UNIVERSIDAD DE MURCIA

FACULTAD DE DERECHO

Nuevas tecnologías y relaciones laborales

María Elisa Cuadros Garrido
2017

NUEVAS TECNOLOGÍAS Y RELACIONES LABORALES

Tesis para la colación del grado de Doctora presentada por la Licenciada MARÍA ELISA CUADROS GARRIDO y realizada bajo la dirección de la Dra. Dña. Carmen SÁNCHEZ TRIGUEROS, Profesora Titular de Derecho del Trabajo y de la Seguridad Social de la Universidad de Murcia

A mi padre, Antonio, que me inculcó el amor por el Derecho de los Trabajadores, ese David contra Goliat que me apasiona.

ABREVIATURAS UTILIZADAS

AMETT	Acuerdo Marco Europeo sobre el Teletrabajo
AN	Audiencia Nacional
AS	Aranzadi Social
Art.	Artículo
AA.VV.	Autores varios
BOE	Boletín Oficial del Estado
CC	Código Civil
CCAA	Comunidades Autónomas
CCol	Convenio Colectivo
CE	Constitución Española
CGPJ	Consejo General del Poder Judicial
D	Decreto
DIRCE	Directorio Central de Empresas
DOCE	Diario Oficial de la Comunidad Europea
Ed.	Editorial
ECPA	*Electronic Communications Privacy Act*
ET	Estatuto de los Trabajadores
ETT	Empresa de trabajo temporal
FD	Fundamento de Derecho
INSS	Instituto Nacional de la Seguridad Social
IT	Incapacidad temporal
JS	Juzgado de lo Social
JUR.	Jurisprudencia Aranzadi
L	Ley
LISOS	Ley de Infracciones y Sanciones en el Orden Social
LGSS	Texto Refundido de la Ley General de la Seguridad Social
LO	Ley Orgánica
LOPJ	Ley Orgánica del Poder Judicial
LORTAD	Ley Orgánica Reguladora del Tratamiento Automatizado de Datos

LOPD	Ley Orgánica de Protección de Datos
LPL	Ley de Procedimiento Laboral
LRJS	Ley Reguladora de la Jurisdicción Social
MSCT	Modificación sustancial de condiciones de trabajo
O	Orden
OCDE	Organización para la Cooperación y el Desarrollo Económico
OIT	Organización Internacional del Trabajo
OM	Orden Ministerial
Op. cit.	Obra citada
RD	Real Decreto
RDL	Real Decreto-Ley
RDLeg.	Real Decreto Legislativo
Rec.	Recurso
RJ	Repertorio de Jurisprudencia Aranzadi
Res.	Resolución
RL	Relaciones Laborales
RTSS	Revista de Trabajo y Seguridad Social
S	Sentencia
SMAC	Servicio de Mediación, Arbitraje y Conciliación
SS	Sentencias
TICs	Tecnologías de la Información y la Comunicación
TC	Tribunal Constitucional
TCE	Tratado de la Comunidad Europea
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia
UE	Unión Europea
Vid.	Véase
Vol.	Volumen

ÍNDICE

INTRODUCCIÓN

I. Una sociedad digitalizada

La globalización lo avasalla todo. Se trata de un fenómeno polivalente, aunque marcadamente económico, y caracterizado por la supresión de los obstáculos que tradicionalmente habían venido limitando la circulación del capital[1], se extiende a muchos otros ámbitos[2]. Conlleva una especie de totalitarismo de la cultura, sobre todo anglosajona, que menoscaba la identidad cultural propia de cada país; impone una ideología que determina una subordinación de las instituciones públicas a las demandas del capital[3]. Esa ideología es la que ha acuñado la conocida fórmula: "Menos Estado, más mercado"[4] . Y en otro terreno, derivó en lo que se viene llamando pensamiento único[5].

El proceso de la globalización alcanza un tremendo impulso, merced a la convicción generalizada de que la fusión de la ciencia y la técnica moderna contiene un potencial infinito. De manera que el progreso puede y debe ser continuo e ilimitado. De ahí la surge le premisa de que todo lo que se desea conseguir se puede lograr si se tiene

[1] CAVAS MARTÍNEZ, F.: «Globalización y Relaciones Laborales», *Revista de sociales y de jurídicas*, núm. 3, 2008, pág. 203.

[2] Cabe apuntar asimismo una globalización de la violencia en sus diversas facciones; la terrorista de lamentable actualidad, de la de tráfico de seres humanos, la de conflictos armados, etc.

[3] LAS HERAS, J.: «"United we stand, divided we fall": poder de clase, cadenas globales de valor y estrategias sindicales en el parque de proveedores de Mercedes-Benz Vitoria-Gasteiz», *Lan harremanak: Revista de relaciones laborales,* núm. 35, 2017, pág. 312.

[4] SOTO MAYOR REINA, C. A. «¿Qué es el pensamiento único?», *http://www2.uned.es/ntedu/espanol/master/primero/modulos/tecnologia-y-sociedad/lecdoc.htm*

[5] El concepto de pensamiento único fue descrito por primera vez por el filósofo alemán Arthur Schopenhauer en 1819 como aquel que se sostiene a sí mismo, constituyendo una unidad lógica independiente - por más amplio y complejo que sea - sin tener que hacer referencia a otras componentes.

fe en la tecnociencia, pues gracias a ella "siempre hay algo nuevo y mejor para encontrar" [6].

El signo de los tiempos actuales en la historia de los ciudadanos e instituciones muestra que nunca se ha tenido acceso a tantos y variados datos, y que existen múltiples tecnologías, herramientas y disciplinas científicas, que intentan lidiar con esa enorme cantidad de datos dispersos, de los cuales bien puede decirse que aguardan el momento en que puedan ser explotados[7].

El tratamiento masivo de información surge del uso de la tecnología y también del cambio de hábitos en las interacciones sociales, puesto que los macrodatos[8] aparecen en cada uso tecnológico que se realiza[9]. El término *Big Data*[10] se refiere a sistemas informáticos basados en la acumulación a gran escala de datos y de los procedimientos usados para identificar patrones recurrentes dentro de esos datos. Alude a los sistemas que manejan y se presentan a disposición de determinados usuarios, como grandes conjuntos de datos, salvando los problemas que tienen, entre otros de almacenamiento, de accesos privilegiados, de compartición de recursos, de métodos de búsqueda, de interoperatividad, o de tratamiento técnico, semántico y operativo[11].

---

[6] CELY GALINDO, G.: «Bioética, tecnociencia y proceso de globalización», *Argumentos de razón técnica, Revista española de ciencia, tecnología y sociedad, y filosofía de la tecnología,* núm. 19, 2016, pág. 31.

[7] SERRANO-COBOS, J.: «Big data y analítica web: estudiar las corrientes y pescar en un océano de datos», *Revista científica el profesional de la información*, núm. 6, 2014, pág. 562.

