Creatividad y Sociedad

Derecho, trabajo y creatividad

nº 26 · diciembre 2016

La amenaza de los derechos del trabajador derivada de la innovación tecnológica en la empresa

Eusebi Colàs-Neila
Universitat Pompeu Fabra
eusebi.colas@upf.edu

Recibido: 16 de agosto de 2016
Aceptado: 2 de septiembre de 2016
Recuperado de: Colàs-Neila, E. (2016). La amenaza de los derechos del trabajador derivada de la innovación tecnológica en la empresa. *Creatividad y Sociedad* (26) 259-287
Para citar este artículo: http://creatividadysociedad.com/artículos/26/10. La amenaza de los derechos del trabajador derivada de la innovación tecnológica en la empresa.pdf

Resumen

La introducción de las TIC en la empresa supone un redimensionamiento del poder de control empresarial que puede tener como consecuencia una mengua de la eficacia de los derechos fundamentales del trabajador. La ausencia de respuestas legales específicas conduce a la judicialización de estas cuestiones. En este sentido, la jurisprudencia aporta interpretaciones que disminuyen la protección de los trabajadores, tal y como muestran algunos pronunciamientos sobre control del ordenador, de las comunicaciones electrónicas y sobre video-vigilancia en el lugar de trabajo.

Palabras clave

Tecnologías de la información y la comunicación (TIC) · Derechos fundamentales del trabajador · Poder de control empresaria · Intimidad · Secreto de las comunicaciones · Protección de datos

Abstract

The introduction of ICTs in the workplace involves a resizing of employer's surveillance power, which may have as a consequence a reduced efficacy of employee's human rights. The lack of specific legal responses leads to a judicialisation of these issues. In this regard, case law has given solutions that diminish employee's protection, as some judgements on computer's and electronic communications control and video surveillance in the workplace demonstrates.

Key words

Information and communication technologies (ICT) · Employee's human rights · Employer's surveillance power · Privacy · Secrecy of communications · Data protection

1. La era digital: un nuevo escenario para las relaciones laborales

Hablar de innovación tecnológica en la actualidad implica centrar necesariamente nuestra atención en las tecnologías de la información y de la comunicación (en adelante, TIC). Es tal su importancia en las sociedades contemporáneas, que ese lugar preeminente que ocupan ha sido considerado a la hora de dar nombre a nuestra época, utilizando denominaciones tales como edad o era de la información (McLuhan, 1964; Castells, 1998) o 'mundo digital' (2000).

No obstante, no es la única vicisitud que experimentan las sociedades actuales, sino que se hallan sometidas a una multiplicidad de transformaciones que dan forma a la manera en la que aquellas se organizan y a las relaciones de distinto tipo que tienen lugar en ellas (Tezanos, 2002). Así, desde la perspectiva del empleo y el Derecho del Trabajo, destacan especialmente, junto a aquél, dos procesos de cambio adicionales: la globalización de la economía y las finanzas, de un lado, y la expansión de la ideología neoliberal, de otro. Uno de los impactos más destacados sobre las relaciones laborales de la acción sinérgica de todos ellos, es la alteración de las relaciones de poder a favor de las empresas, entendido este en un sentido amplio, no sólo jurídico (Loy, 2005; Arthurs, 2006).

En efecto, las TIC son las protagonistas de una nueva revolución tecnológica que impone a los juristas el reto de determinar su impacto real (Peccei, 1982) y adaptar unas normas nacidas en un mundo 'analógico' al nuevo medio ambiente 'digital' (Fernández Esteban, 1998). Se trata, sin duda, de un proceso creativo de normas e instituciones necesario para ofrecer respuestas satisfactorias a los problemas que ocasiona la tecnología en las relaciones sociales. Un buen ejemplo de ello es el paso de la construcción inicial del derecho a la intimidad en al ámbito norteamericano, como el 'derecho a ser dejado en paz' (Warren y Brandeis, 1890), al nuevo derecho a la 'autodeterminación informativa' (Pérez Luño, 1984) o el 'derecho al olvido' en Inter-

net, como una de las manifestaciones de este último que ha adquirido recientemente mayor notoriedad tras la STJUE de 13 de mayo de 2014 (asunto C-131/12), en el caso de Google y la Agencia Española de Protección de Datos (AEPD).

Ciertamente, como afirmó Neffa (1990), no es posible sostener la existencia de una suerte de determinismo tecnológico. Es por ello que los efectos derivados de la introducción de las TIC en las relaciones laborales conforman un catálogo muy variado, tanto para empresas como para trabajadores, de signo positivo y negativo. De un lado, pueden comportar resultados muy beneficiosos para ambos sujetos. Piénsese, por ejemplo, en las ventajas organizativas y productivas que suponen para las empresas, o en la posibilidad de flexibilizar las formas en las que se presta el trabajo para poder atender a otras obligaciones o intereses de tipo familiar y personal. No obstante, en la práctica, de forma mayoritaria, el dominio empresarial en el sentido otorgado a las TIC implica que el beneficio sea habitualmente unidireccional.

De otro lado, poseen efectos negativos para ambos sujetos. En lo que aquí interesa, desde el punto de vista del trabajador, las TIC, que muchas veces no únicamente pueden ser utilizadas como instrumento de trabajo sino también como mecanismos de control a distancia de la prestación laboral, incrementan de facto las facultades de control que el ordenamiento jurídico atribuye al empresario. Este redimensionamiento del poder de vigilancia ofrece al empresario la posibilidad para conocer cómo se desarrolla la actividad laboral así como aspectos relativos a la propia personal del trabajador, lo que supone una amenaza potencial para la eficacia de los derechos fundamentales del trabajador.

Así, en los últimos años se ha retomado un tema clásico en nuestra disciplina, como es el de la eficacia de los derechos fundamentales en la relación laboral, que es revisitado al analizar los nuevos desafíos impuestos en la era digital.

2. El renovado protagonismo de los derechos fundamentales del trabajador en la empresa digitalizada

Una idea fundamental que debe tenerse en cuenta es que las características técnicas de las TIC incrementan de facto las posibilidades de control empresarial. Son diversos los motivos que sustentan esta afirmación. En primer lugar, permiten obtener un conocimiento directo e inmediato –o a posteriori-, continuado, fehaciente y fácilmente accesible sobre cómo se desarrolla la actividad laboral. Como ha señalado de forma precisa González Ortega (2004, p. 48), el control de la actividad laboral es 'mucho más permanente, intenso, contrastado y detallado'.

