador y, en particular, el derecho a la intimidad personal que garantiza el artículo 18.1 de la CE, sobre la calificación de la decisión empresarial que se funda en la información obtenida de esta forma.

Con carácter previo, es preciso señalar que la ilicitud de la prueba comporta la imposibilidad de que sea tenida en cuenta por el órgano judicial para la valoración de los hechos. En efecto, de conformidad con los artículos 11.1 de la LOPJ y 90.2 de la LRJS, no debe admitirse la prueba lograda mediante procedimientos que suponen violación de derechos fundamentales; su resultado, en cuanto ilegítimamente obtenido, debe considerarse como no aportado a los autos. La utilización de una prueba obtenida con lesión de un derecho fundamental (a la intimidad, al secreto de las comunicaciones, a la protección de datos de carácter personal, etc.) comporta, además, la vulneración del derecho a la presunción de inocencia, según la STC 169/2003, de 29 de septiembre, lo que exige la nulidad de la prueba y de las actuaciones, *v. gr*. el expediente disciplinario, basadas en la misma.

Una primera consecuencia de ello sería, salvo que se puedan acreditar con otros medios de prueba sin conexión causal con la prueba invalidada, que no se pueden dar por probados los incumplimientos imputados al trabajador. A partir de tal circunstancia se plantea qué calificación merece la medida disciplinaria impuesta, si la improcedencia del despido (arts. 55.4 ET y 108.1 LRJS) o la revocación de la sanción (art. 115.1 LRJS), dado que no queda acreditado el incumplimiento, o la nulidad de la sanción, si se entiende que la misma implica la vulneración de un derecho fundamental (arts. 55.5 ET y 108.2 LRJS). Sobre la cuestión cabe identificar hasta tres posturas en la doctrina judicial[103]:

a) La denominada «postura de la incomunicación» defiende la calificación de improcedencia del despido, pues la vulneración del derecho fundamental no proviene de la sanción misma, sino del medio de prueba utilizado[104]. Según esta tesis, la nulidad opera únicamente cuando la sanción tiene por móvil la lesión de un derecho fundamental o implica en sí misma o de forma directa la lesión del tal derecho[105].

[103] Sistematizadas con mucha claridad por Preciado Domènech, C. H. y Purcalla Bonilla, M. A.: *La prueba en el proceso social*, *op. cit*., págs. 165-169.

[104] STSJ de Castilla-La Mancha, núm. 715/2014, de 17 de junio.

[105] STSJ de Cataluña, de 5 de septiembre de 2000 (rec. núm. 2890/2000); STSJ de Aragón, núm. 1097/2007, de 4 diciembre; STSJ de Madrid, núm. 553/2005, de 28 de junio.

Frente a la anterior tesis, la doctrina constitucional considera que la nulidad de la prueba se extiende o irradia también a las decisiones que se sustentan en ella, por lo que el despido (o sanción menor) será calificado como nulo por vulneración de derechos fundamentales. La llamada «tesis de la irradiación» descansa sobre la teoría del fruto del árbol prohibido, recogida en la STC 196/2004, de 15 de noviembre, según la cual procede anular el despido acordado en virtud de una prueba obtenida con vulneración del derecho a la intimidad[106]. Dicha doctrina ha sido reiterada en posteriores pronunciamientos tanto del Tribunal Constitucional[107] como del Supremo[108]. Desde luego, una interpretación de la cuestión a la luz del artículo 55.1 c) de la LOTC opera a favor de esta tesis, en la medida en que la lesión de un derecho fundamental no solo comporta la nulidad del propio acto constitutivo de tal lesión, sino también la reposición de la situación al momento anterior a producirse la misma y la reparación de todas las consecuencias derivadas de dicho acto. Y ello porque, como ha advertido la doctrina, el restablecimiento del trabajador en la integridad de su derecho no se producirá en el plano sustantivo si se califica el despido como improcedente[109].

Cabría, en fin, sostener una «postura intermedia», según la cual sería posible mantener la validez de la sanción, cuando la misma se apoye en otras pruebas independientes o totalmente desvinculadas de aquella obtenida ilícitamente por vulnerar el derecho fundamental[110].

106 En este sentido, véanse las SSTSJ de Galicia, núm. 1607/2008, de 3 de marzo, y del País Vasco, de 12 de septiembre de 2006 (rec. núm. 1270/2006).

107 Así, la STC 29/2013 (FJ 4.º), razona sin más que «habiéndose acordado la medida disciplinaria con base en una lesión del artículo 18.4 de la CE, las sanciones controvertidas no podrían dejar de calificarse como nulas (de acuerdo con la calificación nacida de las SSTC 88/1985, de 19 de julio, FJ 4.º; o 134/1994, de 9 de mayo, FJ 5.º, entre otras)».

108 *Cfr*. STS de 13 de mayo de 2014 (RCUD 1685/2013). Para un análisis de dicha sentencia, véase García Romero, B.: «Workplace Privacy and Employee monitoring. Dismissal based on the capture of the employee images on a video camera made without the knowledge of affected worker and with a different purpose from the one declared by the company», *International Labour Law Reports*, vol. 34, 2015.

109 Preciado Domènech, C. H. y Purcalla Bonilla, M. A.: *La prueba en el proceso social*, *op. cit.*, págs. 167 y 168.

110 Pues todas aquellas pruebas conectadas causalmente con la obtenida ilícitamente procederían indirectamente de la vulneración del derecho a la intimidad y en virtud de la «doctrina de los frutos del árbol prohibido» (recogida en el art. 90.2 LRJS) quedarían también invalidadas. Sobre la cuestión, véase *in extenso*, Preciado Domènech, C. H. y Purcalla Bonilla, M. A.: *La prueba en el proceso social*, *op. cit.*, págs. 99-104.