[8] Macrodatos es todo aquello que tiene que ver con grandes volúmenes de información que se mueven o analizan a alta velocidad y que pueden presentar una compleja variabilidad en cuanto a la estructura de su composición. *Vid*. TASCÓN, M.: «Introducción: Big Data. Pasado, presente y futuro», *Telos: cuadernos de información e innovación*, núm. 95, 2013, pág. 48.

[9] LÓPEZ RIVERO, A. J.: «Tratamiento estadístico de Big Data: un cambio de paradigma tecnológico en la utilización de la información», *Cuadernos salmantinos de filosofía*, núm. 42, 2015, pág. 333.

[10] Concepto conocido también como *Datos Masivos* o *Macrodatos,* empleado por primera vez en 1997 en un artículo de los investigadores de la NASA, Michael Cox y David Ellsworth, ambos afirmaron que el alto ritmo de crecimiento de los datos empezaba a ser un problema para los sistemas informáticos de aquel momento, por la incapacidad de los mismos de poder acumular tantos datos.

[11] DÁVARA RODRÍGUEZ, M. A.: *Manual de Derecho Informático*, ed. Aranzadi, 2015, pág. 597.

En definitiva, *Big Data* comprende el desarrollo de sistemas de recopilación, gestión y procesamiento de cantidades enormes de datos que exceden la capacidad del *software* convencional. Esta denominación no se refiere exclusivamente al volumen, sino también a la variedad y a la velocidad con la que estos datos pueden ser cruzados, representados y convertidos en información[12] y es que, tradicionalmente, estos son los principales conceptos agrupados que han definido el *Big Data*, las denominadas "*3 V*"[13]: *volumen* [14], *variedad* [15] y *velocidad* [16].

Todo ello es, pues, consecuencia a su vez del desarrollo del *Internet de las Cosas*[17], es decir, la transmisión de datos entre máquinas de todo tipo, como teléfonos

---

[12] SEGURA VAZQUEZ, A.: «El pastor, el doctor y el Big Data», *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, núm.2, 2014, pág. 249.

[13] La reconocida empresa multinacional estadounidense de tecnología y consultoría IBM, menciona hasta así *6V*, en la actualidad, a las *3V* clásicas añade: *Valor* (la información es relevante para los individuos, instituciones o gobiernos), *Variabilidad* (o Visualización, significa que los sistemas *Big Data* deben disponer del mismo tipo de elasticidad que es requerido en *cloud computing* y otros entornos virtualizados; una visualización interactiva que permita a los usuarios personalizar e interactuar con los resultados. Estas representaciones visuales algunas veces tendrán que ir acompañadas de una breve narrativa para proporcionar contexto y sentido) y *Veracidad* (es necesario validar la corrección o veracidad de gran cantidad de datos que llegan a gran velocidad). *Vid.* SEVILLANO PÉREZ, F.: «Big data», *Revista Economía Industrial*, núm. 395, 2015, pág. 77.

[14] Según las previsiones en 2020 más de 25 mil millones de dispositivos estarán conectados a Internet, acrecentando aún más un volumen de datos que, según los pronósticos, llegará a multiplicarse por 10 en tan solo 6 años. El problema es que el volumen de datos está creciendo a mayor velocidad que los recursos de computación y la capacidad de procesamiento de los procesadores que existen en el mercado.

[15] Alude a la naturaleza de la información a tratar: las soluciones *Big Data* se encargan de datos tanto estructurados (provienen de fuentes de información conocidas y que, por tanto, son fáciles de medir y analizar a través de los sistemas tradicionales), como datos desestructurados que provienen de todas partes y presentan mayor grado de dificultad de análisis y medición: sensores, *posts* o comentarios en redes sociales o blogs, fotos o videos, registros de transacciones comerciales, señal GPS de teléfonos móviles o automóviles, etc.

[16] Se refiere no solo a la alta frecuencia con la que se generan nuevos datos, sino a la necesidad de dar respuesta a la información en tiempo real. Se validan la corrección o veracidad de gran cantidad de datos que llegan a gran velocidad.

[17] "Internet de los objetos" (IoT, por sus siglas en inglés), concepto que nació en el Instituto de Tecnología de Massachusetts. Se trata una revolución en las relaciones entre los objetos y las personas, incluso entre los objetos directamente, que se conectaran entre ellos y con la Red y ofrecerán datos en tiempo real, es la digitalización del mundo físico.

móviles, semáforos y sensores en la ropa. Cuando interactuamos a través del software para aplicaciones, usando el correo electrónico, el *smartphone*, realizando transacciones bancarias online o comentando un estado en las redes sociales, etc., dejamos un rastro digital que el *Big Data* puede procesar significativamente al producirse una confluencia entre medios y datos. Si bien desde esta perspectiva, el dominio sobre el que se opera aparece ligado a los datos personales trazados por interacciones que no tienen por qué ser de carácter íntimo; quizás, podríamos decir que son precisamente los algoritmos los que traducen esas prácticas mundanas a una práctica confesional acerca de gustos, preferencias y deseos.

Se estima que, actualmente, en el mundo se produce una media anual de poco menos de un terabyte[18] por persona y que, a nivel mundial colectivo, se producen cerca de cinco zettabytes[19] de datos por año[20].

Los países, la banca y el sector empresarial no son ajenos a la relevancia que está adquiriendo esta tecnología como herramienta de gestión social a través del tratamiento de la información personal, los ejemplos son de toda índole:

- De acuerdo con las estimaciones de Orbis Research[21], el mercado de tecnologías analíticas predictivas basadas en la Inteligencia Artificial generará 18.500 millones de dólares en 2021[22].
- Con el seguimiento de la información proporcionada por las quejas de sus propios clientes, la empresa Telefónica en el primer semestre de 2016 ha conseguido ahorrar 2,8 millones de euros en su departamento de reclamaciones.[23]

---

[18] Unidad de medida de cantidad de información cuyo símbolo es *TB* y equivale a un millón de bytes. Equivale a unas 300 horas de video o a 3,6 millones de fotografías digitales.

[19] Unidad de medida de cantidad de información cuyo símbolo es *ZB*, procede del latín "*septem*", que significa siete (como *Hepta-*), viene a equivaler a multiplicación por la sexta potencia de 1000. Un zetabyte es un sextillón de bytes (1.000. 000. 000. 000. 000. 000. 000 bytes).

[20] TORRES VARGAS, G. A. y ARIAS DURÁ, R.: «El cómputo ubicuo y su importancia para el cómputo del Internet de las cosas y el big data», *Revista General de Información y Documentación*, núm. 2, 2014, pág. 221.

[21] Empresa multinacional que posee una de las mayores bases de investigación relacionada con el mercado, realiza informes a petición de particulares o instituciones públicas.