De otro lado, gracias a ellas no sólo se pueden obtener datos, a través de múltiples aplicaciones, sobre cómo se trabaja, sino también sobre la propia persona del trabajador. De este modo, como advirtiera tempranamente Zanelli (1993), es posible construir un perfil muy detallado de la personal del trabajador a partir de diversos datos fragmentados, aparentemente inocuos por si solos.

Así mismo, debe ponerse el acento en el hecho que muchos instrumentos de trabajo son, a la vez, mecanismos de control. Así, es posible distinguir, de un lado, aquellas TIC cuya finalidad directa es principal o únicamente el control, como las videocámaras, tarjetas con chip, banda magnética o radiofrecuencia, por citar algunos; y de otro, las TIC cuya finalidad es servir como instrumento de trabajo que consienten, en paralelo, controlar también su desarrollo, como los: instrumentos y aplicaciones informáticas y de comunicación electrónica.

Finalmente, es necesario tener en cuenta que comportan el peligro de atenuar o anular la eficacia de una pluralidad de derecho fundamentales de los trabajadores. No sólo de derechos directamente vinculados al objeto de tales tecnologías, especialmente los relacionados en el art. 18 CE (derecho a la intimidad, secreto de las

comunicaciones y protección de datos), sino también de otros derechos que pueden verse mediatamente afectados, como el de libertad sindical o libertad de expresión.

Las TIC modifican las fórmulas para controlar la actividad laboral y los resultados que pueden obtenerse, pero el fundamento legal se mantiene invariable. El art. 20.3 ET reconoce al empresario la adopción de las medidas de vigilancia y control que considere más oportunas para verificar si el trabajador cumple sus obligaciones laborales, siempre respetando la dignidad humana del trabajador, tanto en su adopción como en su aplicación. En paralelo, el art. 4.2.e) ET reconoce el derecho del trabajador al respecto de su intimidad y a la consideración debida a su dignidad, en una suerte de recordatorio de la aplicabilidad de los derechos fundamentales también en el ámbito del contrato de trabajo. A pesar que el reconocimiento constitucional de los derechos fundamentales es suficiente para su ejercicio, la ausencia de un desarrollo legal específico puede dificultar aquél, sobre todo considerando la forma tan general en la que se formula el poder de control, tal y como tradicionalmente ha puesto de manifiesta gran parte de la doctrina (Rodríguez-Piñero, 1990; Baylos, 1991; Goñi, 1988).

La ausencia de una respuesta legal específica conduce en algunos casos a la búsqueda de soluciones alternativas, como la elaboración de códigos o protocolos empresariales de utilización o la regulación a través de instrumentos colectivos (Colàs, 2012, pp. 121-144). No obstante, la principal consecuencia ha sido la judicialización de esta materia, lo que implica la aplicación directa de la Constitución. Tal y como ha venido reiterando la jurisprudencia constitucional, los derechos fundamentales son el principal límite que deben enfrentar los poderes empresariales[1]. Así, ningún interés empresarial puede anular genéricamente el ejercicio de los derechos fundamentales. Debe traerse a colación aquí las palabras del Alto Tribunal en la icónica STC 88/1985, de 19 de julio cuando afirma que 'la celebración de un contrato de trabajo no implica en modo alguno la privación para [el trabajador]… de los derechos que la

1 Por citar sólo algunas, pueden verse STC 96/1989, de 29 de mayo; STC 126/1990, de 5 de julio; STC 99/1994, de 11 de abril

Constitución le reconoce como ciudadano'; lo contrario, supondría una clara manifestación 'de "feudalismo empresarial" [que] repugnan al Estado social y democrático de Derecho y a los valores superiores de libertad, justicia e igualdad a través de los cuales ese Estado toma forma y se realiza (art. 1.1)'. Ello no obstante, los derechos fundamentales experimentan 'adaptaciones o modulaciones que procuran equilibrar los intereses del trabajador y del empresario' (STC 197/1998, de 13 de octubre).

Los enunciados constitucionales que reconocen derechos fundamentales están formulados en forma de principios. Por tanto, al tener una dimensión de peso, es precisa su aplicación caso por caso, ponderando las circunstancias concurrentes en cada momento (Alexy, 1993). La técnica seguida habitualmente es la aplicación del principio de proporcionalidad, que parte de la posición preeminente de los derechos fundamentales en el ordenamiento jurídico, motivo por el cual las limitaciones que experimentes deben ser excepcionales y restrictivas (Goñi, 2014). Así, la empresa debe acreditar un legítimo interés en la adopción de la medida, que supere tres juicios diversos: idoneidad de la medida para alcanzar su objetivo; indispensabilidad de la misma, por no existir ninguna otra que, con idéntica eficacia y de manera más moderada, permita conseguirlo; y, finalmente, ponderación o equilibrio de la medida, si de ella se derivan más beneficios para el interés general que perjuicios para otros bienes o intereses.

Sucede que, como a continuación se verá, los criterios que ha venido sentando la jurisprudencia, no exentos de controversia, han discurrido por un camino de progresiva reducción del ámbito protegido por los derechos fundamentales a favor de los intereses empresariales. De entre el amplio espectro de instrumentos y aplicaciones para el control a distancia que permiten las TIC, tres supuestos concretos ilustran esta circunstancia: el control de los instrumentos informáticos, la fiscalización de las comunicaciones electrónicas en la empresa y la video-vigilancia en el centro de trabajo. A continuación se esbozarán los principales criterios sentados por la jurisprudencia en estos aspectos.

3. La deriva regresiva del Tribunal Supremo ante el control empresarial del ordenador

En una primera etapa, principalmente a lo largo de la década pasado, la jurisprudencia estuvo caracterizada por una diversidad de posicionamientos. Una característica común de la jurisprudencia en una primera etapa, al ponderar las facultades de control empresarial y los derechos fundamentales del trabajador, fue partir de la propiedad empresarial de las TIC como fundamento justificador[2]. A partir de aquí, pueden encontrarse divergencias importantes en relación, cuanto menos, a dos grandes aspectos: el derecho afectado por la actividad de control y el fundamento jurídico sobre el que ejercer la misma.

