

Poder de control, sistemas tecnológicos y derechos de los empleados públicos

Susana Rodríguez Escanciano
Catedrática de Derecho del Trabajo
y de la Seguridad Social
Universidad de León

Índice: **1.- LAS POTENCIALIDADES TECNOLÓGICAS DE CONTROL EN EL MARCO DE LAS ADMINISTRACIONES PÚBLICAS. 2.- LÍMITES: SUS VIDRIOSAS ARISTAS. 2.1.-** Los quehaceres extralaborales: excepciones. 2.1.1.- Menoscabo de los intereses de la Administración. 2.1.2.- Riesgos para la integridad física de terceros. 2.1.3.- Control de situaciones de incapacidad temporal. 2.1.4.- “Locus laboris”. Sus difusas fronteras. 2.2.- La vigilancia en tiempo y lugar de trabajo. Los peligros de una visibilidad permanente ante la Administración electrónica y las obligaciones de transparencia. **3.- DERECHOS FUNDAMENTALES VS LIBERTAD DE EMPRESA. 4.- ACTIVISMO JUDICIAL. 4.1.-** Vídeo vigilancia. Data vigilancia. 4.2.- Terminales informáticos. 4.2.1.- Mensajería electrónica. 4.2.2.- Navegación por internet. 4.2.3.- Aproximación a la casuística apreciación de los Tribunales. A) Tribunal Europeo de Derechos Humanos. B) Tribunal Constitucional. C) Tribunal Supremo. D) Algunas sentencias de los Tribunales Superiores de Justicia. **5.- REDES SOCIALES 5.- ALGUNOS PRESUPUESTOS DE VALIDEZ EN EL CONTROL EMPRESARIAL. 6.- VIGILANCIA AUDITIVA. 7.- INSTRUMENTOS DE CONTROL DE ACCESO: TARJETAS, INFRARROJOS, RADIOFRECUENCIA Y CONTROLES BIOMÉTRICOS. 8.- GEOLOCACIÓN. 9.- ALGUNOS PRESUPUESTOS DE VALIDEZ EN EL CONTROL. 10.- EL PREOCUPANTE FENÓMENO DEL TECNO-ESTRÉS. 10.1.-** Los denominados entornos administrativos “cibercientíficos” como caldo de cultivo óptimo para el surgimiento de dolencias psicosociales. 10.2.- El teletrabajo y la sensación de claustrofobia.

1. LAS POTENCIALIDADES TECNOLÓGICAS DE CONTROL EN EL MARCO DE LAS ADMINISTRACIONES PÚBLICAS

Cierto es que las nuevas tecnologías de la información y comunicación se han establecido y consolidado rápida, firme y definitivamente en el actual contexto laboral, privado y público, incardinándose como un elemento más en las formas y modos de prestar servicios y –cómo no-- en las relaciones entre empleados y empresarios, máxime si pertenecen al sector público, pues en los tiempos actuales es casi inimaginable una Administración no conectada a la red o que no disponga de equipos informáticos ante las exigencias de la denominada “administración electrónica”, escenario en el que la tramitación *on line* debe constituir la actuación habitual de las Administraciones en sus múltiples vertientes de gestión interna, de relación con los ciudadanos y de relación de aquellas entre sí. No menos verdad resulta que, además de contribuir de forma decisiva al incremento de la eficacia y de la eficiencia, permitiendo optimizar recursos y mejorar la dispensa de servicios a favor de los usuarios, presentan un doble lado oscuro¹:

¹ PEREZ DE LOS COBOS ORIHUEL, F.: *Nuevas tecnologías y relación de trabajo*, Valencia (Tirant Lo Blanch), 1991, pág. 72.

Por una parte, un manejo por los empleados para fines privados durante la jornada de trabajo, que plantea, desde la perspectiva de gestión, numerosos inconvenientes o perjuicios, derivados del daño económico, *lucrum cesans*, es decir, del tiempo no dedicado al desarrollo efectivo del trabajo sino a menesteres diversos que redundan en la disminución del rendimiento. De otro, la intensificación en las posibilidades de vigilancia y control de los empleados en su puesto de trabajo y fuera del mismo y su utilización como medio de prueba para acreditar los comportamientos irregulares justificativos de una separación del servicio, de un despido o de otro tipo de sanciones, circunstancia que en algunas ocasiones puede suponer, al tiempo, un atentado a los derechos fundamentales, aludidos en el art. 14 h) EBEP (intimidad, dignidad, propia imagen, secreto de las comunicaciones, protección de datos personales...)².

Este cúmulo de situaciones acaece además en un marco normativo en el que no existe una respuesta capaz de proporcionar un punto de equilibrio entre los intereses contrapuestos, lo cual ha abocado a los órganos judiciales a realizar una labor creadora, *quasi* legislativa, con múltiples contradicciones y una consecuente falta de seguridad jurídica³. Partiendo de la obligación de los empleados públicos de “desempeñar con diligencia las tareas que tengan asignadas” (art. 53.1 EBEP), el art. 20.2 EBEP, en sus escuetos términos, dispone que “los sistemas evaluación del desempeño... se aplicarán sin menoscabo de los derechos de los empleados públicos”. Por su parte, para el personal laboral, el art. 20.3 ET establece que el empresario “podrá 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 aplicación la consideración debida a su dignidad”.

A la luz de estos preceptos, se abre un amplio margen de libertad a la Administración a la hora de elegir entre medios de supervisión muy variados, máxime si se tiene en cuenta que cuanto más sofisticados parezcan más efectivos serán para conseguir el resultado propuesto, siendo muy difícil dar respuesta, *a priori*, al interrogante sobre la licitud o ilegalidad de las pruebas aportadas a efectos disciplinarios o sancionadores, siendo necesarios estar muy atentos a las circunstancias de hecho de cada supuesto concreto.

La insuficiencia normativa obrante en nuestro ordenamiento se revela, además, crónica, porque el tenor legal, para los funcionarios ya estaba incluido en la versión primigenia del EBEP y para el personal laboral no ha superado su vieja formulación inicial, que data de 1980, pese a los adelantos tecnológicos que han incrementado exponencialmente las posibilidades de control y pese a las innumerables modificaciones estatutarias que han tenido lugar durante todo este tiempo, déficit que se habrá de cubrir, no obstante, antes del 25 de mayo de 2018, fecha tope para regular la traslación del derecho de la protección de datos personales al ámbito laboral al calor del Reglamento UE 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016, que ha venido a derogar a la Directiva 95/46, y que específicamente señala que la normativa laboral deberá prever “medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses

² MARTIN VALVERDE, A.: “Contrato de trabajo y derechos fundamentales”, *Revista de Derecho Social*, núm. 6, 1999, pág. 16.

³ DESDENTADO BONETE, A. y MUÑOZ RUÍZ, A.B.: “Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 39, 2014.

legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo”⁴. En la actualidad, se está tramitando un Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, destacando, en una primera aproximación a la espera del texto final, la obligación para las Administraciones Públicas de contar con un Delegado de Protección de Datos.

2.- LÍMITES: SUS VIDRIOSAS ARISTAS

Teniendo en cuenta que tanto los trabajadores laborales del sector público como funcionarios tienen muchas características en común con los trabajadores del sector, no en vano en todos concurren las notas de dependencia y ajenidad y, la normativa europea, a través de sucesivas Directivas, ha ampliado el concepto de trabajador, incluyendo tanto a los empleados del sector público como del ámbito privado, las interpretaciones vertidas por los tribunales, normalmente del orden social, en cuanto a las posibilidades de control tienen plena virtualidad y pueden ser trasladadas sin ninguna dificultad a las Administraciones públicas y al sector público empresarial y fundacional. Es más, siendo coincidente el punto de origen también lo va a ser el de destino, pues si se entiende adecuado el control, irá acompañado de consecuencias sancionadoras, únicamente diferenciadas por el régimen disciplinario aplicable, que para los empleados públicos (funcionarios y laborales) se encuentra regulado en los arts. 93 y ss. EBEP, con las únicas salvedades siguientes: para los laborales se recoge una regla de supletoriedad inversa [, pues su régimen disciplinario “se regirá, en lo no previsto en el presente título, por la legislación laboral” (art. 93.4)], teniendo en cuenta, además, que el EBEP contiene reglas muy relevantes, incluyendo la necesaria readmisión en despidos disciplinarios improcedentes de trabajadores fijos (art. 96.2), unos larguísimos plazos prescriptivos (art. 97) y la posibilidad de que por convenio colectivo se tipifiquen faltas disciplinarias (art. 95)⁵.

Bajo tal premisa y tomando como referente los pronunciamientos del orden social, dos fronteras claras se imponen, en una primera aproximación, a la actuación de supervisión implementadas por los gestores de recursos humanos en las Administraciones Públicas, la primera relacionada con el necesario respeto a los derechos fundamentales y la segunda relativa a la obligatoriedad de circunscribir dicha actividad de control —salvo excepciones justificadas— a la comprobación de aquellas cuestiones estrictamente vinculadas con la prestación de servicios⁶.

2.1.- Los quehaceres extralaborales: excepciones

Empezando por el segundo de los condicionantes mencionados, es menester recordar que, como regla general, la facultad de control que el ordenamiento atribuye al empresario (*in casu*, Administración) se reduce a “verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales”, lo que excluye, lógicamente, su vida privada.

⁴ GOÑI SEIN, J.L.: “Intimidad del trabajador y poder de vigilancia y control empresarial”, en AA.VV (GARCÍA MURCIA, J., Coord.): *Jornada sobre derechos fundamentales y contrato de trabajo*, Oviedo (Principado de Asturias), 2017, pág. 36.

⁵ Por extenso, CÁMARA DEL PORTILLO, D.: *Régimen disciplinario de los empleados públicos*, Madrid (Marcial Pons), 2008.

⁶ SANTIAGO REDONDO, K.M.: “Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE”, *Relaciones Laborales*, núm. 1, 2014.

Como regla general, el poder de dirección, y en su caso las facultades disciplinarias, no pueden alcanzar a las actividades extralaborales, que precisamente por desarrollarse al margen de los aspectos técnico-organizativos del trabajo, y por estar amparadas en derechos constitucionales de rango fundamental (vida íntima o privada), quedan fuera del radio de acción de los poderes empresariales⁷. Ello no obstante, no cabe ocultar que el deseo de organizar de la manera más eficiente posible la actividad administrativa, teniendo, además, en cuenta la escasez de recursos disponibles dadas las restricciones de las Leyes Presupuestarias a la incorporación de nuevos efectivos, puede suscitar en la Administración un interés – comprensible desde el punto de vista de la competitividad—en conocer determinados aspectos pertenecientes a la esfera personal de sus empleados, pero que a su juicio pueden repercutir en la dedicación o implicación, y en definitiva en el rendimiento, y que por ello pueden condicionar el acceso o la conservación del empleo.

2.1.1.- Menoscabo explícito de los intereses propios de la Administración

Cierto es que, en primer lugar, existen ocasiones en las que la vida privada del trabajador tiene trascendencia laboral, esto es, una conducta privada puede causar efectos negativos para la Administración, por lo que pueden estar justificadas excepcionalmente injerencias empresariales. Estos efectos negativos para una empresa privada se concretan, fundamentalmente, en pérdida de imagen o de prestigio, lo que puede repercutir lógicamente en sus beneficios económicos⁸, argumentación que, mutatis mutandis, se puede aplicar también a la Administración, sustituyendo el lucro empresarial por el interés público y la confianza en las instituciones. Desde luego, cualquier actuación empresarial punitiva exige que la conducta extralaboral se pruebe, pues no se puede actuar con base en meras sospechas. Y una vez acreditada tal conducta, el empresario sólo está legitimado para intervenir cuando el comportamiento del trabajador pueda repercutir nocivamente sobre el adecuado cumplimiento de la prestación de trabajo o sobre los intereses de la empresa. En consecuencia, tal quehacer extramuros del puesto de trabajo que perjudique a la empresa permitirá al empleador hacer uso del poder de dirección, normalmente en su vertiente disciplinaria, quedando impedido para interferir en la vida privada de los trabajadores sin esa afectación a los intereses empresariales⁹.

Así, por ejemplo, la embriaguez habitual, el alcoholismo o la drogadicción no deberán ser fiscalizadas empresarialmente, salvo que, naturalmente, repercutieran negativamente en el trabajo (disminución del rendimiento, ausencias o impuntualidades, riesgo de lesiones o de accidentes, pérdida de lealtad hacia la Administración, etc.)¹⁰. En todo caso, como excepciones que son, deberán ser interpretadas restrictivamente, sin perder nunca de vista que ni el estado civil del trabajador, ni la orientación o conducta sexual, ni los embarazos o abortos, ni mucho menos sus creencias o actuaciones políticas, religiosas o sindicales, pueden ser objeto de control empresarial con repercusión positiva o negativa en su relación laboral, por cuanto, además de atentar contra su intimidad, colisionarían con el principio de no discriminación.

⁷ GOÑI SEIN, J.L.: *El respeto a la esfera privada del trabajador*, Madrid (Civitas), 1988, pág. 261.

⁸ SALA FRANCO, T.: “El derecho a la intimidad y a la propia imagen y las nuevas tecnologías de control laboral”, en AA.VV (BORRAJO DACRUZ, E., Dir.): *Trabajo y libertades públicas*, Madrid (La Ley), 1999, pág. 227.

⁹ RODRÍGUEZ CARDO, I.A.: “Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador”, *Actualidad Laboral*, núm. 12, 2014, pág. 1400.

¹⁰ SALA FRANCO, T.: “El derecho a la intimidad y a la propia imagen y las nuevas tecnologías de control laboral”, en AA.VV (BORRAJO DACRUZ, E., Coord.): *Trabajo y libertades públicas*, Madrid (La Ley), 1999, pág. 228.

2.1.2.- Riesgos para la integridad física de terceros

Siempre en actividades laborales que implican un gran nivel de responsabilidad sobre la integridad física de otras personas, se ha considerado que no constituye una vulneración de la intimidad del trabajador el control empresarial destinado a comprobar que, durante su tiempo libre, el trabajador realiza un tipo de vida ordenado. Y es que en estos casos los juzgadores consideran que la falta de sueño y el consumo de alcohol, fármacos o sustancias tóxicas, aunque se produzca en el tiempo libre del trabajador y no genere retrasos o ausencias injustificadas, ni se deje traslucir en forma de embriaguez o toxicomanía en el lugar de trabajo, también tiene, por sí sólo, una gran trascendencia en la prestación laboral, pues es susceptible de repercutir negativamente en el cumplimiento con destreza por parte del trabajador de sus obligaciones, lo que, sin duda, habida cuenta del tipo de actividad laboral desarrollada, puede generar un riesgo para terceras personas (otros compañeros de trabajo, clientes, usuarios, pacientes o incluso meros transeúntes) que la Administración no tiene por qué asumir. A esta consideración se ha llegado en ciertas ocasiones en supuestos de pilotos de líneas aéreas, cirujanos o transportistas, pudiendo extenderse esta misma consideración, entre otros ejemplos, a aquellos tipos de actividades profesionales en las que el seguimiento de ciertas pautas de alimentación, entrenamiento o descanso se consideran fundamentales, no sólo para garantizar el óptimo rendimiento del trabajador, sino también como forma de asegurar que el empleado supere exitosamente los estrictos controles de salud que su profesión exige (como ocurre con los deportistas profesionales, personal sanitario, empleados que utilizan una licencia de armas...)¹¹.

2.1.3.- Control de la situación de incapacidad temporal

Se entiende que, al permanecer viva la relación laboral en la circunstancia de baja por enfermedad, el trabajador continúa en todo momento obligado a mantener escrupulosamente un tipo de conducta claramente respetuosa con la buena fe contractual, quedando habilitado el empresario para verificar la veracidad del estado de enfermedad o accidente, siempre con el debido respeto a los derechos fundamentales del trabajador, idea que con mayor facilidad se puede aplicar a los funcionarios empleados públicos que han de contar con la preceptiva licencia por enfermedad. En la empresa privada, es habitual la utilización de un informe de un detective, extremo que ha adquirido en la práctica forense la condición de prueba testifical cualificada (una vez ratificada), y, por ello, no es extraño que el juzgador conceda a este tipo de prueba una especial relevancia. No se trata, desde luego, de una posición establecida por ley, ya que formalmente es una prueba testifical más, sometida a las reglas de la sana crítica y rebatible mediante otras pruebas, pero se valora especialmente que “el testimonio emitido por los detectives privados tiene, en favor de su veracidad, no sólo la garantía de profesionalidad exigible y, en principio, presumible en una profesión, reglamentada legalmente, sino también la que, de modo innegable, proporciona la precisa y continuada dedicación al objeto del ulterior testimonio a emitir y las complementarias acreditaciones, gráficas o sonoras, de que este último suele ir acompañado”¹². Sería muy recomendable que del informe del detective se excluyesen datos sensibles, pues si el propósito consiste en confirmar una sospecha de incumplimiento cualquier otra información que el empresario pueda obtener de ese control y seguimiento resulta impertinente y no justificaría ninguna medida disciplinaria, sin que pudiera admitirse como prueba

¹¹ SELMA PENALVA, A.: “La información reflejada en las redes sociales y su valor como prueba en el proceso laboral. Análisis de los últimos criterios jurisprudenciales”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 39, 2014, pág. 364.

¹² SSTSJ Andalucía/Sevilla 4 abril 2008 (rec. 1509/2007).

en un juicio¹³. En todo caso, el seguimiento se ha de producir en espacios públicos, ya se trate de la vía pública, ya de establecimientos abiertos al público (locales, comercios, bares, etc.), en los que haya otras personas que también podrían haber visto u oído lo mismo, pero no se admite la vigilancia en el domicilio o espacios privados (art. 48.3 Ley 5/2014, de 4 de abril, de Seguridad Privada)¹⁴. En la Administración podrá intervenir la Inspección de Servicios.