[22] BILBAO, N. (23 de agosto de 2016), «SAS y Samsung SDS ofrecerán soluciones de analítica y Big Data en conjunto», *http://www.silicon.es/sas-samsung-sds-ofreceran-soluciones-analitica-big-data-conjunto-2316195#4Ik5bFrFmqP6Itse.99*

[23] SAIZ, L. (2016, 8 de junio) expansión.com, «Conflictos legales del Big Data en las empresas»,

- Cuba ha contratado en mayo de 2016 a una consultora española para saber todo lo que comentan los turistas de todo el mundo en Internet sobre el país después de haber visitado la isla. La información, y sobre todo los comentarios negativos, son procesados por el gobierno cubano para planificar un plan de mejora hotelera[24].
- Un informe encargado por el Gobierno de EEUU en el año 2014, ha concluido que un nuevo poder está emergiendo alrededor del *Big Data*, y señala cómo este está llamado a cambiar la manera en que nos comunicamos, trabajamos y vivimos en un entorno en el que la recolección de datos es cada vez más ubicua, multidimensional y permanente[25].
- En 2010, los empleados de una tienda estadounidense de descuentos recibieron una visita inesperada. Un hombre furioso entró en el establecimiento, a las afueras de Minneapolis y exigió ver al director. "*Mi hija ha recibido esto por correo*", dijo el señor, mostrando unos cupones para ropa de bebé. "*Todavía está en el instituto… ¿acaso intentan animarla a que se quede embarazada*?", espetó. No fue un error: la adolescente iba a tener un hijo. Un patrón de compra y búsqueda en la Web la había delatado[26].

Las tecnologías de la tercera generación permiten penetrar en la "*caja negra*" que constituye el razonamiento propio de cada individuo traicionado por las huellas que ha dejado, pudiéndose establecer así el modo en que cada persona realiza sus operaciones y confecciona conclusiones, incluso, predictivas[27].

Hoy en día, sin duda, la información es poder, por ejemplo, el equipo de campaña

---

http://www.expansion.com/juridico/actualidad-tendencias/2016/06/08/57586331468aebd40c8b46a6.html

[24] economiadigital.com (2016, 29 mayo), «Todos hablan del big data pero nadie sabe lo qué es», *http://www.economiadigital.es/es/notices/2016/05/todos-hablan-de-big-data-pero-nadie-sabe-lo-que-es-y-ya-es-hora-84109.php*

[25] SEGURA VAZQUEZ, A: «El pastor, el doctor y el Big Data», *op.cit*., pág. 249.

[26] La historia real, está relatada por Charles Duhigg en su libro *El poder de los hábitos, vid.* elpais.com (2016, 4 de junio) «"Big data" la nueva materia prima» *http://economia.elpais.com/economia/2016/06/03/actualidad/1464954943_672966.html*

[27] THIBAULT ARANDA, J.: «La vigilancia del uso de Internet en la empresa y la protección de datos personales», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 1, 2009, págs. 215-216.

electoral del Presidente Donald Trump, podía consultar una lista que se autoconfiguraba con base en los parámetros introducidos y que permitía enviar un mensaje a cada persona que se autoidentificaba como republicana, mujer, casada y mayor de 35 años, con más de 500 amigos en *Facebook* para hablar, por ejemplo, del tema "*familia*". Actualmente, por los partidos políticos se busca segmentar[28] lo más y mejor posible para llegar, con el mensaje adecuado, a la mayor parte de población. La información es muy valiosa, y una buena segmentación puede conseguir aprovechar al máximo los esfuerzos humanos y económicos para ganar por ejemplo, unas elecciones[29].

En los últimos tres años se ha generado tanta información como en toda la historia de la humanidad lo que, unido a una capacidad de análisis y de extracción de información personal sin precedentes, puede conllevar graves riesgos para la intimidad de las personas[30]. El trabajo con *Big Data* trae a la luz un problema con un clásico digital: la privacidad. El acceso a los datos críticos de las empresas es cada vez más una necesidad para poder integrar la información de múltiples fuentes de datos, a menudo de terceros, y poder analizarla, pero ese acceso raya en muchas ocasiones la frontera de lo privado[31].

Por esta razón, las nuevas tecnologías y la globalización de la actividad empresarial, van unidas a un especial interés de los titulares por asegurar la tutela de sus bienes inmateriales, en múltiples países o, incluso, a escala global, pues se pretende explotar el elemento inmaterial en cada uno de esos estados, bien de manera directa o a

---

[28] La segmentación se utiliza en las campañas electorales de todo el mundo para adaptar los mensajes del candidato a cada colectivo determinado, con el fin de conseguir una aproximación más efectiva. El objetivo es que el electorado se sienta escuchado y próximo a un partido. La segmentación crea mensajes dirigidos directamente a estos grupos, para así reclutar votantes que, de otra forma, no se hubieran identificado nunca con el candidato o para activar a aquellos que están de acuerdo en una temática concreta pero no tanto en el resto.

[29] PEYTIBI CARBONEL, F. X.: «La segmentación electoral, cuando la información es poder», *Revista Más poder local*, núm. 13, 2012.

[30] AEPD (2014, 30 junio), «El director de la AEPD subraya la importancia de conciliar los beneficios de la tecnología con preservar los derechos y las libertades individuales», *https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/jun_14/140630_NP_Curso_ProteccionDatos_UIMP.pdf*

[31] TASCÓN, M.: «Introducción: Big Data. Pasado, presente y futuro», *op..cit*, pág. 49.

través de acuerdos de licencia[32]. Una información constituye un secreto empresarial, cuando tiene carácter reservado, posee valor competitivo y existe voluntad de mantenerla en secreto por parte de su titular[33].

II. Conductas ilícitas, paralelas y cambiantes

De modo que estamos asistiendo a una evolución de la delincuencia de las nuevas tecnologías que se sofistica y tecnifica a medida y, de manera análoga, a la que lo realiza el medio en el que actúan, así encontramos varias etapas:

- Primera generación de criminalidad; lo característico era la utilización física de ordenadores para la comisión de delitos.
- *Ciberdelincuencia* económica[34]. Posteriormente, comienza una segunda época marcada por el fenómeno de *cibercriminalidad,* cuya nota definitoria es que la conducta típica se comete a través de Internet y los delitos son contra el orden económico o patrimonial. La doctrina califica estos delitos como "informáticos *stricto sensu*" [35], a saber: intrusión en equipos ajenos o *hacking*, revelación de contenidos albergados en programas y archivos informáticos, fraudes *phising*[36], *vishing*[37] y

[32] DE MIGUEL ASENSIO, P. A.: «Derechos de propiedad industrial», *Revista de Derecho Privado de Internet. Estudios y Comentarios Legislativos*, núm.12, 2015 (BIB 2015\12).

[33] MORÓN LERMA, E.: *El secreto de empresa: protección penal y retos que plantea ante las nuevas tecnologías*, ed. Aranzadi, 2002, pág. 50.

[34] VELASCO NUÑEZ, E.: *Delitos cometidos a través de Internet. Cuestiones procesales*, *op. cit*., pág. 42.

[35] URBANO CASTRILLO, E.: «Los delitos informáticos tras la reforma del CP de 2010», *Revista Aranzadi Doctrinal* núm. 9, 2011 (BIB 2010\2465).