En relación al derecho afectado, la utilización de instrumentos informáticos como mecanismos de comunicación electrónica generó en un primer momento dudas respecto a la aplicación en estos casos del derecho al secreto de las comunicaciones. Algunas sentencias consideraron que no era aplicable. Dado que se trata de un instrumento de trabajo, propiedad de la empresa, utilizado de forma inadecuada con una finalidad extraprofesional, el empleador estaba legitimado para controlar el uso realizado de los mismos y del desarrollo de la actividad laboral[3]. En cambio, otros pronunciamientos vinieron entendiendo que, en tanto que el correo electrónico permite transmitir todo tipo de información, sí que se puede aplicar, partiéndose en muchos casos de la doc-

2 A título de ejemplo pueden citarse las siguientes: STSJ de Castilla y León (Burgos), de 10 de mayo de 2006 (rec. 1249/2005); STSJ de Cataluña, de 6 de junio de 2003 (rec. 5425/2001); STSJ de Cataluña de 5 de julio de 2000 (rec. 1718/2000); y STSJ de Andalucía (Málaga) de 25 de febrero de 2000 (rec. 2207/1999)

3 STSJ de Cataluña de 4 de noviembre de 2004 (rec. 3603/2003), STSJ de Cataluña de 6 de junio de 2003 (rec. 5425/2001) y STSJ de Cataluña de 5 de julio de 2000 (rec. 1718/2000).

trina sentada en la STEDH de 3 de abril de 2007 (caso Copland contra el Reino Unido)[4].

De otro lado, sobre el fundamento normativo aplicable, inicialmente algunas decisiones judiciales consideraron aplicable de forma analógica lo dispuesto en el art. 18 ET[5]. Sin embargo, la mayoría se han fundamentado en la facultad de control de la actividad laboral que se reconoce en el art. 20.3 ET[6], a pesar de las acertadas sugerencias de parte de la doctrina (González, 2004).

La STS de 26 de septiembre de 2006 (rec. 966/2006) es el primer pronunciamiento de este Tribunal respecto al control del uso dado al ordenador. Nos encontramos ante un supuesto en el que, ante los problemas de funcionamiento de un ordenador, es examinado por un técnico, advirtiendo la existencia de un virus debido a accesos a páginas web poco seguras. Se accede a los ficheros temporales, en los que aparecen visitas realizadas a páginas y vídeos de contenido pornográfico. Tras la reparación del ordenador, al devolverlo a la empresa, se proceder a la misma operación de visionado de los ficheros temporales ante los representantes de los trabajadores.

El Tribunal afirma que el empresario puede examinar el ordenador en tanto que instrumento de trabajo del cual es titular matizando que, para su licitud, es preciso que la empresa establezca previamente reglas sobre el uso de los instrumentos informáticos, con la posibilidad de incluir prohibiciones absolutas o parciales, e informar de ellos

4 Entre otras, véanse STSJ de Madrid de 9 de junio de 2010 (rec. 1253/2010), STSJ de Madrid de 28 de diciembre de 2008 (rec. 4472/2007), STSJ de Cataluña de 11 de junio de 2003 (rec. 8186/2002) y STSJ de Andalucía (Sevilla) de 9 de mayo de 2003 (rec. 591/2003).

5 Pueden destacarse los siguientes: STSJ de Madrid de 22 de diciembre de 2010 (rec. 3102/2010), STSJ de Cantabria de 18 de enero de 2007 (rec. 1149/2006), STSJ de Galicia de 20 de octubre de 2006 (rec. 2945/2006), STSJ de Castilla-La Mancha de 17 de mayo de 2006 (rec. 1282/2005), STSJ de Madrid de 31 de mayo de 2005 (rec. 628/2005); STSJ del País Vasco de 21 de diciembre de 2004 (rec. 2609/2004), STSJ de Cataluña de 21 de septiembre de 2004 (rec. 2650/2004) y STSJ de Cantabria de 26 de agosto de 2004 (rec. 840/2004)

6 Criterio que ha acabado siendo mayoritariamente aplicado. Para ver su evolución jurisprudencial, pueden citarse las siguientes resoluciones: STSJ de Asturias de 11 de noviembre de 2011 (rec. 1840/2011); STSJ de la Comunidad Valenciana de 5 de octubre de 2010 (rec. 2195/2010); STSJ de Cantabria de 24 de junio de 2009 (rec. 381/2009); STSJ de Andalucía (Sevilla) de 25 de noviembre de 2008 (rec. 515/2008); STSJ de Galicia de 6 de noviembre de 2008 (rec. 4148/2008); STSJ de Madrid de 16 de enero de 2008 (rec. 4311/2007); STSJ de Madrid de 13 de noviembre de 2001 (rec. 2899/2001).

a los trabajadores. Esta información debe abarcar así mismo a la existencia de controles y las medidas que se adoptarán.

> '…lo que debe hacer la empresa de acuerdo con las exigencias de la buena fe es establecer previamente las reglas de uso de esos medios e informar 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, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones'.

En el caso concreto, se concluye que se vulnera el derecho a la intimidad y, por tanto, la prueba obtenida no es válida. El fundamento es la inexistencia de una prohibición absoluta y válida de uso extraprofesional de los instrumentos informáticos que debe ser establecida previamente por la empresa. Tampoco existió advertencia previa sobre el control del ordenador, siendo necesario informar previamente sobre la existencia de controles y las medidas aplicables. De otro lado, zanja el debate sobre el precepto estatutario aplicable en estos casos a favor del art. 20.3 ET pues se trata de instrumentos de trabajo, que no tienen la consideración de efectos personales.

Esta doctrina es seguida en lo esencial por la STS de 8 de marzo de 2011 (rec. 1826/2010), donde se llega a la conclusión de que se vulnera el derecho a la intimidad, insistiéndose en la falta de advertencia previa sobre los límites del uso a dar y sobre la realización de controles. No obstante, poco tiempo después, la doctrina se modifica sustancialmente.