También es frecuente el descubrimiento empresarial, a través del manejo de redes sociales por los trabajadores, de fraudes en los procesos de bajas por incapacidad temporal¹⁵, admitiéndose como prueba lícita si el propio afectado ha dado a conocer la noticia de forma voluntaria y en un medio accesible con carácter general¹⁶. Cabe citar la Sentencia de la Sala de lo Contencioso Administrativo del Tribunal Supremo de 21 de diciembre de 2009¹⁷, que entiende adecuada la sanción muy grave impuesta a un policía vasco que, estando de baja, desarrolla actividades privadas en la empresa constructora de su esposa

2.1.4.- “Locus laboris”. Sus difusas fronteras

Siendo claros los contornos en los supuestos anteriores, en los momentos actuales “cualquier utensilio conectivo, sean correos electrónicos, móviles, tabletas, teléfonos inteligentes, etc., transmuta los escenarios de desenvolvimiento de las ocupaciones laborales pues ubican a los trabajadores fuera de las unidades productivas típicas: empresas-Administraciones, centros y puestos. La unidad locativa por excelencia, o sea, el puesto de trabajo, se antoja movible, abierto, multifuncional y des-espacializado”¹⁸. Desde este punto de vista, debe de ir cobrando fuerza el conocido “derecho de desconexión” del trabajador en aras a no perjudicar el bienestar de su salud mental¹⁹, si bien concebido desde una perspectiva mucho más amplia que la diseñada por la Ley 2016-1088, de 8 de agosto, conocida como “Loi Travail” francesa, que se limita a introducir un punto 7 en el artículo L. 2242-8 del Código de Trabajo francés, en virtud del cual la negociación anual incluirá: “las modalidades del pleno ejercicio por el trabajador de su derecho a la desconexión y la puesta en marcha por la empresa de dispositivos de regulación de la utilización de los dispositivos digitales, con el fin de asegurar el respeto al tiempo de descanso y vacaciones, así como de su vida personal y familiar. A falta de acuerdo, el empleador, previa audiencia del comité de empresa o, en su defecto, de los delegados de personal, elaborará una política de actuación al respecto. Esta política definirá las modalidades de ejercicio del derecho a la desconexión y preverá, además, la puesta en marcha de acciones de formación y de

¹³RODRÍGUEZ CARDO, I.A.: “Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador”, cit., pág. 1409.

¹⁴ STEDH de 27 de mayo de 2014, asunto De La Flor Cabrera contra España. SSTS 19 julio 1989 (núm. 13116/1989) y 6 noviembre 1990 (núm. 17467/1990).

¹⁵ FERRANDO GARCÍA, F.: “Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 399, 2016, págs. 60 y ss.

¹⁶ SELMA PENALVA, A.: “La información reflejada en las redes sociales y su valor como prueba en el proceso laboral. Análisis de los últimos criterios jurisprudenciales”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 39, 2014, pág. 381.

¹⁷ Rec. 5471/2006.

¹⁸ ALEMÁN PÁEZ, F.: “El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi travail nº 2016-1088”, *Trabajo y Derecho*, núm. 30, 2017, págs. 12 y ss.

¹⁹ SAN 17 julio 1997 (Ar. 3370).

sensibilización sobre un uso razonable de los dispositivos digitales, dirigida a los trabajadores, mandos intermedios y dirección”²⁰.

En paralelo, la expansión de distintas plataformas de internet, conocidas como redes sociales, amplían el concepto lugar de trabajo como presupuesto de la comisión de infracciones en materia laboral, pues los nuevos dispositivos permiten conectarse desde cualquier ubicación y en cualquier momento²¹.

Resulta preocupante, sin embargo, el hecho de que los Tribunales olviden, en ocasiones, la ilicitud de aquellos sistemas de control de tiempos de trabajo excesivamente rigurosos y exhaustivos, es decir, aquéllos que permiten controlar minuto a minuto la actividad laboral y las más irrelevantes pausas y ausencias, sin dejar "el más mínimo espacio vital" dentro de la organización. Sistemas de control de esta naturaleza, salvo que se justificara su carácter indispensable para el necesario desarrollo del proceso productivo y no tuviera cabida otro método menos gravoso para los derechos del trabajador, deberían considerarse por los órganos judiciales atentatorios a la dignidad y libertad del operario²², máxime cuando no cabe una identificación absoluta entre "vida íntima" y "vida privada" (entendida ésta como "no laboral") a través de la cual negar la existencia --y consiguiente exigencia para el empresario-- del derecho a la intimidad del trabajador en el centro de trabajo, sobre todo cuando aquél no está realizando la prestación laboral (descansos, por ejemplo), pero con necesaria extensión a otros lugares (lavabos, vestuarios, aseos, comedores...), cuyo control y vigilancia (continua o esporádica) por medios audiovisuales suponen --de ordinario-- un ataque frontal al derecho a la intimidad²³; como también lo son, sin duda, las intromisiones audiovisuales mediante otros medios técnicos en comportamientos, actitudes o gestos del trabajador durante la jornada de trabajo verdaderamente irrelevantes a la hora de valorar la prestación laboral pero cuya posesión por el empresario puede ocasionarle consecuencias negativas (*licenza comportamentali*)²⁴.

Lo contrario, un examen tan exhaustivo y permanente que llegue a acabar con cualquier resquicio de intimidad y autonomía en el lugar de trabajo supondría situar el poder de vigilancia en una dimensión inhumana, capaz de poner en peligro no sólo la libertad y la dignidad del trabajador, sino también su propio equilibrio psíquico, y de elevar el poder empresarial al grado de "omnipotente, anónimo e invisible"²⁵.

²⁰ VALLECILLO GÁMEZ, M.R.: “El derecho a la desconexión: ¿novedad digital o esnobismo del viejo derecho al descanso?”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 408, 217, págs. 167 y ss.

²¹ TALENS VISCONTI, E.E.: “Aspectos jurídicos sobre los comentarios de los trabajadores proferidos a través de las redes sociales”, *Trabajo y Derecho*, núm. 23, 2016, págs. 66 y ss.

²² DE VICENTE PACHÉS, F.: "Las facultades empresariales de vigilancia y control en las relaciones de trabajo", *Tribuna Social*, núm. 57, 2004, pág. 31.

²³ STSJ Madrid 17 abril 2009 (AS 1656). Digna de especial mención es la STSJ Madrid 20 diciembre 2006 (AS 1069), que entiende cómo el módulo de espera o de descanso del personal de asistencia en tierra en un aeropuerto es un ámbito privado en el que no cabe instalar un sistema de vigilancia con grabación de imagen y sonido y con presencia de un detective camuflado, pese a que se acredita que en el módulo se produce el consumo de bebidas alcohólicas y drogas, se juega al fútbol utilizando cajas y deteriorando el mobiliario, se consumen productos de alimentación de aviones entregados por una azafata y un empleado del catering y se ensucia el local.

²⁴ Traducidas en la doctrina española como "licencias comportamentales", PÉREZ DE LOS COBOS ORIHUEL, F.: *Nuevas tecnologías y relación de trabajo*, Valencia (Tirant Lo Blanch), 1990, págs. 77-78.

²⁵ BELLAVISTA, A.: *Il controllo sui lavoratori*, Turín (Giappichelli), 1985, pág. 67.

2.2.- La vigilancia en tiempo y lugar de trabajo. Los peligros de una visibilidad permanente ante la Administración electrónica y las obligaciones de transparencia

El poder directivo encuentra en las nuevas tecnologías un instrumento clave para mejorar la efectividad de la organización y el rendimiento del empleado, quedando superados los métodos más tradicionales propios del sistema fordista aplicables también en las Administraciones Públicas, basados en la vigilancia personal, directa e inmediata de la ejecución del trabajo por otros más sofisticados, que permiten un control más penetrante e incisivo por continuo y exhaustivamente panorámico de la actividad laboral²⁶, aumentado, sin duda, por la puesta en marcha de la Administración digital y de los principios de transparencia en la gestión pública como consecuencia de las obligaciones legales incorporadas en nuestro ordenamiento jurídico.

La aplicación de la informática a la gestión de personal (el denominado "*management information system*" o "*scientific management*"²⁷) provoca una metamorfosis de la actividad laboral que, de altamente esquematizada y fungible, deviene sensiblemente personalizada y rígidamente controlable y controlada, poniendo en peligro algunos de los aspectos más vulnerables de la personalidad humana, la dignidad y la intimidad del individuo²⁸. Ya no es sólo que el control espacio-temporal esté cediendo paso, en los centros o unidades de trabajo computerizadas y en las Administraciones Públicas, a la coordinación telemática e informática a cargo de un ordenador (lo cual supone "la sustitución del control periférico, discontinuo y parcial realizado por la jerarquía humana por uno centralizado y objetivo --en cuanto incorporado a la máquina y a su memoria-- que se verifica en tiempo real")²⁹, sino algo que trasciende al mero ajuste, alcanzando el rango de propia evolución cualitativa, en tanto introduce nuevos sistemas de trabajo informatizados en los cuales "la actividad del trabajador y las informaciones sobre dicha actividad constituyen un todo"³⁰, no en vano muchos instrumentos tecnológicos incorporados a las prestaciones laborales son a la vez medio de trabajo e instrumento de inspección (contadores de teclas o de tiempos de conexión en paradigmáticos ejemplos).

El control (no biunívoco, al no consentir el recíproco) queda incorporado a la máquina (a la propia herramienta de trabajo), rompiendo "esa unidad aristotélica de tiempo, lugar y acción sobre la cual se había basado hasta ahora el clásico trabajo industrial"³¹ y obteniendo, con el cambio, un trabajador "transparente", estrechamente vigilado, conocido en gran parte de sus facetas gracias a la elaboración y utilización de su "perfil completo", capaz de llevar en su manifestación extrema a un --intolerable-- control total, no en vano las tecnologías de tercera generación permiten penetrar en la caja negra que constituye el razonamiento propio de cada individuo traicionado por las huellas que ha dejado en el propio sistema³². En definitiva, las nuevas tecnologías están

²⁶ GOÑI SEIN, J.L.: *El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial*, Madrid (Civitas), 1998, pág. 147.

²⁷ SIMITIS, S.: "Developments in the protection of worker's personal data", *Conditions of work Digest*, Vol. 10/2, 1991, pág. 7.

²⁸ CARDONA RUBERT, M.B.: "Tutela de la intimidad informática en el trabajo", *Revista de Derecho Social*, núm. 6, 1999, pág. 24.

²⁹ PEREZ DE LOS COBOS ORIHUEL, F.: *Nuevas tecnologías y relación de trabajo*, Valencia (Tirant Lo Blanch), 1991, pág. 72.

³⁰ GAETA, L.: "La dignidad del trabajador y las 'perturbaciones' de la innovación", en AA.VV (APARICIO TOVAR, J. y BAYLOS GRAU, A., Dirs.): *Autoridad y democracia en la empresa*, Madrid (Trotta), 1992, pág. 68.

³¹ VENEZIANI, B.: "Nuove tecnologie e contratto di lavoro: profili di Diritto comparato", *Giornale di Diritto del Lavoro e di Relazioni Industriali*, núm. 3, 1987, pág. 54.

³² THIBAUT ARANDA, J.: "La vigilancia del uso de internet en la empresa y la protección de datos personales", *Relaciones Laborales*, 2009, Tomo I, pág. 216.

reforzando el "ojo electrónico", haciéndolo "penetrante, dominante y ubicuo"³³, Conllevan, en definitiva, como efecto más destacado, a un auténtico "control capilar" de los trabajadores en el puesto de trabajo e, incluso fuera del mismo. Como con acierto se ha dicho, es posible "saber qué hará un empleado (comportamiento), qué conseguirá (rendimiento) y cómo estará (satisfacción)"³⁴, posibilidades que van acompañadas de riesgos frente a los derechos fundamentales (inespecíficos) de los trabajadores).

3.- DERECHOS FUNDAMENTALES VS EFICACIA EN LA GESTIÓN PÚBLICA

Como es sabido, el art. 103 CE establece los principios que deben regir la actuación de las Administraciones Públicas, entre los que destacan el de eficacia y el de legalidad, al imponer el sometimiento pleno de la actividad administrativa a la Ley y al Derecho, con manifestación clara en los principios de dirección por objetivos y control de la gestión y evaluación de los resultados (art. 3 Ley 40/2015, de 1 de octubre, Régimen Jurídico del Sector Público). Como idea de partida, los derechos empresariales de vigilancia y control no pueden anular sin más los propios derechos constitucionales de los trabajadores, pues como ha señalado el Tribunal Constitucional, en doctrina ya consolidada, "la celebración de un contrato de trabajo no implica la privación en modo alguno para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano" porque "ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad, ni la libertad de empresa legítima que quienes prestan servicios en aquéllas por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico-constitucional"³⁵. Así pues, no cabe duda que el trabajador (también, lógicamente, el empleado público, en el marco de las relaciones laborales, ostenta la titularidad, en cuanto persona, de los derechos fundamentales de alcance general³⁶.

La incardinación en lo que el art. 1.1 ET describe como "el ámbito de organización y dirección de otra persona" adquiere su verdadero relieve si se tiene en cuenta que el contrato de trabajo es un vínculo de tracto sucesivo y de ejecución continuada, que suele absorber buena parte del tiempo y de las energías del trabajador, de modo que la implicación personal de éste en el cumplimiento de la relación contractual profesional no suele ser precisamente un episodio pasajero en el desenvolvimiento de su vida cotidiana³⁷, de suerte que los poderes del empresario, con fundamento constitucional en el principio de libertad de empresa consagrado por el art. 38 CE, quedan sometidos, en un modelo pluralista y democrático de relaciones laborales, a límites y contrapesos que aquél no puede desconocer en el uso de sus facultades directivas, dentro de los cuales la primacía indiscutible corresponde a los derechos fundamentales³⁸, idea que lógicamente

³³ MERCADER UGUINA, J.R.: "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?", *Relaciones Laborales*, núm. 10, 2001, pág. 14.

³⁴ Citando a TABURET, GOÑI SEIN, J.L.: "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016", *Revista de Derecho Social*, núm. 78, 2017, pág. 18.

³⁵ SSTCo 88/1985, de 19 de julio; 99/1984, de 11 de abril; 90/1977, de 6 de mayo y 904/1997, de 25 de noviembre.

³⁶ STCo 88/1985, de 19 de junio.

³⁷ MARTIN VALVERDE, A.: "Contrato de trabajo y derechos fundamentales", *Revista de Derecho Social*, núm. 6, 1999, pág. 16.

³⁸ Entre otros, BAYLOS GRAU, A.: "En torno al Estatuto de los Trabajadores: la prohibición de inquirir sobre la ideología, creencia y vida privada del trabajador", en AA.VV.: *Lecciones de Derecho del Trabajo en homenaje a los profesores Bayón Chacón y Del Peso y Calvo*, Madrid (Universidad Complutense), 1980, págs. 309 y ss.

puede trasladarse a los supuestos en los que el empleador es un Ente público.

Parece evidente, por ende, que los derechos constitucionales de cualquier persona acompañan al trabajador durante toda la vida de la relación laboral, como un límite ínsito a las prerrogativas empresariales. Pero no puede sorprender, tampoco, que la doctrina constitucional elaborada en torno a la incidencia de la Norma Fundamental y de los derechos en ella reconocidos sobre el contrato de trabajo pase por reconocer que la relación laboral puede comportar matizaciones o restricciones de los derechos fundamentales del trabajador como ciudadano, derivadas de la peculiar naturaleza del negocio jurídico y del ámbito empresarial en el cual han sido y son ejercidos tales derechos, si bien nunca caben limitaciones o privaciones injustificadas³⁹.

Así pues, aun cuando los derechos constitucionales condicionan la dinámica y contenido del contrato de trabajo, vetando decisiones empresariales capaces de vulnerar su efectividad, lo cierto es que, al propio tiempo, los derechos fundamentales del trabajador también aparecen afectados por la existencia del vínculo laboral y, sobre todo, por el principio constitucionalmente reconocido de libertad de empresa⁴⁰; en este caso por el nexo con la Administración y la necesaria satisfacción de los intereses generales. Caben, pues, modulaciones a los derechos personales del trabajador como consecuencia del nexo contractual/administrativo, pero ello sólo es posible, de acuerdo con la doctrina sentada por el propio Tribunal Constitucional, en situaciones extremas, esto es, únicamente cuando la limitación aparezca como inevitable y absolutamente necesaria y adecuada desde el punto de vista del ordenado desenvolvimiento de la actividad empresarial⁴¹.

4.- ACTIVISMO JUDICIAL

En esta tesitura de alcanzar una situación de equilibrio entre el poder directivo u organizativo y los derechos fundamentales del empleado, sopesando prudencialmente los intereses en juego y evitando ilógicos e irracionales ataques frontales e insidiosos a aquéllos⁴², pueden encontrarse manifestaciones muy variadas de un conjunto proteico de casos prácticamente ilimitado, a traducir en la práctica en estrategias empresariales diversas realizadas, a modo de ejemplo, sobre los accesos o desplazamientos del trabajador en el lugar de trabajo a través de puertas gobernadas electrónicamente y con un lector conectado a un ordenador (*badges* con códigos de identificación personal), sobre las llamadas telefónicas efectuadas gracias a la imbricación del teléfono utilizado por el trabajador con una centralita "computerizada" y sobre el uso del correo electrónico, sobre la navegación por páginas web o el alojamiento en *dropbox*⁴³ o, cómo no, la interacción en redes sociales, no siendo infrecuentes tampoco la instalación de programas espías, los controles biométricos o por infrarrojos, los test sobre el patrón de consumo de alcohol y drogas, los identificadores por radiofrecuencia como instrumentos

³⁹ SSTCo 99/1994, de 11 de abril y 204/1997, de 25 de noviembre.

⁴⁰ Recuérdese cómo en el sistema constitucional español no existen derechos absolutos o ilimitados; todo derecho constitucional tiene sus límites, "que derivan... no sólo de su posible conexión con otros derechos constitucionales, sino también con otros bienes constitucionalmente protegidos", STCo 11/1981, de 8 de abril.

