EL DERECHO A LA INTIMIDAD DE LOS TRABAJADORES EN EL ÁMBITO DE LA EMPRESA

Remedios Roqueta Buj
Catedrática de Derecho del Trabajo y de la Seguridad Social
Universidad de Valencia

I. LAS FACULTADES EMPRESARIALES DE VIGILANCIA Y CONTROL Y EL DERECHO A LA INTIMIDAD PERSONAL DEL TRABAJADOR

El poder de dirección del empresario, imprescindible para la buena marcha de la organización productiva (organización que refiere a otros derechos reconocidos constitucionalmente en los arts. 33 y 38 CE) y consagrado expresamente en los apartados 1 y 2 del art. 20 del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores (ET), comprende la facultad de *"adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana"* (art. 20.3 ET). Pese a que el art. 20.3 del ET sólo alude a la *"dignidad humana"*, no hay que olvidar que ésta se halla presente en todos los derechos fundamentales. Por consiguiente, el ejercicio del poder de vigilancia y control empresarial ha de respetar los derechos fundamentales del trabajador, como ha reconocido el Tribunal Constitucional específicamente en relación con el derecho a la intimidad personal en sus sentencias 98/2000, de 10 de abril, y 186/2000, de 10 de julio. En definitiva, la actividad de control empresarial se encuentra limitada por los derechos del trabajador a la dignidad (art. 10 CE) y a la intimidad personal (art. 18.1 CE).

La Constitución no ofrece una definición del derecho a la intimidad personal, lo que obliga a recurrir a la Declaración Universal de Derechos Humanos y demás tratados suscritos por España sobre la materia[1]. Pues bien, el Tribunal Constitucional, a la luz de los mismos, señala que el derecho a la intimidad personal reconocido en el art. 18.1 de la Constitución se halla *"estrechamente vinculado a la propia personalidad y deriva, sin ningún género de dudas, de la dignidad de la persona que el art. 10.1 CE reconoce"*[2]. Dicho derecho implica *"la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana"*[3]. Es más, *"el atributo más importante de la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de esos datos"*[4]. Se trata, por consiguiente, de que ese ámbito propio de la vida personal y familiar debe quedar excluido del conocimiento ajeno y de las intromisiones exteriores de los demás, salvo autorización del interesado, por lo que de algún modo se introduce un concepto subjetivo de intimidad, al depender del sujeto la determinación de esa esfera[5]. La conexión de la intimidad con la libertad y dignidad de la persona *"implica que la esfera de la inviolabilidad de la persona frente a injerencias externas, el ámbito personal y familiar, sólo en ocasiones tenga proyección hacía el exterior, por lo que no comprende en principio los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada"*[6]. Sin embargo, no se

[1] Cfr. arts. 8 y 10 del Convenio Europeo de Protección de los Derechos Humanos y de las Libertades Fundamentales; y arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Por todos, De Vicente Pachés, F., *El Derecho del Trabajador al Respeto de su Intimidad*, Madrid, 1998, págs. 59 y ss.
[2] Cfr. STC 127/2003, de 30 de junio.
[3] Cfr. STC 231/1988, de 2 de diciembre. En el mismo sentido, las SSTC 197/1991, de 17 de octubre; 57/1994, de 28 de febrero; 98/2000, de 10 de abril; 186/2000, de 10 de julio; 70/2002, de 3 de abril; 218/2002, de 25 de noviembre; y 127/2003, de 30 de junio.
[4] STC 142/1993, de 22 de abril.
[5] De Vicente Pachés, F., *El Derecho del Trabajador…,* cit., págs. 77-78.
[6] SSTC 170/1987, de 30 de octubre; 142/1993, de 22 de abril; y 186/2000, de 10 de julio.

puede ignorar *"que, mediante un análisis detallado y conjunto de esos hechos, es factible en ocasiones acceder a informaciones atinentes a la vida íntima y familiar del trabajador, que pueden resultar lesivas del derecho a la intimidad personal protegido por el art. 18.1 CE"*[7]. En fin, el trabajador goza de un ámbito de reserva (limitado) en el lugar de trabajo, que no se contrae a los lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos[8]. En este sentido, el Tribunal Constitucional afirma que *"no puede compartirse, al limitar apriorísticamente el alcance del derecho a la intimidad de los trabajadores a las zonas del centro del trabajo donde no se desempeñan los cometidos propios de la actividad profesional, negando sin excepción que pueda producirse lesión del derecho fundamental en el ámbito de desempeño de las tareas profesionales"* y que *"no puede descartarse que también en aquellos lugares de la empresa en los que se desarrolla la actividad laboral puedan producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores, como podría serlo la grabación de conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, en las que se aborden cuestiones ajenas a la relación laboral que se integran en lo que hemos denominado propia esfera de desenvolvimiento del individuo"*[9].

El ejercicio de los derechos fundamentales por el trabajador, sin embargo, *"admite limitaciones o sacrificios en la medida en que se desenvuelve en el seno de una organización que refleja otros derechos reconocidos constitucionalmente en los arts. 38 y 33 CE y que impone, según los supuestos, la necesaria adaptabilidad para el ejercicio de todos ellos"*[10]. Dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento jurídico, esa modulación que se sigue del contrato de trabajo sólo puede derivar de *"una acreditada necesidad o interés empresarial"*[11]. No obstante, la mera invocación de la justificación es insuficiente para recortar derechos fundamentales del trabajador en la empresa. En efecto, de

[7] STC 98/2000, de 10 de abril.
[8] Goñi Sein, J.L., *El respeto a la esfera privada del trabajador*, Madrid, 1988, pág. 23; y STC 98/2000, de 10 de abril.
[9] STC 98/2000, de 10 de abril.
[10] Cfr. STC 90/1997, de 6 de mayo.
[11] Cfr. SSTC 99/1994, de 11 de abril; 90/1997, de 6 de mayo; y 186/2000, de 10 de julio.

conformidad con la doctrina del Tribunal Constitucional, *"la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad"*, y *"para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"*[12]. Lo que entraña la necesidad de proceder a una ponderación adecuada que respete la definición y valoración constitucional de los derechos fundamentales y que atienda a las circunstancias concurrentes en cada caso concreto[13].

Por último, hay que señalar que el art. 20.3 del ET se completa con otras previsiones legales, singularmente las contenidas en los arts. 18, 64.1.4º.d), 5.c) y 20.2 del ET.

Pero vayamos por partes:

a) El art. 18 del ET previene que *"sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo"* y que *"en su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible"*. Este artículo no sólo especifica las condiciones de aplicación en un determinado ámbito de la facultad in genere recogida en el art. 20.3 del ET, sino que, además, establece una excepción a la

[12] STC 186/2000, de 10 de julio.
[13] STC 151/2004, de 20 de septiembre.

inicial discrecionalidad que caracteriza la elección del medio de control en este precepto[14]. Existe, de este modo, una relación de complementariedad entre los arts. 18 y 20.3 del ET, que supera la mera especificación de las facultades de elección del medio de control en un determinado supuesto, integrando una colaboración normativa en la que el primero completa algunos aspectos de la regulación genérica del segundo[15].

b) Las facultades empresariales de vigilancia y control han de ejercerse de buena fe[16]. En efecto, el ET proclama de modo expreso el deber general del empresario de ejercer de modo "regular" (y en la regularidad entra el actuar de buena fe, al que se opone la conducta abusiva) su poder directivo [arts. 5.c) y 20.2][17]. Dicho deber obliga al empresario a adecuar su libertad de decisión, más allá de los que pudieran considerarse sus puros intereses egoístas, a los intereses objetivos de la empresa, a los que no son ajenos los trabajadores, y se opone a que el empresario pueda adoptar decisiones abusivas o fraudulentas que lesionen los derechos de éstos. De este modo, las facultades empresariales de vigilancia y control de los trabajadores deben desarrollarse de forma correcta y leal, adecuándose a las específicas causas que las justifican. Es decir, dichas facultades y, por ende, el sacrificio de los intereses subjetivos de los trabajadores no ha de representar más que "un efecto meramente accidental", nunca un resultado deliberadamente buscado de forma encubierta[18].

c) De conformidad con el art. art. 64.1.4º.d) del ET, los representantes legales de los trabajadores deberán emitir informe previo a *"la implantación o revisión"* por el empresario de los *"sistemas de organización y control del trabajo"*. La referencia al *"control del trabajo"* contenida en el art. 64 del ET y no al control del cumplimiento de las *"obligaciones y deberes laborales"* en general

[14] Martínez Fons, D., *El Poder de Control del Empresario en la Relación Laboral*, Madrid, 2002, pág. 292.
[15] Martínez Fons, D., *El Poder de Control…,* cit., pág. 292.
[16] Rubio de Medina, Mª.D., *El despido por utilización personal del correo electrónico*, Barcelona, 2003, págs. 9 y ss.
[17] Por todos, Montoya Melgar, A., *La buena fe en el Derecho del Trabajo,* Madrid, 2001, págs. 79 y ss.
[18] Goñi Sein, J.L., *El respeto a la esfera privada…,* cit., pág. 144.

que se prevé en el art. 20.3 del ET, podría dar pie a entender que se refiere sólo a los sistemas de control del efectivo cumplimiento por el trabajador de la prestación debida y en los términos señalados por el empleador; interpretación que se refuerza desde su inclusión en el art. 64.1.4º.d) del ET junto a la eventual adopción de los sistemas de organización del trabajo[19]. Téngase en cuenta, sin embargo, que el art. 20 del ET, aunque intitulado *"dirección y control de la actividad laboral"*, en su apartado tercero extiende las facultades de dicho control a la observancia de la totalidad de las obligaciones y deberes laborales. Por lo tanto, la representación legal de los trabajadores deberá emitir informe previo a la implantación o revisión por el empresario de todos los sistemas de control, tanto de los dirigidos a evaluar el cumplimiento de la prestación laboral, como de los orientados a verificar el incumplimiento de las obligaciones laborales. Por otra parte, por *"sistemas de control"* debe entenderse *"cualquier medio o mecanismo de vigilancia –consiguientemente con vocación de permanencia- que permita, de forma sistemática, obtener la información idónea y suficiente para satisfacer la verificación del comportamiento observado en relación con los estándares establecidos inicialmente, completando, de este modo, el objetivo del control"*[20]. No obstante, y aunque el concepto de *"sistemas"* no integra la adopción de medidas puntuales, en determinados supuestos será precisa también la intervención de la representación legal de los trabajadores a posteriori a fin de asegurar que la adopción de la medida de control empresarial está justificada y que se desarrolla con el máximo respeto a los derechos fundamentales de los trabajadores.

II. **EL CONTROL AUDIOVISUAL**

El control mediante mecanismos audiovisuales ha de respetar los derechos fundamentales del trabajador, especialmente el derecho a la intimidad personal, como ha reconocido el Tribunal Constitucional en sus sentencias

[19] Martínez Fons, D., *El Poder de Control…,* cit., págs. 162 y ss.
[20] Martínez Fons, D., *El Poder de Control…,* cit., pág. 162.

98/2000, de 10 de abril, y 186/2000, de 10 de julio, y por consiguiente, ha de estar justificado, y lo estará si tiene como fin: - Controlar la seguridad del centro cuando existen riesgos de atentado contra el patrimonio de la empresa, del personal o de los clientes de la empresa, al tratarse, por ejemplo, de un museo, de una Caja de Ahorros o de un hipermercado[21], o se han producido múltiples sustracciones de material y pertenencias del empresario, del personal o de los clientes de la empresa[22]; - Controlar la seguridad del centro contra los riesgos de atentado contra la vida o integridad de las personas[23] o los riesgos laborales[24]; - Garantizar la seguridad de las operaciones de la empresa, como por ejemplo, controlar el desarrollo de los sucesivos sorteos o juegos que se van produciendo en un casino o en un bingo[25], si bien en este caso la instalación de micrófonos no está justificada, al permitir la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores, como de los clientes[26]; - Verificar el cumplimiento de las obligaciones laborales por parte de los trabajadores de la empresa cuando, por ejemplo, ésta ha detectado faltas de puntualidad y pérdidas de tiempo injustificadas entre sus empleados[27] o se trata de controlar el contenido de las pantallas de los ordenadores de los trabajadores[28]; - Cuando existan razonables sospechas de la comisión por parte del trabajador de graves irregularidades en su puesto de trabajo, cuando, por ejemplo, la limpieza del

[21] SSTSJ de Andalucía de 9 de marzo de 2001 (AS/2788), de Galicia de 20 de marzo de 2002 (AS/3385), de la Comunidad de Madrid de 28 de junio de 2005 (AS/2080), de Galicia de 22 de diciembre de 2005 (AS/778, 2006), de la Comunidad de Madrid de 14 de junio de 2006 (AS/3406) y de Extremadura de 15 de mayo de 2007 (JUR/247253).
[22] SSTSJ de Galicia de 28 de septiembre de 1999 (AS/2952), de las Islas Canarias de 25 de octubre de 2002 (JUR/170618, 2003), de Castilla-La Mancha de 28 de febrero de 2005 (JUR/201257), de Castilla y León de 18 de septiembre de 2006 (AS/2995) y de Aragón de 3 de junio de 2008 (Rec. núm. 470/2008).
[23] STSJ de Andalucía de 9 de marzo de 2001 (AS/2788).
[24] STSJ de Aragón de 3 de junio de 2008 (Rec. núm. 470/2008).
[25] STSJ de Andalucía de 9 de enero de 2003 (AS/1373).
[26]Como señala la STC 98/2000, de 10 de abril de 2000*, "este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa"*.
[27] STSJ de Castilla y León de 18 de septiembre de 2006 (AS/2995).
[28] STSJ de la Comunidad Autónoma del País Vasco de 19 de junio de 2007 (AS/3357).

establecimiento es insuficiente[29], existen descuadres en el balance[30] o el trabajador apaga intencionadamente las cámaras frigoríficas donde se guardan los alimentos que consumen los residentes[31].