[36] De la palabra inglesa "fishing" (pescar) hace alusión al acto de "cazar" usuarios mediante engaños o "anzuelos" con una apariencia amigable para que el usuario crea que provienen de una fuente segura, y de este modo obtener información financiera así como contraseñas.

[37] Proviene de la unión de las dos palabras "voice" (voz) y phising. Para llevar a cabo esta conducta delictiva, los delincuentes hacen uso de una Voz IP o voz automatizada, y llaman aleatoriamente a algunos números, a la persona que contesta se le informa que su tarjeta de crédito está siendo utilizada fraudulentamente por lo cual debe comunicarse con un número específico de su entidad bancaria; o, simplemente se le solicita verificar algunos datos personales llamando a un número telefónico específico.

pharming[38], falsificación informática, y daños a los elementos lógicos del sistema o *cracking*[39]. Este tipo actuaciones delictivas, suponen cerca del 70% de las denuncias por delitos informáticos en nuestro país[40]. A nivel mundial representan un beneficio anual diez veces mayor que el presupuesto de la ONU[41].

- *Ciberdelincuencia* intrusiva[42]. Hoy en día nos encontramos, en la evolución de la tercera generación de delitos informáticos, que se relaciona con el desarrollo de la *Web 2.0* o *Red Social*[43] -conocida también como *Internet de los usuarios o ciudadana*- y la expansión del fenómeno de las redes sociales y de los sistemas de mensajería instantánea, que conlleva a que los delitos en Internet ya no solo afecten al orden patrimonial sino que puedan hacerlo también a otros intereses más personales, como la libertad sexual, el honor o la propia dignidad personal[44].

Cuando la víctima llama al número solicitado, le contesta una grabación pidiéndole la verificación de algunos datos personales o financieros.

[38] Deriva del término inglés "*farm*" (granja), modalidad del delito de estafa en la que el sujeto activo manipula el software de los servidores DNS *(Domain Name System)* o el de los equipos de los propios usuarios, de manera que, cuando el navegante cree estar accediendo a una página *web* de su confianza, en realidad, está siendo redirigido a un destino distinto, normalmente, una página *web* controlada por el atacante. Posteriormente estos datos son utilizados para sustraer dinero a la persona atacada.

[39] Conducta delictiva en la que un individuo denominado *cracker* (aquel que utiliza técnicas de *hacking* con fines criminales o maliciosos) altera, modifica, elimina, borra los datos de un programa informático o de un documento con la finalidad de obtener un beneficio de dicha manipulación.

[40] VELASCO NUÑEZ, E.: *Delitos cometidos a través de Internet. Cuestiones procesales*, *op.cit*., pág. 42.

[41] GARCÍA DE SOLA y VERA, J. M: «Hackers cómo pueden destruir tu vida», *Revista One Magazine Seguridad nacional*, núm. 9, 2014, pág. 55.

[42] VELASCO NUÑEZ, E.: *Delitos cometidos a través de Internet. Cuestiones procesales*, *op. cit*., pág. 43.

[43] Alude a las características de ciertos servicios que han contribuido a la rápida transformación de Internet por el modo de interactuación de los navegantes con la Red (y no solo en esta): blogs y las redes sociales, así como en general los servicios que permiten compartir y difundir contenidos generados por los propios usuarios. *Vid*. DE MIGUEL ASENSIO, P. A.: «Caracterización y organización de Internet: perspectiva jurídica», *Revista de Derecho Privado de Internet. Estudios y Comentarios Legislativos*, núm.7, 2015 (BIB 2015\7).

[44] MIRÓ LLINARES, F.: «Estudios y Comentarios Legislativos La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing», *Revista electrónica de ciencia penal y criminología*, núm.15, 2013, pág. 3.

Los ciberataques constituyen la principal amenaza para ocho de los más importantes países del mundo entre los que se encuentran Estados Unidos, Japón, Alemania, Suiza y Singapur y aparece entre los cinco problemas principales en 27 economías[45]. Un dato que demuestra cómo ha afectado a las empresas de muchos países, se recoge en el Informe *Global Risk World Economic Forum* 2016[46] que apunta que "*los delitos cibernéticos cuestan a la economía mundial aproximadamente 445.000 millones de dólares, lo que supera los ingresos de Chile*"[47]. El mencionado estudio también destaca la importancia de identificar la interconexión entre riesgos para priorizar áreas de acción, el lema escogido fue *La Cuarta Revolución Industrial*[48]. En sus conclusiones aseguraron que todas estas alarmas globales ya están afectando a las vidas de las personas y al funcionamiento de economías e instituciones y urge a la necesidad de actuar y construir *resiliencia*[49] para lograr un mundo mejor para todos.

Es evidente que la tecnología se ha desarrollado a unos pasos mucho más agigantados que los sistemas legislativos pueden contemplar, extremo que beneficia a los ciberdelincuentes, si los ataques cibernéticos no están plenamente regulados por los

---

[45] KMG ESPAÑA (2016, 18 enero), «El mapa de los riesgos mundiales de la próxima década», *http://www.revistavalores.es/davos-ante-los-riesgos-de-la-proxima-decada-clima-inmigracion-y-revolucion tecnologica/?utm_campaign=KPMG+Spain&utm_source=linkedin&utm_content=sf19043822&utm_medium=spredfast&sf19043822=1#.Vuh7TktWtow*

[46] Foro Económico Mundial *http://www.weforum.org/* En su 11ª edición, el Informe Global de Riesgos 2016 llama la atención sobre formas en que las amenazas globales podrían evolucionar e interactuar en la próxima década. Este informe se ha elaborado con la opinión de más de 750 expertos del mundo de los negocios, de las universidades, de la sociedad civil y del sector público sobre los peligros a los que se enfrenta el planeta en los próximos diez años en términos de impacto y de probabilidad.

[47] *http://www.weforum.org/reports/the-global-risks-report-2016*

[48] Lo que los economistas describen como la Industria 4.0 está destinada a ser la 4ª Revolución Industrial; tras la automatización de la industria en el siglo XVIII, la división del trabajo y la producción en cadena de principios del siglo XX, y la revolución tecnológica de finales del siglo XX, ahora estamos hablando de la digitalización de los sistemas de producción que impactará enormemente en las empresas y en la manera en la que la economía afecta a las personas, la sociedad y los países. El Internet de las Cosas/Servicios representa un cambio del proceso de producción centralizado a un proceso de fabricación inteligente, gracias a los avances tecnológicos. Esto tiene la capacidad de conectar todo a una red, que permite recibir información desde muchas fuentes para ser almacenada, transferida, analizada, personalizada o automatizada sin intervención humana.