⁴¹ Por todas, STCo 90/1999, de 26 de mayo.

⁴² Entre muchos, MONTOYA MELGAR, A.: "Dirección y control de la actividad laboral", en AA.VV (BORRAJO DACRUZ, E., Dir.): *Comentarios a las Leyes Laborales. El Estatuto de los Trabajadores*, T. V, Madrid (Edersa), 1985, págs. 143 y ss. ó DURAN LOPEZ, F.: "Inviolabilidad de la persona del trabajador", en AA.VV.: *Comentarios a las Leyes Laborales. El Estatuto de los Trabajadores*, T. IV, Madrid (Edersa), 1983, págs. 531 y ss.

⁴³ TASCÓN LOPEZ, R.: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*, Madrid (Civitas), 2005, págs. 131 y ss.

de localización a distancia, las webcam conectadas a un ordenador gracias al protocolo TCP/IP, los microchips y otros sistemas de vídeo vigilancia⁴⁴.

Semejante urdimbre tecnológica exige parar la atención en los pronunciamientos de los más altos tribunales habidos sobre la materia, que han adquirido un papel muy relevante en la cobertura del vacío normativo existente, con el fin último de superar el particularismo ofrecido por los diversos medios tecnológicos en el ánimo de construir una regla general capaz de servir de orientación a los operadores jurídicos sobre la relevancia de la información obtenida como medio de prueba, a efectos de sustentar una imputación de comportamientos objeto de sanción disciplinaria.

4.1.- Vídeo vigilancia. Data vigilancia

Los límites a la utilización de las cámaras de vídeo en la vigilancia empresarial es uno de los grandes puntos de controversia judicial, por cuanto este instrumento es susceptible de ampliar los grandes poderes del empresario y de comprimir claramente los derechos de los trabajadores. La videovigilancia en tanto que permite la captación y grabación en un soporte físico de la imagen, así como la repetición ilimitada y el análisis detenido de los fotogramas conservados, constituye no solo un instrumento de supervisión del cumplimiento de la actividad laboral del trabajador y un valioso instrumento de prueba de los incumplimientos, sino una herramienta que permite crear una base de datos de información personal (*data vigilancia*), y obtener perfiles sociales de los trabajadores afectados⁴⁵.

Lógico es pensar, atendiendo al principio de buena fe contractual, que si el empresario no informa al trabajador que está siendo controlando, entonces la injerencia empresarial merece un juicio de ilicitud, máxime cuando según el art. 40.1 a) EBEP atribuye a las juntas de personal o a los comités de empresa el derecho a recibir información sobre programas de mejora del rendimiento. Ahora bien, no cabe olvidar que a veces el aviso al trabajador o funcionario o a sus representantes de la concreta vigilancia puede impedir la verificación efectiva de conductas irregulares⁴⁶. De ahí que, en el sentir mayoritario de los órganos judiciales, los controles ocultos, realizados sin consentimiento previo de los trabajadores (a través de micro filmadoras, circuitos cerrados de televisión, dispositivos webcam, digitalización de imágenes), únicamente deben considerarse lícitos por motivos de seguridad para las personas o las cosas (“cajas negras” en los aviones, en paradigmático ejemplo) o en aquellos supuestos en los cuales se trata de poner al descubierto una conducta irregular de un concreto empleado objeto de fundada sospecha por la empresa (competencia desleal, espionaje industrial, boicot empresarial, desvío de clientes, sabotaje informático, atentado a la integridad del patrimonio de la empresa o de los compañeros, deslealtad institucional...), siempre y cuando no exista otro medio menos lesivo de los derechos fundamentales para conseguirlo⁴⁷.

⁴⁴ GOÑI SEIN, J.L.: “Controles empresariales: geolocalización, correo electrónico, internet, videovigilancia y controles biométricos”, *Justicia Laboral*, núm. 39, 2009, pág. 11 ó FARRIOLS i SOLA, A.: "Introducción", en AA.VV (FARRIOLS i SOLA, A., Dir.): *La protección de datos de carácter personal en los centros de trabajo*, Madrid (Cinca), 2006, págs. 15 y ss.

⁴⁵ GOÑI SEIN, J.L.: “Intimidad del trabajador y poderes de vigilancia y control empresarial”, en AA.VV (GARCÍA MURCIA, J., Coord.): *Jornada sobre derechos fundamentales y contrato de trabajo*, Oviedo (Principado de Asturias), 2017, pág. 46.

⁴⁶ SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: “Nuevas tecnologías y relaciones laborales: una tipología jurisprudencial”, *Revista Aranzadi Derecho y Nuevas Tecnologías*, núm. 10, 2006, Tomo I, pág. 47.

⁴⁷ SSTSJ Cataluña 31 julio 2003 (Jur. 214062), Madrid 6 julio 2004 (Ar. 2317), País Vasco 21 octubre 2004 (AS 3927), 12 septiembre 2006 (AS 2602) y 17 abril 2012 (AS 1676), Valencia 4 julio 2007 (AS 2879), Canarias/Las Palmas 30 abril 2009 (AS 1763), Islas Baleares 4 abril 2009 (AS 1763) ó Navarra 28 septiembre 2010 (La Ley, núm. 7583).

Así pues, la tesis más generalizada considera que la no exigibilidad de información previa sobre el control estaría justificada cuando con ella se frustraría la finalidad pretendida respecto de un trabajador concreto sin que exista un medio más inocuo, siendo suficiente con el cumplimiento de los criterios de idoneidad, necesidad y proporcionalidad en sentido estricto⁴⁸. Acoge, por tanto, como parámetro fundamental para valorar la corrección de una medida de control empresarial, el conocido “principio de proporcionalidad”, elaborado por el Tribunal Constitucional a partir de un triple test gradualista: 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 más moderada para la consecución de tal propósito con igual eficacia (juicio de indispensabilidad o estricta necesidad); y, finalmente, si es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés empresarial que perjuicios sobre otros bienes o valores en conflicto (juicio riguroso de adecuación). Así se han pronunciado, entre muchas, las Sentencias del Tribunal Constitucional 98/2000, de 10 de abril y 186/2000, de 10 de julio, relativas, respectivamente, a la instalación de un circuito cerrado de televisión y una red de micrófonos en el espacio de la ruleta rusa del Casino de Latoja ante la sospecha de robos, y a la colocación de una cámara de vídeo en la zona de calzado y textil de un economato de la empresa Ensidesa consecuencia de un llamativo descuadre.

Resulta interesante, a efectos de ponderar los intereses en juego, tener en cuenta el Repertorio de Recomendaciones Prácticas de la OIT en materia de protección de datos de los trabajadores, en virtud del cual “el secreto en materia de vigilancia sólo debería permitirse cuando: a) se realice de conformidad con la legislación nacional (en referencia a la legislación de protección de datos); o b) existan sospechas suficientes de actividad delictiva u otras infracciones graves”. Por tanto, aun cuando la regla general es que si la recogida de datos tiene como objeto garantizar la seguridad, no debería utilizarse para controlar la prestación laboral, si bien procede flexibilizar esta postura cuando no existe otro medio de control efectivo ante la existencia de indicios fundados de transgresiones⁴⁹. En todo caso, no se admite la provocación del incumplimiento para grabarlo en tanto se trata de una medida contraria al deber de buena fe.

Sin embargo, más recientemente, el Tribunal Constitucional, en su Sentencia 29/2013, de 11 de febrero, ha exigido también que se proporcione noticia al trabajador de la utilidad de la supervisión laboral, pues fue sancionado en virtud de las imágenes obtenidas por cámaras de vídeo-grabación instaladas en los accesos y en los recintos universitarios, sin poner en conocimiento del trabajador (personal de administración y servicios de la Universidad de Sevilla) su posible uso para controlar las horas de entrada y de salida. Entiende el Máximo Intérprete de la Norma Fundamental que la instalación de cámaras en el lugar de trabajo sin conocimiento del empleado no sólo constituye una ilegítima privación del derecho a disponer de los propios datos personales, no en vano las imágenes grabadas en un soporte físico quedan integradas en la cobertura del art. 18.4 CE, sino una intromisión en el ámbito protegido por el derecho a la esfera

⁴⁸ La STSJ Valencia 27 abril 1994 (AS 3821), en la que una cámara oculta del control horario de una limpiadora de una consulta odontológica demuestra que durante dos semanas no cumple el horario, entiende que la medida estaba justificada porque se asentaba sobre unas sospechas reales dado que la limpieza era insuficiente, era idónea para la finalidad pretendida porque la trabajadora tenía un horario definido y un lugar concreto de trabajo que permitía su control por tal medio, era necesaria porque la grabación servía de prueba de la irregularidad y era equilibrada en cuanto se limitó al tiempo suficiente para constatar que la conducta era ya un hábito y no una excepción puntual.

⁴⁹ BLAZQUEZ AGUADO, E.M: “La implantación de un protocolo de videovigilancia en el centro de trabajo”, Revista Aranzadi de Derecho y Nuevas Tecnologías, núm. 43, 2017 (BIB 2017/808), pág. 3.

privada del trabajador. Teoría seguida por algunos pronunciamientos de los Tribunales ordinarios que expresamente exigen, sin matizaciones, como previo y preceptivo, el informe a los representantes de los trabajadores y a los propios trabajadores afectados de la instalación y de la existencia de videocámaras cuando constituyan elementos de control de la actividad laboral, en uso de la facultad empresarial del art. 20.3 ET⁵⁰.

En el ordenamiento español, la Ley 15/1999, de 13 de diciembre, de Protección de Datos (LOPD), viene a señalar que deben respetarse los principios de finalidad, proporcionalidad y pertinencia, siendo necesario notificar la creación del fichero correspondiente a la cámara a la Agencia Española de Protección de Datos, debiendo reconocerse a los trabajadores los derechos de acceso, rectificación o cancelación, pudiendo mantener las grabaciones durante el tiempo imprescindible para los fines que motivaron su recogida y borrándolas en todo caso antes de que expire el plazo de un mes establecido para la cancelación, entendiéndose innecesario el consentimiento pero preceptiva la información previa⁵¹. Es más, el parámetro de finalidad se debe entender de manera restrictiva, de modo que no cabe justificar en abstracto la legitimidad de estos medios desde un genérico control de la prestación de trabajo, sino que hay que demostrar en el caso concreto y en función de las circunstancias concurrentes si el empleo de una técnica de control puede colisionar con el ámbito privado y si lo hace justificadamente o no⁵², pues al calor del art. 18.4 CE se deben concretar las características y el alcance de la recopilación de datos que va a realizarse, esto es, indicando en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente si pueden llegar a utilizarse para la imposición de sanciones disciplinarias por incumplimientos de las obligaciones dimanantes del contrato de trabajo⁵³.

Sin embargo, tampoco se puede descartar por completo un control oculto, pues ciertamente a veces el recurso a las grabaciones sólo es eficaz si se adopta de forma secreta y, por tanto, imponer la obligación de informar a los afectados puede hacer inútil la medida, pues se suele recurrir a ella para detectar actividades fraudulentas o ilícitas del trabajador sobre las que hay atisbos claros. Así, cambiando sustancialmente su parecer anterior, el Tribunal Constitucional, en sentencia 39/2016, de 3 de marzo, admite como prueba lícita, justificativa de un despido derivado de la apropiación de dinero en una caja registradora, las grabaciones de una cámara de vigilancia instalada ante la existencia de sospechas previas y ello pese a que no se informó expresamente a la trabajadora de la colocación ni la finalidad del sistema de control. Entiende el Máximo Intérprete de la Constitución que el deber empresarial de información se vio cumplido mediante la simple visualización del correspondiente distintivo informativo (el cartel indicativo de “zona videovigilada”) en un lugar visible.

Como factor de complejidad adicional, la postura de los órganos judiciales ordinarios no es

⁵⁰ STS 13 mayo 2014 (rec. 1685/2013), en la cual se considera que la existencia en el supermercado donde presta servicios la trabajadora de un sistema de cámaras dirigido a evitar robos por parte de los clientes hace que el despido, aun quedando constatado que no había escaneado algunos productos en beneficio de un cliente, sea considerado nulo al ser contrario al derecho fundamental a la intimidad personal y a la propia imagen.

⁵¹ POQUET CATALÁ, R.: *El actual poder de dirección y control del empresario*, cit., pág. 247.

⁵² RODRIGUEZ-PIÑERO Y BRAVO-FERRER, M.: “Intimidación del trabajador y contrato de trabajo”, *Relaciones Laborales*, núm. 8, 2004, pág. 48.

⁵³ TAPIA HERMIDA, A.: “El control de la actividad laboral mediante la captación y grabación de imágenes personales (vídeo-vigilancia)”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 362, 2013, pág. 153.

del todo clara. Para algunos, sea cual sea el derecho fundamental afectado, si la finalidad empresarial declarada sobre las cámaras de vídeo es de seguridad, la actuación sancionadora sobre un empleado que actúa cometiendo infracciones particularmente graves no debe considerarse como un hecho desviado o hallazgo casual al que no cabe otorgar ninguna relevancia sino, al contrario, ha de entenderse plenamente justificada⁵⁴. Así, procede mencionar la Sentencia del Tribunal Supremo de 7 de julio de 2016, que siguiendo la última línea argumental del Tribunal Constitucional, acepta como válida la prueba de videovigilancia que capta un hurto en una tienda cuando las cámaras se colocan como una reacción a una situación de pérdidas importantes de material en el interior del centro de trabajo y con carteles que advertían de su presencia, lo que hace que los trabajadores conozcan su existencia y finalidad. Queda cumplido el principio de proporcionalidad, pues se trata de un medio de control idóneo, no cabe otra medida más moderada pero igual de eficaz y es una intervención equilibrada al derivarse más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Con carácter más reciente, ha vuelto a pronunciarse el Alto Tribunal en sentencia de 31 de enero de 2017⁵⁵, que reconoce justificado un despido al haber quedado probada la manipulación de tickets y el hurto de diferentes cantidades de dinero, entendiéndose que sólo es necesario que los trabajadores tengan conocimiento de la existencia, ubicación e instalación del sistema de videovigilancia pero no de que pueda tener una finalidad disciplinaria, no en vano en el marco de una relación laboral no es necesario un consentimiento individual ni colectivo de las grabaciones, ya que éste se entiende implícito, razón por la cual sólo debería concurrir dicha información explícita cuando el tratamiento de las imágenes se use con una finalidad totalmente ajena al cumplimiento del vínculo contractual. En el mismo sentido se manifiestan la Sentencias de 1 de febrero⁵⁶ y de 2 de febrero de 2017⁵⁷, entrando a valorar esta última la situación de un trabajador de un gimnasio a quien tras varias quejas emitidas por compañeros sobre su actuación profesional que permitía la entrada al recinto de personas ajenas al club, la empresa procede a despedir utilizando para acreditar los hechos justificativos de tal decisión las imágenes de una cámara que el trabajador conocía pero de la que no había sido informado expresamente sobre su finalidad exacta⁵⁸.

También ha tenido ocasión de pronunciarse el Tribunal Europeo de Derechos Humanos en una sentencia de 28 de noviembre de 2017 (asunto *Antovic and Mirkovic contra Montenegro*)⁵⁹, que, sin embargo, considera inadecuada la instalación de cámaras en los auditorios universitarios donde se imparten clases por invadir el derecho a la vida privada de los profesores demandantes, quienes no autorizaron dicha grabación y únicamente conocieron la instalación por el informe que proporcionó el Decano en la Junta de Facultad con el fin de garantizar la seguridad de los bienes y las personas, incluidos los estudiantes y la vigilancia de la enseñanza.

⁵⁴ GOÑI SEIN, J.L.: “Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?”, *Ponencia temática presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, celebrado en Pamplona el 29-30 de mayo de 2014*, pág. 68.

⁵⁵ Rec. 331/2015.

⁵⁶ Rec. 3262/2015.

⁵⁷ Rec. 554/2016.

⁵⁸ Una visión crítica en PRECIADO DOMENECH, C.H.: “La vídeo vigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal”, *Revista de Derecho Social*, núm. 77, 2017, pág. 194.

⁵⁹ Aplicación n° 70838/13.

Entre los pronunciamientos de suplicación, cabe aludir, como ejemplos más actuales, a aquel que considera que la instalación de una cámara sin conocimiento de los trabajadores resulta una medida correcta siempre que se ubique en los lugares de trabajo, no en espacios privados como aseos o vestuarios, y sin que las filmaciones tengan posterior difusión, entendiéndose procedente el despido de una enfermera de una residencia de ancianos que incumplió instrucciones sobre la dispensa de la medicación⁶⁰. En parecido sentido, puede mencionarse la aceptación de la instalación de una cámara en el baño de una residencia para graves discapacitados físicos y mentales, que confirman el maltrato proporcionado por un celador⁶¹. En fin –y como muestra de la variedad de supuestos en presencia y de la ausencia de soluciones claras–, no se ha considerado violado el derecho a la intimidad de un representante del empresario, que es grabado con el móvil de la trabajadora mientras le entregaba a ésta una carta en la que se le imponía una sanción de empleo y sueldo⁶².