Ahora bien, no basta con alegar cualquiera de estas circunstancias justificativas de la medida de control audiovisual[32]. Si la empresa invoca como causa justificativa de la adopción de esta excepcional medida de control, la existencia de diferencias en el balance, debe ofrecer datos de las diferencias existentes entre las mercancías y el dinero obtenido en la caja que pongan de manifiesto la existencia de una supuesta actuación irregular del trabajador[33].

Además, debe constatarse si la medida de control audiovisual cumple con los tres requisitos siguientes: a) En primer lugar, "si tal medida es susceptible de conseguir el objetivo propuesto" (juicio de idoneidad); b) En segundo lugar, "si (la medida) es necesaria, en el sentido de que no exista otra más moderada para la consecución de tal propósito con igual eficacia" (juicio de necesidad); c) En tercer lugar, "si (la medida) es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto" (juicio de proporcionalidad).

---

[29] STSJ de la Comunidad Valenciana de 27 de abril de 2004 (AS/3821).

[30] STC 186/2000, de 10 de julio; y SSTSJ de Extremadura de 29 de enero de 2008 (Rec. núm. 765/2007) y de la Comunidad Autónoma de les Illes Balears de 28 de abril de 2008 (Rec. núm. 91/2008).

[31] STSJ de la Comunidad de Madrid de 9 de mayo de 2006 (AS/2030).

[32] STSJ de Galicia de 30 de noviembre de 2001 (AS/390).

[33] STSJ de la Comunidad de Madrid de 9 de julio de 2003 (AS/3210). Por su parte, la STSJ de la Comunidad de Madrid de 6 de julio de 2004 (AS/2325) frente a la consideración del juez de instancia de que la empresa no ha ofrecido datos sobre las diferencias existentes entre la mercancía y lo facturado ni sobre el desvío de dinero, afirma lo siguiente: *"Si se tiene en cuenta que la imputación referida al dinero consiste en sustracción de propinas que no se registran en caja, difícilmente la empresa puede aportar datos contables al respecto, máxime cuando existe la norma de no admitirse propinas de los clientes, y si a pesar de ello éstos las dejan, destinarse a un Fondo Social a disposición del Comité Intercentros. En cuanto a la diferencia entre la mercancía almacenada y la facturada, debe observarse que la propia naturaleza de la actividad (bar) puede hacer especialmente difícil advertir que se ha producido un cierto desfase salvo que el mismo fuese notorio. En efecto, en determinados tipos de consumiciones no es posible calibrar la cantidad exacta servida al cliente pues ni la bebida ni la comida se presenta no se sirve ni se presenta siempre en recipientes o envases individuales; lo mismo ocurre con los aperitivos, tapas o raciones."*

A tales efectos, habrá que atender no sólo al lugar del centro de trabajo en que se instalan por la empresa sistemas audiovisuales de control, sino también a otros elementos de juicio para dilucidar en cada caso concreto, si esos medios de vigilancia y control respetan el derecho a la intimidad de los trabajadores. No obstante, tales elementos de juicio son distintos en función de la finalidad que se persigue con la instalación de los medios de control, esto es, según se trate de dar un plus de seguridad o de verificar el cumplimiento indiscriminado de las obligaciones laborales por parte de los trabajadores (**a**), o de comprobar las sospechas de prestación irregular de los servicios por parte de algún trabajador (**b**).

a) Cuando se trata de dotar a la empresa de seguridad o de verificar el cumplimiento indiscriminado de las obligaciones laborales por parte de los trabajadores, la doctrina judicial considera que la medida de control supera los tres requisitos a los que queda sometido el juicio de proporcionalidad cuando a través de ella se consigue el fin pretendido, no se cuenta con otro medio más racional y proporcionado de control, los trabajadores saben de la existencia de las cámaras, y la filmación es la indispensable y estrictamente necesaria para satisfacer el interés empresarial merecedor de tutela y protección, situándose las cámaras en zonas de paso y de trabajo sin captación de sonido y sin persecución visual de los trabajadores ni de sus actos, y sin que las cámaras tengan posibilidad de zoom ni de modificar su enfoque[34]. También se pondera de forma favorable el que las cámaras no permitan el visionado en tiempo real de las imágenes que captan, quedando las mismas almacenadas en soporte físico sobre el que se vuelve a grabar cada cierto tiempo[35]. Por el contrario, y aunque la instalación de cámaras tenga causa y fundamento legítimos, ello no

[34] SSTSJ de Andalucía de 9 de marzo de 2001 (AS/2788), de Galicia de 30 de noviembre de 2001 (AS/390, 2002) y 20 de marzo de 2002 (AS/3385), de las Islas Canarias de 25 de octubre de 2002 (JUR/170618, 2003), de Andalucía de 9 de enero de 2003 (AS/1373), de Castilla-La Mancha de 28 de febrero de 2005 (JUR/201257), de la Comunidad de Madrid de 28 de junio de 2005 (AS/2080), de Galicia de 22 de diciembre de 2005 (AS/778, 2006), de la Comunidad de Madrid de 14 de junio de 2006 (AS/3406), de Castilla y León de 18 de septiembre de 2006 (AS/2995), de Extremadura de 15 de mayo de 2007 (JUR/247253), de la Comunidad Autónoma del País Vasco de 19 de junio de 2007 (AS/3357) y de Aragón de 3 de junio de 2008 (Rec. núm. 470/2008).

[35] STSJ de Aragón de 3 de junio de 2008 (Rec. núm. 470/2008).

faculta a la empresa a mantener en el tiempo este sistema de vigilancia cuando se haya reducido la causa que lo motivó y sobre todo cuando se lleva a cabo con cámaras que pueden ser manipuladas por la empresa sin conocimiento de los trabajadores ni de sus representantes, de manera que permitan vigilar los concretos puestos de trabajo[36]. No obstante, si en el curso de una vigilancia no centrada en los trabajadores se comprueba que alguno de ellos comete una falta disciplinaria (por ejemplo, una sustracción de material de la empresa), quedará justificado el enfoque exclusivo que de éste puedan hacer las cámaras[37], si bien dicho enfoque deberá superar el juicio de proporcionalidad que se expone en el siguiente apartado.

b) En los supuestos en que existen razonables sospechas de la comisión por parte del trabajador de graves irregularidades en su puesto de trabajo, los tribunales consideran que la medida de control audiovisual supera[38]: - El juicio de idoneidad, cuando permite verificar que el trabajador comete efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes; - El de necesidad, si la grabación sirve de prueba de tales irregularidades; - Y el de proporcionalidad, si la grabación de imágenes se limita a la zona de trabajo en la que pueden cometerse las supuestas irregularidades (por ejemplo, la caja o la barra de la cafetería, o la zona de laboratorio) y a una duración temporal limitada en el tiempo, la suficiente para comprobar que no se trata de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada[39]. No se pueden filmar los

[36] STSJ de la Comunidad Valenciana de 11 de julio de 2008 (Rec. núm. 1754/2008).
[37] STSJ de las Islas Canarias de 25 de octubre de 2002 (JUR/170618, 2003).
[38] STC 186/2000, de 10 de julio; y SSTSJ de la Comunidad Valenciana de 11 de enero de 2001 (AS/1601), de La Rioja de 5 de diciembre de 2000 (AS/135), de Andalucía de 9 de marzo de 2001 (AS/2788), del Principado de Asturias de 22 de marzo de 2002 (AS/632), de La Rioja de 30 de mayo de 2002 (AS/2207), de la Comunidad Valenciana de 14 de enero de 2004 (AS/1476), de Extremadura de 14 de abril de 2004 (AS/1071), de la Comunidad Valenciana de 27 de abril de 2004 (AS/3821), de la Comunidad de Madrid de 6 de julio de 2004 (AS/2325), de Galicia de 7 de julio de 2005 (AS/2499), de la Comunidad de Madrid de 9 de mayo de 2006 (AS/2030), de la Comunidad de Madrid de 4 de julio de 2007 (AS/2246), de la Comunidad Valenciana de 13 de junio de 2007 (AS/2808), de Extremadura de 29 de enero de 2008 (Rec. núm. 765/2007) y de la Comunidad Autónoma de les Illes Balears de 28 de abril de 2008 (Rec. núm. 91/2008).
[39] No se estima equilibrada la medida de control audiovisual en el siguiente supuesto de hecho [STSJ de Madrid de 9 de julio de 2003 (AS/3210)]: *"la causa de la adopción*

lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos[40]. Sin embargo, no se conculca la intimidad de los trabajadores si a

---

de esa excepcional medida de control, colocando una cámara oculta, «se debió a diferencias en el balance» y que instaló en el office de Bar Inglés, ya que se consideró que era allí donde podrían producir las pérdidas de las que ignoraban fuesen de género o dinero. Razones todas ellas que han de considerarse inadecuadas, innecesarias y desproporcionadas, puesto que el lugar escogido para la instalación de la cámara fue el Office del Bar Inglés, como tal dependencia auxiliar del mismo, donde se ubica precisamente la terminal de pago y caja registradora de los movimientos de cobro realizado en ese departamento, como se aprecia gráficamente en el reportaje fotográfico aportado -folios 128 a 132- que curiosamente no fue nunca filmada, ni intervenida, ni controlada, extremos perfectamente factibles y visibles en una organización compleja y ejemplar en tantas cosas, como es la empresa demandada, y por último resultó ser medida desproporcionada para los fines y pretensiones declarados de comprobar ese descuadre en el balance, del que por cierto no se ofrecieron datos de las diferencias existentes entre las mercancías y el dinero obtenido en al caja, que pusieran de manifiesto la existencia de esa supuesta irregular situación y la posible incidencia de la conducta imputada a dos de los demandantes de consumo reiterado de bebidas alcohólicas y de otros productos -no concretados- y que se decían impagados".

[40] SSTSJ de la Comunidad de Madrid de 14 de septiembre de 2000 (AS/4136), de las Islas Canarias de 25 de julio de 2001 (AS/4603), de Cantabria de 29 de abril de 2002 (JUR/157929) y de Andalucía de 2 de octubre de 2007 (AS/3311).

La STSJ de la Comunidad de Madrid de 4 de junio de 2007 (AS/2246) afirma lo siguiente: *"…estaba justificada la instalación por la empresa BT España, SA, en cuyo centro de trabajo sito en Madrid prestaba servicios quien hoy recurre, de una cámara para la captación y grabación de imágenes en la sala o cuarto donde se hallaban ubicadas varias máquinas destinadas a expender productos tales como café en sus diversas variedades, bebidas y otros alimentos sólidos, al objeto de comprobar lo que estaba sucediendo en cuanto al trato y manejo de las mismas, resulta innegable, teniendo en cuenta las quejas manifestadas pocos días antes por escrito por parte de la firma propietaria de dichas máquinas, en relación, de un lado, con el desajuste que frecuentemente existía entre los productos dispensados y la recaudación obtenida y, de otro, con los repetidos episodios de manipulación violenta de los sistemas de cierre y distribución con que cuentan; tampoco cabe cuestionar que la medida adoptada fuese necesaria, dado que era la única y más segura forma de averiguar lo que estaba aconteciendo y desvelar, así, la identidad de los posibles responsables de ello, sin que tuviese sentido la implantación de un sistema permanente de seguridad en la mencionada sala mediante personal adecuado durante toda la jornada laboral; a su vez, que fue una decisión idónea para la finalidad perseguida es asimismo evidente, ya que su designio no fue otro que conocer la veracidad de las quejas de la empresa suministradora del servicio y, sobre todo, despejar dudas en cuanto a la actuación de la mayoría del personal que trabaja en las oficinas de BT España, SA en Madrid, evitando de este modo que sobre él pesara una injusta y genérica imputación de actuación irregular en punto al manejo de las máquinas expendedoras de bebidas y otros productos; y finalmente, se trató también de una medida proporcionada y equilibrada, desde el mismo momento que la cámara fue colocada en la sala en la que, como dijimos, estaban las máquinas, enfocando únicamente a éstas, cuarto que, además, no solía ser utilizado como lugar de descanso y esparcimiento, ya que en el centro de trabajo existe otra sala destinada específicamente a fumar y comer, a lo que se une que, como con indudable valor fáctico consta en el fundamento segundo de la sentencia de instancia, tan repetida cámara sólo estuvo instalada "un par de días",*

través de las cámaras se visualizan las puertas de acceso a los aseos cuando se trata de controlar las ausencias que se producen durante la jornada laboral si la producción se realiza en cadena y el personal es retribuido por hora efectivamente trabajada y se constata un uso anómalo de las tarjetas dispuestas por la empresa para controlar el acceso a los aseos del personal del centro[41], o la entrada a los vestuarios cuando se han cometido robos en las taquillas de los trabajadores[42]. Por lo demás, el que los trabajadores elijan dejar sus bolsos o pertenencias personales en una zona de trabajo, ello no la convierte también en una zona vedada por los fines a los que sirven las cámaras de vigilancia[43].