[49] Proviene del inglés norteamericano *resilience* es un concepto usado inicialmente en el ámbito de la psicología, que significa que el convencimiento que tiene un individuo o equipo en superar los obstáculos de manera exitosa sin pensar en la derrota, a pesar de que los resultados estén en contra, al final, hace surgir un comportamiento ejemplar a destacar en situaciones de incertidumbre con resultados altamente positivos. Esta capacidad de resistencia, se ha trasladado también al lenguaje de ciberseguridad. La resiliencia sólo es posible si se puede prevenir el peligro y para eso hay que utilizar los mismos medios que utilizan los que quieren atacar las organizaciones.

Estados, "*se nada*" en el vacío legal, por lo que a título de *lege ferenda*, parece razonable, por un lado, que exista una regulación adecuada del ciberespacio, ya que ante la ausencia de normativa suficiente al efecto, el individuo es más vulnerable ante una conducta lesiva en el espacio virtual que en el real[50], y por otro lado, sería deseable que existiera una jurisdicción especializada en este tipo de delitos pues los juzgados de instrucción, contemplados aisladamente, por su carácter local, carecen de experiencia, pericia y mecanismos logísticos adecuados para enfrentarse a la compleja dinámica delictiva que dimana de la Red[51].

III. Un mundo productivo digitalizado

Toda esta revolución en actividades tan distintas tiene su correspondiente impacto en el mercado de trabajo, donde aparecen nuevas profesiones como científicos de datos (una conocida consultora calcula que sólo en Estados Unidos se necesitarán entre 140.000 y 190.000 de estos profesionales en 2019), ingenieros de visualización y analistas de negocio 2.0, que son los encargados de traducir toda la información recopilada mediante *Big data* a propuestas concretas de negocio[52].

En el espionaje industrial clásico el único motivo para acceder a las instalaciones de la empresa espiada, era la apropiación de sus secretos, el espionaje en sí mismo, por contra, la superación de las barreras de acceso a un sistema informático, constituía un reto para los *hackers*, cuyo objetivo no era el espionaje, sino el mero acceso a ese sistema[53]. Del romántico *hacker* de los inicios que por motivos de autoestima demostraba que era capaz de entrar en sistemas altamente secularizados (OTAN, NASA, Pentágono, etc.) se

---

[50] LUCENA CID, I.V.: «El concepto de intimidad en los nuevos contextos tecnológicos» en AA. VV. GALÁN MUÑOZ, A. (Dir.): *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación*, ed. Tirant Lo Blanch, 2014, pág. 42.

[51] GUDÍN RODRÍGUEZ- MAGARIÑOS, F.: «La lucha contra el ciberblanqueo como vía para acabar con el phising», *Revista Aranzadi Doctrinal* núm. 9, 2014 (BIB 2014\4287).

[52] LÓPEZ MORALES, T. (2016, 15 marzo) «Cómo el Big Data puede cambiar tu vida» *http://www.expansion.com/actualidadeconomica/analisis/2016/03/15/56e6c83546163fe8598b45b3.html*

[53] SAN MARTIN, D.: «TIC y riesgos en materia de espionaje industrial: hacia un nuevo escenario de amenazas», *Togas. Biz*. núm.71, 2007.

está dejando paso al más experto delincuente que lo único que persigue es apoderarse del dinero ajeno[54].

La materia prima del quehacer *hacker* son los errores y fallos de seguridad del *software*. A modo de símil, podríamos decir que los *hackers* son como "*buscadores de oro baldeando toneladas de lodo, hasta que encuentran las verdaderas pepitas*"[55] que ellos llaman *0-days*[56]. En este caso, no hay más oro que el que voluntariamente o de manera inconsciente entierran las compañías de *software* en sus productos, y que curiosamente nunca se responsabilizan de los efectos que sus errores puedan tener una vez sus productos estén en el mercado[57], lo que podría dar lugar a un ataque *zero-day*[58].

IV. Reacciones supranacionales frente al problema

Y ya adentrándonos en el ámbito laboral, es destacable la Recomendación del Grupo de Trabajo del artículo 29[59], que aconseja que por parte de la empresa se empleen las medidas que resultan de los recursos informáticos para prevenir posibles abusos por parte de los trabajadores, pues considera que la prevención debería prevalecer sobre la detección; es decir, que es mejor para el empleador prevenir la utilización abusiva de Internet [60], en lugar de que *a posteriori* se tengan que tomar medidas disciplinarias tras haberse producido un mal uso de la Red por parte de sus trabajadores.

---

[54] VELASCO NUÑEZ, E.: *Delitos cometidos a través de Internet. Cuestiones procesales,* ed. La Ley, 2010, pág. 45.

[55] Un experto de este tipo puede ganar hasta medio millón de euros por una vulnerabilidad "*zero day*".

[56] Fallo de un programa o sistema informático que nadie conoce, salvo quien lo descubre.

[57] DÁVILA MURO, J.: «Cuando el malware se viste de ciberarma», *Revista SIC ciberseguridad, seguridad de la información y privacidad*, núm. 108, 2014, pág. 92.

[58] Ataque a través de *exploit* o fragmento de *software* que se utiliza con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

[59] En virtud del artículo 29 de la Directiva 95/46/CE, de 24 de octubre de 1995 del Parlamento Europeo y del Consejo, se creó el Grupo de Trabajo del art. 29; órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

[60] Véase las págs. 4-5 y 24 del Documento del grupo de Trabajo de la UE relativo a la Vigilancia de las comunicaciones electrónicas en al lugar de trabajo, aprobado el 29 de mayo de 2002.*http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/B.2.52-cp--wp55---vigilancia-comunicaciones-electr-oo-nicas-trabajadores.pdf*.

En este sentido, el Comité de Ministros del Consejo de Europa, el 1 de abril de 2015, aprobó la Recomendación CM/rec(2015)5[61] relativa al tratamiento de datos personales en el entorno laboral[62], en relación con el uso de Internet por los empleados, advierte que deben prevalecer las medidas preventivas por ejemplo, filtrar las páginas web sobre las de control o monitorización. La Recomendación CM/rec(2015)5 aborda con ánimo marcadamente garantista diversas cuestiones que afectan al tratamiento de datos de los trabajadores. Con clara vocación de garantizar tanto los derechos de los trabajadores individualmente afectados, como de los de sus representantes, la Recomendación dispone la obligación empresarial de informar con anterioridad a la adopción de las medidas de control a las personas afectadas, así como también de consultar a las autoridades nacionales responsables de la protección de datos y a la representación del personal, de acuerdo a la normativa legal y convencional de cada Estado, la medida a adoptar antes de ser puesta en marcha.

V. Prevención de ilícitos laborales

La realidad delictiva evidencia que del empleado negligente (que por su escasa formación llega incluso a enseñar datos privados ajenos sin querer) se ha ido pasando al desleal o resentido que al abandonar la empresa la ataca causándole desperfectos con el único afán de venganza[63].