Dando un paso más, procede alertar también que la recogida de imágenes del trabajador realizando su actividad laboral en un lugar que se encuentra a la vista de todos los que están en el centro de trabajo sobre la que previamente se ha informado, puede no tener carácter lesivo para la intimidad, pero sí puede afectar al derecho a la propia imagen, entendido como interés del sujeto en evitar la difusión incondicionada de su aspecto físico que constituye el primer elemento configurador de su intimidad y de su esfera personal en cuanto instrumento básico de identificación y proyección exterior y factor personal imprescindible para su propio reconocimiento como individuo. Es conocido el caso del despido del cortador de jamón que se negó a que su imagen, realizando tareas de corte, fuera difundida en una campaña de promoción. En realidad, no estaba en juego la salvaguarda de “una esfera de propia reserva personal, frente a intromisiones ilegítimas”, sino la facultad del empleado de impedir la captación, grabación y reproducción de su imagen en el sentido que indica la Ley Orgánica 1/1982, que atribuye la facultad de disponer de la representación del aspecto físico de una persona que permita su identificación, lo que conlleva tanto el derecho a determinar la información gráfica generada por los rasgos físicos que le hagan reconocible que puede ser captada o tener difusión pública, como el derecho a impedir la obtención, reproducción o publicación de su propia imagen por un tercero no autorizado⁶³. Recientemente, la Audiencia Nacional ha considerado que la empresa tiene que pedir consentimiento expreso a los trabajadores para cada actividad laboral concreta, tal y como sucede con la realización de servicios de vídeo llamada a la luz de un contrato mercantil con el cliente⁶⁴. Asimismo, recientemente se ha considerado que la empresa sólo puede imponer el uso de uniformes a los trabajadores, siempre por motivos razonables justificados en las características de la actividad productiva, esto es, en aras a la eficiencia y calidad de los servicios prestados, que no impliquen discriminación por razón de sexo⁶⁵.

4.2.- Terminales informáticos

No menos controvertida es la cuestión relativa a los registros sobre el ordenador utilizado por el trabajador, recurriendo muchas veces a programas espías (*web bugs*), que permiten el acceso subrepticio al ordenador del trabajador sin violar su *password*, o “registradores de teclas”

⁶⁰ STSJ Galicia 25 abril 2014 (rec. 4347/2013).

⁶¹ STSJ Andalucía 13 noviembre 2017 (rec. 1461/2016).

⁶² STS, Civil, 20 noviembre 2014 (rec. 3402/2012).

⁶³ SSTCo 99/1994, de 11 de abril; 117/1994, de 25 de abril y 23/2010, de 27 de abril.

⁶⁴ SAN 15 junio 2017 (rec. 137/2017).

⁶⁵ STSJ Madrid 19 junio 2017 (rec. 644/2016).

que facilitan la averiguación de las contraseñas, sobre todo para inspeccionar el sistema de mensajería o los accesos a internet⁶⁶.

4.2.1.- Mensajería electrónica

El uso del correo electrónico como herramienta de comunicación en el trabajo ha tenido una implantación exponencial hasta el punto de equipararse e incluso en algunos casos superar al teléfono como sistema de transmisión de información tanto a nivel interno dentro de la propia empresa como en el marco externo. Por un lado, mediante la utilización de esta vía, el trabajador puede visualizar, de manera rápida, la información recibida en cualquier formato como: texto, gráficos, imágenes, sonidos..., permitiendo almacenar los mensajes y reenviarlos de forma sencilla. Por otro, fomenta las relaciones interpersonales entre quienes estando, geográficamente separados, tienen intereses comunes o tienen que resolver asuntos de interés general⁶⁷.

No obstante, a pesar del efecto positivo que el correo electrónico ejerce sobre los trabajadores y la eficiencia y eficacia en la prestación del servicio, suele ser valorado por la dirección de las empresas o Administraciones Públicas con gran recelo, poniendo el énfasis en el eventual perjuicio que su uso puede causar a aquéllas. Ciertamente, la utilización abusiva de un instrumento de trabajo para fines propios plantea, desde la perspectiva empresarial, numerosos inconvenientes y perjuicios. Fundamentalmente, se señala el daño económico que, no obstante ser inapreciable en cuanto al coste de la conexión, lo es en cuanto al lucro cesante, o sea, el tiempo que el trabajador deja de dedicar a la prestación efectiva de su actividad profesional, disminuyendo su propio rendimiento y el de sus compañeros a los que envía mensajes. De otra parte, ese uso desviado puede comprometer la capacidad del sistema informático de la corporación, la seguridad, imagen o competitividad, mediante la transmisión de información confidencial, relativa a empleados, proveedores, usuarios o clientes⁶⁸.

Muchas son, pues, sus ventajas desde el punto de vista de la agilidad, inmediatez, posibilidad de adjuntar archivos en tiempo real, multilocalización..., pero no pocos son los inconvenientes⁶⁹, de ahí el interés del empresario o del director de recursos humanos en detectar aquellas conductas incorrectas, manifestadas muchas veces en mensajes que, amparados bajo el principio de secreto de las comunicaciones, puedan suponer una transgresión de la buena fe contractual o un abuso de la confianza depositada en el trabajador.

4.2.2.- Rastros de navegación por internet

A diferencia de lo que sucede en el supuesto anterior (correo-e), la navegación por internet en páginas web no relacionadas con el trabajo (al igual que la participación en chats abiertos o la intervención en foros de discusión o wikis)⁷⁰ no tiene amparo en el derecho al secreto de las

⁶⁶ MIÑARRO YANINI, M.: "Las facultades empresariales de vigilancia y control en las relaciones de trabajo: especial referencia a las condiciones de su ejercicio y a sus límites", *Tribuna Social*, núm. 158, 2004, pág. 13.

⁶⁷ SAMPEDRO BURGOS, G.: "Reflexiones sobre la aplicación de la normativa de protección de datos en el ámbito del control del empresario y sistemas de denuncias internas", *Revista General de Derecho del Trabajo y de la Seguridad Social (Justel)*, núm. 26, 2011, pág. 4.

⁶⁸ DE NIEVES NIETO, N.: "El uso de correo electrónico e internet en la negociación colectiva", *Relaciones Laborales*, 2009, Tomo I, pág. 252.

⁶⁹ MIRO MORROS, D.: "El uso del correo electrónico en la empresa: protocolos internos", *Actualidad Jurídica Aranzadi*, núm. 874, 2013 (BIB 2013/2511), págs. 1 y ss.

⁷⁰ FERNANDEZ VILLAZON, L.A.: *Las facultades empresariales de control de la actividad laboral*, Pamplona (Aranzadi), 2003, pág. 144.

comunicaciones⁷¹. En este caso, existe un acceso a información, pero no una verdadera interacción personal objetivamente tutelable, razón por la cual el juego de la facultad empresarial será más amplio a la hora de verificar los posibles incumplimientos contractuales del trabajador consistentes en consultar páginas web para fines particulares durante la jornada de trabajo, tal y como sucede con otras comunicaciones que transitan en abierto por el espectro radioeléctrico, cuales son las radiocomunicaciones bajo el tradicional “banda AM”, o la más moderna “banda lateral única” –“single side band, SSB”— o las que se producen a través de canales de baja frecuencia, como el “*bluetooth*” o el “*near field communication*”⁷².

Desde el punto de vista técnico, las posibilidades que existen en la actualidad para controlar la navegación por internet pueden dividirse en cuatro grupos: programas de “monitorización” (aplicaciones que se instalan en el ordenador y que permiten saber en tiempo real las páginas visitadas, la duración de la conexión y las veces que se ha accedido sin que el usuario tenga conocimiento de ello), “cortafuegos” (permiten vetar y vigilar a la vez el acceso a determinadas páginas de internet, por lo que se consigue que el uso del ordenador sea exclusivo para fines profesionales), “proxy” (ayudan a saber los sitios que han sido visitados por el trabajador) y “sniffers” (no se instalan en el equipo informático sino en el servidor, alertando sobre lo que el trabajador realiza a lo largo de la jornada laboral)⁷³.

Bajo tales premisas, pese a la facilidad de todas estas variables, no cabe desconocer tampoco su sujeción al límite indeclinable constituido por el derecho a la intimidad, debiendo, por tanto, aplicarse los requisitos del conocido principio de proporcionalidad. No cabe duda que la visita de determinados lugares web permite conocer directamente información sobre aspectos de la vida personal del trabajador relacionados con su intimidad (aficiones personales, gustos culinarios, preferencias sexuales, políticas, sindicales o religiosas...). Al tiempo, el análisis conjunto de los sitios a los que accedió el trabajador, así como su frecuencia y tiempo de conexión, permiten reconstruir perfiles subjetivos íntimos del trabajador⁷⁴.

4.2.3.- Aproximación a la casuística apreciación de los Tribunales

El registro directo de los terminales informáticos utilizados por los trabajadores (*hardware*) y el control del uso de internet y del correo electrónico ha dividido a la doctrina y a la jurisprudencia sin que todavía hoy se haya alcanzado una postura claramente asentada⁷⁵, en una evolución en la que pueden destacarse los siguientes hitos fundamentales:

A) Tribunal Europeo de Derechos Humanos

Es necesario traer a colación, en primer lugar, la doctrina del Tribunal Europeo de Derechos Humanos vertida en la Sentencia de 3 de abril de 2007, conocida como caso *Copland* (2007/23), que, aplicando el art. 8.1 de la Convención Europea de Derechos

⁷¹ LOPEZ MOSTERIO, R.: "Despido por uso de correo electrónico e internet", *Actualidad Laboral*, núm. 41, 2001, págs. 1132 y ss.

⁷² FERNANDEZ VILLAZON, L.A.: "A vueltas con el control empresarial sobre la actividad laboral: 'test de honestidad', telemarketing, registro de terminales y uso --o abuso-- de internet", *Tribuna Social*, núm. 168, 2004, pág. 40.

⁷³ TOSCANI GIMENEZ, D. y CALVO MORALES, D.: "El uso de internet y el correo electrónico en la empresa: límites y garantías", *Nueva Revista Española de Derecho del Trabajo*, núm. 165, 2014, pág. 202.

⁷⁴ MARTINEZ FONS, D.: "Uso y control de las tecnologías de la información y comunicación en la empresa", *Relaciones Laborales*, núms. 23-24, 2002, pág. 200.

⁷⁵ CAMAS RODA, F.: "La influencia del correo electrónico y de internet en el ámbito de las relaciones laborales", *Revista de Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 50, 2001, págs. 139 y ss.

Humanos, entiende que los trabajadores conservan su derecho a la intimidad aun cuando los dispositivos electrónicos (teléfono, correo electrónico e internet) sean propiedad del empresario y su utilización se produzca durante el horario de trabajo, de suerte que las injerencias empresariales sobre tal derecho, o bien deben contar con el conocimiento del titular, o bien deben de estar previstas expresamente en una ley que las justifique.

El Tribunal Europeo de Derechos Humanos vuelve a pronunciarse en sentencia de 16 de enero de 2016 (asunto 61496/08, caso *Barbulescu*), en virtud de la cual se entiende que la empresa puede monitorizar, previa advertencia, los instrumentos informáticos que utiliza un trabajador. Esta interpretación tiene su origen en un litigio por despido en el que un responsable de ventas de una empresa rumana crea a instancias de la corporación, una cuenta de Yahoo Messenger para la gestión y relaciones con los clientes, pero que utiliza también para entablar conversaciones privadas (con su pareja y con su hermano), circunstancia que se descubre en un control empresarial de la citada cuenta. La compañía había entregado previamente a los trabajadores un protocolo interno por el cual se dejaba clara “la prohibición de usar computadoras, fotocopiadoras, teléfonos, télex y fax para fines personales”⁷⁶. No existe, por tanto al calor del sentir mayoritario de la sala, una “expectativa razonable de privacidad” cuando se ha establecido una prohibición absoluta de uso personal en la política interna de la empresa, sin que se establezcan obligaciones adicionales en el sentido de justificar el amplio alcance de dicha prohibición o de informar a los trabajadores de forma precisa acerca de las medidas de control⁷⁷.

Este asunto es revisado en Gran Sala, dictándose la sentencia de 5 de septiembre de 2017 (asunto 217/61, caso *Barbulescu II*), en la que se rectifica el criterio anterior y se reconoce que los tribunales rumanos no verificaron si, pese a la existencia de instrucciones del empleador sobre el uso de los dispositivos, el trabajador había sido advertido con anterioridad de la vigilancia que ésta iba a llevarse a cabo de las comunicaciones electrónicas efectuadas desde su cuenta profesional, ni tampoco hasta qué punto se ha producido una intromisión en la vida privada del trabajador en el ámbito de la relación de trabajo que hubiera podido alcanzarse por vías menos invasivas⁷⁸. Considera que no es suficiente, atendiendo al Código de Buenas prácticas para la protección de los datos personales del trabajador de 1999 y a la Recomendación del Comité de Ministros del Consejo de Europa (CM/Rec. 2015), sobre tratamiento de datos personales en el ámbito de la relación laboral, que la empresa hubiera remitido una notificación a sus empleados en la que se ilustraba sobre el despido de una trabajadora por motivos disciplinarios, después de haber utilizado para fines privados el internet, el teléfono y la fotocopiadora, sino que es necesario un aviso previo, antes de que comience la supervisión.

B) Tribunal Constitucional

La Sentencia 241/2012, de 17 de diciembre, prescinde del anterior juicio de proporcionalidad para adoptar ahora el canon de expectativa de intimidad. La demandante de

⁷⁶PÉREZ DE LOS COBOS ORIHUEL, F.: “El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos”, *Nueva Revista Española de Derecho del Trabajo*, núm. 196, 2017 (BIB 2017/814), págs. 1 y ss.

⁷⁷ GARCÍA GONZÁLEZ, R. y PASTOR MERCHANT, J.: “Límites a la necesaria flexibilización de los derechos a la intimidad y al secreto de las comunicaciones en el ámbito laboral: una reflexión tras la sentencia del TEDH de 12 de enero de 2016 en el caso *Barbulescu*”, *Diario La Ley*, 4 de marzo de 2016 (ref. D-95).

⁷⁸ CUADROS GARRIDO, M.E.: “La mensajería instantánea y la STEDH de 5 de septiembre de 2017”, *Aranzadi Doctrinal*, núm. 11, 2007 (BIB 2017/43157), pág. 9.

amparo es una trabajadora que venía desempeñando labores de teleoperadora especialista para la empresa Global Sales Solutions Line, S.L. Dicha empleada y una compañera instalaron un programa informático denominado “Trillian”, de mensajería instantánea, en el disco duro de un ordenador, que era de uso indistinto por todos los trabajadores de la empresa y al que se accedía sin clave. La instalación del programa contravenía una orden empresarial expresa. A través de dicho soporte informático, las trabajadoras entablaban conversaciones en las que vertían comentarios despectivos, críticos e insultantes en relación con compañeros de trabajo, superiores y clientes. Dichas apreciaciones fueron descubiertas, por casualidad, por otro empleado que intentó utilizar la unidad “C” de ese ordenador, dando cuenta de ello a la empresa. El Tribunal Constitucional entiende que las conversaciones efectuadas por estas trabajadoras no quedan garantizadas por “el derecho al secreto de las comunicaciones” porque se trata de una forma de correspondencia abierta que permite su interceptación sin censura jurídica en base a las facultades directivas reconocidas al empleador en el ET. No existe en ese caso, a juicio del Máximo Intérprete de la Constitución, una “expectativa razonable de confidencialidad derivada de la utilización del programa instalado”, atendiendo al carácter abierto del canal utilizado, una computadora de uso común⁷⁹.

Sin embargo, el Tribunal Constitucional da un nuevo giro en la Sentencia 170/2013, de 17 de octubre, pues el derecho a la propiedad empresarial de los instrumentos de trabajo (ordenador) y el poder y control de la actividad laboral salen reforzados. En este caso, la empresa Alcaliber SA procede a interceptar el contenido de los correos electrónicos de un trabajador, registrados en el ordenador facilitado por la empresa, ante las sospechas de un comportamiento irregular derivado de la revelación a terceros de datos empresariales confidenciales, tipificando el convenio colectivo como falta leve la utilización para fines privados de los medios informáticos proporcionados por la empresa. Incidentalmente, el Tribunal entiende, sin perjuicio de lo que después se dirá en cuanto al secreto de las comunicaciones, que tal control empresarial no vulnera el derecho a la intimidad, pues se cumplen los requisitos del juicio de proporcionalidad: es una medida justificada, pues su práctica se fundó en la sospecha de un comportamiento irregular del trabajador; es una medida idónea para la finalidad de verificar si el empleado cometía efectivamente la irregularidad sospechada (la revelación a terceros de datos empresariales de reserva obligada); es una medida necesaria, dado que el contenido de los correos electrónicos serviría de prueba del comportamiento irregular, no siendo suficiente el mero acceso a otros elementos de la comunicación como la identificación del remitente o destinatarios, que por sí solos no permitían acreditar el ilícito indicado; en fin, es una medida ponderada o equilibrada, pues únicamente se ha accedido al contenido de correos electrónicos que han reflejado información relativa a la actividad empresarial sin incorporar aspectos personales o familiares del trabajador⁸⁰.

Pero lo importante de esta nueva doctrina es que la previsión convencional en virtud de la cual se tipifica como falta leve el uso privado de medios tecnológicos de la empresa legitima el control empresarial sin necesidad de informar al trabajador. Esta tipificación se equipara, por el Tribunal Constitucional, a la existencia de prohibición absoluta del uso extraprofesional del correo electrónico, habilitando a la empresa para desplegar medidas de control al objeto de la verificación de su cumplimiento o no por los trabajadores, entendiendo que el afectado debía saber esta

⁷⁹ APARICIO ALDANA, R.K.: “Las nuevas tecnologías en las relaciones laborales. Análisis de la STC 241/2012, de 17 de diciembre”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 36, 2014, pág. 290.

⁸⁰ SANTIAGO REDONDO, K.M.: “Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE”, *Relaciones Laborales*, núm. 1, 2014, pág. 130.

posibilidad de inspección porque, a su vez, debía conocer el convenio colectivo aplicable a la empresa, de modo que no podía existir una expectativa fundada y razonable de confidencialidad, no en vano la comunicación se produce en un canal abierto.

C) Tribunal Supremo

El Tribunal Supremo, no sin fisuras, ha venido entendiendo que no existe un derecho del trabajador a la utilización personal de los ordenadores de la empresa, pues ésta puede prohibir tal proceder, limitarlo y someterlo a control, pero esto tampoco significa que la supervisión empresarial no tenga que respetar determinadas exigencias. La expectativa de confidencialidad derivada de una práctica social de tolerancia no puede ser desconocida, salvo alerta prohibitiva en contrario. De este modo, si la empresa ha establecido unas reglas de uso de estos medios (con aplicación de prohibiciones absolutas o parciales) y ha informado a los trabajadores sobre los extremos de los controles, la actuación del trabajador en contra de tales prevenciones ha de considerarse ilegítima.