Por último, no cabe ningún tipo de publicación y de divulgación de las imágenes captadas, o de conservación de las mismas una vez visualizadas dentro de un tiempo razonable y en las instalaciones de la empresa por la persona encargada del control, salvo que se haya apreciado infracción sancionable en cuyo supuesto podrán ser conservadas durante y a los solos efectos de prueba[44]. Además, como las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en los arts. 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, y 5.1.f) del Real Decreto 1720/2007, de 21 diciembre, que consideran como dato de carácter personal la información gráfica o fotográfica, ello exige respetar la normativa existente en materia de protección de datos, y en particular lo dispuesto en la Instrucción 1/2006, de 8 de noviembre, de la Agencia de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (BOE 12-12-2006)[45].

---

solamente se procedió a la grabación de imágenes, que no a la captación de conversaciones y, además, la misma "únicamente grababa lo sucedido en las máquinas y no en el resto de la sala". Por consiguiente, su uso se ajustó a los presupuestos que exige la doctrina constitucional."

[41] SSTSJ de la Región de Murcia de 3 de febrero de 2003 (JUR/93451 y 93452). Véase también la STSJ de Galicia de 21 de abril de 1995 (AS/1514).

[42] STSJ de Cataluña de 24 de mayo de 2007 (AS/2677).

[43] STSJ de Extremadura de 29 de enero de 2008 (Rec. núm. 765/2007).

[44] STSJ de Galicia de 21 de abril de 1995 (AS/1514).

[45] Cfr. la STSJ de la Comunidad Autónoma de les Illes Balears de 28 de abril de 2008 (Rec. núm. 91/2008).

III. CONTROL SOBRE EL USO DE LOS MEDIOS TECNOLÓGICOS DE INFORMACIÓN Y COMUNICACIÓN

El poder de vigilancia y control empresarial previsto en el art. 20.3 del ET va dirigido a comprobar el efectivo cumplimiento por el trabajador *"de sus obligaciones y deberes laborales"*. No obstante, se ha afirmado, por algún autor, que hay que distinguir entre la utilización de los medios tecnológicos de información y comunicación de la empresa como instrumentos de control y vigilancia de la prestación laboral y el control del uso, adecuado o inadecuado, por el trabajador de dichos medios[46]. En este sentido se afirma que mientras el primero persigue un control objetivo o general del cumplimiento de la prestación laboral en sentido positivo, el segundo, en cambio, se dirige a la supervisión, aislada y personal del correcto cumplimiento por parte de un trabajador concreto o grupo de trabajadores de las obligaciones y reglas laborales. Se trata en este último caso, pues, de un control más invasivo, más incisivo respecto de la intimidad personal. Y, por ello, se sostiene que para analizar la legitimidad de los mecanismos de control empresarial sobre el uso inadecuado de los medios tecnológicos de información y comunicación por parte de los trabajadores hay que acudir al art. 18 del ET[47]. Sin embargo, a nuestro juicio, tal diferenciación carece de fundamento a estos efectos, puesto que la verificación de los deberes y obligaciones laborales permite la aplicación de un control extensivo sobre la actividad del trabajador[48]. En efecto, a pesar de que el poder de vigilancia y control previsto en el art. 20.3 del ET tiene por objeto la ejecución de la prestación laboral en sí misma considerada, a partir de una interpretación extensiva de la buena fe contractual se amplía hasta alcanzar ciertos comportamientos o actuaciones que no aparecen estrictamente relacionados con la mera valoración, cuantitativa o cualitativa, del

[46] En este sentido, González Ortega, S., "La informática en el seno de la empresa. Poderes del empresario y condiciones de trabajo", en AA.VV., *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo,* Alicante, 2004, págs. 38 y ss.
[47] Cfr. STSJ de Andalucía de 25 de febrero de 2000 (AS/562).
[48] En el mismo sentido, Martínez Fons, D., *El Poder de Control…,* cit., págs. 143 y ss.

cumplimiento de la prestación laboral[49]. Y así, los tribunales utilizan el art. 20.3 del ET como referente para analizar la legitimidad de las formas de control empresarial del uso extralaboral de los equipos informáticos y sistemas de comunicación.

En este sentido, la STS de 26 de septiembre de 2007 (RJ/7514) afirma que *"el control del uso del ordenador facilitado al trabajador por el empresario no se regula por el artículo 18 del Estatuto de los Trabajadores, sino por el artículo 20.3 del Estatuto de los Trabajadores y a este precepto hay que estar con las matizaciones que a continuación han de realizarse"*. Es más, esta resolución judicial, dictada en unificación de doctrina, viene a corregir de plano la doctrina judicial que extendía las garantías formales previstas en el art. 18 del ET a los requisitos que se realizan en los ordenadores[50]. A juicio de Tribunal Supremo, no cabe la *"aplicación directa"* del art. 18 del ET *"al control del uso del ordenador por los trabajadores, ni tampoco su aplicación analógica, porque no hay ni semejanza de los supuestos, ni identidad de razón en las regulaciones (artículo 4.1 del Código Civil)"*. No obstante, y aunque la presencia de un representante de los trabajadores o de un trabajador de la empresa no es un requisito específico de los registros informáticos, constituye, como sucede con lo que establece el art. 569 de la Ley de Enjuiciamiento Criminal para intervenciones similares, *"una garantía de la objetividad y de la eficacia de la prueba"*. Es decir, *"esa exigencia no puede, por tanto, aplicarse al control normal por el empresario de los medios de producción, con independencia de que para lograr que la prueba de los resultados del control sea eficaz tenga que recurrirse a la prueba testifical o pericial sobre el control mismo"*.

Las facultades empresariales de vigilancia y control sobre el uso de los medios tecnológicos de información y comunicación pueden clasificarse con arreglo a los siguientes criterios:

---

[49] Martínez Fons, D., *El Poder de Control…,* cit., pág. 39.

[50] Sobre esta doctrina judicial ver, por todos, ROQUETA BUJ, R., *Uso y control de los medios tecnológicos de información y comunicación en el ámbito de la empresa*, Editorial Tirant lo Blanch, Valencia, 2005, pág. *. Véase también la STSJ de Cantabria de 18 de enero de 2007 (AS/1030).

En primer lugar, hay que distinguir entre el control dirigido a evaluar el cumplimiento de la prestación que integra el objeto del contrato de trabajo y el control del uso inadecuado de los medios tecnológicos de información y comunicación de la empresa por parte del trabajador. Conviene diferenciar estos dos planos ya que la segunda modalidad de control resulta más incisiva, pues se dirige a la supervisión de comportamientos individuales de incumplimiento y, por ello, debe respetar al máximo los derechos fundamentales del trabajador a la intimidad personal y al secreto de las comunicaciones[51]

En segundo lugar, hay que distinguir entre el control de los medios informáticos y del acceso a Internet, de un lado, y el control de las llamadas telefónicas y mensajes electrónicos, de otro. En este sentido, resulta claro que la utilización de los medios informáticos en la empresa no puede equipararse, sin más, al uso del teléfono o de la mensajería electrónica, puesto que éstos constituyen sistemas de comunicación entre el trabajador y un tercero[52].

En tercer lugar, hay que diferenciar según cuáles sean las condiciones de utilización de los medios tecnológicos de información y comunicación de la empresa[53]. Y es que los límites al control empresarial no serán los mismos según la naturaleza o condición otorgada por el empresario a dichos medios, esto es, según que se utilicen para fines exclusivamente profesionales, o cumplan una función mixta, pudiendo ser empleados por el trabajador tanto para fines laborales como de carácter privado.

1. La vigilancia y el control de la prestación laboral

1.1. Control informático

Los trabajadores informáticos, esto es, aquellos que cumplen sus funciones en un ambiente informatizado, contando como instrumento de trabajo

[51] González Ortega, S., "La informática en el seno de la empresa…", cit., págs. 38-44.
[52] Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 40.
[53] Thibault Aranda, J., *El Teletrabajo, Análisis jurídico-laboral,* Madrid, 2001, págs. 136-137; y STSJ de Andalucía de 9 de mayo de 2003 (AS/2840).

con el ordenador, pueden ser controlados por el empresario a través de éste. En efecto, mediante programas que permanecen activos en la memoria del ordenador (softaware y equipos de producción remota) se puede controlar de modo exhaustivo e, incluso, en tiempo real, la actividad laboral, tanto de los trabajadores controlables in situ por sus superiores como de los teletrabajadores[54]. En palabras de Pérez de los Cobos Orihuel, *"son los mismos instrumentos que el trabajador utiliza para realizar la prestación laboral, los que controlan ésta"*, de suerte que en estos casos *"el control ha dejado de ser una actividad ajena y aneja a la prestación de trabajo, para tornarse un elemento integrante de la prestación misma"*[55]. La posibilidad de adoptar estos mecanismos de control informático es, en principio, válida y tolerada por el art. 20.3 del ET.

Dos son, sin embargo, las limitaciones que se imponen al empresario:

1ª) Las medidas a adoptar deben estar encaminadas a verificar única y exclusivamente el cumplimiento de los deberes laborales y guardar en su aplicación la consideración debida a la dignidad del trabajador. El control informático sólo puede registrar los aspectos que se refieran exclusivamente al desempeño de la prestación de trabajo y, además, ha de ser sobrevenido a la actividad laboral, recogiendo sólo el resultado de la misma, esto es, la cantidad y calidad del trabajo realizado. No caben los controles que recaigan sobre la persona misma del trabajador y nieguen ese espacio de libertad e intimidad en el puesto de trabajo, donde sea posible la libre manifestación de la persona[56]. Y un control de la persona del trabajador, del trabajador en actividad, podría invadir ese espacio de privacidad del mismo en la empresa[57]. El control de la actividad *"sólo es posible cuando se presente conectado de forma tan inescindible con el resultado productivo, que sólo pueda obtenerse este último*

[54] Por todos, Martínez López, F.J. y otros, "Los sistemas de control de la actividad laboral mediante las Nuevas Tecnologías de la Información y las Comunicaciones", *R.L.*, nº 12, 2003, págs. 110-111 y 108-109.
[55] Pérez de los Cobos Orihuel, F., *Nuevas tecnologías y relación de trabajo*, Valencia, 1990, pág. 73.
[56] De Vicente Pachés, F., *El Derecho del Trabajador…,* cit., pág. 322.
[57] De Vicente Pachés, F., *El Derecho del Trabajador…,* cit., pág. 323; y Martínez Fons, D., *El Poder de Control…,* cit., pág. 33.

con la admisión del control sobre fragmentos del comportamiento del trabajador vinculado a dicho resultado"[58]. En cualquier caso, este control, inevitable por motivos justificados, no puede tornarse en una exasperante e incomoda presión para los trabajadores. En esta dirección, cabría proponer medidas similares a las ofrecidas por la doctrina a propósito de la instalación y utilización de aparatos de filmación, a saber[59]: permitir el acceso a los programas de software introducidos en los ordenadores de los trabajadores únicamente a los técnicos y superiores y a los representantes de los trabajadores, destruir periódicamente el historial de uso de los ordenadores correspondiente a los períodos en los que no se haya verificado ninguna anormalidad, etc.

2ª) Pero, además, el control informático debe respetar el derecho a la intimidad informática en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (LOPD). Téngase en cuenta que a través de los datos así obtenidos no sólo se pueden conocer de la forma más completa posible las aptitudes o deficiencias del trabajador, sino que también se puede reconstruir bastante aproximadamente el perfil moral, ideológico o sindical del trabajador[60].

1.2. Control de las llamadas telefónicas y de los mensajes electrónicos

En aquellos supuestos en que la prestación laboral se cumple, esencialmente, mediante el uso de los sistemas de comunicación empresariales y el contacto con los clientes de la empresa y la observancia de las pautas de comportamiento establecidas por el empresario, además de

[58] Garilli, A. y Bellavista, A., "Innovaciones tecnológicas y Estatuto de los trabajadores: los límites a los poderes del empresario entre la tutela individual y colectiva (artículos 4-9-13)", en AA.VV., *El Estatuto de los Trabajadores italiano veinte años después,* cit., pág. 222, citado por De Vicente Pachés, F., *El Derecho del Trabajador…*, cit. pág. 323.
[59] Por todos, Goñi Sein, J.L., *El respeto a la esfera privada…,* cit., pág. 145; y Martínez Fons, D., *El Poder de Control del Empresario…,* cit., págs. 112 y ss.
[60] Sobre el particular véanse, por todos, Cardona Rubert, B., *Informática y contrato de trabajo,* Valencia, 1999, págs. 68 y ss; Thibault Aranda, J., *El Teletrabajo, Análisis jurídico-laboral,* Madrid, 2001, págs. 141 y ss, y *Control multimedia de la actividad laboral*, Valencia, 2006, págs. 119 y ss; y Martínez Fons, D., *El Poder de Control…,* cit., págs. 185 y ss.

conformar la imagen y el crédito de la empresa, se integran en el contenido de las obligaciones laborales (empresas de ventas a través de teléfono, telemarketing, bancos o entidades aseguradoras "sin oficinas", información telefónica, funciones de captación y conversación a través de línea de verificación adicional 906), resulta evidente el interés del empresario en conocer cómo se desarrollan las comunicaciones de sus empleados[61]. En principio, el acceso directo o sin restricciones a dichas comunicaciones puede suponer una injerencia en la esfera de la intimidad del trabajador y una violación del derecho al secreto de las comunicaciones. Sin embargo, en estos casos la vigilancia sobre el modo en que se desarrollan las comunicaciones es el único medio que permite evaluar el cumplimiento de esta peculiar prestación laboral y obtener datos para mejorar el perfil o exigencias profesionales de los empleados a través de una formación adicional, o, en último término, incrementar la seguridad de las transacciones comerciales de la empresa. Por ello, los derechos a la intimidad y al secreto de las comunicaciones deben ceder ante el interés empresarial[62]. Pero sólo cuando la prestación del trabajador consista en la comunicación misma; por contra, cuando las comunicaciones constituyan un aspecto secundario o marginal de la prestación laboral, de manera que la comprobación del cumplimiento de ésta no venga condicionada por la revisión de aquéllas, un control tan penetrante e incisivo como el descrito no sería jurídicamente de recibo[63].