Poco más de medio año después, la STS de 6 de octubre de 2011 (rec. 4053/2010) enjuicia un caso en el que se había notificado personalmente a todos los trabajadores, por escrito, la prohibición de usos extraprofesionales de los medios informáticos de la empresa. Ante la sospecha de usos no profesionales de un ordenador

(por la utilización excesiva del ratón, cuando el aplicativo corporativo no lo requería), se procede al control mediante un sistema pasivo de captura de pantalla, que no permitía acceder a los archivos del ordenador. La comprobación de los resultados se realiza ante la trabajadora y los representantes de los trabajadores.

La variación principal respecto a la doctrina previa es que se permite el control oculto, sin previa advertencia de la monitorización del ordenador. En esta ocasión, el TS entiende no vulnerado el derecho a la intimidad en el control empresarial del ordenador pues existía una prohibición absoluta y válida de uso extraprofesional, en la que, y este es el dato relevante, está implícita la posibilidad de control:

> 'En estas condiciones, el trabajador afectado sabe que su acción… no es correcta y sabe también que está utilizando un medio que, al estar lícitamente sometido a vigilancia del otro, ya no constituye un ámbito protegido de su intimidad… [pues lo contrario] equivaldría a admitir que el trabajador podría crear, a su voluntad y libre albedrío, un reducto de intimidad, utilizando un medio cuya propiedad no le pertenece y en cuyo uso está sujeto a las instrucciones del empresario'.

Es preciso, no obstante, tener en cuenta la existencia de un voto particular en el que se insiste en la validez de la doctrina previa, afirmando que el nuevo posicionamiento 'comporta un retroceso en la protección de los derechos fundamentales, concretamente del derecho a la intimidad del trabajador, tal y como venía siendo interpretada'.

4. Las exiguas expectativas razonables de confidencialidad en las comunicaciones electrónicas en la empresa

El Tribunal Constitucional también se ha pronunciado en los últimos años res-

peto al control de las comunicaciones electrónicas en la empresa, en una línea que reduce muy notablemente el ámbito de protección de los derechos fundamentales del trabajador.

De un lado, en la STC 241/2012, de 17 de diciembre, se enjuició el caso de dos trabajadoras que instalaron en un ordenador de la empresa, sin conocimiento de esta, que lo había prohibido expresamente, un programa de mensajería instantánea. Es de destacar que la instalación se produce en un PC de uso común, sin ningún tipo de contraseña o clave de acceso. Ambas mantienen conversaciones en las que se realizan comentarios críticos, despectivos e insultantes hacía algunos compañeros. Un trabajador encuentra casualmente los ficheros y la empresa accede a las carpetas del PC y lee sistemáticamente los mensajes.

Para el Tribunal, el empresario, en ejercicio de sus facultades de dirección y control, puede regular el uso y control de las TIC siempre con pleno respeto a los derechos fundamentales. A partir de aquí, concluye, en primer lugar, que no se vulnera el derecho a la intimidad en el caso enjuiciado en tanto que el fichero de registro en el que almacenaron sus conversaciones se hallaba en un ordenador que podían utilizar diferentes trabajadores, sin clave de acceso, lo que supone un acto dispositivo de las trabajadoras que elimina la privacidad de la conversación y, por tanto, su contenido puede trascender a terceros:

> '…fue la propia demandante y otra trabajadora… con sus propios actos, quienes provocaron con su voluntaria actuación que no se vea afectado el derecho a la intimidad al posibilitar el conocimiento de las conversaciones por otro usuario del ordenador, trabajador de la empresa, que casualmente y sin ninguna intencionalidad tuvo acceso a su contenido…'.

De otro lado, tampoco se considera vulnerado el derecho al secreto de las comunicaciones pues la instalación del programa de mensajería, sin conocimiento de la

empresa y con la previa prohibición expresa de esta, eliminaba cualquier expectativa razonable de confidencialidad. A ello se añade, nuevamente, que se trataba de un ordenador de uso común, sin clave de acceso, lo que implica una comunicación abierta, sin protección constitucional, algo sobre lo que la doctrina ha sido muy crítica, defendiendo la necesidad de autorización judicial para tener conocimiento de la misma (Martín Alonso, 2013):

> '…[la] información archivada en el disco duro era accesible a todos los trabajadores, sin necesidad de clave alguna… [lo que] permite afirmar su incompatibilidad con los usos personales… la pretensión de secreto carece de cobertura constitucional, al faltar las condiciones necesarias para su preservación (…) [la] prohibición expresa de instalar programas… se conculca… no existiendo una situación de tolerancia… y, por ende, al uso personal del ordenador, no podría existir una expectativa razonable de confidencialidad…'.

No obstante, debe ponerse en valor el muy crítico y acertado voto particular del magistrado Valdés Dal-Ré, para quien '…la idea que… aflora [en la sentencia] sobre el modelo constitucional de relaciones laborales… representa un paso atrás en la muy acreditada jurisprudencia constitucional dictada en tres décadas por el Tribunal en materias laborales'. Entiende la opinión discrepante que, al regular el uso y control de las TIC, la empresa debe tener en cuenta que el derecho de libertad del art. 18.3 CE es un límite a sus actos de disposición y que el contrato de trabajo 'no incomunica al trabajador.. [ubicándole] en una situación de soledad hacia el exterior'. La titularidad de las TIC no otorga al empresario 'un derecho a restricciones caprichosas… no sólo de la utilidad individual, sino también la función social, definen inescindiblemente el contenido del derecho de propiedad sobre cada categoría o tipo de bienes (STC 37/1987, de 26 de marzo, FJ 2)'.

Entiende que el carácter formal del concepto de secreto, implica que la protección constitucional se produce incluso a pesar del incumplimiento de órdenes

empresariales. Ello, en todo caso, puede conducir a imponer las sanciones que sean pertinentes, pero en ningún caso permite vulnerar derechos fundamentales, 'ni tampoco las intromisiones empresariales enderezadas a verificar o comprobar la existencia de las comunicaciones, incluso cuando ex post, cometida la vulneración y gracias a esa legítima práctica, quede acreditado que aquellas sanciones eran ajustadas a derecho'.