En este sentido se pronuncia la Sentencia del Tribunal Supremo de 26 de septiembre de 2007⁸¹, en la que se enjuicia el despido del Director General de una empresa que prestaba servicios en un despacho sin llave, en el que disponía de un ordenador sin clave de entrada y conectado a la red de la empresa. Un técnico informático comprueba los fallos del ordenador, detectando la existencia de virus informáticos derivados de acceso a páginas poco seguras de internet. Entiende el Tribunal que no es aplicable el art. 18 ET porque el registro del ordenador supone el control de un medio de producción, no de un efecto privado del trabajador. Se debe acudir, pues, al art. 20.3 ET, produciéndose un ataque al derecho a la intimidad del empleado al no haber sido avisado sobre la práctica del control ni sobre los límites al uso de este instrumento para fines privados.

En esta misma línea, cabe citar la Sentencia del Tribunal Supremo de 8 de marzo de 2011⁸², cuyo relato fáctico consiste en un control empresarial realizado en los meses de enero y febrero sobre las redes de información con el objeto de revisar la seguridad del sistema de la corporación y detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados, evidenciándose que desde el ordenador utilizado por los jefes de turno se accedió a internet en horas de trabajo con un total de 5.566 "visitas" a páginas referidas al mundo multimedia-vídeos, piratería informática, anuncios, televisión, contactos, etc. La gran mayoría de esas visitas se produjeron en los turnos de trabajo del despedido y en tramos horarios en los que aquél estaba en el despacho. El Tribunal entiende que se ha ocasionado un atentado al derecho a la intimidad del trabajador porque no ha habido advertencia previa por parte de la empresa de los límites de utilización de estos medios para fines privados ni sobre los controles que se iban a practicar⁸³.

No obstante, en un breve espacio de tiempo, el Alto Tribunal introduce una matización en la doctrina anterior, que supone una cierta marcha atrás en la protección del derecho fundamental a la intimidad y al secreto de las comunicaciones. Así, la Sentencia del Tribunal

⁸¹ TOL 1.153.301

⁸² TOL 2.074.769.

⁸³ SEPULVEDA GOMEZ, M: "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites", *Temas Laborales*, núm. 122, 2013, pág. 210.

Supremo de 6 de octubre de 2011⁸⁴ entiende que las órdenes empresariales destinadas a concretar la finalidad de los instrumentos de control no deben someterse a los principios de proporcionalidad, idoneidad y necesidad, si existe una prohibición absoluta que impuso el empresario sobre el uso de medios de la empresa (ordenadores, móviles, internet, etc.) por los trabajadores para fines propios, tanto dentro como fuera del horario de trabajo, y no caprichosamente sino ante las sospechas fundadas de que se estaban desobedeciendo tales órdenes impartidas al respecto. Al objeto de comprobar el cumplimiento de tal prescripción, se instaló un programa espía capaz de captar las pantallas a las que accedía una trabajadora para su posterior visualización. Se trataba de un sistema poco agresivo que no permitía ver los archivos del ordenador que estaban protegidos por las contraseñas de cada uno de los usuarios. El Tribunal Supremo entiende que la orden expresa de prohibición lleva implícita la advertencia sobre la posible instalación de sistemas de control, sin que sea posible admitir que surja un derecho a que se respete la intimidad porque no existe tolerancia empresarial del uso personal sino que éste es ilícito. Tal y como establece este fallo, “si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no concurrir una situación de tolerancia del uso personal, tampoco existe ninguna expectativa razonable de intimidad”. Se bajan, por tanto, las barreras de la protección de la intimidad o el secreto, pues la tolerancia de la empresa es la que crea una expectativa de confidencialidad, de forma que si hay prohibición de uso personal, deja de haber tolerancia, y ya no existirá esa expectativa, con independencia de la información que la empresa haya podido proporcionar sobre el control y su alcance, que deviene innecesaria⁸⁵.

Sin embargo, el Tribunal Supremo, en sentencia de 13 de mayo de 2014⁸⁶, vuelve a considerar que el hecho de que el empresario haya establecido unas reglas sobre el manejo de los ordenadores o haya previsto ciertas prohibiciones no significa que esté facultado para fiscalizar de cualquier forma, exigiendo con total rotundidad que los empleadores informen expresamente a sus empleados de la posibilidad de llevar a cabo controles de la actividad laboral con carácter previo a su materialización, no siendo suficiente que estos últimos conozcan la existencia del control del medio técnico por motivos de seguridad empresarial. Es necesario, por tanto, que los trabajadores hayan sido informados de la existencia específica del control de la actividad laboral y de los mecanismos a aplicar en orden a comprobar la corrección de los usos, sin perjuicio de la posible aplicación de medidas de carácter preventivo, como puede ser la prohibición total o parcial de determinadas conexiones.

Por otra parte, conviene recordar que la Sala de lo Penal del Tribunal Supremo, en sentencia de 16 de junio de 2014⁸⁷, interfiere en la jurisprudencia dictada por la Sala Cuarta en relación a las facultades del empresario para adoptar medidas de control y vigilancia en un triple sentido: de un lado, en relación con los correos electrónicos que estén “sin abrir” por el destinatario rige la protección constitucional que otorga el art. 18.3 CE al secreto de las comunicaciones, siendo necesario contar con autorización judicial; de otro, las comunicaciones “ya abiertas” por el destinatario que únicamente permanecen en las bandejas de entrada y salida,

⁸⁴ TOL 2.366.592.

⁸⁵ NORES TORRES, L.E.: “Algunas cuestiones sobre la utilización de las redes sociales como medio de prueba en el proceso laboral”, *Actualidad Laboral*, núm. 3, 2014, pág. 315.

⁸⁶ TOL 4.424.627

⁸⁷ TOL 4.511.548.

así como otros aspectos adyacentes (historial de navegación web, acceso al disco duro del ordenador, direcciones, frecuencias...), están tutelados por el art. 18.1 CE, referido al derecho a la intimidad, y por el 18.4 CE, relativo a la protección de datos personales, pero no por el derecho al secreto de las comunicaciones, debiendo estar a la conocida teoría de la proporcionalidad en el acceso; en fin, para el registro de medios electrónicos, propiedad del trabajador, utilizados en el tiempo y lugar de trabajo, es necesario contar con autorización judicial⁸⁸.

Sea como fuere, el criterio de la Sala Segunda tiene la finalidad de fijar una clara doctrina referente a la validez probatoria de los controles sobre el correo electrónico en vía penal, de modo que para evitar que las pruebas pierdan su eficacia, la empresa deberá solicitar la intervención judicial en la obtención de los mensajes cerrados y privados del trabajador (art. 539 de la Ley de Enjuiciamiento Criminal). Ahora bien, en el ámbito laboral, y a efectos de servir de prueba lícita de un comportamiento irregular del trabajador, debe considerarse vigente la doctrina mayoritaria de la Sala Social según la cual cuando rige en la empresa una prohibición expresa de uso privado de los medios informáticos facilitados al trabajador para el desarrollo de su actividad productiva, no existe una expectativa de confidencialidad respecto al conocimiento de las comunicaciones mantenidas a través de la cuenta de correo corporativa y que pueden registradas en el ordenador propiedad de la empresa. En fin, si el trabajador utilizara sus propios dispositivos (en el fenómeno conocido como *BYOD, bring your own device*) no resultaría aplicable el art. 20.3 ET, sino que el empresario debería atenerse a lo previsto en el art. 18 ET, pues se trata de un efecto personal (en el centro de trabajo y en horas de trabajo, respetando al máximo la dignidad e intimidad del trabajador y contando con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa).

En todo caso, nada impide que uno de los integrantes de la conversación utilice el contenido como prueba, tal y como sucede con las conversaciones de whatsapp, pudiendo citar los siguientes pronunciamientos de suplicación, sin ánimo exhaustivo⁸⁹: la Sentencia del Tribunal Superior de Justicia del País Vasco de 13 de mayo de 2014 que declara nulo el despido de una empleada de hogar, que puede demostrar el acoso sexual al que está sometida a través de la reproducción de varios mensajes de su empleador enviados por whatsapp. O la Sentencia del Tribunal Superior de Justicia de Cantabria de 18 de junio de 2014, que declara procedente el despido de un conductor de autobús que utilizaba este medio mientras conducía. O la Sentencia del Tribunal Superior de Justicia de Cataluña 3 de febrero de 2015, que considera ajustado a derecho el despido de unas cuidadoras de niños en una guardería, que vierten comentarios inapropiados sobre uno de los menores. O la Sentencia del este mismo Tribunal de 18 de julio de 2016, que considera procedente el despido disciplinario de un profesor por mantener conversaciones íntimas por whatsapp con una alumna de 14 años. Todo ello sin olvidar que la Sentencia del Tribunal Superior de Justicia de Madrid de 10 de junio de 2015 considera baja voluntaria del trabajador la comunicación de whatsapp en la que pone de manifiesto de modo indiscutible su intención de no volver al trabajo. En fin –y por no seguir--, la Sentencia del Tribunal Superior de Justicia de Madrid de 8 de junio de 2017 considera válida la dimisión de un trabajador a través de expresiones claras y reiteradas vertidas en este medio, quedando impedida la reincorporación posterior.

⁸⁸ MIRO MORROS, D.: “El uso del correo electrónico en la empresa: protocolos internos”, *Actualidad Jurídica Aranzadi*, núm. 874, 2013 (BIB 2013/2511), págs. 1 y ss.

⁸⁹ STSJ Cantabria 11 diciembre 2015 (rec. 859/2015).

No cabe olvidar, a la postre, que la facultad conferida al empresario de prohibir terminantemente el uso del correo electrónico para fines privados plantea serias dudas de compatibilidad con los derechos a la intimidad y al secreto de las comunicaciones de los terceros no vinculados mediante una relación laboral con el empresario o con la Administración, que reciben y envían mensajes al trabajador a través del medio de comunicación corporativo, razón por la cual se ha afirmado la necesidad de cumplir con las exigencias de transparencia en el referido control, recurriendo a elementos de configuración del correo que permitan advertir a los comunicantes externos que se están relacionado con un sistema que puede ser abierto por persona distinta del destinatario, de forma análoga a los avisos que se utilizan en caso de grabación de las conversaciones telefónicas mantenidas con servicios de atención al cliente⁹⁰.

D) Algunas sentencias de los Tribunales Superiores de Justicia

Entre los pronunciamientos de suplicación, pueden mencionarse algunos significativos, tal y como sucede con una sentencia que considera justificada la extinción del contrato de un empleado de Iberia por manipular datos informáticos con el fin de simular su presencia en la empresa⁹¹. El trabajador, que prestaba servicios como personal de tierra, actuaba en connivencia con una compañera de trabajo adscrita al departamento de recursos humanos que era la encargada de verificar las incidencias relacionadas con el control de presencia. De forma habitual, y siempre accediendo a las peticiones del empleado, la compañera iba anotando unas horas de comienzo o finalización de la jornada de trabajo que no se correspondían con la realidad, evitando que aparecieran las faltas de puntualidad cometidas por el trabajador. El empleado y su colaboradora conectaban normalmente por correo electrónico mediante el email que proporcionaba la empresa. El propio trabajador reconoció que en el manual de la empresa se decía que el uso de los medios facilitados por Iberia (ordenador y correo electrónico) eran únicamente para usos profesionales y no personales y, además, había sido avisado con antelación de que se iba a proceder a extraer el disco duro de su ordenador, y dicha operación se realizó con la presencia de él mismo, de dos personas de recursos humanos, de un jefe de unidad, de una compañera y de un miembro de la sección sindical.

Ilustrativa, a estos efectos, es también la Sentencia del Tribunal Superior de Justicia de la Rioja de 11 de noviembre de 2015, que considera procedente el despido disciplinario de una trabajadora que, como coordinadora de la empresa, ordenó a un técnico la instalación de un programa espía mediante el cual se podía acceder desde el ordenador de la actora a los terminales utilizados por los trabajadores y visionar todo cuanto estuvieran haciendo. En orden a impedir que los compañeros se percataran del funcionamiento de este programa se modificó la apariencia del escritorio a una pantalla azul, pues al activarse el mentado mecanismo el fondo de escritorio cambiaba de color.

Igualmente, la Sentencia del Tribunal Superior de Justicia de Cataluña de 16 de junio de 2015 considera procedente el despido de una empleada que había cruzado correos electrónicos con otros compañeros de trabajo, en los que consta como emisora, receptora o como copia, donde hace alusiones a otros trabajadores, al administrador y al dueño de la empresa con un lenguaje soez, insultos y graves ofensas contra su honor. La Sala considera que aunque estos

⁹⁰ FERRANDO GARCÍA, F.M.: “Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 399, 2016, pág. 59.

⁹¹ Sentencia del Tribunal Superior de Justicia Madrid 19 diciembre 2012 (TOL 3.007.536).

correos no fueron difundidos ni se les dio publicidad, no pueden considerarse privados, máxime cuando la empresa de forma clara ha impartido instrucciones indicando que el ordenador y el correo solo pueden utilizarse para fines laborales, reservándose además el derecho a revisarlos.

En este mismo sentido, la Sentencia del Tribunal Superior de Justicia de Cataluña de 13 de junio de 2016 considera procedente el despido, por transgresión de la buena fe contractual, de una trabajadora que, teniendo despacho propio en la empresa, con un equipo informático general y siendo responsable del departamento de limpieza, utilizó para fines privados la cuenta de correo electrónico corporativo. Y ello porque la empresa había redactado un protocolo, transmitido a todo el personal, sobre uso de los equipos informáticos, en el que se especificaba que la cuenta de correo electrónico puesta a disposición de cada trabajador por la empresa era para el uso exclusivo de tareas profesionales, pudiendo ser auditada en cualquier momento, y estando prohibida expresamente la utilización de forma abusiva e incontrolada de los recursos telemáticos de la empresa, incluido internet, para actividades que no estuvieran directamente relacionadas con el puesto de trabajo de cada usuario.

Asimismo, la Sentencia del Tribunal Superior de Justicia de Murcia de 29 de marzo de 2017 considera procedente el despido de un trabajador por reenviarse correos electrónicos desde el correo corporativo de la empresa a su dirección de correo electrónico personal con documentos adjuntos que contenían datos personales de los clientes, incumpliendo una prohibición empresarial expresa de usar tal medio fraudulentamente.

En fin, y teniendo en cuenta que la navegación por internet no está amparada por el secreto de las comunicaciones y que, por lo tanto, la facultad de control empresarial es más amplia, si bien no cabe duda que el conocimiento de las visitas de determinados lugares web permite obtener directamente la información sobre aspectos de la vida personal de los trabajadores relacionados con su intimidad, la gama de pronunciamientos al respecto es muy variada, desde los más estrictos a tenor de los cuales cualquier acceso extralaboral supone un quebranto de la buena fe, mientras otros más acertados atienden a la frecuencia o duración de las conexiones. Entre los más próximos en el tiempo, cabe mencionar, a título de ejemplo, la Sentencia del Tribunal Superior de Justicia de Extremadura de 23 de diciembre de 2015 que considera procedente el despido de un profesor que se conectó, a través del ordenador existente en el aula, a una página de internet de alto contenido sexual y pornográfico mientras los estudiantes realizaban un examen, teniendo en cuenta que el sistema de proyección no se había desconectado y las imágenes fueron contempladas por los alumnos.

5.- REDES SOCIALES

Sin duda, las redes sociales (facebook, twenti, twiter, tumbir, flickr, myspace, Ning, Xing, Plaxo, Hi5, Secondlife, Instagram, Lindekin...) brindan un nuevo escenario donde la inmediatez, la transparencia y el concepto de comunidad aportan nuevas oportunidades para las tradicionales formas de comunicación, expresión o divulgación⁹². Por lo que afecta al mundo de las relaciones laborales, se ha dicho que las redes sociales permiten interactuar a los empleados de una manera colaborativa y compartiendo conocimientos con rapidez y transparencia, al tiempo que sirven como un importante medio de captación de trabajadores y como una efectiva herramienta de

⁹² ORTIZ LÓPEZ, P.: “Redes sociales: funcionamiento y tratamiento de información personal”, en AA.VV.: *Derecho y Redes Sociales*, Madrid (Civitas), 2013, pág. 21.

marketing para que las empresas den a conocer sus actividades y novedades⁹³, ideas trasladables a las Administraciones Públicas.

Pese a estas bondades (innovación y desarrollo, gestión de procesos de selección, fomento de networking entre empleados...), el manejo de redes sociales en el ámbito laboral también tiene su lado oscuro, pues respecto de los comentarios o imágenes incorporados a tales instrumentos, los órganos judiciales han venido considerando que pueden justificar decisiones empresariales de dar por terminado el vínculo contractual, bien porque conllevan declaraciones perjudiciales o denigrantes para la empresa, los compañeros o clientes, pues el derecho a la libertad de expresión no ampara el derecho al insulto⁹⁴, bien porque evidencian incumplimientos laborales del propio empleado (fraude en bajas de incapacidad temporal, competencia desleal, sabotaje industrial, utilización de productos de la empresa para fines personales, acosos...) ⁹⁵.