En todo caso, es necesario que los sistemas de comunicación de la empresa tengan la condición de herramientas de trabajo y que los trabajadores conozcan las limitaciones de su uso impuestas por el empresario y la posibilidad de acceder a los sistemas de comunicación por éste[64]. En estas condiciones debe considerarse legítima la facultad del empresario de

---

[61] Thibault Aranda, J., *El Teletrabajo*, cit., págs. 130-131.
[62] En este sentido, Thibault Aranda, J., *El Teletrabajo*, cit., págs. 130-131; y Martínez Fons, D., *El Poder de Control…,* cit., pág. 168.
[63] Martín Morales, R., *El régimen constitucional del secreto de las comunicaciones,* Madrid, 1995, págs. 68-69; y Thibault Aranda, J., *El Teletrabajo*, cit., pág. 131.
[64] Goñi Sein, J.L., "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", en AA.VV., *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo,* Alicante, 2004, págs. 80-81.

interceptar las comunicaciones de sus trabajadores sin requerir su consentimiento ni recabar autorización judicial. En efecto, en tales casos las comunicaciones realizadas por el trabajador se pueden considerar también como propias de la empresa[65] y, además, como la interceptación no es clandestina, se respeta el contenido esencial del derecho al secreto de las comunicaciones que garantiza el art. 18.3 de la CE, pues en la medida en que el trabajador sabe que lo pueden estar observando conserva el control sobre los datos y circunstancias personales. Y éste es el fin jurídico último que tanto el citado artículo como el art. 18.1 de la CE persiguen[66]. A mayor abundamiento, si las directrices de la política empresarial en orden al uso de los sistemas de comunicación han sido comunicadas y son conocidas de antemano por los trabajadores, no es necesario que la empresa, antes de activar el control que va a ejercer, lo ponga en conocimiento del trabajador[67]. De otro modo, éste, alertado por una señal de que está siendo controlado, puede mejorar temporalmente su actuación haciendo creer que el trabajo controlado es representativo de todas las tareas que realiza. Por otra parte, para preservar los derechos a la intimidad y al secreto de las comunicaciones del interlocutor del trabajador, totalmente ajeno a la relación jurídica que eventualmente legitima la limitación de tales derechos, se habrán de arbitrar determinados mecanismos, como por ejemplo, grabar únicamente la parte de la comunicación que corresponda al trabajador o advertirle de la posibilidad de que la empresa pueda acceder o intervenir, total o parcialmente, la

[65] En efecto, a pesar de que el empresario sea el titular de los medios a través de los que se producen dichas comunicaciones, no aparece *"integrado dentro del procedimiento comunicativo y, en consecuencia, dentro del concepto de comunicación"* (Cfr. Martínez Fons, D., *El Poder de Control…,* cit., pág. 138. En el mismo sentido, Marín Alonso, I., *El poder de…*, cit., pág. 153). Ahora bien, como señala Goñi Sein, *"las comunicaciones realizadas por el trabajador con un fin únicamente laboral, se deben considerar, también, como propias de la empresa, al ser realizadas por el comitente en el ejercicio de la actividad encargada"* (Cfr. Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 81. En el mismo sentido, la STSJ de Andalucía de 9 de mayo de 2003 (AS/2840)]. De este modo, el contenido de las comunicaciones que el trabajador realiza de acuerdo con las órdenes que recibe del empresario no se puede considerar patrimonio exclusivo de los trabajadores sino que pasa a ser también de la empresa.

[66] Thibault Aranda, J., *El Teletrabajo,* cit., pág. 131.

[67] Martínez, Fons, D., *El Poder de Control…,* cit., pág. 177. En sentido contrario, Thibault Aranda, J., *El Teletrabajo*, cit., pág. 131.

comunicación[68]. En este último supuesto, el cliente puede interrumpir la comunicación, dándola por terminada, o continuarla, en cuyo caso debe entenderse prestado su consentimiento a que se actúe algún tipo de control sobre la comunicación[69].

Por el contrario, si los trabajadores pueden utilizar los sistemas de comunicación empresariales con fines personales, todas las comunicaciones, tanto las personales como las profesionales, están protegidas por el art. 18.3 de la CE y, consecuentemente, gozan, en principio, de inviolabilidad. El empresario no puede acceder al contenido de los mensajes de carácter profesional que emiten o reciben sus trabajadores, a pesar de tener un legítimo interés en ello, sin recabar la autorización judicial o requerir su consentimiento, no siendo suficiente a tales efectos la advertencia empresarial previa de que las comunicaciones pueden ser controladas[70].

En todo caso, los controles que puedan establecer los empresarios en uso de su derecho a fiscalizar la actividad laboral de los trabajadores serán lícitos mientras no produzcan resultados inconstitucionales. Y para poder afirmar que los derechos fundamentales de los trabajadores se respetan, habrá que determinar en cada caso si la medida empresarial se acomoda a las exigencias de proporcionalidad entre el fin pretendido con ella y la posible restricción de aquellos derechos, esto es, si supera los juicios de *"idoneidad"*, *"necesidad"* y *"proporcionalidad en sentido estricto"*[71].

Por consiguiente, hay que constatar si la medida de control empresarial cumple los tres requisitos o condiciones siguientes, a saber[72]:

---

[68] Por todos, Thibault Aranda, J., *El Teletrabajo*, cit., pág. 131; y Martínez Fons, D., *El Poder de Control…,* cit., págs. 168-169.
[69] Martínez Fons, D., *El Poder de Control…,* cit., pág. 169.
[70] Cfr. Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., págs. 77 a 85.
[71] STS de 5 de diciembre de 2003 (RJ/313).
[72] A este respecto, se puede traer a colación la STS de 5 de diciembre de 2003 (RJ/313, 2004). El supuesto enjuiciado viene configurado por las siguientes circunstancias fácticas: a) La empresa facilita a los Asesores Comerciales un determinado teléfono conocido como Plataforma 2004, de uso exclusivamente profesional al servicio de la empresa, mediante el cual realizan aquéllos su actividad de telemarketing tendente a la fidelización de los actuales clientes de telefónica y a la

captación de otros nuevos mediante gestiones de venta, información, consultas y atención diversa a los clientes; b) La empresa controla la actividad de tales Asesores a través de un Coordinador por grupo de Asesores, cuya función consiste en «monitorizar» -traducida en ver, oír y grabar- aleatoriamente las conversaciones de aquéllos con los clientes, lo que se lleva a cabo en aproximadamente un 0,5% de las llamadas; c) Este control tiene como finalidad controlar el contenido de las llamadas y calificarlas, «para corregir los defectos de técnica comercial y disponer lo necesario para ello, incluso la realización de cursos de formación, comentando, normalmente después de su intervención, el resultado de su calificación al trabajador controlado personalmente para su comentario y, siempre, a través de la página Web del empleado»; d) Los Asesores tienen conocimiento de la existencia, funcionamiento, monitorización y destino estricto de la Plataforma 2004 desde por lo menos el año 2001; e) Los indicados trabajadores disponen de teléfonos no intervenidos en las salas de descanso que les permiten efectuar y recibir llamadas particulares; y f) La monitorización sólo se lleva a cabo sobre las llamadas de entrada, o sea, de las que realizan los clientes a los Asesores y no sobre las de salida.

Pues bien, el Tribunal Supremo declara lo siguiente: *"aquella «monitorización» o control empresarial se realiza en condiciones de respeto a la legislación vigente por cuanto, contemplada en los términos de generalidad en que se desarrolla este conflicto, tiene como único objeto controlar la actividad laboral del trabajador en condiciones de respeto a su esfera íntima inatacable. En efecto, si el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de telemarketing y a la vez disponen de otro teléfono para sus conversaciones particulares, si, como se ha apreciado, los trabajadores conocen que ese teléfono lo tienen sólo para trabajar y conocen igualmente que puede ser intervenido por la empresa, si además la empresa sólo controla las llamadas que recibe el trabajador y no las que hace, si ello lo realiza de forma aleatoria -un 0,5%-, y con la finalidad exclusiva de controlar la buena realización del servicio para su posible mejora, la única conclusión razonable a la que se puede llegar es a la de que se trata de un control proporcionado a la finalidad que con el mismo se pretende, en el sentido antes indicado. En ese mismo sentido se trata de un control que es necesario puesto que no se conoce otro medio más moderado para obtener la finalidad que se pretende -juicio de necesidad-, es idóneo para el mismo fin -juicio de idoneidad- y ponderado o equilibrado porque de ese control se pueden derivar beneficios para el servicio que presta la empresa y no parece que del mismo se puedan derivar perjuicios para el derecho fundamental de los trabajadores -proporcionalidad en sentido estricto-."*[72]. Por todo ello, y aunque no se niega la posibilidad de que la empresa *"pueda por esa vía atentar al derecho de intimidad de cualquier trabajador por cuanto, a pesar de todo, en esas conversaciones con los clientes pueden surgir comentarios que afecten a derechos fundamentales del trabajador incluidos dentro de la esfera de su intimidad en cuanto espacio excluido de cualquier posible intervención ajena -ideología política, afiliación sindical, libertad de expresión, etc.-",* se concluye que *"el servicio de control que aquí se contempla no puede ser considerado contrario a los derechos invocados desde el punto de vista del derecho colectivo, puesto que la práctica empresarial se ha acreditado que va dirigida exclusivamente a controlar el trabajo de sus empleados con una finalidad meramente laboral y con medios ponderados y por lo tanto acomodados a las exigencias garantistas de la normativa denunciada como infringida."* Véanse también las SSTSJ de Cataluña de 26 de enero de 2006 (AS/801) y de la Comunidad de Madrid de 30 de enero de 2006 (AS/852).

a) Si es susceptible de conseguir el objetivo propuesto, esto es, comprobar el correcto cumplimiento de la prestación laboral, y en su caso, adoptar las medidas para que ésta se desarrolle de la forma más organizada, eficiente, productiva, rentable o segura posible. La finalidad de la medida de control empresarial no puede ser otra que la de comprobar el adecuado cumplimiento de la prestación laboral y el correcto funcionamiento de la organización productiva[73]. Sólo se podrán controlar momentos, aspectos o circunstancias de la prestación laboral con repercusión contractual, tanto porque expresen el grado de cumplimiento del contrato, o la calidad del trabajo, como porque sirvan para vigilar o determinar el cumplimiento de obligaciones empresariales como la de seguridad[74].

b) Si, además, es necesaria en el sentido que no exista otra medida más moderada para la consecución del propósito antes indicado con igual eficacia. Indudablemente existen otros procedimientos que permiten, en cierto modo, comprobar el grado de cumplimiento de la prestación laboral, como las encuestas realizadas con posterioridad a los clientes de la empresa acerca del nivel de satisfacción con el servicio prestado. Sin embargo, como quiera que estos procedimientos pueden generar nuevos problemas en relación a la intimidad y tutela de datos personales de los clientes de la empresa, no parece que los mismos excluyan, ab initio, la adopción de procedimientos de intervención de las comunicaciones[75].

c) Y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre los derechos fundamentales en conflicto, considerándose a tales efectos diferentes elementos de juicio: si los controles son conocidos por los trabajadores o han sido instalados subrepticiamente, si la interceptación de las comunicaciones se hace o no indiscriminada y masivamente, si se controlan sólo las llamadas de entrada que realizan los clientes a los trabajadores o también las de salida, si los trabajadores disponen o no de teléfonos no

[73] Gónzalez Ortega, S., “La informática…”, cit., pág. 39.
[74] Gónzalez Ortega, S., “La informática…”, cit., pág. 39.
[75] Martínez Fons, D., *El Poder de Control…,* cit., págs. 169-170.

intervenidos para efectuar y recibir llamadas particulares, etc. Cuando no se controlen todas las comunicaciones, los criterios de selección de los trabajadores a controlar no pueden ser discriminatorios, esto es, no se puede elegir a un trabajador y no a otro por su pertenencia a un sindicato, por ejemplo, ni tampoco arbitrarios[76], sino que tienen que se aleatorios o fundarse en razones objetivas como el acceso a informaciones confidenciales por parte de determinados trabajadores[77]. A tales efectos, puede utilizarse un "sistema automático de selección de trabajadores", como es el que escoge, mediante la presión de un pulsante eléctrico, a saltos y sin determinación previa, a algunos trabajadores[78]. Las inspecciones tampoco pueden ser exhaustivas o continuas, pues en tal caso se trataría de un control ilícito porque serían actos contrarios a la tutela dispensada por el art. 18.3 de la Constitución y también a la consideración debida a la dignidad e intimidad del trabajador, que prohíbe los controles que nieguen un cierto espacio de libertad en el puesto de trabajo, o donde no sea posible la libre manifestación de la persona[79].