De otro lado, la posibilidad de acceso común sin contraseña al ordenador, no hace variar las consideraciones anteriores, poniendo sentido común en un ámbito que habitualmente carece de él. Abrir una carpeta, archivo o enlace, sabiendo que se contienen datos de comunicaciones ajenas, no es diferente a abrir una carta dirigida a otra persona. En este sentido es de destacar cómo se enfatiza que de los fundamentos jurídicos se deducen hechos que no se corresponden con los efectivamente probados, pues el acceso casual a los ficheros no era tan sencillo: era preciso abrir muchas carpetas para poder acceder a los mensajes.

Sin embargo, la posición mayoritaria vuelve a seguirse en la posterior STC 170/2013, de 7 de octubre, en la que se enjuicia el despido de un trabajador por enviar información confidencial de la empresa a través de instrumentos informáticos de aquélla. Dato relevante es la ausencia de instrucción alguna o protocolo sobre el uso de los instrumentos informáticos, ni previsión sobre procedimiento para controlarlos. Tan sólo el convenio colectivo aplicable contenía dos escuetas referencias a las TIC. De un lado, se tipificaba como falta leve el uso de los medios informáticos de la empresa con una finalidad diversa de la estrictamente laboral. De otro, se permitía su uso a los representantes de los trabajadores para el cumplimiento de sus funciones.

El TC se fundamenta en la doctrina contenida en la sentencia anteriormente señalada para concluir que el derecho fundamental al secreto de las comunicaciones no se ha vulnerado. La circunstancia de hecho que considera jurídicamente relevante es la tipificación en el convenio colectivo como falta leve del uso extraprofesional de las TIC. De ahí, deriva, sorprendentemente, una prohibición expresa que permite su

control en aplicación del art. 20.3 ET. No existe por tanto, para el Tribunal, una expectativa fundada y razonable de confidencialidad, pues estamos ante una comunicación abierta.

> 'La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización… En el supuesto analizado la remisión de mensajes enjuiciada se llevó pues a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales indicadas, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario; sometido en consecuencia a su posible fiscalización, con lo que, de acuerdo con nuestra doctrina, quedaba fuera de la protección constitucional del art. 18.3 CE'.

Del mismo modo, se concluye que no se vulnera el derecho a la intimidad al no existir una razonable expectativa de intimidad. El razonamiento se sustenta también en la previsión de una falta laboral en el convenio colectivo en los casos de utilización extraprofesional de los instrumentos informáticos que permite su control. Esta conclusión es diversa a la jurisprudencia del TEDH (casos Halford contra RU de 1997 y Copland contra RU de 2007), tal y como el propio Tribunal admite. No obstante, lo justifica, nuevamente, en la previsión convencional referida:

> '…el régimen jurídico aplicable en la empresa respecto al uso de las herramientas informáticas de su propiedad hacía factible y previsible la posibilidad de que el empresario ejerciera su facultad legal de vigilancia sobre los correos electrónicos del trabajador'.

Por tanto, a juicio del Tribunal, existe información empresarial suficiente y precisa que demuestra la transgresión de la buena fe contractual, lo que motiva el despido, y hace que la medida empresarial sea justificada, idónea y necesaria. Como se ha

sostenido (Monereo y López, 2014), el Tribunal finalmente hace prevalecer intereses relativos a la productividad de la empresa sobre la protección de los derechos fundamentales, utilizando una 'interpretación de fundamentación bastante dudosa' que legitima el control cuando se sospeche de una actividad ilícita; lo importante, como señalan, no es si se vulnera la Constitución con la actuación empresarial sino si esta permite obtener pruebas para comprobar sus sospechas.

Esta restrictiva aproximación al secreto de las comunicaciones en el ámbito laboral es también la línea de tendencia del Tribunal Europeo de Derechos Humanos en su más reciente jurisprudencia. En efecto, la STEDH de 12 de enero de 2016, Barbulescu contra Rumania, conoce del caso de un trabajador que es despedido por utilizar para fines personales un programa de mensajería instantánea, instalado en su ordenador a petición de la empresa, para comunicarse con sus clientes. La empresa monitorizó conversaciones privadas mantenidas con su hermano y su prometida, sobre cuestiones de salud y de carácter sexual, que la llevó a despedirlo por vulnerar las normas internas de la empresa sobre la utilización de los medios informáticos con una finalidad profesional.

El TEDH asume que es razonable que el empleador desee verificar que los trabajadores desarrollan su actividad laboral adecuadamente durante la jornada laboral. En este sentido, indica que el acceso a las comunicaciones personales del trabajador se realizó en la creencia de que se trataba de contenidos relacionados con su actividad profesional y que resultó necesario en tanto que, para acceder a su cuenta, era preciso comprobar las grabaciones. Además, fue una medida proporcionada, pues no se accedió a información adicional contenida en el ordenador puesto a su disposición para la ejecución de su prestación laboral. Por todo lo cual se concluye que no se vulneró el art. 8 CEDH.

No obstante, el voto particular emitido entiende que sí se viola dicho precepto por cuanto, más allá de la prohibición establecida por la empresa, no existía una política de vigilancia de los instrumentos de comunicación electrónica implementada, con reglas claras y precisas. De otro lado, por cuanto se accede a datos de carácter personal y en

especial a datos sensibles. Y finalmente, en relación con esto último, porque tales datos son revelados en el proceso disciplinario posterior que conduce a su despido. El control no puede producirse de forma discrecional, no es ilimitado, incluso si existen sospechas sobre un comportamiento irregular del trabajador.

Como se ha puesto de manifiesto acertadamente, parece otorgar 'una patente de legitimidad' cuando se trata del control de las comunicaciones cuando previamente se informe sobre la no posibilidad de su uso no personal, pero no se resuelve si esa prohibición puede tener un 'carácter totalizador' que permita conocer cualquier contenido de las comunicaciones que tengan lugar (Goñi, 2016).

5. La protección de datos del trabajador y los mecanismos de video-vigilancia: nuevo viraje restrictivo en la jurisprudencia del Tribunal Supremo

La STC 29/2013, de 11 de febrero, contrasta con la jurisprudencia anteriormente analizada respecto al control de los instrumentos informáticos y de las comunicaciones electrónicas en la empresa[7]. En ella se analiza la licitud de las sanciones impuestas a un trabajador por incumplir su horario. Tras detectar algunas irregularidades en el registro de las horas de entrada y salida, a efectos de confirmar tales sospechas, se solicita al departamento de seguridad que controle el horario del trabajador a través de las cámaras de seguridad del centro de trabajo, una de las cuales enfocaba a su despacho. Las imágenes captadas fueron utilizadas para corroborar el incumplimiento de las obligaciones laborales del trabajador e imponer las correspondientes sanciones disciplinarias.