El hallazgo, a menudo casual, de esta información publicada por el propio trabajador o por sus conocidos, puede desencadenar el poder disciplinario, de modo que el carácter público de estos medios resulta determinante a la hora de valorar la legitimidad en la obtención de la prueba por parte del empresario, no entrando en juego la protección del derecho a la intimidad si el propio afectado ha dado a conocer la noticia de forma voluntaria y en un medio accesible con carácter general. Entre los pronunciamientos más relevantes, cabe mencionar, sin ánimo exhaustivo, la Sentencia del Tribunal Superior de Andalucía de 10 de noviembre de 2011, que considera procedente el despido de una empleada de un supermercado que publica en Facebook una serie de fotografías acompañada de otra compañera en la que se muestran con fajos de billetes en forma de abanico delante de la caja fuerte del establecimiento vestidas con el uniforme del supermercado. También, la Sentencia del Tribunal Superior de Justicia de Madrid de 26 de julio de 2016, que considera procedente el despido de un trabajador que publicó en su cuenta de Facebook comentarios ofensivos, de carácter sexual, hacia dos compañeras, que además eran esposas de otros empleados. O, en fin, la Sentencia del Tribunal Superior de Justicia del País Vasco de 26 de octubre de 2010, que considera procedente el despido de un trabajador que, a través de los comentarios vertidos en su página personal de Myspace, pone de manifiesto que estaba saltando en un concierto y que había continuado cantando en la gira de actuación de su grupo musical durante la situación de incapacidad temporal.

Particularmente significativa es la Sentencia de la Sala de lo Contencioso Administrativo del Tribunal Supremo de 21 de abril de 2008⁹⁶, en la que un funcionario fue sancionado con la separación del servicio por realizar una segunda actividad en el sector privado, consistente en dirigir y administrar una sociedad anunciada en diversas redes sociales.

Por otra parte, las redes sociales no sólo van a tener importancia en los procesos de despido o de imposición de sanciones, sino también en los de contratación (*firing and hiring*),

⁹³ TALENS VISCONTI, E.E.: “La libertad de expresión de los representantes de los trabajadores y nuevas tecnologías. Su alcance en las redes sociales”, *Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Pamplona, 2014, pág. 1.

⁹⁴ TALENS VISCONTI, E.E.: “Despido de un trabajador por comentarios contra la empresa vertidos en internet”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 35, 2014 (BIB 2014/2014), pág. 3.

⁹⁵ FERRANDO GARCÍA, F.: “Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 399, 2016, págs. 60 y ss.

⁹⁶ Rec. 5464/2004.

porque en el sector público el reclutamiento debe respetar los principios de mérito y capacidad, a través de una doble vía: la primera responde a su uso como plataforma virtual destinada tanto a la búsqueda y reclutamiento de candidatos como a la evaluación y selección de los mismos; la segunda obedece a su diseño como recurso para la obtención de información de cada candidato: edad, centros de estudio, domicilio, aficiones, creencias religiosas, ideología política, tendencia sexual, afectividad, círculo de amigos, características de la personalidad, imágenes, salud...⁹⁷

Ante esta creciente problemática, que el reconocimiento del “derecho al olvido” en los buscadores de internet no ha podido evitar, cabe señalar la importancia, de nuevo, de la aplicación de los principios de la Ley de Protección de Datos y algunos referentes de Derecho Comparado, pudiendo mencionar cómo entre marzo de 2012 y agosto de 2013, doce Estados en EE.UU aprobaron leyes para la protección del acceso a la contraseña de redes sociales (denominadas “*social media password protection legislation*”), con el objetivo de prohibir a los empresarios la posibilidad de solicitar a candidatos, e incluso a empleados, la clave de acceso a sus cuentas privadas de redes sociales⁹⁸. Especial mención merece la denominada Ley de la Intimidad de las Comunicaciones Electrónicas (*Electronic Communications Privacy Act*) de 1986, que ha evitado una excesiva conflictividad en la Corte Suprema de los Estados Unidos por el control de las comunicaciones electrónicas en el puesto de trabajo⁹⁹. En nuestro país, el Tribunal Supremo, en sentencia de 21 de septiembre de 2015, ha considerado abusiva una cláusula contractual que requiere incorporar el número de móvil y la dirección de correo electrónico del trabajador,

6.-VIGILANCIA AUDITIVA

El control empresarial de las conversaciones telefónicas del trabajador es, en principio, una hipótesis descartada porque se hallan amparadas por el secreto de las comunicaciones (art. 18.3 CE) y el propio derecho a la intimidad (art. 18.1 CE) , y solo mediante autorización judicial es posible una injerencia en las mismas¹⁰⁰. La grabación de una conversación suele ser más sensible para la intimidad que la de una imagen porque las palabras pueden revelar pensamientos y sentimientos internos, permitiendo comprobar fácilmente incumplimientos en el trabajo, adoptar medidas disciplinarias y probarlas en juicio. Sobre la intervención de las llamadas telefónicas efectuadas por el trabajador, existe una jurisprudencia bastante asentada que admite el control de los datos externos de las llamadas realizadas desde el lugar de trabajo (número de destinatario, duración...), si bien no faltan pronunciamientos que ponen en duda esta práctica aparentemente neutra, pues el Tribunal Europeo ha declarado que podría vulnerar el art. 8 de la Convención Europea de Derechos Humanos que protege el derecho al secreto de las comunicaciones¹⁰¹, opinión que ha sido acogida por alguna Sentencia del Tribunal Constitucional¹⁰². A pesar de ello, la

⁹⁷ LLORENS ESPADA, J.: “El uso de facebook en los procesos de selección de personal y la protección de los derechos de los candidatos”, *Revista de Derecho Social*, núm. 68, 2014, págs. 53 y ss.

⁹⁸ BEL ANTAKI, J.: “Redes sociales y su incidencia jurídico-laboral en los derechos fundamentales del trabajador”, *Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Pamplona, 2014, pág. 14.

⁹⁹ Pudiendo citar únicamente el caso *City of Ontario v. Quon*, decidido en 2010, y el caso *O’Connor v. Ortega*, decidido en 1987, comentados por VIZCAINO RAMOS, I.: “La jurisprudencia de la Corte Suprema de los Estados Unidos sobre el control de ordenadores personales en el puesto de trabajo. Un estudio del caso *City of Ontario v. Quon*”, *Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Pamplona, 2014.

¹⁰⁰ GOÑI SEIN, J.L.: “Intimidad del trabajador y poderes de vigilancia y control empresarial”, cit., pág. 14.

¹⁰¹ Sentencia de 2 de agosto de 1984, caso *Malone versus Reino Unido*.

¹⁰² STCo 34/1996, de 11 de marzo.

doctrina judicial ordinaria es favorable y la admite en el ámbito de las relaciones de trabajo por entender que cumple con el requisito de proporcionalidad, pero limita muy estrictamente la posibilidad de intervenir el contenido de las conversaciones en aras a garantizar el derecho al secreto de las comunicaciones¹⁰³.

Ahora bien, este último veto quiebra cuando la prestación de trabajo consiste precisamente en la atención telefónica (teleoperadores) o cuando se trata del sector de la actividad de telemarketing (promoción de productos a través de llamadas telefónicas) o atención telefónica en servicios públicos, pues --como se ha encargado de reconocer algún pronunciamiento judicial-- la comprobación de los datos externos resulta notoriamente insuficiente en estos casos, teniendo en cuenta que el destinatario es determinado por la empresa, siendo necesario también que la organización productiva conozca el contenido de la conversación no sólo para evitar que se efectúen contactos no permitidos sino también como medio de prueba de las operaciones comerciales realizadas¹⁰⁴.

Por tanto, no todo sistema de escucha de conversaciones es ilícito, sino que a la hora de aplicar el principio de ponderación, el interés de la empresa tiene que ser muy alto para inclinar la balanza en su favor. Así, de nuevo utilizando el ejemplo del sector del telemarketing donde el propio objeto de la prestación del trabajo consiste en conversaciones con los clientes, ha entendido el Tribunal Supremo que si el teléfono se ha puesto a disposición de los trabajadores como exclusiva herramienta de trabajo y éstos conocen que puede ser intervenido por la empresa, no cabe alegar tacha alguna en el proceder empresarial de averiguar el contenido de los diálogos a través de la audiovigilancia¹⁰⁵. Es claro, en casos como éste, que si las conversaciones no pudieran ser auditadas, la prestación de trabajo tampoco podría ser dirigida y vigilada por el empresario, siendo necesario, no obstante, como ha reconocido el Tribunal Europeo de Derechos Humanos, que se avise al trabajador sobre la posible interceptación de las llamadas¹⁰⁶.

Procede aclarar, a la postre, que como ha dejado señalado el Tribunal Constitucional, “quien graba una conversación de otros atenta al derecho reconocido en el art. 18.3 CE, pero “quien graba una conversación con otro no incurre en esa infracción”. Excluye, por tanto, que el derecho al secreto de las comunicaciones pueda oponerse frente a quien tomó parte en esa comunicación¹⁰⁷.

Es más, la injerencia de las conversaciones adquiere también relevancia constitucional desde el punto de vista del art. 18.4 CE, en la medida en que las palabras asociadas a una persona identificada o identificable se consideran extremos personales y la interceptación constituye tratamiento de datos sometida a la normativa de protección de datos. Cabe establecer, no obstante, la siguiente diferenciación: Por un lado, si se trata de meras escuchas telefónicas de conversaciones no grabadas, limitándose al acopio en tiempo real, no existirá fichero y no será

¹⁰³ STCo 114/1984, de 29 de noviembre y STS 10 marzo 1990 (Ar. 2045). En la doctrina judicial menor, STSJ Madrid 9 junio 2004 (JUR 2005, 20495).

¹⁰⁴ STS 5 diciembre 2003 (Ar. 313/2004).

¹⁰⁵ STS 5 diciembre 2003 (RJ 2004/313).

¹⁰⁶ Sentencia de 25 de junio de 1997, asunto 1997/37, caso *Halford*.

¹⁰⁷ SSTCo 175/2000, de 26 de junio y 56/2003, de 24 de marzo. También, STS, Civil, 20 noviembre 2014 (rec. 3402/2012). DÍAZ RODRÍGUEZ, J.M.: “Las grabaciones ocultas realizadas entre empresarios y trabajadores y su utilización como prueba en juicio”, *Trabajo y Derecho*, núm. 6, 2015, págs.. 81 y ss.

necesario la inscripción en el registro de protección de datos, pero el responsable del tratamiento no queda eximido de la obligación de informar a los trabajadores de que las conversaciones pueden ser controladas. Por otro, si las conversaciones quedan grabadas en una cinta, disco duro o cualquier otro soporte que permita localizar los diálogos atendiendo a criterios como el día y hora de grabación, los datos obtenidos se consideran datos de carácter personal, merecedores de todo el sistema garantista establecido en la LOPD, debiendo proceder a crear un fichero, notificado previamente la Agencia Española de Protección de Datos, para su inscripción en el registro, y a informar al trabajador de que sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad de dicho tratamiento, así como la información disponible sobre el origen de la información y las comunicaciones realizadas o previstas en los mismos. En suma, no se permite este tipo de interferencias en las conversaciones de los trabajadores si previamente no se ha cumplido con el deber de información previa.

Por tanto, en el supuesto de sospecha de comportamiento irregular, haya o no concurrido tratamiento de datos, si no ha habido comunicación previa de la posibilidad de control de las conversaciones, la interferencia o se produce con autorización judicial o de lo contrario constituye un ilícito¹⁰⁸.

7.- INSTRUMENTOS DE CONTROL DE ACCESO: TARJETAS, INFRARROJOS, RADIOFRECUENCIA Y CONTROLES BIOMÉTRICOS

El control del acceso y localización del trabajador en la entidad empresarial o Administración Pública, a través de sistemas de fichas, tarjetas electrónicas identificativas, huellas o, incluso, mediante infrarrojos, es considerado lícito cuando obedece a motivos de seguridad -- bien por el tipo de actividad desarrollada por la empresa o bien por el valor de los elementos utilizados en ella-- o "contribuye a comprobar el efectivo cumplimiento de las obligaciones de los trabajadores, obligaciones que se inician en el momento de la puntual incorporación a sus puestos de trabajo y en una estricta observancia de los tiempos de la prestación"¹⁰⁹.

Así, por ejemplo, las tarjetas identificativas permiten al empleado, tras conectarlas o acercarlas a un lector, acceder a ciertas salas, operar con el ordenador, poner en marcha máquinas de trabajo..., facilitando al tiempo el trazo de los movimientos realizados y de su ubicación concreta en cada momento.

Por su parte, las etiquetas de identificación por radiofrecuencia facilitan el procesamiento de datos sin contacto físico ni interacción visible entre el lector o grabador y la etiqueta. No puede extrañar, por tanto, que la Recomendación de la Comisión de las Comunidades Europeas de 12 de mayo de 2009, en su apartado 7º, aconseje que los Estados velen porque los operadores (las empresas) elaboren y publiquen una política de información precisa, concisa, exacta y fácil de comprender del uso de estos sofisticados instrumentos, incluyendo la identidad y el domicilio de los operadores, su finalidad, los extremos procesados y un resumen de la evaluación del impacto sobre la intimidad y las medidas para reducirlo. Es más, la Agencia de Protección de Datos recomienda, en su Guía sobre Seguridad y Privacidad de la Tecnología RFID, informar a los trabajadores sobre la existencia del tratamiento de forma clara y accesible, indicando la

¹⁰⁸ GOÑI SEIN, J.L.: "Intimidad del trabajador y poderes de vigilancia y control empresarial", cit., pág. 55.

¹⁰⁹ STSJ, Cont-Admtivo, Cantabria 21 febrero 2003 (Jur. 122751).

localización de las etiquetas, la existencia de lectores, su posible monitorización y el modo de desactivación.

Las nuevas tecnologías habilitan, incluso, para que el control del acceso a las dependencias empresariales y del horario de trabajo se realice a través de anillos inteligentes o de sistemas biométricos, que pueden ser de dos tipos: por una parte, los que permiten el análisis de aspectos físicos y morfológicos de la persona, a través de la comprobación de las huellas dactilares, la verificación de los patrones de la mano, el reconocimiento facial, la geometría del iris, los rasgos de la voz o las características de la retina; por otra, los que facilitan la valoración de los comportamientos de una persona, mediante la comprobación de su escritura, su firma o la presión de las teclas del ordenador. La principal ventaja de estos mecanismos radica en que no permiten la suplantación del sujeto sometido a la vigilancia, a diferencia de las tarjetas de identificación tradicionales que admitían la transferibilidad¹¹⁰.

En el entorno laboral, estos sistemas biométricos de reconocimiento resultan muy útiles para el control del acceso físico a instalaciones; en particular, lugares críticos como centrales energéticas o sensibles o de acceso restringido. Sirven también para ejercer el tradicional control horario y de presencia de los trabajadores, ya sea para evaluar los momentos de entrada y salida, ya sea para calcular el tiempo dedicado por los trabajadores a la actividad profesional, lo que se revela particularmente útil en empresas con horario flexible o con jornadas irregulares. Y son, asimismo, una solución idónea para garantizar el acceso a los equipos técnicos, a través de lectores de huellas o detectores de la mirada como alternativa más segura que las claves de acceso¹¹¹.

Con mayor detalle, en todo proceso de reconocimiento biométrico se pueden diferenciar dos fases: una, la de inscripción o alistamiento de muestras biológicas, que consiste en la captación por medio de un sensor específico para cada tipo de técnica biométrica, de una serie de rasgos específicos del usuario, y en la transformación de esos datos en una secuencia numérica conformándose una plantilla, que queda registrada en una base de datos; otra, la de comparación, en la que se vuelve a recoger una muestra biométrica y la huella así obtenida se compara con la plantilla almacenada, al objeto de comprobar la equivalencia¹¹².

Precisamente, la primera fase de recogida y tratamiento de los datos biométricos puede poner en peligro los derechos fundamentales de los trabajadores al suponer riesgos para la vida privada, no en vano --y como mero ejemplo-- el iris puede revelar el consumo de drogas y de alcohol o el padecimiento de enfermedades como hipertensión o diabetes. De ahí que la doctrina judicial venga aplicando el juicio de proporcionalidad para valorar la licitud de la decisión empresarial de instalación de estas técnicas. En consecuencia, cabe entender permitido su uso si es el único medio que puede cumplir con la finalidad asignada, es decir, no existe otro menos gravoso con el que cubrir las necesidades empresariales, y se trata de un cauce imprescindible¹¹³. Todo ello sin olvidar que los datos biométricos son datos personales a la luz de la LOPD, debiendo aplicar todos los principios de tutela que esta Ley establece, entre

¹¹⁰ POQUET CATALÁ, R.: *El actual poder de dirección y control del empresario*, Pamplona (Aranzadi), pág. 282.

¹¹¹ GOÑI SEIN, J.L.: "Intimidad del trabajador y poderes de vigilancia y control empresarial", cit., pág. 61.

¹¹² POQUET CATALÁ, R.: *El actual poder de dirección y control del empresario*, cit., pág. 285.

¹¹³ STSJ Murcia 25 enero 2010 (rec. 1107/2009).

los cuales se encuentra la obligación de informar a los afectados y la notificación del fichero a la Agencia de Protección de Datos¹¹⁴.

En este contexto, quizá los pronunciamientos judiciales más llamativos son los referidos al citado control biométrico de la mano que permite identificar al trabajador mediante un reconocimiento tridimensional: largo, ancho y espesor. Cuestionada la licitud de semejante método utilizado en una Administración regional como fichaje horario del personal, el Tribunal considera, en primer lugar, que resulta idóneo para conseguir el objetivo propuesto, cual es “lograr un mayor nivel de eficacia en la Administración pública controlando el efectivo cumplimiento de sus obligaciones por parte de los empleados públicos”. Reconoce el órgano judicial que “la existencia de otros posibles sistemas igualmente idóneos para conseguir la referida finalidad no convierte el medio enjuiciado en ilícito, siendo legítimo que la Administración opte, dentro de la legalidad, por aquel cauce que considere más conveniente”. En segundo término, la medida se entiende necesaria debido al “notorio carácter imperfecto de los sistemas de control más comúnmente usados”, que no impiden “la sustituibilidad en su cumplimiento”. Finalmente, se concluye que la implantación supone más ventajas para el interés general que perjuicios sobre otros valores en conflicto, porque de esta forma se garantiza que el empleado público cumplirá debidamente sus obligaciones y ello redundará en una mayor eficiencia de la Administración para la consecución de los intereses generales¹¹⁵.