2. La vigilancia y el control del uso inadecuado de los medios tecnológicos de información y comunicación

Los trabajadores que utilizan los medios tecnológicos de información y comunicación de la empresa con fines personales, estando prohibida dicha utilización, incurren en un ilícito contractual. Además, pueden aprovechar este sistema de comunicación para cometer otros ilícitos contractuales en perjuicio de la empresa[80]. En todos estos supuestos es evidente que el empresario tiene un legítimo interés en ejercer algún tipo de fiscalización sobre el uso que hacen los trabajadores de tales medios.

---

[76] De Vicente Pachés, F., *El Derecho del Trabajador…,* cit., pág. 232; Thibault Aranda, J., *El Teletrabajo,* cit., pág. 138; y Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 81.

[77] Thibault Aranda, J., *El Teletrabajo,* cit., pág. 138; y Agut García, C., "Las facultades empresariales de vigilancia y control sobre útiles y herramientas de trabajo y otros efectos de la empresa", *T.S.,* nº 163, 2004, pág. 31.

[78] De Vicente Pachés, F., *El Derecho del Trabajador…,* cit., pág. 255.

[79] Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 81.

[80] Ribas, J. y otros, "Actos desleales de trabajadores usando sistemas informáticos e internet", *R.L.*, nº 21, 2004, págs. 105 y ss.

En relación con esta problemática, cabe distinguir varias hipótesis[81]:

En primer lugar, la adopción de controles preventivos, esto es, la adopción de medidas de verificación del uso por los trabajadores de los instrumentos tecnológicos de información y comunicación de la empresa, desconectadas de cualquier episodio precedente de uso irregular de los mismos. En principio, la prevención debería primar sobre la detección, es decir, habría que utilizar, más que dispositivos de control de los comportamientos de los trabajadores, herramientas técnicas para limitar los abusos, por ejemplo, bloqueando el acceso a algunas direcciones de Internet o chats o instalando advertencias automáticas[82]. Es posible, sin embargo, que estas medidas sean insuficientes. En tal caso, y desde la estructura lógica del poder de vigilancia y control empresarial, es admisible la adopción de medidas de verificación destinadas a asegurar la observancia de la buena fe que preside la relación laboral[83]. No obstante, al tratarse de medidas restrictivas de los derechos fundamentales de los trabajadores, debe darse *"una conexión directa entre la conducta controlada y la razón para controlarla"*, por lo que parece razonable requerir, inicialmente, la presencia de un ilícito contractual previo[84]. Sin embargo, en determinadas situaciones podría admitirse la adopción de controles preventivos. Así sucede cuando se trata de empresas que por sus dimensiones o por la complejidad o peculiaridad de sus sistemas de información y comunicación han de adoptar unas medidas eficaces de protección o cuando las circunstancias lo exijan, y así será cuando exista una razonable probabilidad basada en circunstancias objetivas –como puede ser la existencia de episodios previos de abuso en el uso de las herramientas de trabajo-[85]. No obstante, estos controles preventivos no han de suponer en ningún caso la intromisión en los contenidos privados sino exclusivamente en

[81] Martínez Fons, D., *El Poder de Control…,* cit., págs. 147 y ss.
[82] Cfr. el Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, realizado por el grupo de trabajo sobre protección de datos constituido en la UE al amparo del art. 29 de la Directiva 95/46/CE (5401/01/ES/Final WP 55).
[83] Martínez Fons, D., *El Poder de Control del Empresario…,* cit., pág. 148.
[84] Martínez Fons, D., *El Poder de Control del Empresario…,* cit., pág. 148; y Gónzalez Ortega, S., "La informática…", cit., pág. 46.
[85] Martínez Fons, D., *El Poder de Control del Empresario…,* cit., págs. 148-149.

los aspectos cuantitativos, limitándose a indagar en el tipo de aplicaciones utilizadas, páginas web consultadas o cantidad de correos enviados. Además, dichos controles deben ser aleatorios o fundarse en razones objetivas y su existencia debe ser conocida de antemano por los trabajadores. Evidentemente, los mismos son posibles, si el trabajador los acepta en un anexo al contrato de trabajo[86]. En cualquier caso, no son posibles las "pruebas de honestidad o de lealtad", consistentes en someter a los trabajadores a pruebas, de las que no tienen conocimiento, para comprobar si los mismos responden a los parámetros de lealtad y de buena fe que la empresa entiende exigibles[87]. Someter al trabajador a este tipo de pruebas comportaría un uso abusivo de la facultad empresarial de control en la medida en que existe una provocación al incumplimiento, una especie de predeterminación del mismo.

En segundo lugar, el control efectuado, individual o plural, en la utilización por los trabajadores de los medios tecnológicos de información y comunicación de la empresa, sobre la base de pruebas o indicios suficientes que permiten atribuirles el uso ilícito de tales medios. Los indicios suficientes no se identifican con la certeza absoluta, sino con los principios de la lógica que, inicialmente, abonan la conclusión del empleador[88]. En tal caso, las medidas de verificación de la utilización de los medios reseñados se dirigen a obtener las pruebas del ilícito laboral y, por tanto, es admisible un control oculto[89]. Estos controles deberán efectuarse con la máxima discreción y en un lugar separado de la presencia intrusiva de terceros[90]. Además, los mismos no comprenden, por supuesto, la publicación o divulgación de las informaciones obtenidas[91].

2.1. Control informático y de la navegación a través de Internet

[86] STSJ de Cataluña de 11 de marzo de 2004 (AS/1231).
[87] Gónzalez Ortega, S., "La informática…", cit., pág. 44. Cfr. la STSJ de Madrid de 11 de mayo de 2004 (JUR/241595).
[88] Martínez Fons, D., *El Poder de Control…,* cit., pág. 147.
[89] Martínez Fons, D., *El Poder de Control…,* cit., pág. 147.
[90] Thibault Aranda, J., "El Derecho español", en AA.VV., *Tecnología Informática y Privacidad de los Trabajadores*, Elcano (Navarra), 2003, pág. 50.
[91] SSTSJ de Cataluña, de 23 de octubre de 2000 (AS/4536); de Madrid, de 10 de abril de 2003 (AS/3257); y de Andalucía, de 9 de mayo de 2003 (AS/2840).

A partir de la utilización de los medios informáticos y de la navegación en Internet, en numerosas ocasiones se pueden obtener informaciones relacionadas con la intimidad del trabajador[92]. Como señala la STS de 26 de septiembre de 2007 (RJ/7514), existe un hábito generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa y *"esa tolerancia crea una expectativa también general de confidencialidad en esos usos* {…} *que no puede ser desconocida"*. La garantía de intimidad, según remarca esta sentencia, *"se extiende a los archivos personales del trabajador que se encuentran en el ordenador"*[93] y a *"los denominados archivos temporales, que son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de Internet"*[94]. En este sentido, el Tribunal Supremo afirma que, aunque *"se trata más bien de rastros o huellas de la «navegación» en Internet y no de informaciones de carácter personal que se guardan con carácter reservado"*, estos archivos *"también entran, en principio, dentro de la protección de la intimidad"*, pues, como señala la sentencia de 3 de abril de 2007 del Tribunal Europeo de Derechos Humanos los mismos pueden *"contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladores sobre determinados aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etc.)"*. Por lo demás, la garantía de la intimidad se extiende a los archivos temporales tanto si se encuentran en el disco duro del ordenador del trabajador como si quedan reflejados en el servidor de la empresa[95].

---

[92] Martínez Fons, D., "El control de la correspondencia electrónica personal en el lugar de trabajo", *R.L.,* nº 9, 2003, pág. 51; Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 49; y STSJ de Castilla y León de 8 de noviembre de 2004 (AS/3073).

[93] En el mismo sentido, las SSTSJ de la Comunidad Autónoma del País Vasco de 12 de septiembre de 2006 (AS/2602), de Cantabria de 18 de enero de 2007 (AS/1030) y de la Comunidad Autónoma del País Vasco de 24 de abril de 2007 (AS/2512).

[94] Cfr. las SSTSJ de Galicia de 4 de octubre de 2001 (AS/3366) y de 5 de junio de 2006 (AS/1762, 2007). Sobre este particular ver el Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, realizado por el grupo de trabajo sobre protección de datos constituido en la UE al amparo del art. 29 de la Directiva 95/46/CE (5401/01/ES/Final WP 55).

[95] STSJ de la Comunidad Valenciana de 22 de diciembre de 2005 (AS/1278, 2006).

Ahora bien, como pone de relieve la STS de 26 de septiembre de 2007 (RJ/7514), esa tolerancia no puede *"convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio"*. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe *"es establecer previamente las reglas de uso de esos medios con aplicación de prohibiciones absolutas o parciales e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, 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"*. De esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, *"no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad» en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (TEDH 1997, 37) (caso Halford) y 3 de abril de 2007 (TEDH 2007, 23) (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo par la protección de los derechos humanos"*[96]. Además, la empresa deberá solicitar del comité de

[96] En el mismo sentido, las SSTSJ de Cataluña de 10 de septiembre de 2001 (AS/2776), de la Comunidad de Madrid de 13 de mayo de 2003 (AS/3649), de Cataluña de 10 de octubre de 2006 (AS/1668, 2007). y de la Comunidad Valenciana de 4 de julio de 2007 (AS/2879). Ahora bien, el que el ordenador no tenga clave de acceso, unido a su localización en un despacho sin llave, *"no supone por sí mismo una aceptación por parte del trabajador de un acceso abierto a la información contenida en su ordenador"* [STS de 26 de septiembre de 2007 (RJ/7514)].

No obstante, la STSJ de Cantabria de 18 de enero de 2007 (AS/1030) exige además que el registro respete los principios de causalidad, indispensabilidad y proporcionalidad. En este sentido, afirma lo siguiente: *"… no se puede compartir la tesis que asimismo se sustenta en la sentencia de instancia sobre la necesidad y el equilibrio del sistema de control utilizado, al que se considera un instrumento proporcionado y necesario a la finalidad perseguida, pues frente a lo que allí se afirma, la recogida de datos no se limitaba a realizar una estadística de los accesos a Internet que no fueran los oficiales de la pagina «Credit Services» y los enlaces permitidos por esta, sino que especificaba asimismo los recursos de Internet solicitados (paginas*

empresa la emisión del informe previsto en el art. 64.1.4º.d) del ET[97]. En este caso, por lo demás, los criterios de selección de los trabajadores no podrán ser discriminatorios ni arbitrarios, sino aleatorios o fundados en razones objetivas[98].

Pero, sin previa advertencia sobre el uso y el control del ordenador, cualquier control informático o de la navegación en Internet debe ser

---

web, gráficos, fotografías...etc.), y tal acopio de datos, en la medida en que entrañaba un control sistemático de los sitios visitados, así como de su frecuencia, tiempo de conexión y navegación, permiten reconstruir aspectos subjetivos relativos a la intimidad del trabajador, y ello excede sin duda de la finalidad declarada: conocer el uso que se hacía de Internet en horas de trabajo, que era el parámetro que debió modular el nivel y la intensidad de la recogida de datos, y que al ser rebasado deslegitima el comportamiento empresarial, pues constituye un principio básico de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que sólo se podrán recoger datos de carácter personal para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido (art. 4.1), lo que también se deduce del Considerando 28 de la Directiva 1995/46 cuando indica que «todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos». Tampoco se puede compartir el criterio de que el medio técnico elegido fuera adecuado y necesario puesto que se pudo acudir a otras medidas menos ingerentes sobre la privacidad del trabajador, que igualmente podían satisfacer el interés empresarial en un grado similar al empleado. En este sentido llama la atención que se hayan eludido los controles preventivos, adoptando controles indirectos sobre la navegación mediante la instalación de advertencias automáticas o filtros que impidiesen visitar las paginas o lugares no autorizados o, incluso, se pudo instalar un control meramente estadístico relativo al tiempo de conexión a los sitios no autorizados, que asimismo hubiera permitido tomar conocimiento de los datos imprescindibles para la comprobación del uso que se venía haciendo de los accesos a Internet que no fueran los oficiales de la pagina «Credit Services» y del tiempo invertido en ello. La conclusión de cuanto se deja dicho no puede ser otra sino que el sistema de control cuestionado, rebasó ampliamente los limites con el que la citada sentencia 186/2000 STC concibe tal facultad empresarial mediante el uso de los nuevos medios técnicos, al resultar inadecuado al fin perseguido y, además porque, los datos capturados en la actividad de control desplegada fueron excesivos, lo que deslegitima el comportamiento empresarial, de conformidad con lo previsto en el art. 7.2 de la Ley Orgánica 1/1982, de 5 de mayo (RCL 1982, 1197), de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, que considera ilegitimas las conducta empresariales que utilicen «... aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción»".

[97] SSTSJ de la Comunidad Valenciana de 19 de julio de 2005 (AS/3205) y 22 de diciembre de 2005 (AS/1278, 2006).