7 En un sentido similar, puede verse la STS de 13 de mayo de 2014 (rec. 1685/2013).

Destaca de este supuesto es la consideración del derecho a la protección de datos como bien tutelable ante los mecanismos de control en la empresa. En primer lugar, se parte de la consideración de datos de carácter personal de las imágenes obtenidas mediante un sistema de video-vigilancia que se almacenen en cualquier soporte físico y, por lo tanto, se encuentran en el ámbito de protección ofrecido por el art. 18.4 CE:

> '…[este] derecho fundamental amplía la garantía constitucional a todos aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil (ideológico, racial, sexual, económico o de cualquier otra índole) o para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo (STC 292/2000, de 30 de noviembre)'.

Lo relevante en este caso es que el tratamiento de tales datos se produce sin haber informado previamente al trabajador sobre la finalidad de las imágenes captadas por los dispositivos de video-vigilancia. Ciertamente, el derecho de información es núcleo esencial del derecho de protección de datos. En este sentido, el Tribunal sostiene la necesidad de informar de forma previa y expresamente, de manera precisa clara e inequívoca sobre la finalidad del control y su eventual utilización, así como quién posee dichos datos. Así:

> 'no hay una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales, y que tampoco podría situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. Esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esen-

> cial. En efecto, se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos (art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD), cuando lo cierto es que cabe proclamar la legitimidad de aquel propósito (incluso sin consentimiento del trabajador, art. 6.2 LOPD) pero, del mismo modo, declarar que lesiona el art. 18.4 CE la utilización para llevarlo a cabo de medios encubiertos que niegan al trabajador la información exigible.

Del mismo modo que en el caso del control del ordenador y de las comunicaciones electrónicas analizado anteriormente, se produce aquí un viraje de la doctrina en un sentido restrictivo de la eficacia del derecho fundamental. Así, el Pleno del Tribunal Constitucional, en Sentencia 39/2016, de 3 marzo, adopta una posición rotunda en la restricción del ámbito de protección del derecho de protección de datos. En este caso, se enjuicia el despido de una trabajadora de un comercio sobre la que recaían sospechas de apropiarse de dinero de la caja y realizar operaciones de cambio fraudulentas para ocultarlo. Por ese motivo, se instala una cámara en la tienda, orientada a la caja, figurando en la entrada del local el distintivo informativo que exige la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

En materia de protección de datos, el principio básico, como se ha visto, es el consentimiento del afectado, quien tiene la capacidad de gestionar el flujo de informaciones que sobre él circulan. Cuando se hace referencia a la video-vigilancia en el centro de trabajo, se excepciona dicho consentimiento, en este caso del trabajador, siempre que concurran dos circunstancia. De un lado, que el dispositivo de captación de imágenes tenga una finalidad de control laboral o se configure como un mecanismos de seguridad, y de otro que el ejercicio de tales facultades se desarrolle de forma regular, respetando la normativa aplicable y sin vulnerar los derechos

fundamentales. Preocupa la consideración del Tribunal al respecto de entender el consentimiento implícito al suscribir el contrato de trabajo, lo que conlleva reconocer el ejercicio del poder de dirección del empresario. Por tanto, sólo en el caso en el que la utilización de los datos se produzca con una finalidad distinta al cumplimiento de las obligaciones dimanantes del contrato, será preciso recabar dicho consentimiento.

Esta dispensa de consentimiento expreso, no obstante, no exonera del deber de informar. Ahora bien, en este caso se cercena el contenido del derecho de información reconocido en la anterior sentencia, pues no es necesario especificar la finalidad concreta que se asigna al control. El cartel informativo situado en la entrada de la tienda, bastaba, pues la trabajadora 'podía conocer la existencia de las cámaras y la finalidad para la que habían sido instaladas':

> 'El trabajador conocía que en la empresa se había instalado un sistema de control por video-vigilancia, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control. Lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque sólo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados.'

Debe subrayarse muy especialmente, ante el desatino que supone este cambio jurisprudencial, la argumentación contenido en el voto particular formulado por el Magistrado Valdés Dal-Ré, al que se remite y que es compartido plenamente. En unas consideraciones muy críticas con la opinión mayoritaria del Tribunal, se enfatiza que el pronunciamiento sostiene una concepción de los poderes de vigilancia y control que los convierte en una suerte de fuente constitucional, a partir de la que se plantea una ficticia colisión de derechos, que se sitúa extramuros del Estado social y democrático

de Derecho que proclama nuestra Constitución. El resultado es que 'los derechos del trabajador son suprimidos o debilitados para asegurar la autoridad indiscutida del empresario'.

6. La erosión de los derechos fundamentales derivada de la innovación tecnológica

La finalidad del Derecho del Trabajo ha venido siendo, tradicionalmente, la de proteger a la parte débil de la relación laboral, el trabajador, actuando como mecanismo de compensación de desigualdades en la ordenación de las relaciones de trabajo asalariado. No obstante, esa finalidad tuitiva está siendo sometida a un proceso de impugnación que se plasma claramente en el contenido y orientación de las últimas reformas laborales que se han sucedido en nuestro país durante la crisis, de signo profundamente regresivo y desintegradoras del nivel de protección alcanzado tras largo tiempo de conquista de derechos. En efecto, las crisis económica, financiera y de deuda pública, han sido utilizadas en el argumentario político como pretexto para el diseño e implantación de políticas de austeridad dirigidas a contener el gasto público y conseguir la consolidación fiscal. Su principal consecuencia ha sido la erosión de las condiciones de vida y trabajo de una parte importante de los ciudadanos y el desmantelamiento del modelo social europeo, en especial en los países periféricos (Countouris y Freedland, 2013).