Atendiendo a este razonamiento, muy cuestionable resulta, sin embargo, la implantación de chips subcutáneos entre el dedo índice y el pulgar por la que han optado algunas compañías belgas, pues no sólo puede atentar frente a la privacidad del trabajador sino también causar efectos nocivos para la salud física.

8.- GEOLOCACIÓN

Lógicamente, un cierto control extramuros del centro de trabajo podrá realizar el empresario cuando la prestación se realice fuera de él a través de los sistemas de geolocalización. A estos efectos hay que tener en cuenta que hasta la aparición de los sistemas GPS, las empresas del sector del transporte por carretera sólo podían vigilar diariamente las circunstancias de la circulación de sus vehículos, en cuanto a las horas de arranque, parada, duración de los desplazamientos y velocidad, mediante un tacógrafo. Tal dispositivo corresponde a una obligación impuesta por el Real Decreto 640/2007, de 18 de mayo, por el que se establecen excepciones a la obligatoriedad de las normas sobre tiempos de conducción y descanso y el uso del tacógrafo en el transporte por carretera. Dicho mecanismo carece de capacidad para mostrar en todo momento la posición del vehículo ni las específicas rutas seguidas, por lo que su colisión con el derecho a la intimidad del trabajador se considera mínima, debiendo el empresario conservar las hojas de registro durante un año y facilitar copia a los trabajadores que así lo soliciten¹¹⁶.

Más problemas plantean, sin duda, los modernos medios de “teletrack”, que permiten conectar varios vehículos pertenecientes a la misma empresa, o de “geolocalización, mediante un

¹¹⁴ STS, Cont-Admto, 2 julio 2007 (rec. 5017/2003).

¹¹⁵ SSTSJ, Contencioso-Administrativo, 10 enero 2003 (RJCA 5 y 528) y 14 y 29 marzo 2003 (JUR 136789 y RJCA 742).

¹¹⁶ FERNÁNDEZ GARCÍA, A.: “Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial”, *Aranzadi Social*, núm. 17, 2010, pág. 97.

microchip”, capaces de identificar unívocamente al trabajador sin necesidad, en muchos casos, de batería ni fuente de alimentación¹¹⁷.

La Agencia de Protección de Datos en su Informe 193/2008 establece que los extremos obtenidos a través del sistema de geolocalización (rutas seguidas, tiempos de parada, velocidad, consumo de combustible del vehículo, etc.) están asociados a información concerniente a una persona física identificada o identificable a través de los lugares que frecuenta, por lo que según el art. 3 a) LOPD se consideran datos de carácter personal, merecedores de todo el sistema garantista previsto en esta Ley. Por tal motivo, en vía judicial, además de cumplir el principio de proporcionalidad, el control mediante GPS “totalmente camuflado”, “con difícil acceso” y “sin advertencia a los trabajadores de su instalación” se ha calificado como una infracción de la buena fe empresarial porque no respeta el deber de información¹¹⁸.

En esta misma línea, algún pronunciamiento judicial considera que efectivamente queda afectado el derecho a la intimidad del trabajador si el empresario utiliza un sistema de control del trabajo de sus empleados que se desarrolla fuera de sus dependencias a través de un sistema de localización permanente del teléfono móvil facilitado como instrumento de trabajo, sin consentimiento ni conocimiento de los trabajadores, máxime si éstos han de tenerlo a su disposición en todo momento por estar sujetos a disponibilidad permanente, ya que si bien resulta un medio idóneo para controlar su labor, en modo alguno resulta necesario a este fin¹¹⁹. Ejemplo paradigmático puede encontrarse en un pronunciamiento judicial que ha considerado factor de riesgo la instalación de un dispositivo denominado “acelerómetro” en cada uno de los teléfonos móviles de los trabajadores con un componente micro-electromecánico cuya función es captar los movimientos bajo el pretexto de servir a un protocolo de actuación ante un posible accidente¹²⁰.

No faltan, sin embargo, sentencias más permisivas de conformidad con las cuales --y en paradigmático ejemplo-- un sistema de control de movimientos mediante GPS instalado en el vehículo de la empresa utilizado por el trabajador en sus desplazamientos puede ser considerado lícito, pues no existe otro mecanismo eficaz para verificar el cumplimiento de la prestación laboral al realizarse ésta fuera del lugar de trabajo, máxime si se tiene en cuenta que mediante un dispositivo de esta naturaleza se obtiene exclusivamente información sobre la localización del vehículo y no se graban imágenes ni sonido¹²¹, interpretación extensible a los mecanismos GMS incorporados a los teléfonos móviles. Queda acogida, así, una preocupante doctrina que ya había sido utilizada con relativa frecuencia en cuanto hacía al control del empleado fuera del puesto a través de medios tradicionales, como solía ser mediante la contratación de un detective privado

¹¹⁷ GARCÍA COCA, O.: “Nuevas tecnologías y sistemas de control de acceso al centro de trabajo: confrontación con el derecho fundamental a la protección de datos de carácter personal”, en AA.VV.: *Comunicación presentada al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Pamplona, 2014, pág. 6.

¹¹⁸ SSTSJ Madrid 13 octubre 2010 (AS 2930) y 29 septiembre 2014 (rec. 1993/2013) ó Castilla-La Mancha 17 junio 2014 (rec. 1162/2013).

¹¹⁹ STSJ País Vasco 2 julio 2007 JUR 365564).

¹²⁰ STSJ Cataluña 23 mayo 2013 (rec. 6212/2012).

¹²¹ Sentencia del Juzgado de lo Social, núm. 32, Madrid 1 octubre 2003, citada por SAN PEDRO GULLÓN, V.: “Facultades empresariales de vigilancia y control en el centro de trabajo”, *Tribuna Social*, núm. 160, 2004, pág. 20. En el mismo sentido, SSTSJ Madrid 28 diciembre 2004 (AS 2302), La Rioja 26 septiembre 2006 (AS 280), Andalucía 20 junio 2007 (AS 1089), Castilla-La Mancha 28 mayo 2009 (AS 463) ó 5 marzo 2012 (rec. 5194/2011). En la doctrina, PÉREZ DEL PRADO, D.: “¿Puede el empresario controlar a sus trabajadores mediante dispositivos GPS? Algunas notas sobre el cómo, el dónde y el por qué”, *Información Laboral. Jurisprudencia*, núm. 10, 2009, págs. 2 y ss.

encargado de vigilar al operario, admitida cuando existe una sospecha fundada de incumplimiento, exigiendo que no haya posibilidad de acudir a otro medio de control más adecuado, se desarrolle en lugares observables por el ojo humano desde sitios públicos y sea ponderada o equilibrada¹²².

En todo caso, de lo que no cabe duda es queda excluido el seguimiento permanente o ilimitado, debiendo existir algún mecanismo que permita desactivar el sistema fuera de las horas de trabajo, pues la geolocalización no debe servir para prolongar la subordinación del trabajador más allá del límite temporal determinado por la prestación pactada y tampoco repercutir los datos obtenidos fuera del tiempo de trabajo en el ámbito contractual¹²³.

9.- ALGUNOS PRESUPUESTOS DE VALIDEZ EN EL CONTROL

Los dispositivos electrónicos, digitales y visuales no sólo son instrumentos verificadores del cumplimiento laboral, sino que son también magníficos medios de prueba, que permiten acreditar el incumplimiento de sus obligaciones laborales por el trabajador en el proceso laboral, siendo claros los términos del art. 90.2 Ley 36/2011, de 10 de octubre, reguladora de la Jurisdicción Social (LRJS), al fijar un límite infranqueable, cual es el respeto a los derechos fundamentales y libertades públicas, señalando que no se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan vulneración de tales postulados¹²⁴, lo cual puede conducir a la inadmisión o, en su caso, a su no valoración en el juicio si en su momento fue admitida de forma provisional¹²⁵. Por su parte, el art. 60.4 Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa (LRJCA), establece que “la prueba se desarrollará con arreglo a las normas generales establecidas para el proceso civil”, de modo que resulta de aplicación el art. 287 LEC que alude a la ilicitud de la prueba por vulneración de derechos fundamentales, idea que reitera el art. 78.17 LRJCA para el procedimiento abreviado.

La dificultad estriba aquí en dilucidar cuando la prueba obtenida a través de medios tecnológicos es respetuosa con los derechos fundamentales (inespecíficos) de los trabajadores sin que exista una guía o referente claro, más allá de unas meras pautas no del todo sólidas¹²⁶: 1) La existencia de unas reglas empresariales sobre el uso de los medios informáticos y el conocimiento de tales reglas por los trabajadores se convierte en el primer y principal requisito para legitimar el registro y evitar el riesgo de la vulneración del derecho a la intimidad y del secreto

¹²² DÍAZ RODRÍGUEZ, J.M.: “Detectives en el ámbito laboral: poder empresarial y prueba judicial”, *Actualidad Laboral*, núm. 7, 2001, págs. 800 y ss. ó SALCEDO BELTRÁN, C.: “Intervención de detectives en las relaciones laborales”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 368, 2013, págs. 213 y ss. En la doctrina judicial, entre muchas, SSTs 19 julio 1989 (Ar. 5878), 11 junio 1990 (Ar. 5049), 17 junio 1996 (Ar. 5166) ó 21 junio 2012 (rec. 2194/2011); asimismo, Sentencias del Tribunal Superior de Justicia Galicia 16 marzo 1993 (Ar. 1356), Castilla-La Mancha 28 marzo 1996 (Ar. 1939), Navarra 3 octubre 2008 (rec. 238/2008), Madrid 5 noviembre 2010 (AS 3121), Cataluña 5 marzo 2012 (núm. 1706/2012) y Andalucía/Granada 24 mayo 2012 (rec. 738/2012).

¹²³ GOERLICH PESET, J.M.: “Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas”, en AA.VV.: *El derecho a la privacidad en el nuevo entorno tecnológico. XX Jornadas de la Asociación del Letrados del Tribunal Constitucional, Tribunal Constitucional y Centro de Estudios Constitucionales*, Madrid, 2016, págs.. 135-136.

¹²⁴ LOUSADA AROCHENA, J.F.: “La Ley de Jurisdicción Social: una primera aproximación”, *Actualidad Laboral*, nº 21, 2011, pág. 27.

¹²⁵ LOUSADA AROCHENA, J.F.: “La prueba ilícita en el proceso laboral”, *Aranzadi Social*, nº 11, 2006, pág. 110.

¹²⁶ TASCÓN LÓPEZ, R.: “Tecnovigilancia empresarial y derechos de los trabajadores”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, nº 415, 2017, págs. 87 y ss., autor a quien se sigue en la presente exposición.

de las comunicaciones. Nada impide la confección de estos protocolos en las Administraciones Públicas, no en vano el art. 54.3 EBEP deja claro que los empleados públicos “obedecerán las instrucciones y órdenes profesionales de los superiores”. 2) Cuando la empresa guarda silencio y no adopta expresamente una decisión o instrucción sobre el uso y control de los medios laborales tecnológicos, se entiende que el trabajador adquiere una “expectativa razonable de intimidad” y, en consecuencia, puede disfrutar de un “uso social” de los instrumentos y herramientas laborales, sin que el empresario pueda, en consecuencia, pasar de la tolerancia a la sanción, de forma abrupta e imprevista. 3) Esta “expectativa de intimidad” puede ser limitada no sólo a través de una instrumentación o reglamentación clara y concreta de las prohibiciones totales o parciales de uso o sino de una previsión en convenio colectivo, aunque sea en el apartado relativo a las infracciones y sanciones. 4) Aunque hayan quedado fijadas reglas de actuación del trabajador en el manejo de las herramientas tecnológicas, el establecimiento de un ulterior control a través de un sistema permanente de supervisión queda condicionado a la observancia de dos obligaciones. De un lado, proporcionar la debida información, tanto a los representantes de los trabajadores de la instalación de la medida de control (art. 64.1.3 ET), como al trabajador afectado sobre la recogida de datos (imágenes, sonidos, archivos...), así como sobre su finalidad (de control de la actividad laboral y medio de prueba para la acreditación de los ilícitos laborales que justifique la adopción de hipotéticas futuras sanciones); ahora bien, la no observancia de estos requisitos no tiene por qué tener relevancia constitucional, pues lo importante es que el trabajador haya sido informado siquiera de una forma tan genérica como a través de un distintivo de videovigilancia o por resultar de general conocimiento en la empresa. De otro, el respeto al principio de proporcionalidad, pues tal doctrina no puede entenderse derogada como referente en la valoración de las posibles lesiones de derechos fundamentales a través del control empresarial, si bien ha de ser reubicada como un criterio de cierre del sistema, es decir, establecidas las reglas de uso e informada la adopción de la medida de control, la misma ha de ser razonable y no puede resultar abusiva o desproporcionada (sobre todo si la información al trabajador ha sido escasa o defectuosa), pues en tal caso desde luego merecería reproche jurídico. 5) En fin, si el empresario no pretende una instalación permanente *ad futurum* de un sistema de vigilancia en la organización productiva, sino un control puntual y esporádico basado en una “desconfianza” o “razonable sospecha” de un incumplimiento laboral (actividades delictivas o dolosas), puede obviarse la regla de información y proceder a confeccionar la prueba con mayor opacidad (control oculto), en lo que se denomina “el principio de intervención indiciaria”¹²⁷.

En cualquier caso, a la espera de que el legislador asuma el papel protagonista, de manera conjunta a la función complementaria de la autorregulación de las partes implicadas, la inutilidad de una prueba ilegal es, en definitiva, doble: ni se debe admitir la práctica de dicha prueba (decisión judicial de inadmisión), ni se deben aceptar por el juez sus resultados fácticos en el caso de haberse practicado dentro o fuera del proceso (decisión judicial de exclusión de sus resultados a la hora de su valoración)¹²⁸.

10.- EL PREOCUPANTE FENÓMENO DEL TECNO-ESTRÉS

La delgada y vulnerable línea de la salud mental, tan amenazada en la civilización moderna, queda especialmente sometida al riesgo no sólo en situaciones límite sino también

¹²⁷ MORALES VALLEZ, C.E.: “El control de los medios tecnológicos por el empresario a la luz de la sentencia del TEDH de 12 de enero de 2016”, *CEF.-Laboral Social*, febrero 2016, www.laboral-social.com

¹²⁸ DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo*, cit., pág. 144.

en contextos más cotidianos singularmente propicios para ponerla en peligro, tal y como sucede con el trabajo en el sector público, paradigmático contexto de exposición, teniendo en cuenta la necesidad de trabajar con TICs ante las nuevas exigencias legislativas relacionadas con la Administración electrónica y las obligaciones de transparencia, acompañadas de circunstancias más clásicas que no han sido erradicadas como la ambigüedad de las relaciones de puestos de trabajo, la generalización de ineficaces mecanismos de promoción, la continuidad de estructuras organizativas marcadamente rígidas y burocratizadas, la ausencia de mecanismos eficaces de resolución de conflictos interpersonales, la falta de reglas claras sobre asignación de tareas, la carencia de formación cualificada por los costes que conlleva, el deficiente reconocimiento de la labor bien hecha, etc.¹²⁹.

10.1.- Los denominados entornos administrativos “cibercientíficos” como caldo de cultivo óptimo para el surgimiento de dolencias psicosociales

Las nuevas formas de actividad en los modelos de industria 4.0 o en los sistemas cibercientíficos a los que no son ajenas las Administraciones Públicas, intensivas en el uso de tecnologías de la información y comunicación (TICs) y de otros adelantos (robótica, microelectrónica, virtualización, optométrica...)¹³⁰, aun cuando presentan innumerables ventajas para la eficacia y la eficiencia en la prestación de servicios públicos y provocan acusados progresos en la reducción de la toxicidad y penosidad de los puestos, no dejan de integrar el entramado adecuado para el surgimiento de dolencias psicosociales, acrecentado por un cuádruple cúmulo de circunstancias: primera, una amenaza constante de destrucción de empleos públicos ante el desempeño por robots de gran parte de las tareas o del posible acceso indirecto a bienes y servicios dado el generalizado contexto de privatizaciones, circunstancias capaces de justificar despidos colectivos u otras medidas de reestructuración de efectivos; segunda, una monotonía provocada por el empobrecimiento de las tareas al reducir las habilidades y capacidades exigidas; tercera, un requerimiento excesivamente exigente en relación con las aptitudes del empleado sobre todo como consecuencia de la Administración digital, que pueden justificar una inadaptación al puesto de trabajo o una disminución sustancial del rendimiento, causas de despidos objetivos o de otras medidas de ajuste si se trata de funcionarios; en fin, y no menos importante pero ya conocida, una implementación de sistemas de control de la actividad laboral excesivamente rigurosos o exhaustivos, bien dentro de la Administración, bien a distancia, llegando a alcanzar incluso a conductas extralaborales, no en vano los códigos de espacio y tiempo van a quedar difuminados, sobre todo tras las exigencias de la Ley de Transparencia.

La manifestación principal de todas estas realidades radica en que el empleado público deviene atrapado en el proceso productivo en el sentido más amplio del término, sumido en un continuo esfuerzo adaptativo y severamente vigilado, con el perjuicio para la separación entre la vida profesional y la privada¹³¹, circunstancias capaces de provocar no sólo, como ya se ha visto, atentados a sus derechos fundamentales sino también severas patologías emocionales o

¹²⁹ RIVAS VALLEJO, P.: *La prevención de los riesgos laborales de carácter psicosocial*, Granada (Comares), 2009, pág. XIII.

¹³⁰ Tras la automatización de la industria en los siglos XVIII y XIX (considerada industria 1.0), la división del trabajo y la producción en cadena de principios del siglo XX (industria 2.0), y la revolución tecnológica de finales del siglo pasado (industria 3.0), la nueva se basa en la digitalización de la economía.

¹³¹ GOERLICH PESET, J.M.: “¿Repensar el Derecho del Trabajo? Cambios tecnológicos y empleo”, *Gaceta Sindical*, núm. 27, 2016, pág. 181.

cognitivas asociadas al “tecnoestrés”¹³² en sus distintas manifestaciones (“tecnofobia”, “tecnoansiedad” o “tecnofatiga”, “tecnofilia” o “tecnoadicción”)¹³³.