[98] Thibault Aranda, J., *El Teletrabajo*, cit., pág. 137.

respetuoso con el derecho a la intimidad personal de los trabajadores[99]. Ello significa que la medida empresarial de control ha de estar justificada. En principio, es evidente que el empresario tiene un interés legítimo en vigilar sus instrumentos de trabajo para que no se realice un uso abusivo y para fines personales de los trabajadores[100]. Sin embargo, nos hallamos ante medidas restrictivas del derecho a la intimidad personal de los trabajadores que exigen en su adopción una adecuada ponderación del fin perseguido por el control y su objeto. De conformidad con ello, el registro informático que no suponga intromisión en los contenidos privados del trabajador sino exclusivamente en aspectos cuantitativos que indaguen el tipo de aplicaciones utilizadas, de documentación empleada o almacenada en el ordenador, o de programas instalados en el ordenador, etc[101], o que se limite a realizar una estadística relativa al tiempo de conexión a los sitios de Internet que no guardan relación alguna con el trabajo[102], puede ser admitido si cumple con las demás condiciones de adecuación constitucional. Por el contrario, cualquier medida de control empresarial que pueda implicar directamente a la persona del trabajador, requiere la existencia de razonables sospechas de la comisión de un ilícito laboral previo. Ni que decir tiene que la instalación con carácter sistemático de software de monitorización del desempeño del trabajo o de equipos de producción remota no tiene encaje en nuestro ordenamiento constitucional[103]. Ello supondría un atentado a la intimidad y a la dignidad de la persona del trabajador por la privación total de intimidad que comportaría y sobrepasaría manifiestamente los límites normales del ejercicio de los poderes

---

[99] Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 51, y "El control empresarial del uso de las nuevas tecnologías en la empresa", en AA.VV., *Relaciones Laborales y Nuevas Tecnologías*, Madrid, 2005, págs. 218 y ss.

[100] STSJ de Galicia de 4 de octubre de 2001 (AS/3366).

[101] En este sentido, la STSJ de Cataluña de 30 de marzo de 2006 (JUR/254693) afirma que consistiendo la actuación de la empresa *"no en la de entrar en el contenido de los archivos concretos que contenía el ordenador, lo que hubiera ido en contra de su derecho a la intimidad, sino en comprobar que había mucha documentación que había sido utilizada frecuentemente en cuestiones ajenas a la empresa, lo que demuestra entre otras cosas, la inobediencia a las órdenes de la empresa que no permitías el uso del ordenador para quehaceres propios del trabajador, la transgresión de la buena fe contractual y el uso del tiempo de trabajo pactado para realizar tareas extralaborales"*.

[102] STSJ de la Comunidad Autónoma del País Vasco de 25 de septiembre de 2007 (AS/40, 2008).

[103] Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 87; y Ruano Albertos, J., "Facultades de control por medios informáticos", *T.S.,* nº 162, 2004, pág. 31. En sentido contrario, Thibault Aranda, J., *El Teletrabajo*, cit., págs. 137-138.

instrumentales de vigilancia y control empresariales. El respeto a la dignidad e intimidad del trabajador delimita un ámbito no ilimitado sino restringido de vigilancia, y estos programas, al permitir que el empresario pueda registrar todo y ver directamente el uso que está dando el trabajador al ordenador conectado en la red, no ofrecen garantía alguna a los aspectos reservados e íntimos del trabajador presentes habitualmente cuando trabaja.

La adopción de instrumentos directos de control informático o de la navegación en Internet del trabajador, por tanto, habrá de sustentarse en un interés empresarial suficientemente relevante que justifique la restricción de la esfera personal del trabajador[104]. Lo es, desde luego, el legítimo interés del empresario en poner coto al uso abusivo de los instrumentos informáticos de la empresa para asuntos personales[105], ante la existencia de razonables sospechas de la comisión por parte del trabajador de graves irregularidades en su puesto de trabajo[106]. Además, dicho interés ha de ser acreditado por la empresa; si ésta ni siquiera aduce causa o motivo alguno para la realización del registro informático en cuestión, dicho control violará el derecho a la intimidad del trabajador[107].

La medida de control informático, además de justificada, ha de ser "idónea" para la finalidad pretendida, esto es, verificar si el trabajador comete efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes[108]; "necesaria", en el sentido de que no

---

[104] Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 51.
[105] Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 86.
[106] SSTSJ de Cataluña, de 23 de octubre de 2000 (AS/4536) y 29 de junio de 2001 (AS/3236); y de Madrid, de 10 de abril de 2003 (AS/3257).
[107] SSTSJ de Andalucía de 25 de febrero de 2000 (AS/562), y de la Comunidad Valenciana de 19 de julio de 2005 (AS/3205) y 22 de diciembre de 2005 (AS/1278, 2006).
[108] En este sentido, la STS de 26 de septiembre de 2007 (RJ/7514) afirma lo siguiente: *"….la empresa no podía recoger la información obrante en los archivos temporales y utilizarla con la finalidad que lo ha hecho. Esa actuación en el presente caso ha supuesto una vulneración de su derecho a la intimidad. En efecto, en el supuesto de que efectivamente los archivos mencionados registraran la actividad del actor, la medida adoptada por la empresa, sin previa advertencia sobre el uso y el control del ordenador, supone una lesión a su intimidad en los términos a que se ha hecho referencia en los anteriores fundamentos. Es cierto que la entrada inicial en el ordenador puede justificarse por la existencia de un virus, pero la actuación*

exista otra más moderada para la consecución de tal propósito con igual eficacia[109]; y "equilibrada" o "ponderada", por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto[110]. De este modo, el empresario ha de optar por la opción tecnológica menos invasiva posible en la dignidad del trabajador, limitando el conocimiento de la información del trabajador así como el período temporal de sujeción, a lo estrictamente necesario para asegurar el fin que justifica el control[111]. Si la medida de control empresarial no está justificada o no cumple los tres requisitos o condiciones anteriores, constituirá una vulneración del derecho fundamental a la intimidad del trabajador[112]. Además, cualquier medida de

---

empresarial no se detiene en las tareas de detección y reparación, sino que, como dice con acierto la sentencia recurrida, en lugar de limitarse al control y eliminación del virus, «se siguió con el examen del ordenador» para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada. De esta forma, no cabe entender que estemos ante lo que en el ámbito penal se califica como un «hallazgo casual» (sentencias de 20 de septiembre [RJ 2006, 6402], 20 de noviembre [RJ 2006, 9187] y 1 de diciembre de 2006 [RJ 2006, 9564]), pues se ha ido más allá de lo que la entrada regular para la reparación justificaba."

[109] En este sentido, la STSJ de la Comunidad Autónoma del País Vasco de 12 de septiembre de 2006 (AS/2602) afirma que *"cabían, en concreto, medidas alternativas, pues se pudo pedir el consentimiento del actor desde un primer momento y caso de no darlo éste, instar la autorización judicial de rigor"*.

[110] SSTSJ de Cataluña, de 23 de octubre de 2000 (AS/4536) y 29 de junio de 2001 (AS/3236); de Galicia, de 4 de octubre de 2001 (AS/3366); y de Castilla-León, de 8 de noviembre de 2004 (AS/3073).

[111] STSJ de la Comunidad Autónoma del País Vasco de 30 de mayo de 2006 (AS/1029, 2007). En este sentido, la STSJ de la Comunidad Autónoma del País Vasco de 12 de septiembre de 2006 (AS/2602) afirma lo siguiente: "*Lo cierto y verdad es que había una carpeta con el nombre del demandante, que había datos personales suyos junto con otros de la empresa y que se investigaron y se abrieron sus archivos por un alto directivo de la empresa y por el perito, sin el consentimiento del actor, sin intervención judicial y sin ni siquiera las garantías del artículo 18 del Estatuto de los Trabajadores, cuando se trata de registrar efectos personales del trabajador. La identificación por el nombre del actor de aquella carpeta, consideramos que ya era indicativo de que lo razonable era suponer que se contenían en la misma datos personales. En todo caso, la duda que pudiera albergarse, se disiparía al empezar a examinar los archivos de la carpeta, pues en un alto porcentaje, superior al 75, eran de tal índole. Sin embargo, tampoco se detuvo ahí el primer registro y la posterior peritación: no obstante, conocerse sin especie alguna de duda que había datos personales, se sigue con aquel registro y peritación hasta examinar de forma exhaustiva tal carpeta e incluso se llegó a copiar en disco portátil su íntegro contenido".* Cfr. la STSJ de la Comunidad Autónoma del País Vasco de 23 de enero de 2007 (AS/1723).

[112] STSJ de Andalucía, de 25 de febrero de 2000 (AS/562); y Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 87.

control debe ser respetuosa con el derecho a la intimidad informática del trabajador[113].

Sin embargo, la doctrina judicial ha considerado legítimas las siguientes medidas de control empresarial: los registros en el ordenador del trabajador y la copia de sus ficheros personales[114]; ante la sospecha de utilización del ordenador para la práctica del juego denominado "solitario", colocar en un directorio de la red, la aplicación de un programa que se activa de forma automática cuando se pone en marcha el ordenador e identifica los programas y ventanas del programa windows que se activan en cada momento[115]; acceder a partir del disco duro del ordenador principal de la empresa a los contenidos de las direcciones de Internet visitadas por el trabajador[116]; realizar una copia de seguridad del disco duro del ordenador y proceder a verificar su contenido[117]; instalar en el ordenador del trabajador un programa informático denominado "espía" dedicado a controlar lo que se hace desde el ordenador, ante la aparición en el mismo de páginas de contenido pornográfico, gran parte de las cuales contenían imágenes de pornografía infantil[118]; realizar una copia completa en espejo del disco del ordenador del trabajador[119]; verificar la utilización de Internet por el trabajador a través del ordenador central por el programa Boss Everyware, máxime cuando el trabajador aceptó en un anexo al contrato de trabajo la supervisión periódica de los listados de las páginas web visitadas con indicación de la dirección, fecha, hora y tiempo de conexión; en un supuesto en que en varias ocasiones el ordenador del trabajador permanece en funcionamiento bajando música de la red, bloqueando la línea ADSL e impidiendo el trabajo de sus compañeros, anular la contraseña individual del trabajador –la empresa tenía prohibido instalar "passwords" o contraseñas individuales- mediante la anulación de la contraseña general del

[113] STSJ de Andalucía de 9 de mayo de 2003 (AS/2840); Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 51; y Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., págs. 85 y ss.
[114] STSJ de Andalucía de 25 de febrero de 2000 (AS/ 562).
[115] SSTSJ de Cataluña de 23 de octubre de 2000 (AS/4536) y 29 de junio de 2001 (AS/3236).
[116] STSJ de Galicia de 4 de octubre de 2001 (AS/3366).
[117] STSJ de Madrid de 13 de mayo de 2003 (AS/3649).
[118] STSJ de Galicia de 30 de mayo de 2003 (AS/3128).
[119] STSJ de Cataluña de 23 de febrero de 2004 (AS/444).

servidor y examinar el disco duro del ordenador[120]; o, en fin, instalar el programa "espía" en la terminal del ordenador que usa el trabajador, al objeto de registrar, copiando el disco duro, las entradas del trabajador en Internet y las páginas visitadas[121].

2.2. Control de las llamadas telefónicas y de los mensajes electrónicos

Las facultades empresariales de vigilancia y control del uso del teléfono y del correo electrónico por los trabajadores pueden chocar con los derechos a la intimidad personal y al secreto de las comunicaciones[122]. La protección del derecho al secreto de las comunicaciones *"alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos"*[123]. Sin embargo, cuando la comunicación queda registrada en soporte físico o, en su caso, virtual, el

[120] STSJ de Cataluña de 22 de julio de 2004 (AS/2696).
[121] STSJ de Castilla y León de 8 de noviembre de 2004 (AS/3073).
[122] Así lo subraya la STS de 26 de septiembre de 2007 (RJ/7514). Algunas resoluciones judiciales, sin embargo, al enjuiciar el control empresarial de las comunicaciones electrónicas de los trabajadores en la empresa, analizan únicamente la posible vulneración del art. 18.1 de la CE, relativo a la intimidad personal, y no del art. 18.3 de la CE respecto del secreto de las comunicaciones [Cfr. SSTSJ de Madrid, de 30 de octubre de 2001 (LA LEY JURIS: 981480/2001), 18 de septiembre de 2002 (AS/2828) y de 10 de abril de 2003 (AS/3257); de Cataluña, de 6 de junio de 2003 (AS/2272); de Galicia, de 21 de noviembre de 2003 (JUR/57945, 2004); de Cataluña, de 21 de septiembre de 2004 (AS/2880); y de Castilla y León de 10 de mayo de 2006 (AS/682, 2007)]. Esta postergación del derecho al secreto de las comunicaciones en la empresa, aunque en algunas ocasiones pueda estar justificada, con carácter general no es de recibo [Marín Alonso, I., *El poder de control empresarial…,* cit., págs. 137 y ss]. La misma puede explicarse, en parte, por la regulación que la Ley Orgánica 1/1982, en desarrollo del art. 18.1 de la CE, realiza sobre la utilización de aparatos de escucha, o de cualquier otro mecanismo, para conocer la vida íntima de terceros o sus cartas privadas (art. 7.2). Esta normativa, apropiada para solucionar los problemas derivados de la interceptación o grabación de conversaciones cara a cara entre trabajadores, no es, sin embargo, adecuada para resolver los supuestos de interceptación del correo electrónico del trabajador en el lugar de trabajo. El art. 18.3 de la CE protege, en todo caso, el proceso comunicativo entablado a través de un soporte técnico entre personas que no se encuentran cara a cara, sin importar, por tanto, el carácter íntimo o no del contenido de los mensajes, mientras que el art. 18.1 de la CE ampara, a diferencia de aquél, esta última eventualidad, es decir, la reserva que incumbe a los comunicantes o a los terceros que hayan interceptado la comunicación cuando el mensaje sea de naturaleza íntima o reservada.
[123] SSTC 123/2002, de 20 de mayo; y 56/2003, de 24 de marzo.

secreto *"puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje -con conocimiento o no del mismo- o captación de otra forma del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)"*[124]. Puede decirse así que *"el secreto que integra el derecho contemplado en el art. 18.3 CE puede extenderse en ciertas circunstancias, más allá de la comunicación, a lo comunicado y que es posible, de este modo, que el apoderamiento de la correspondencia ajena ya recibida, abierta, leída y archivada por su destinatario atente también contra la "impenetrabilidad" de un proceso comunicativo que en principio, en lo temporal, ya había fenecido, y en lo material, había salido ya del cauce que garantizaba constitucionalmente su secreto"*[125]. En consecuencia, el derecho al secreto de las comunicaciones realizadas mediante correo electrónico se extiende también a los mensajes recibidos y archivados[126], ya sea en el servidor empleado por la empresa, ya sea en el buzón del correo electrónico del trabajador[127]. No obstante, es necesario que tales mensajes presenten la evidencia externa que permita tener la constancia objetiva de que son objeto de una comunicación secreta, tutelada por el art. 18.3 de la Constitución[128]. De otro modo, nos hallaríamos ante meros

[124] STC 70/2002, de 3 de abril.