Es importante no perder de vista este contexto, en el que se rompe el equilibrio en la conformación de poderes que el Derecho del Trabajo trata de imponer, al analizar los efectos de la innovación tecnológica en la empresa sobre los derechos de los trabajadores. Esta no es más que una pieza más del complejo rompecabezas que conforman las relaciones laborales contemporáneas, cuya foto final muestra

claramente el deterioro de la función tuitiva de nuestra disciplina, que se hace más necesaria, si cabe, en las sociedades digitales, fagocitada por el incremento del poder de las empresas. A ese debilitamiento contribuye decisivamente el papel jugado por la jurisprudencia que otrora cimentara y consolidara la protección de los derechos fundamentales del trabajador.

Ello no obstante, la jurisprudencia anteriormente analizada de la Sala de lo social del Tribunal Supremo, contrasta con la diversa aproximación al secreto de las comunicaciones electrónicas que se realiza por la Sala de lo penal, en la STS de 16 de junio de 2014 (rec. 2229/2013), que conoce de un supuesto en el que el trabajador había sido condenado por falsedad documental y estafa. Aunque en el caso en particular no se produce vulneración del derecho al secreto de las comunicaciones, en tanto que no consta que se accediera a ninguna cuenta de correo electrónico ni fichero en el que se guardara tipo alguno de documentación para la obtención de pruebas, la sala entendió necesario sentar una doctrina clara en materia de control de las comunicaciones electrónicas en la empresa. Ello por cuanto en la sentencia de instancia se producen una serie de afirmaciones que, como se verá, no se ajustan a su interpretación del art. 18.3 CE. Así, en aquella se señalaba que, encontrándonos ante un ordenador propiedad de la empresa, facilitado al trabajador para desempeñar su actividad laboral, incluso pudiendo utilizarlo para comunicaciones personales, ya asumía, o cedía en su caso, la falta de confidencialidad.

A pesar de señalarse que los criterios sobre el control de los instrumentos informáticos deben quedar circunscritos a la jurisdicción social, afirma que la previsión del art. 18.3 CE es clara y contundente respecto a la necesidad de autorización judicial:

> '…no contempla, por tanto, ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado ('correo corporativo'), para ex-

> cepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia'.

La posición garantista de la Sala es tal, que incluso entiende que no sería operativa la renuncia o autorización del trabajador dado que, a diferencia de lo que ocurre con otros derechos reconocidos en el propio art. 18 CE, esta no prevé que la autorización del interesado habilite a injerencia alguna. Se trata, pues, de una protección especialmente 'enérgica', respecto de los otros derechos reconocidos en el mismo precepto, al exigir autorización judicial:

> '...encuentra un lógico fundamento en la gravedad y trascendencia de esta clase de injerencias, en tanto que se introducen y revelan toda clase de aspectos referentes a la privacidad del comunicante, tanto los de interés para la investigación como otros por completo ajenos a ese legítimo interés, dicha injerencia además se produce en una ominosa aunque inevitable situación de absoluta indefensión, por ignorancia coetánea, del sometido a ella y, lo que es aún más decisivo, porque por mucho que el investigado, como en el caso presente, sea empleado de la dueña del instrumento, la incursión en sus comunicaciones produce automática e inmediatamente la injerencia en el correspondiente derecho al secreto de los terceros que con él comunican, ajenos a esa relación con el titular de la herramienta y de sus condiciones de uso'.

Todo lo anterior no significa que dentro del ámbito laboral no se puedan utilizar estos mecanismos de investigación de conductas graves, sino de dar cumplimiento a las previsiones constitucionales, que precisan de autorización judicial, algo que también recoge, como la sentencia señala, la propia normativa procesal laboral, en el art. 90, apartados 2 y 4 LRJS. Por lo tanto, concluye, en relación al procedimiento penal, la eficacia de la prueba que consiste en la intervención de comunicaciones, precisa de autorización judicial, matizando que no quedarían protegidos por el secre-

to de las comunicaciones los datos del tráfico o el uso del equipo informático para acceder a otros servicios, como Internet.

Esta la sentencia de la Sala de lo penal, en la que se utilizan criterios diferentes a la doctrina seguida por la Sala de lo social, plantea dudas razonables sobre cómo proceder en el control de los medios informáticos. Tal y como apunta la propia sentencia, si se pretendiera utilizar como prueba algún documento protegido por el secreto de las comunicaciones, podría pensarse en recurrir a lo que prevé el art. 90.4 LRJS. Ante la necesidad de aportar documentos, con independencia del soporte, en un proceso judicial que, eventualmente, que afectaran el derecho a la intimidad o cualquier otro derecho fundamental, prevé la posibilidad de solicitar al Juez o Magistrado dicha actuación, siempre que no existan medios alternativos de prueba. Aquél, mediante auto y ponderando previamente los intereses afectados mediante el juicio de proporcionalidad, podrá autorizarla.

De otro lado, en estos casos se olvida a menudo la existencia del derecho a la protección de datos cuya aplicación debería plantearse. Así, debería tenerse en cuenta la finalidad de los datos obtenidos mediante el control empresarial, más allá de la conculcación del derecho a la intimidad y del secreto de las comunicaciones. De este modo, se procedería a una consideración omnicomprensiva de los diversos bienes jurídicos en juego que se ven amenazados por las TIC. En este sentido, a pesar del posterior giro doctrinal, el TC, en su Sentencia 29/2013, en caso de datos obtenidos a través de video-vigilancia, fue muy claro en relación a la finalidad de los mecanismos de control y de los datos obtenidos, así como de la necesidad de una información previa muy detallada al respecto. No obstante, es importante considerar la diferente función otorgada al derecho a la intimidad y al derecho a la protección de datos en aquel pronunciamiento:

> '… [la] función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea

> excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado…'.

Ante algunos de los razonamientos utilizados por la jurisprudencia que erosionan la eficacia de los derechos del trabajador, es importante tener en cuenta algunos criterios del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales de la UE[8], fijados en su Dictamen núm. 8/2001, sobre tratamiento de datos personales en el contexto laboral y especialmente en el Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Así, para que la actividad de control empresarial sea legal y justificada, existen una serie de elementos que son precisos. Debe resultar necesaria para un objetivo específico, sin que se pueda utilizar un método tradicional menos invasivo de la esfera privada del trabajador. Así mismo, es imprescindible considerar la finalidad del control, que debe ser determinada, explícita y transparente, no pudiendo dársele posteriormente un uso diferente.