El hecho cierto es que existen múltiples monografías y artículos sobre las nuevas tecnologías y las relaciones laborales, pero en ellos, apenas, se ha analizado la cuestión de la prevención de posibles conductas abusivas, como previa a la comisión de posibles ilícitos, actuando como la Ley de Prevención de Riesgos Laborales lo hace sobre los accidentes laborales, *a priori* y no *a posteriori*. En esta investigación se va a insistir en este aspecto, al que no se le ha dado la importancia que merece, siendo la prevención en

[61] *https://wcd.coe.int/ViewDoc.jsp?id=2306625*

[62] A la vista de los cambios producidos en el ámbito del empleo debido al creciente uso de las tecnologías de la información y la globalización, y que la anterior Recomendación del Consejo en esta materia databa de 1989, la revisión ya era necesaria.

[63] VELASCO NUÑEZ, E.: *Delitos cometidos a través de Internet. Cuestiones procesales*, *op. cit*., pág. 44.

las tecnologías de la información y la comunicación una cuestión fundamental. En primer lugar, se han de establecer previamente las reglas del juego; antes del inicio de la relación laboral se ha informar de manera suficiente al trabajador de la política de la empresa respecto al uso de las nuevas tecnologías y de los posibles medios de control y finalidad de los mismos, y una vez iniciada la relación laboral, se ha de usar la tecnología informática de manera preventiva, para evitar "fugas de información"[64] durante el transcurso de la relación laboral, y se han de realizar de manera esporádica controles aleatorios para no convertir en tolerancia ciertas prácticas o malos hábitos que pudieran existir (si se prohíbe pero no se controla se puede crear un clima de permisividad).

Determinar previamente las reglas del juego o no hacerlo, enlaza con la reciente doctrina del Tribunal Constitucional: SSTC 241/2012, de 17 de diciembre[65], 29/13, de 11 de febrero[66] y 170/2013, de 7 de octubre[67]. En dicha doctrina, se pone el acento en la importancia de la delimitación previa, como sabemos; consiste en una operación jurídica previa, absolutamente imprescindible que no excluye una posterior ponderación[68], aunque sí delimita su campo de actuación; por tanto, no existirá ponderación cuando el método delimitador revele que no existe conflicto de derechos fundamentales ente los del trabajador y los del empresario. Aunque la promulgación de la STC Pleno 39/2016, de tres de marzo[69], como veremos contradice en parte, la afirmación anterior.

[64] Los incidentes de "pérdida de datos", se convierten en incidentes de "fuga de datos", en los casos en los que en los medios de comunicación de la empresa que contienen información sensible se pierde esta información, y posteriormente, es adquirida por personas no autorizadas.

[65] STC 241/2012, de 17 de diciembre (RTC 2012\241).

[66] STC 29/2013, de 11 de febrero (RTC 2013\29).

[67] STC 170/2013, de 7 de octubre (RTC 2013\170).

[68] La ponderación de intereses en conflicto, es lo que justifica que una vez acreditado el interés empresarial, sea legítimo el sacrificio de un derecho fundamental del trabajador.

[69] STC 39/2016, de 3 marzo (RTC 2016\39).

VI. Un nuevo escenario para el conflicto laboral

La doctrina más autorizada señala con acierto, que el efecto más relevante de las nuevas tecnologías en el ámbito de las relaciones laborales consiste en haber abierto un nuevo escenario conflictivo, en el que las partes siguen siendo los litigantes de siempre, trabajador y empresario, pero la controversia ya no suscita un problema de legalidad o de contractualidad, sino de colisión entre dos categorías de derechos fundamentales[70].

A este escenario conflictivo se puede llegar por dos vías, una, por el control que la empresa realiza del uso de las nuevas tecnologías por parte del trabajador, y otra, por el recurso a los adelantos tecnológicos por parte del empleador para controlar al personal contratado[71].

Y situándonos en esa controversia en la que pugnan dos intereses legítimos pero contradictorios, la doctrina se encuentra en la actualidad dividida por las últimas sentencias del TC y TS, en dos posturas, la primera entiende que la contienda la va ganando el empresario en detrimento de los derechos del trabajador, llegando incluso a hablarse de "desfundamentalización" de los mismos[72] y la segunda que sitúa la cuestión en otro punto, afirmando que no hay avance ni retroceso en la guerra, pues las últimas batallas que han resuelto los tribunales, plantean una cuestión de delimitación y por tanto de falsos conflictos de derechos fundamentales. A lo largo de este estudio se ahondará en el análisis de estas dos tendencias, previa delimitación de los intereses (constitucionales o de legalidad ordinaria) que están en juego, tratando de ofrecer una respuesta clara en un terreno movedizo[73].

---

[70] VALDÉS DAL-RÉ, F.: «Presentación del Seminario Internacional sobre medios de comunicación y control empresarial», *Relaciones Laborales revista crítica de teoría y práctica*, núm. 30, 2009, págs. 1-8.

[71] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, ed. Tirant Lo Blanch, 2015, pág. 37.

[72] CARRASCO DURÁN, M.: «El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa», *Revista Aranzadi Doctrinal* núm. 9, 2014 (BIB 2013\2695).

[73] SEMPERE NAVARRO A.V. y SAN MARTÍN MAZZUCCONI, C., afirman que la situación existente, obliga al Juez al casuismo y aun así el terreno es "*movedizo*", no existen criterios claros lo que

PARTE GENERAL: BASES CONCEPTUALES Y CONTEXTO

I. NUEVAS TECNOLOGÍAS Y RELACIONES LABORALES

1. Automatización, informatización, robotización

La implantación masiva de robots y sistemas automáticos de trabajo en la industria, y progresivamente en el sector servicios, es un rasgo característico de las economías tecnológicas avanzadas.

El sociólogo Ulrich Beck[74], en su obra *La sociedad del riesgo. Hacia una nueva modernidad*[75], expone una noción de la magnitud del aumento de la productividad, que

obliga a apelar al sentido común del órgano judicial. *Vid.* SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI,C.: «¿Puede la empresa controlar el ordenador usado por su trabajador?», *Repertorio de Jurisprudencia* núm. 21, 2007 (BIB 2007\1868).

[74] Sociólogo alemán (15 de mayo de 1944 -1 de enero de 2015), fue profesor de la Universidad de Múnich y de la *London School of Economics*, estudia aspectos como la modernización, los problemas ecológicos, la individualización y la globalización. Contribuyó con nuevos conceptos a la sociología contempóranea, incluyendo la llamada "*sociedad del riesgo*" y la "*segunda modernidad*". Distingue una primera modernización, que discurre a lo largo de la industrialización y la creación de la sociedad de masas; y una segunda modernización, propia de la sociedad actual que tiende a la globalización y está en constante desarrollo tecnológico. En la era industrial la estructura cultural y social era la familia, pero luego ese núcleo se rompió dando lugar a la individualización, aumentándose la incertidumbre del individuo en la sociedad de riesgo. Según su pensamiento, la situación deriva del neoliberalismo económico, y no solo afecta al plano personal, sino que también a las instituciones. Algunos autores critican esta postura por considerarla en exceso alarmista.