[125] ATC 30/1998, de 28 de enero. En el mismo sentido, la STC 123/2002, de 20 de mayo.

[126] STSJ de Cataluña de 16 de septiembre de 2002 (AS/2637); Falguera i Baró, M.A., "Uso por el trabajador del correo electrónico de la empresa para fines extraproductivos y competencias de control del empleador", *R.L.*, Vol. II, 2000, pág. 496, y "Trabajadores, empresas y nuevas tecnologías", en AA.VV., *Derecho a la intimidad y nuevas tecnologías*, Consejo General del Poder Judicial, Madrid, 2004, pág. 214; Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 42; y Marín Alonso, I., *El poder de control empresarial…,* cit., págs. 149 y ss.

[127] Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 42.

[128] ATC 30/1998, de 28 de enero; y STC 70/2002, de 3 de abril. En este sentido, el Auto de la Audiencia Provincial de Barcelona de 2 de febrero de 2006 (AC/440) afirma lo siguiente: *"En nuestro caso, el perito informático de las demandantes no interfirió un proceso de comunicación ajeno. Puede discutirse, y así se hará, la posibilidad del empresario de acceder al correo electrónico de su empleado, pero ni siquiera en ese caso podría obviarse algo sustancial del caso que nos ocupa, como es que el Sr. Luis Miguel, en un período de siete horas formateó el disco duro, modificó el reloj, modificó el nombre de usuario y reinicializó el sistema operativo del ordenador de la empresa. Esta operación de borrado, que efectivamente fue anunciada por el requerido tras negarse a permitir el acceso a los contenidos del ordenador que utilizaba, supuso deshacer el armazón de dicha información y convertirla en una amalgama de datos no susceptible de clasificación, en la que los datos del correo electrónico se mezclaba de*

efectos personales del trabajador protegidos no por el derecho al secreto de las comunicaciones, sino, en su caso, por el derecho a la intimidad previsto en el art. 18.1 de la Constitución[129].

La doctrina científica y judicial que ha abordado esta cuestión, sin embargo, no es pacífica. Así, un sector doctrinal se ha inclinado por considerar que el empresario no puede acceder a las comunicaciones de sus trabajadores porque ello supondría una vulneración de su derecho al secreto de las comunicaciones[130], pudiendo tan sólo controlar, en determinadas circunstancias, los denominados datos externos de las llamadas telefónicas y de los mensajes electrónicos[131]. Por el contrario, una cierta línea doctrinal mantenida en algunas sentencias de suplicación da prevalencia a la propiedad de los sistemas de comunicación, admitiendo el control de las comunicaciones

---

forma indiscriminada con archivos word, excel, imágenes u otros formatos. La búsqueda ciega que el perito llevó a cabo, según opera la herramienta Encase o similares y ratificó el Sr. Bevilacqua, no supone por tanto la lectura de toda la información para detectar lo relevante para la empresa, sino la utilización de palabras clave que sólo permiten rescatar lo que interesa, si es que no hubiera sido borrado en la reinstalación. El borrado usual (pues existen otros de bajo nivel que sí eliminan la información), no hace desaparecer los datos, sino que elimina las entradas de los mismos y hace imposible acceder a ellos: al romperse el código de entrada en sistema binario, los datos permanecen, pero confundidos e indistinguibles en una enorme cantidad de ceros y unos, de modo que el programa empleado pretende detectar los patrones binarios de ciertas palabras, y una vez detectados, reinterpretar por encima y por debajo hasta reconstruir un texto. Las apelantes utilizan la imagen de un archivador volcado sin orden ni concierto en el suelo, del que se rescata tan sólo una hoja concreta. Pero más gráfica es la idea de un aparato de destrucción de documentos que almacena los restos, del que se rescatan ciertos fragmentos de papel para, mediante su interpretación, reconstruir uno de aquellos documentos. Pretender que la información así obtenida, es decir, los mensajes de correo electrónico rescatados de un ordenador formateado y entregado voluntariamente por su usuario, constituyen una comunicación protegible por la doctrina constitucional expuesta, es exacerbar esa protección: la comunicación no era localizable como tal ex ante y no es que hubiera finalizado bastantes meses atrás, sino que fue deliberadamente destruida por el comunicante, por lo que estuvo muy lejos de cualquier interferencia en un proceso comunicativo ajeno. Los textos reconstruidos podrían ser muestra de una violación a la intimidad de los demandados, pero no una afrenta al secreto de las comunicaciones".

[129] Cfr. STC 70/2002, de 3 de abril.

[130] De Vicente Pachés, F., *El Derecho del Trabajador…,* cit., pág. 321; y Cardona Rubert, B., *Informática y contrato de trabajo…,* cit., págs. 79-83-84.

[131] Falguera i Baró, M.A., "Uso por el trabajador del correo electrónico…", cit., págs. 496-497; Rubio de Medina, Mª., *El despido por la utilización personal…,* cit., pág. 17; Marín Alonso, I., *El poder de control empresarial…,* cit., págs. 208 y ss; y Tascón López, R., "El poder de control empresarial en la era tecnológica: visión panorámica de una cuestión inacabada", *C.E.F., R.T.S.S.*, nº 267, 2005, págs. 44-48.

por parte del empresario porque se considera que el teléfono o el ordenador desde los que se emiten son propiedad de la empresa[132]. Sin embargo, no existen reglas ecuménicas determinadas, debiéndose hacer una valoración ad hoc en función de las circunstancias concurrentes en cada caso[133].

Así, cabe distinguir los siguientes supuestos de hecho[134]: **a**) Cuando la empresa restringe el uso del teléfono y del correo electrónico a fines estrictamente profesionales o comerciales y prohíbe el uso con fines personales. **b**) Cuando la empresa facilita al trabajador dos teléfonos o cuentas de correo electrónico distintos (uno para uso profesional y otro para uso personal). **c**) Cuando la empresa facilita al trabajador un único teléfono y/o cuenta de correo electrónico de los que hace un uso indistinto, tanto para fines profesionales como particulares.

a) Cuando la empresa restringe el uso del teléfono y del correo electrónico a fines estrictamente profesionales o comerciales y prohíbe el uso con fines personales, el acceso del empresario a las comunicaciones del trabajador puede colisionar con el derecho a la intimidad de éste, más no con el derecho al secreto de las comunicaciones[135]. Recuérdese que las comunicaciones realizadas por el trabajador con un fin únicamente laboral, se deben considerar también como propias de la empresa al ser realizadas por el comitente en el ejercicio de la actividad encargada. Por consiguiente, siempre y

[132] SSTSJ de Galicia de 21 de noviembre de 2003 (JUR/57945, 2004) y de la Comunidad Autónoma del País Vasco de 23 de enero de 2007 (AS/1723).

[133] Cfr. el Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, realizado por el grupo de trabajo sobre protección de datos constituido en la UE al amparo del art. 29 de la Directiva 95/46/CE (5401/01/ES/Final WP 55).

[134] Thibault Aranda, J., *El Teletrabajo*, cit., págs. 137 y ss; y Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., págs. 81 y ss.

[135] Cfr. SSTSJ de Cataluña, de 5 de julio de 2000 (AS/3452); de Andalucía, de 9 de mayo de 2003 (AS/2840); de Cantabria, de 26 de agosto de 2004 (AS/2513); y de Cataluña, de 4 de noviembre de 2004 (JUR/16535, 2005). Algunas resoluciones judiciales aplican la misma solución a supuestos en los que la empresa no ha previsto nada a propósito de las condiciones de uso de los instrumentos informáticos y telemáticos empresariales porque entienden que el trabajador no puede utilizar tales instrumentos para fines ajenos a los estrictamente laborales sin expresa autorización de la empresa. En este sentido se expresan, por ejemplo, las SSTSJ de Galicia, de 4 de octubre de 2001 (AS/3366); de Andalucía, de 9 de mayo de 2003 (AS/2840); y de Cataluña, de 6 de junio de 2003 (AS/2272).

cuando los trabajadores tengan conocimiento de las condiciones de uso de las herramientas de trabajo y de la posibilidad de que el empresario pueda fiscalizar sus comunicaciones, éste podrá acceder a las mismas sin necesidad de requerir el consentimiento del trabajador ni de recabar autorización judicial[136]. Además, tanto en el caso de que el trabajador es advertido previamente de las condiciones de uso de los sistemas de comunicación empresariales –exclusivamente profesionales- y de la posibilidad de acceder a los mismos por parte de la empresa y no da una respuesta negativa, como cuando se le avisa como condición de acceso al sistema que la comunicación debe ser estrictamente laboral y lo acepta, puede entenderse sin problemas que otorga el consentimiento a que la empresa ejerza algún control sobre sus comunicaciones[137].

De todas maneras, estando ante una limitación de un derecho fundamental como el de la intimidad, tal medida ha de estar justificada[138], esto es, han de existir razonables sospechas de la comisión por parte del trabajador de ilícitos contractuales, como filtraciones de información confidencial de la empresa a terceros o ataques a otras personas, que puedan redundar en perjuicio de la empresa, o la existencia de un correo electrónico dirigido a un trabajador por persona supuesta, etc[139]. El empresario no queda apoderado, ni siquiera en los casos de uso con fines estrictamente profesionales de los sistemas de comunicación empresariales, para llevar a cabo controles preventivos, esto es, para fiscalizar, con carácter universal e indiscriminado, el uso que los trabajadores hacen de los mismos[140]. Por otra parte, la renuncia voluntaria del trabajador al secreto de las comunicaciones, al igual que sucede con la renuncia de otros derechos fundamentales en la relación de trabajo, no

[136] Thibault Aranda, J., *El Teletrabajo*, cit., págs. 137 y 138, y "El Derecho Español", cit., págs. 71-72; Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 43; y Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 81.

[137] En este sentido, Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 8; y Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 81. Cfr. STSJ de Cataluña de 4 de noviembre de 2004 (JUR/16535, 2005).

[138] Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 43; y Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., pág. 81.

[139] SSTSJ de Galicia, de 29 de abril de 2001 (AS/3653); de Andalucía, de 9 de mayo de 2003 (AS/2840); y de Cantabria, de 26 de agosto de 2004 (AS/2513).

[140] En sentido contrario, Thibault Aranda, J., *El Teletrabajo*, cit., pág. 137.

debe entenderse incondicionada: será precisa la existencia de sospechas o indicios suficientes de la comisión de un ilícito laboral[141]. Estos controles serían contrarios a la consideración debida a la dignidad, que proscribe los controles que nieguen un cierto espacio de libertad en el puesto, o donde no sea posible la libre manifestación de la persona. Es más, en un puesto de trabajo de cierta responsabilidad, que precisa el uso del correo electrónico con mucha asiduidad, *"no puede considerarse ni proporcional, ni necesaria tal intromisión en la intimidad como es la lectura de su correo, para concluir que recibe, o envía un par de mensajes al día, como en otras circunstancias, se consideraría irrelevante recibir o hacer un par de llamadas telefónicas personales, en trabajadores con cargos de Dirección"*[142]. Por otra parte, si la empresa ejerce esta supervisión en el marco de un previo conflicto laboral y de forma coetánea a la interposición de una papeleta de conciliación por extinción contractual, se evidencia *"un claro objetivo de buscar un motivo para despedir a la actora y no la defensa del patrimonio o de los intereses de la empresa"*; fines que tienen que ser caracterizados como ilegítimos[143].