Se debe partir, pues, de un principio de transparencia en el control, que implica que el empresario debe proporcionar información al interesado. Así, se insiste en la necesidad de una política empresarial que describa detalladamente si se puede, y en qué medida, realizar un uso extraprofesional de las TIC. Los motivos y finalidad de la vigilancia deben ser claros, debiendo determinar también las medidas de vigilancia adoptadas, indicando cuando se informará a los trabajadores de la infracción de directrices internas y de los medios de reacción. En cualquier caso, se debe garantizar

8 Se trata de un organismo autónomo encargado del seguimiento de la aplicación de la Directiva 95/46/CE, de 24 de octubre, 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, en cuyo art. 29 se previó su creación. Téngase en cuenta que el actual Reglamento general de protección de datos, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, deroga la Directiva 95/46/CE.

los derechos de acceso, rectificación, supresión o bloqueo de los datos que no se traten de acuerdo con lo previsto en la Directiva.

La deseable adecuada consideración de ese principio de transparencia por nuestra jurisprudencia, conduciría necesariamente a pronunciamientos más respetuosos con la eficacia de los derechos de los trabajadores y a recobrar un elemento genético imprescindible de nuestra disciplina: el principio pro operario (Alarcón Caracuel, 1990). De lo contrario, como afirma Valdés Dal-Ré en el voto particular emitido en la STC 39/2016, se seguirá transitando por 'una senda que revela una orientación que tiende a vaciar de contenido sustantivo un modelo constitucional de relaciones laborales acorde con el Estado social y democrático de Derecho (art. 1.1 CE)'.

Bibliografía

Alarcón, M. R. (1990). La vigencia del principio 'pro operario'. En A. Montoya, A. Martín Valverde y F. Rodríguez-Sañudo (coord.), Cuestiones actuales de Derecho del trabajo: Estudios ofrecidos por los catedráticos españoles de Derecho del Trabajo al profesor Manuel Alonso Olea. Madrid: Ministerio de Trabajo y Seguridad Social.

Alexy, R. (1993). Teoría de los derechos fundamentales (Trad. E. Garzón Valdés). Madrid: Centro de Estudios Constitucionales.

Arthurs, H. (2006). Who's afraid of globalization? Reflections on the future of labour law. En J. D. Craig y S. M. Lynk (ed.), *Globalization and the future of Labour Law*. Cambridge: Cambridge University Press.

Baylos, A. (1991). *Derecho del Trabajo: modelo para armar*. Madrid: Trotta.

Castells, M. (1998). *La Era de la Información. La sociedad red (vol. 1)* (Trad. C. Martínez Gimeno y J. Alborés). Madrid: Alianza Editorial.

Colàs, E. (2012). *Derechos fundamentales del trabajador en la era digital: una propuesta*

metodológica para su eficacia. Las comunicaciones electrónicas en la empresa como estudio de caso. Albacete: Bomarzo.

Countouris, N. y Freedland, M. (2013). Preface. En N. Countouris y M. Freedland (ed.), *Resocialising Europe in a Time of Crisis*. Cambridge: Cambridge University Press.

Fernández, Mª. L. (1998). *Nuevas tecnologías, Internet y Derechos Fundamentales*. Madrid: McGraw-Hill.

González, S. (2004). La informática en el seno de la empresa. Poderes del empresario y condiciones de trabajo. En M. R. Alarcón Caracuel y R. Esteban Legarreta (ed.), *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*. Albacete: Bomarzo.

Goñi, J. L. (2016). La vigilancia empresarial de las conversaciones electrónicas de los trabajadores. A propósito de la sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016, Barbulescu v. Rumania. *Trabajo y Derecho*, n. 18.

Goñi, J. L. (2014). Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación? En AA.VV., *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social*. Madrid: Cinca – AEDTSS.

Goñi, J. L. (1988). *El respeto a la esfera privada del trabajador*. Madrid: Civitas.

Grupo de protección de las personas en lo que respecta al tratamiento de datos personales de la UE (2002). *Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo*. Bruselas: 5401/01/ES/Final (WP 55).

Grupo de protección de las personas en lo que respecta al tratamiento de datos personales de la UE (2001). *Dictamen número 8/2001, sobre el tratamiento de datos personales en el contexto laboral*. Bruselas: 5032/01 (WP 49).

Loy, G. (2005). El dominio ejercido sobre el trabajador. *Relaciones Laborales*, n. 19-20.

Marín, I. (2013). La mensajería electrónica en la empresa: un paso atrás en la protección constitucional del derecho al secreto de las comunicaciones. (A propósito de la STC 241/2012, de 17 de diciembre). *Relaciones Laborales*, n. 3.

McLuhan, M. (1964). *Understanding Media. The Extensions of Man*. New York: McGraw-Hill.

Monereo, J. L. y López, B. M. (2014). El control empresarial del correo electrónico tras la STC 170/2013. *Aranzadi Social,* n. 11.

Neffa, J. C. (1990). Nuevas tecnologías informatizadas y sus efectos sobre el trabajo humano en las empresas. En AA.VV., *El Derecho y las nuevas tecnologías (Separata de la Revista de Derecho Industrial, 33)*. Buenos Aires: Depalma.

Negroponote, N. (1995). *El mundo digital* (Trad: M. Abdala). Barcelona: Ediciones B.

Peccei, A. (1982). Las ciencias sociales y el desarrollo humano. En R. Cohen (ed.), *Repercusiones sociales de la revolución científica y tecnológica*. Madrid: Tecnos / UNESCO.

Pérez, A. E. (1984). *La intimidad como derecho fundamental*. En AA.VV., Derechos Humanos, Estado de Derecho y Constitución. Madrid: Tecnos.Rodríguez-Piñero y Bravo-Ferrer, M. (1990). Diez años del Estatuto de los Trabajadores. *Relaciones Laborales*, t. I.

Tezanos, J. F. (2002). Desigualdad y exclusión en las sociedades tecnológica. *Revista del Ministerio de Trabajo y Asuntos Sociales (Asuntos Sociales)*, n. 35.

Warren, S. y Brandeis, L. (1890). Right to Privacy. *Harvard Law Review*, v. 4, n. 5.

Zanelli, P. (1993). *Nuove tecnologie. Legge e contrattazione collettiva*. Milano: Giuffrè.