Desde tal perspectiva, la premisa de partida se presenta obvia: tan peligrosa es su inamovilidad cognitiva o cualitativa como su instalación en una inercia frenética de cambio y ajuste funcional permanente¹³⁴, sin olvidar un claro efecto inherente de “despersonalización”. Sin lugar a dudas los métodos corporativos, anclados en una concepción desconocedora del valor del capital humano, y centrados exclusivamente en una “dirección por resultados” (“*results magnaging*”)¹³⁵, convierten el ambiente de trabajo en un espacio hostil y deshumanizado capaz de generar patologías sociolaborales asociadas al estrés, provocando enfermedades mentales y neuronales por mucho que se establezcan reparadoras compensaciones económicas a favor de quienes las sufren¹³⁶.

La tensión que todo trabajo supone, normalmente genera un cansancio que suele (o debería) eliminarse tras un adecuado descanso¹³⁷. Ahora bien, cuando la exigencia profesional es constante la fatiga llega a cronificarse, el sujeto ve alterada su eficiencia funcional y comienzan a manifestarse síntomas que, a la larga, afectan de manera drástica a la salud y estabilidad de los afectados (pérdidas de concentración, memoria, debilidad general, merma de la capacidad de resistencia, falta de sueño, dolores musculares y articulares, problemas gastrointestinales y cardiovasculares...)¹³⁸, llevando, incluso, al consumo compulsivo de fármacos. Es más, y en ocasiones, el abuso de estos medicamentos termina en auténticas adicciones a ansiolíticos y antidepresivos y en hábitos tóxicos, tales como el exceso de café, alcohol, tabaco y otro tipo de drogas¹³⁹. Las consecuencias surgen, a su vez, con claridad meridiana: mayor siniestralidad, absentismo, presentismo laboral con escasos resultados, conflictos interpersonales y baja productividad¹⁴⁰.

No existe previsión alguna en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (LPRL), de aplicación también en las Administraciones Públicas, que alerte sobre las sensaciones no placenteras o negativas que puede sufrir el trabajador sometido a

¹³² Como ejemplo paradigmático, cabe mencionar la STSJ Madrid 6 julio 2016 (EDJ 6895), que reconoce una incapacidad permanente absoluta a un ingeniero de telecomunicaciones con alergia al wifi, pues esta afección le impide trabajar en entornos con campos electromagnéticos.

¹³³ ALFARO DE PRADO SAGRERA, A.: “Estrés tecnológico: medidas preventivas para potenciar la calidad de vida laboral”, *Temas Laborales*, núm. 102, 2009, pág. 125.

¹³⁴ ALEMÁN PÁEZ, F.: “El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi travail n° 2016-1088”, en prensa, pág. 6.

¹³⁵ ODIORNE, G.S.: *El lado humano de la dirección*, Madrid (Díaz de Santos), 1989, págs. 52 y ss.

¹³⁶ DOUGLAS, M.E. y DOUGLAS, D.N.: *El management del tiempo en el trabajo en equipo*, Barcelona (Paidós), 1997, pág. 125.

¹³⁷ NTP 445: *Carga mental del trabajo: fatiga*, 1997.

¹³⁸ TASCÓN LÓPEZ, R.: “Los riesgos psicosociales en relación con las circunstancias de la actividad (especial atención a determinados sectores de importancia en Castilla y León)”, en AA.VV (ÁLVAREZ CUESTA, H., Dir.): *Aspectos jurídicos de la salud mental de los trabajadores en Castilla y León*, León (Eolas), 2016, págs. 53 y ss.

¹³⁹ MARTÍNEZ SELVA, J.M.: *Estrés laboral. Guía práctica para empresarios y empleados*, Madrid (Pearson), 2004, pág. 36. Con superior detalle, a través del cuestionario “RTT et modes de vie”, AFSA, C. y BISCOUP, P.: “L’evolution des rythmes de travail entre 1995 et 2001: quel impact des 35 heures?”, *Economie et Statistique*, núms. 376-377, 2004, págs. 182-187.

¹⁴⁰ GONZÁLEZ COBALEDA, R.: “Riesgos psicosociales, derechos fundamentales y NTIC: una perspectiva de protección diferente”, *Revista de Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 387, 2015, pág. 41.

una insoportable fatiga cognitiva¹⁴¹ a sistemas punteros de supervisión ante la exigencia de una mayor disponibilidad temporal y dependencia personal hacia el empresario sin límites de horario o de jornada demasiado claros¹⁴², capaz de provocar un agotamiento emocional (*burnout thecnological*), cúmulo de demasiada presión y pocos motivos de satisfacción¹⁴³, sufriendo una especie de síndrome de “*karoshi*”, típico de los empleados japoneses¹⁴⁴.

Así pues, el manejo de los recursos tecnológicos como herramienta de trabajo influye decididamente en el grado de satisfacción laboral¹⁴⁵, pudiendo llegar, en su extremo negativo, a desembocar en auténticas patologías (agrupadas bajo el rótulo de “tecno-estrés”), derivadas, en todo caso, de un claro desajuste ocupacional¹⁴⁶, consecuencia, por un lado, de una demanda excesiva o sobrecarga en el trabajo¹⁴⁷ o de la imposición de un alto ritmo productivo, con presiones para decidir o ejecutar casi de inmediato, acompañadas de la exigencia de mucha concentración o atención sostenida durante largos espacios temporales ante la continua necesidad de adaptación y reciclaje, así como a la difícil desconexión del trabajo¹⁴⁸ o, por otro y en su envés, de la asignación de cometidos monótonos o repetitivos (“the daily grind of work”)¹⁴⁹, capaces, igualmente de generar una situación de fatiga fruto de la ausencia de motivación¹⁵⁰. Todo ello sin olvidar que son importantes los deterioros sufridos en la salud por la utilización de pantallas alfanuméricas o gráficas como instrumento de trabajo (fatiga visual, trastornos posturales y fatiga psicológica), de ahí que se haya promulgado una norma específica preventiva en este contexto de gran incidencia para las Administraciones Públicas (el Real Decreto 448/1997, de 14 de abril)¹⁵¹.

De este modo, con el objetivo de observar lo previsto en el art. 14 LPRL cuando establece que “en cumplimiento del deber de protección, el empresario deberá garantizar la seguridad y la salud de los trabajadores a su servicio en *todos* los aspectos relacionados con el trabajo”, así como en el art. 15.1.g) LPRL cuando determina que, al planificar la prevención, el

¹⁴¹ ESCUDERO MORATALLA, J.F. y POYATOS I MATAS, G.: “Acoso laboral: diversas posibilidades procesales para ejercitar la acción”, *Temas Laborales*, núms. 47-48, 2003, pág. 804.

¹⁴² RODRÍGUEZ PÉREZ, M.C.: “La dimensión de los riesgos psicosociales y el papel de la Inspección de Trabajo en su control y represión”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 323, 2010, pág. 12.

¹⁴³ BRILLHART, P.E.: “Technostress in the workplace. Managing stress in the electronic workplace”, *The Journal of American Academy of Business*, Cambridge, September, vol. 5, Issue 1/2, págs. 302 y ss.

¹⁴⁴ VELÁZQUEZ FERNÁNDEZ, M.: *Impacto laboral del estrés*, Madrid (Lettera), 2005, pág. 27.

¹⁴⁵ NTP 212: *Evaluación de la satisfacción laboral: métodos directos e indirectos*, 1998 (CANTERA LÓPEZ, F.J.)

¹⁴⁶ FRENCH, J.R.P. y CAPLAN, R.D.: “Organizational stress and individual strain”, en AA.VV. (MARROW, A.J., Ed.): *The failure of success*, Nueva York (Amacon), 1973, págs. 30 y ss.

¹⁴⁷ NTP 318: *El estrés: proceso de generación en el ámbito laboral*, 1993 (MARTÍN DAZA, F.); NTP 438: *Prevención del estrés: intervención sobre la organización*, 1997 (MARTÍN DAZA, F. y NOGAREDA CUIXART, C.); NTP 443: *Factores psicosociales: metodología de evaluación*, 1997 (MARTÍN DAZA, F. y PÉREZ BILBAO, J.); NTP 489: *Violencia en el lugar de trabajo*, 1998 (PÉREZ BILBAO, J. y NOGAREDA CUIXART, C.); NTP 604: *Riesgo psicosocial: el modelo demanda-control-apoyo social (II)*, 2003 (VEGA MARTÍNEZ, S.) y NTP 704: *Síndrome de estar quemado o ‘burnout’ (I): definición y proceso de generación*, 2006 (FIDALGO VEGA, M.).

¹⁴⁸ NTP 534: *Carga mental: factores*, 1999 (DE ARQUER, M.I.) o NTP 703: *El método COPSQ (ISTAS 21, PSQCAT 21) de evaluación de riesgos psicosociales*, 2006 (MONCADA I LLUÍS, S.; LLORENS SERRANO, C.; KRISTENSEN, S. Y VEGA MARTÍNEZ, S.).

¹⁴⁹ Un estudio acabado en SEMMER, N.K.: “Individual differences, work stress”, en AA.VV (SCHRABRACQ, M.J.; WINNUST, J.A.M. y COOPER, C.L., Eds.): *The handbook of work and Health Psychology*, Chichester (John Wiley and Sons), 2003, págs. 83-120.

¹⁵⁰ NTP 604: *Riesgo psicosocial: el modelo demanda-control-apoyo social (II)*, cit.

¹⁵¹ NTP 139: *El trabajo con pantallas de visualización*, 1981 (ROJO BEBERIDE, S. y NOGAREDA CUIXART, C.).

empresario buscará “un conjunto coherente que integre en ella la técnica, la organización del trabajo, las condiciones de trabajo, las relaciones sociales y la influencia de los factores ambientales”, resulta de gran interés realizar un análisis casuístico de los factores desencadenantes de la degradación de la calidad de vida de los trabajadores públicos que sufren teconoestrés con el fin establecer mecanismos para prevenir las consecuencias tanto desde las exigencias de la organización del trabajo como del otorgamiento de los preceptivos períodos de asueto¹⁵², salvaguardando “el derecho constitucional a la protección de la integridad psíquica que exige que se intervenga antes de producirse el daño”¹⁵³

10.2.- El teletrabajo y la sensación de claustrofobia

La combinación entre los avances en la digitalización y en la robotización implica una sustancial absorción de los trabajos directos y rutinarios por las máquinas, lo cual provoca que la presencia continuada del trabajador en el centro de trabajo pierda su sentido, afirmación que cobra plena vigencia en relación con la prestación de servicios públicos, ámbito singularmente adecuado, en muchas de sus competencias, para trabajar a distancia. Característica esencial del teletrabajo, entendido como un modo de organizar la actividad laboral que aligera costes de infraestructura ante el uso intensivo de medios tecnológicamente avanzados (teléfono, fax, correo electrónico, módems, redes de área local, videoconferencia, etc.), reduce gastos en transporte y mejora las posibilidades de conciliación de la vida laboral y familiar, es la de permitir la separación física del trabajador de la oficina central o del centro de producción¹⁵⁴.

Atendiendo a tales ventajas, varias experiencias se han implementado en diversas Administraciones: desde los planes pilotos de la Administración General del Estado de los años 2006 y 2007, pasando por el Decreto del Consell 82/2016, de 8 de julio, de Valencia, la Resolución de 28 de noviembre de 2016, de la Secretaría General de la Junta de Extremadura, la Orden de 5 de septiembre de 2016 de la Xunta de Galicia, el Decreto 92/2012, de 29 de mayo, del País Vasco, el Decreto 36/2013, de 28 de junio, de la Comunidad de Islas Baleares o el Decreto 46/2013, de 5 de diciembre, de la Comunidad Autónoma de la Rioja, para llegar a su más elaborada formulación en la Comunidad de Castilla y León a través del Decreto 9/2011, de 17 de marzo. En la actualidad, en la Generalitat de Catalunya el trabajo a distancia representa el 10% del total y el reto es que en el 2025 esté en el 25%.

Ahora bien, la comunicación rápida y constante del empleado con su superior a través de herramientas de procesamiento electrónico de la información¹⁵⁵, unida al desarrollo de un quehacer profesional que exige pasar largos períodos de tiempo solo, sin contacto ni con compañeros ni con usuarios, se han revelado como una fuente de riesgo para la salud mental, asociado a la depresión y la ansiedad. Es indiferente, por lo demás, que la conexión sea *off line* (la realización de la actividad laboral se lleva a cabo a través de un disco compacto, disquetes, USB u otros medios tecnológicos o mecánicos como correo convencional, dado que no existe conexión telemática directa con la empresa), *on line* (el trabajador debe hacer uso de las telecomunicaciones para recibir, informar, recoger órdenes de trabajo y resultados hacia la

¹⁵² SALANOVA, M.: “Trabajando con tecnologías y afrontando el tecnoestrés: el rol de las creencias de eficacia”, *Revista de Psicología del Trabajo y de las Organizaciones*, Vol. 19, núm. 3, 2003, págs. 225 y ss.

¹⁵³ STCo 170/2007, de 10 de mayo.

¹⁵⁴ AA.VV (SÁNCHEZ IGLESIAS, A.L., Coord.): *Situaciones jurídicas fronterizas con la relación laboral*, Pamplona (Aranzadi), 2016, págs. 234 y ss.

¹⁵⁵ GARCÍA ROMERO, B.: *El teletrabajo*, Pamplona (Aranzadi), 2012, pág. 36.

empresa y viceversa), *one way line* (las tareas se desarrollan con un terminal conectado a un ordenador o sistema central de la empresa donde fluyen los datos), *two way line* (el trabajador desarrolla su actividad con un terminal conectado a una red, permitiendo intercambiar la información con la empresa y con los diferentes ordenadores) e, incluso, “*off shore*” (cuando se desarrolla en uno o varios países distintos de aquél donde se ubica la empresa matriz)¹⁵⁶.

Con cualquiera de estos modelos, la salud neuronal del trabajador puede sufrir graves atentados, pues tanto en el “teletrabajo interactivo” como en el que se desarrolla “sin conexión telemática”, el empleado se encuentra expuesto a estrecha vigilancia, bien directa y en tiempo real, bien diferida, mediante la utilización de determinados programas *in accounting*¹⁵⁷. Al tiempo, la necesidad de rápidas respuestas y las posibilidades de conexión permanente están eliminando todas las fronteras entre lo personal y lo profesional, difuminando las separaciones entre jornada de trabajo y tiempo de descanso ante una necesidad de conectividad permanente¹⁵⁸, lo cual provoca un cierto trastorno compulsivo e involuntario a continuar trabajando, unido a un desinterés general por otro tipo de actividades (*workalcoholism*). Además del sedentarismo que provoca trabajar muchas horas delante de un ordenador, la facilidad de acceder a la comida en cualquier momento de la jornada puede conllevar una marcada “obesidad funcional”¹⁵⁹. Ello sin olvidar que siempre es necesaria una fuerte autodisciplina y motivación para realizar las tareas, palpando además un cierto sentimiento de extrañamiento por distancia, monotonía y aislamiento físico¹⁶⁰, particularmente manifiesto cuando el trabajo se desarrolla en el propio domicilio y no tan patente cuando se lleva a cabo en telecentros, es decir, entramados compartidos por varias empresas normalmente pequeñas y medianas, en los que se utilizan recursos comunes¹⁶¹.

Es importante, sin duda, para evitar estos inconvenientes implementar una política de planificación seria en la gestión de los recursos humanos a medio y largo plazo, que analice las disponibilidades y necesidades de personal en el empleado público, teniendo en cuenta las previsiones de jubilaciones, de forma que las ofertas de empleo centradas en tareas de pertinente cobertura sea la base presupuestaria estable y previsible para garantizar una dimensión adecuada de los servicios públicos, en la que no falte una adecuada dosis de formación de los empleados públicos que asegure su adaptabilidad para dar satisfacción a las nuevas demandas de los ciudadanos fruto de la evolución de la técnica que ha cambiado sustancialmente el diseño de las tareas públicas¹⁶².

¹⁵⁶ POQUET CATALÁ, R.: “Teletrabajo y su definitiva configuración jurídica”, *Revista Trabajo y Seguridad Social (Centro de Estudios Financieros)*, núm. 351, 2012, pág. 147.

¹⁵⁷ PURCALLA BONILLA, M.A. y PRECIADO DOMENECH, C.H.: “Trabajo a distancia vs. Teletrabajo: estado de la cuestión a propósito de la reforma laboral de 2012”, *Actualidad Laboral*, núm. 2, 2013, pág. 217.

¹⁵⁸ Importante es la STSJ Castilla y León 3 febrero 2016 (rec. 2229/2015), que obliga a una empresa a abonar horas extraordinarias a los teletrabajadores, comentada por MIRÓ MORROS, D.: “El control de la jornada y el teletrabajo”, *Aranzadi Instituciones*, BIB 2016/3956.

¹⁵⁹ DE LAS HERAS GARCÍA, M.A.: *El teletrabajo en España: un análisis crítico de normas y prácticas*, Madrid (CEF), 2016, pág. 264.

¹⁶⁰ DÍAZ FRANCO, J.J.: “Psicopatología relacionada con alteraciones por quebrantamiento en la organización del trabajo”, en AA.VV (COLLANTES, M.P. y MARCOS, J.I., Coords.): *La salud mental de los trabajadores*, Madrid (La Ley), 2012, pág. 150.

¹⁶¹ SEMPERE NAVARRO, A.V. y KAHALE CARRILLO, D.T.: *Teletrabajo*, Madrid (Francis Lefebvre), 2013, pág. 28.

¹⁶² SUÁREZ CORUJO, B.: “El fraude en el trabajo de duración determinada en las Administraciones Públicas españolas, según el Tribunal de Justicia de la Unión Europea”, cit., pág. 3.