[75] En su libro, escrito en 1986, el autor, expuso una serie de cambios que no estaban siendo advertidos por las ciencias sociales y que afectaban notablemente a las nuevas generaciones; tomó un hito simbólico, el desastre de Chernobyl, que usó para explayarse a otra serie de transformaciones.

hace declinar el trabajo masivo y poco cualificado, a favor de las máquinas, y en detrimento humano. En 1950, cada trabajador alemán abastecía con productos industriales a tres consumidores, a mediados de los años 80 del siglo pasado, el trabajo equivalente de ese operario, ya permitía surtir, a doce personas[76]. Como el índice de consumo ha ido creciendo vertiginosamente, cabe esperar que en 50 años entre un 3-5 % de las personas económicamente activas bastarán para garantizar el abastecimiento de toda la población.

Esto enlaza con un estudio llevado a cabo por la consultora americana McKinsey[77], en su revista *McKinsey Quarterly*[78], que afirma que el 45% de las actividades de particulares por las que hoy se paga, podrían ya automatizarse mediante la adaptación de tecnologías actuales; por lo cual en un futuro próximo habrá que redefinir el trabajo de las personas[79]. *La Segunda Era de las Máquinas*[80] supondrá según un estudio del Foro Económico Mundial de 2017, una pérdida de 7 millones de empleos "*de oficina*" en las 15 economías punteras en cinco años. En el mismo lapso de tiempo, calculan que se crearán sólo dos millones. Por otro lado, la Organización para la Cooperación y

---

[76] BECK, U.: *La sociedad del riesgo. Hacia una nueva modernidad*, ed. Paidós,1998.

[77] Fundada en 1926 por James McKinsey, con el fin de aplicar los principios de contabilidad de gestión a las empresas fue la primera consultora de gestión para contratar a graduados universitarios recientes, en lugar de los gerentes con experiencia. Entre 1980 y 1990, la empresa se expandió internacionalmente y estableció nuevas áreas de práctica. La consultora ha ayudado a establecer muchas de las normas en los negocios y ha contribuido a muchos de los principales éxitos y fracasos en los negocios en la era moderna.

[78] Revista de negocios para altos ejecutivos centrada en la gestión y la teoría de la organización de las empresas, publicada por McKinsey.

[79]elmundo.es (2016, 20 enero), ¿Qué harán los humanos si trabajan los robots?, *http://www.elmundo.es/economia/2016/01/20/5697cf8b268e3e82078b46aa.html*

[80] Término acuñado en el libro *The Second Machine Age*, escrito por Andrew McAfee y Erik Brynjolfsson. En el mismo, plantean que las generaciones futuras requerirán menos personas para ofrecer un crecimiento nunca antes visto, un desplazamiento de la fuerza laboral por los avances tecnológicos. Afirman que no se pueden evitar los avances tecnológicos, hay que prepararse, lo que es válido para los progresos empresariales y para revisar los programas educativos. Consideran impostergable repensar las estructuras de fuerza de trabajo, la educación y el desarrollo de habilidades para preservar la estabilidad social y económica. *Vid*. elmundo.es (2017, 3 marzo) «La segunda era de las máquinas» *http://www.elmundo.com.ve/Firmas/Tecnologia---Argelida-Gomez/La-segunda-era-de-las-maquinas.aspx#ixzz4aIn4OvZR*

Desarrollo Económico (OCDE[81]) habla de un 12% de trabajos automatizables en España, mientras otras investigaciones sitúan la disminución de empleos en la manufactura, la agricultura y los servicios en cerca de un 60%. En lo único en lo que parece haber cierto consenso en estos diversos estudios, es en que los nuevos empleos serán muchos menos que los que se destruyan[82].

Por ahora en nuestro país, estas previsiones no se han visto reflejadas en los datos, pues, España cuenta con 3.236.582 de empresas activas, en base a la última actualización del Directorio Central de Empresas (DIRCE)[83] a fecha 1 de enero de 2016, según los datos publicados el 29 de julio de 2016[84]. Se trata del segundo año en el que el número de empresas crece (un 1,6%) tras seis años consecutivos en los que se reducía.

Por otro lado, el número de programas informáticos instalados para supervisar a los empleados, va *in crescendo* en los últimos años, quizás por su impacto disuasivo para la prevención de los ilícitos, quizás porque permiten un control diferido de la actividad laboral o quizás porque constituyen un medio de prueba para acreditar los comportamientos irregulares[85]. El hecho cierto es que en España 7.000 empleados se someten a la vigilancia de un concreto programa informático que ha resultado éxito de

---

[81] Fundada en 1961, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) es un organismo de cooperación internacional que agrupa a 35 países miembros y su misión coordinar sus políticas económicas y sociales. Conocida como "*club de los países ricos*" agrupa a estados que proporcionan al mundo el 70 % del mercado mundial.

[82] elmundo.es (2017, 21 febrero) «Los robots te pagarán la pensión» *http://www.elmundo.es/papel/futuro/2017/02/21/58aae9f422601ddb488b45b9.html*

[83] El Directorio Central de Empresas (DIRCE) reúne en un sistema de información único, a todas las empresas españolas y a sus unidades locales ubicadas en el territorio nacional. Su objetivo básico es hacer posible la realización de encuestas económicas por muestreo. Se actualiza una vez al año, generándose un nuevo sistema de información al 1 de enero de cada período. Se publica una explotación estadística de los resultados para empresas y unidades locales, desglosados por comunidades autónomas según condición jurídica, actividad económica principal y estrato de asalariados asignado. El DIRCE genera información asociada a: altas, permanencias y bajas, clasificadas estas según sector económico, condición jurídica y estrato de asalariados.

[84] INE (2016, 29 julio) «Estructura y dinamismo del tejido empresarial en España Directorio Central de Empresas» (DIRCE) *http://www.ine.es/prensa/np984.pdf*

[85] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *Revista Justicia Laboral*, núm.39, 2009, pág. 12.

ventas; analiza el tiempo que destina a cada tarea el trabajador, como por ejemplo, consultar el correo electrónico; al parecer "*engañar al sistema informático*", no es tarea fácil[86].

Hace más de veinte años, la monitorización en las empresas era exclusiva de los administradores informáticos, que usaban herramientas del sistema operativo *Unix*[87] para vigilar el tráfico a efectos técnicos. Mientras, en el mundo *Window*s, nacían los primeros filtros parentales -como *CyberPatrol*[88]- que bloqueaban el acceso a los sitios que los niños no debían visitar. Actualmente, los filtros se han ampliado en el mercado a todo tipo de empresas, diversificando las posibilidades de sus productos, que ya no solo "*filtran*" sino que "*espían*" abiertamente "*la vida internaútica*" de los empleados.