Además, la restricción impuesta al derecho a la intimidad ha de ser proporcional al fin que persigue[144]. Así, la medida ha de ser idónea para la finalidad pretendida por la empresa (verificar si el trabajador ha cometido efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria en el sentido de que no exista otra más moderada, menos intrusiva, para probar tales irregularidades[145]; y equilibrada, limitándose a lo que resulte imprescindible, no tomando más conocimiento de lo necesario, y a una duración temporal limitada, la suficiente para comprobar que no se trata de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada. Así, si se trata de verificar el

[141] Martínez Fons, D., "El control de la correspondencia electrónica…", cit., pág. 43.
[142] Cfr. STSJ de Galicia de 29 de abril de 2001 (AS/3653).
[143] STSJ de Cataluña de 16 de septiembre de 2002 (AS/2637). En el mismo sentido, la STSJ de Madrid de 31 de enero de 2002 (AS/916).
[144] STSJ de Andalucía de 9 de mayo de 2003 (AS/2840).
[145] Así, por ejemplo, si la empresa sospecha una actividad privada del trabajador, como la de registro de dominios, la lectura de su correo electrónico debe *"reputarse de innecesaria, en tanto que los Registros son públicos y dicha información puede recabarse, directamente o a través del Juzgado, de la autoridad encargada del Registro"* [STSJ de Galicia de 29 de abril de 2001 (AS/3653)].

uso personal de los medios de comunicación empresariales, el control será legítimo si se destina a discriminar entre las comunicaciones de carácter personal y las de naturaleza profesional y sólo en la medida en que se cumpla con dicha finalidad. En tales casos, el control de los medios de comunicación no exige la intervención del contenido de las comunicaciones, bastando con el registro de otras circunstancias de las mismas, tales como los destinatarios, el tiempo y frecuencia de las llamadas telefónicas, el número de mensajes electrónicos enviados o recibidos y su extensión, etc[146]. Si ello resulta insuficiente para verificar la naturaleza "no profesional" de las comunicaciones o se trata de verificar otros ilícitos contractuales, de suerte que es necesario algún tipo de intervención sobre el contenido de las llamadas telefónicas o mensajes electrónicos, tal intervención ha de acotarse material y temporalmente a lo estrictamente necesario para asegurar que la comunicación no responde al cumplimiento de las obligaciones laborales del trabajador o verificar la comisión del ilícito laboral de que se trate. De otro lado, como quiera que en estas comunicaciones con los clientes de la empresa pueden surgir comentarios que afecten a su intimidad, se deben adoptar las cautelas formales contempladas en el art. 18 del ET[147].

b) En los supuestos en que la empresa facilita al trabajador dos teléfonos o cuentas de correo electrónico diferentes (uno para uso profesional y otro para uso personal), hay que distinguir entre las comunicaciones realizadas a través de uno y otro sistema de comunicación. Las llamadas telefónicas o mensajes electrónicos realizados por el trabajador a través del teléfono o del correo electrónico de uso profesional serán auditables por la empresa en los mismos términos señalados en el supuesto anterior[148], máxime cuando el trabajador cuenta con sistemas de comunicación alternativos para sus asuntos privados[149]. En cambio, las comunicaciones operadas mediante el teléfono o el correo electrónico de uso personal gozan del derecho a la protección del

[146] Thibault Aranda, J., "El Derecho español", cit., pág. 71.
[147] En este sentido, la STSJ de Cantabria de 26 de agosto de 2004 (AS/2513). En sentido contrario, la STSJ de Cataluña de 5 de julio de 2000 (AS/3452).
[148] STSJ de Cataluña de 10 de septiembre de 2001 (AS/2776). En el mismo sentido, FALGUERA BARÓ, M.A., "Trabajadores…", cit., pág. 206.
[149] Cfr. STSJ de Cataluña de 10 de septiembre de 2001 (AS/2776).

secreto de comunicaciones y son, por consiguiente, inviolables[150]. El control, cualquiera que sea la modalidad de su ejercicio (interceptación del contenido de las comunicaciones o registro de los datos externos de las mismas), debe considerarse vedado sin más matizaciones. Así que cualquier interceptación o aprehensión de la comunicación constituirá una violación del derecho al secreto de las comunicaciones, y ello con independencia de que lo comunicado afecte o no a la vida íntima del trabajador porque el art. 18.3 de la CE protege, como se ha visto, el mensaje, sea cuál sea su contenido. La fiscalización de dichas comunicaciones únicamente será admisible si concurren la autorización judicial pertinente[151] o el consentimiento de los comunicantes. Ni que decir tiene que la empresa no puede contratar investigadores para averiguar las direcciones de correo electrónico de sus trabajadores cuando éstas son de carácter personal y privado y no han sido proporcionadas por ella, y acceder al contenido de los correos electrónicos allí archivados, pues ello supone una clara vulneración del derecho fundamental consagrado en el art. 18.3 de la CE[152].

c) En los supuestos en los que la empresa facilita al trabajador un único teléfono y/o cuenta de correo electrónico de los que se hace un uso indistinto, tanto para fines profesionales como particulares, se pueden utilizar determinadas técnicas para discriminar las comunicaciones de carácter profesional de las de naturaleza personal. Así, por ejemplo, la empresa puede adoptar un teléfono que exija al trabajador indicar previamente el carácter de la llamada, o disponer de determinados dispositivos de software que, dependiendo de la naturaleza del mensaje electrónico (analizando el remitente, el tema o porque el trabajador identifique previamente la naturaleza de la comunicación), lo almacenan en una u otra localización del equipo informático.

---

[150] Thibault Aranda, J., "El Derecho español", cit., pág. 69; Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., págs. 81 y ss; y Falguera i Baró, M.A., "Criterios doctrinales en relación con el uso por el trabajador de los medios informáticos empresariales para fines extraproductivos", en AA.VV., *Derecho social y nuevas tecnologías*, Madrid, 2005, pág. 314. Una posición diferente en Martínez Fons, D., "El control de la correspondencia electrónica…", cit., págs. 43 y ss. Cfr. el Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, realizado por el grupo de trabajo sobre protección de datos constituido en la UE al amparo del art. 29 de la Directiva 95/46/CE (5401/01/ES/Final WP 55).

[151] Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., págs. 82-83.

[152] STSJ de Cataluña de 9 de julio de 2002 (AS/2811).

De esta forma, si las llamadas telefónicas se identifican como profesionales o los mensajes electrónicos se ubican en la "carpeta de mensajes profesionales" el empresario podrá proceder a los controles en los mismos términos señalados en el primer supuesto analizado[153]. En cambio, si las llamadas telefónicas se identifican como personales o los mensajes electrónicos se ubican en la "carpeta de mensajes personales", las comunicaciones del trabajador serán inviolables y, por tanto, la empresa no las podrá fiscalizar[154].

En el resto de supuestos de uso indiscriminado del teléfono o del correo electrónico cabría distinguir entre "comunicaciones profesionales" y "comunicaciones personales", esto es, entre aquéllas que aparezcan relacionadas con el objeto de la prestación laboral y aquéllas otras cuyo contenido esté desconectado del cumplimiento de esta prestación. Mientras que las primeras serían fiscalizables por la empresa, las segundas, en cambio, serían inviolables[155]. Ahora bien, esta opción plantea el problema de cómo discriminar entre unas y otras comunicaciones. En principio, bastaría con identificar el destinatario de las llamadas telefónicas, acceder a la "bandeja de salida" del correo electrónico donde se muestra el destinatario del mensaje, el asunto y la fecha y hora en que se escribió, o rastrear determinadas palabras claves bloqueando los mensajes en que se contengan. Sin embargo, hay que tener en cuenta que los trabajadores pueden entablar comunicaciones con sus compañeros de trabajo o con clientes de la empresa totalmente desconectadas del cumplimiento de la prestación laboral y, en cambio, mantener comunicaciones con sus familiares o amigos que sí están relacionadas con el objeto de dicha prestación. Además, cabe la posibilidad de comunicaciones mixtas. Por ello, la identificación de los destinatarios de las comunicaciones o del asunto de los mensajes electrónicos no permite discernir con total seguridad las comunicaciones profesionales de las personales. Por ello, y

[153] Thibault Aranda, J., *El Teletrabajo*, cit., pág. 139.
[154] Thibault Aranda, J., *El Teletrabajo*, cit., pág. 139. Una posición diferente en Martínez Fons, D., "El control de la correspondencia electrónica…", cit., págs. 43 y ss.
[155] SSTSJ de Cataluña, de 16 de septiembre de 2002 (AS/2637); de Madrid, de 18 de septiembre de 2002 (AS/2828); y de Cataluña, de 11 de junio de 2003 (AS/2516), 12 de diciembre de 2003 (AS/295, 2004) y 22 de julio de 2004 (AS/2696); Ferández Villazón, L.A., *Las Facultades Empresariales...*, cit., pág. 144; y Falguera i Baró, M.A., "Criterios doctrinales en relación con el uso…", cit., págs. 314 y ss.

teniendo en cuenta la posición preeminente del derecho fundamental al secreto de las comunicaciones, no cabe sino considerar al empresario un tercero ajeno a la comunicación. Todas las comunicaciones realizadas por el trabajador gozan del derecho a la protección del secreto de las comunicaciones y, por consiguiente, son inviolables[156], salvo que el trabajador consienta expresamente su supervisión[157]. En este caso, la advertencia realizada previamente por la empresa respecto de que el correo electrónico puede ser controlado y el consentimiento presunto otorgado por el trabajador no son suficientes porque se refieren también al uso del correo con fines personales, e incluirían, además, un acceso incondicionado en un ámbito donde no es admisible intervención alguna sin el recurso a la autorización expresa del interesado o de la autoridad judicial[158].

El empresario, no obstante, podrá controlar, en virtud del art. 20.3 del ET, los aspectos accesorios de la comunicación. Recuérdese que, según la doctrina del Tribunal Constitucional, el registro de los elementos circunstanciales de la comunicación constituye una injerencia de menor intensidad en el derecho al secreto de comunicaciones que la interceptación de la comunicación, *"siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad"*[159]. Por ello, teniendo en cuenta el alto grado de publicidad de los citados elementos y habida cuenta el legítimo interés del empresario, es absolutamente razonable que a éste le esté dado controlar tales extremos. En este sentido, la STSJ de Castilla y León de 10 de abril de 2003 (AS/2159) afirma que *"la utilización de unas facturas telefónicas por su titular no afectan al secreto de las comunicaciones del usuario y parece además que es el medio más idóneo, que en forma alguna supone invadir la intimidad del recurrente, para acreditar que el teléfono no se utilizaba para*

[156] Cfr. STS de 10 de marzo de 1990 (RJ/2045); y SSTSJ de Galicia, de 29 de abril de 2001 (AS/3653); de Andalucía, de 9 de mayo de 2003 (AS/2840); del País Vasco, de 21 de diciembre de 2004 (AS/3927); y de Galicia de 20 de octubre de 2006 (JUR/207642). En sentido contrario, Thibault Aranda, J., *El Teletrabajo,* cit., págs. 139-140. Una posición diferente en Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., págs. 83 y ss.
[157] SSTSJ de Madrid, de 13 de mayo de 2003 (AS/3649); y del País Vasco, de 21 de diciembre de 2004 (AS/3927).
[158] Goñi Sein, J.L., "Vulneración de derechos fundamentales…", cit., págs. 84-85.
[159] SSTC 123/2002, de 20 de mayo; y 56/2003, de 24 de marzo.

estar localizado el usuario, que era el fin para el que se le dio su uso, sino para un uso estrictamente personal"[160]. Por otra parte, si el trabajador acepta, en un anexo a su contrato de trabajo, la supervisión periódica de los listados de los correos enviados y recibidos con indicación de la dirección, fecha, hora y tiempo de conexión, es evidente que el control empresarial no viola los derechos fundamentales a la intimidad personal y al secreto de las comunicaciones[161].

Por último, debe tenerse en cuenta que los datos así recogidos tienen carácter nominal en el sentido del art. 3 de la LOPD, por lo que su tratamiento quedará sometido a las disposiciones de la citada Ley sobre declaración de la Agencia de Protección de Datos, naturaleza y periodicidad de los controles practicados, acceso, etc.

En otro orden de consideraciones, debe traerse a colación el supuesto enjuiciado por la SAN de 17 de julio de 1997 (AS/3370). La empresa había comunicado a los "comerciales" que, sí querían utilizar el teléfono móvil de la compañía para asuntos particulares, debían domiciliar la factura en su cuenta particular, y que una vez abonado su importe y deducido el correspondiente a llamadas particulares, sería abonada por la compañía. Pues bien, la Sala de lo Social de la Audiencia Nacional no estima que *"con las órdenes e instrucciones impartidas por la empresa se vayan a comprometer los derechos a la intimidad personal y familiar y al secreto de las comunicaciones telefónicas, pues, de una parte, queda a su voluntad utilizar para sus comunicaciones personales el teléfono móvil que les proporciona la empresa o bien acudir a otros ajenos al tal servicio, y de otra, pueden hacer desaparecer de los recibos los cargos correspondientes a esas llamadas privadas para evitar su identificación, así es que no deben trascender a terceros datos que puedan atentar a los derechos constitucionales antes mencionados, cuando, a mayor abundamiento, la empresa no impone a los trabajadores la obligación de domiciliar el pago de los recibos en la cuenta particular de cada empleado, siendo potestativo para ellos*

[160] En el mismo sentido, la STSJ del País Vasco de 21 de diciembre de 2004 (AS/2927).
[161] STSJ de Cataluña de 11 de marzo de 2004 (AS/1231).

abonarlos de esta manera o cargarlos a la cuenta de la compañía y satisfacer el importe de las llamadas personales, y buena prueba de que el sistema no perjudica los intereses de los trabajadores es que todos ellos han aceptado el propuesto por la empresa"; es más, a juicio de la Audiencia Nacional*, "si bien se mira, en realidad quedaría menos protegido el secreto de las comunicaciones si los recibos del teléfono pasaran directamente a la cuenta de la compañía para su abono"*.