Según un estudio observacional divulgado por la empresa *Colt Data Centre Services*[89] , el 98% de los empleados de empresas con una facturación mínima de 50 millones de euros al año tiene acceso a Internet y al correo electrónico. Según esa misma encuesta, el 41% de las empresas permite un uso moderado de los sistemas informáticos corporativos, frente a un 29% en 2002, lo que quiere decir que la tolerancia ha aumentado. El 50% ni siquiera tiene un protocolo de actuación. El citado estudio revela también que un 26% de las empresas encuestadas no tiene mecanismos técnicos para evitar que un empleado almacene información en soportes extraíbles, y un 35% no tiene ninguna política limitativa al respecto. A la hora de reportar incidentes, el 90% de los casos se debe al uso de los medios profesionales para usos particulares, un 45% a descargas ilegales y un 36% al mal uso o revelación de información confidencial. El estudio también

[86] antena3.com (2012, 8 de mayo). «Un software «espía» determina la productividad y eficiencia de los trabajadores» *http://www.antena3.com/noticias/tecnologia/software-espia-determina-productividad-eficiencia-trabajadores_2012050800236.html*

[87] Sistema operativo registrado oficialmente como UNIX® desarrollado en 1969 por Bell Labs, que se caracteriza por ser portable (programación de alto nivel), multiárea (sistemas operativos multitarea son capaces de dar servicio a más de un proceso a la vez para permitir la ejecución de muchos más programas) y multiusuario (característica de un sistema operativo o programa que permite proveer servicio y procesamiento a múltiples usuarios simultáneamente).

[88] Programa de control parental que permite bloquear sitios web inapropiados, establecer límites de tiempo en los juegos, controlar su acceso y el uso de Internet.

[89] Plataforma de información líder en Europa en suministro de servicios integrados de redes e informática a grandes corporaciones, medianas empresas y mayoristas.

hace hincapié en que muchos empresarios españoles no son conscientes de estar obligados a "*custodiar la información entregada por un tercero*" [90].

Por otro lado, y en base a los datos aportados por el INE, el 98,4% de las empresas españolas de 10 o más empleados dispone de conexión a Internet en el primer trimestre de 2016. Esto supone que el porcentaje de empresas que tienen acceso a Internet ha aumentado de manera paulatina hasta situarse que casi la plenitud. Asimismo, el 77,5% de las empresas con conexión a Internet dispone de sitio o página web y en las mercantiles de 250 o más empleados este porcentaje alcanza el 95,2%[91].

Por todo lo expuesto, resulta evidente que las nuevas tecnologías están plenamente arraigadas en la empresa, y conllevan múltiples ventajas tanto organizativas como de gestión, pero una utilización ilícita en el uso de tales medios por parte del empleador para ejercer control, supone un riesgo para determinados derechos fundamentales de los trabajadores.

Una de las últimas innovaciones tecnológicas que han surgido son las redes sociales como *Facebook, LinkedIn, Twitter, Ning*[92]*, Xing*[93]*, Hi5*[94] *y Second Life*[95], entre otras, que permiten a los usuarios conectarse, comunicarse y compartir información de una forma totalmente novedosa.

---

[90] GÓMEZ, L. (2013, 17 de septiembre) «Cuando el ojo que todo lo ve es el del jefe». *http://sociedad.elpais.com/sociedad/2013/09/16/actualidad/1379356017_007157.html*

[91] INE (2016, 28 de junio) «Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas», *Boletín Informativo del Instituto Nacional de Estadística* núm. 1, 2016. *http://www.ine.es/prensa/np978.pdf*

[92] Creada en 2005, con bajo el nombre chino *ning* que significa paz, la característica de esta red social, con la que trata de diferenciarse es que cualquiera puede crear su propia red social personalizada para un tema en particular o necesidad, dirigida a audiencias específicas.

[93] Fundada en 2003, red de ámbito profesional. También se denomina plataforma de *networking online*, ya que su principal utilidad es la de gestionar contactos y establecer nuevas conexiones entre profesionales de cualquier sector, pertenece a lo que se denomina software social.

[94] Red social que comenzó en 2003, en la actualidad cuenta con más de 70 millones de usuarios, sobre todo de América Latina.

[95] Metaverso (mundo virtual ficticio) lanzado en 2003 al que se puede acceder de manera gratuita desde Internet, sus usuarios conocidos como residentes pueden acceder a SL mediante el uso de uno de los múltiples programas de interfaz llamados viewers (visores), los cuales les permiten interactuar entre ellos mediante un avatar a una representación gráfica, generalmente humana, que se asocia a un usuario.

Un estudio realizado por *Young People´s Consumer Confidence* (YPCC) ha relacionado el ámbito laboral con el entorno personal y ha analizado la repercusión que tienen las redes sociales sobre unos 6.000 casos de jóvenes entre 16 y 34 años en más de cinco países diferentes, indicando que uno de cada diez jóvenes había sido rechazado para un puesto de trabajo debido a las características de su "*perfil virtual*" [96].

Sin embargo en España, el artículo 16. 2[97] de la Ley de Infracciones y Sanciones en el Orden Social (LISOS), lo consideraría una infracción muy grave en materia de empleo; está prohibida la solicitud de datos de carácter personal en los procesos de selección, el empleador no puede basar su decisión de declinar una candidatura por la información obtenida en la Red (cabe hablar de una neutralidad "*ideológica*" de la empresa en el sentido que la contratación del trabajo, no impide ni impone opciones personales del trabajador en el sentido más amplio del término[98]).

Las redes sociales han favorecido el acceso de cualquier persona a la publicación de contenidos en la Web, en muchas ocasiones sin la suficiente información. Algunos casos resueltos arbitralmente en Estados Unidos dan fe de las complicaciones que se pueden generar, ya que, por ejemplo, un neófito en vez de comunicar (como pensaba) a un grupo reducido de amigos, los vídeos y expresiones no muy acordes para el tipo de actividad que desarrollaba, lo que realmente hacía era "*subir*" o hacer accesibles estos mismos contenidos para un enorme número de usuarios, entre ellos los padres de sus alumnos, planteándose el consiguiente conflicto en el plano estrictamente laboral[99].

---

[96] publico.es (2013,30 de mayo) «Uno de cada diez jóvenes no consigue trabajo a causa de su perfil en redes sociales» *http://www.publico.es/actualidad/diez-jovenes-no-perfil-redes.html*

[97] Reza así: «*Solicitar datos de carácter personal en los procesos de selección o establecer condiciones, mediante publicidad, difusión o por cualquier otro medio, para el acceso al empleo por motivos de sexo, origen, incluido el racial o étnico, edad, estado civil, discapacidad, religión o convicciones, opinión política, orientación sexual, afiliación sindical, condición social y lengua dentro del Estado*».

[98] RODRÍGUEZ PIÑERO, M.: «Intimidad del trabajador y contrato de trabajo», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 8, 2004, págs. 93-103.

[99] CALVO GALLEGO, F.J.: «TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales», *Revista Doctrinal Aranzadi Social*, núm. 71, 2012 (BIB 2012\56).

Estas nuevas "*virtual water cooler conversations*[100]" tienen muchas mayores implicaciones, ya que una vez "*colgadas*", permanecen como archivos electrónicos, pudiendo ser copiadas y trasladadas a otros foros, sin posibilidad alguna de control. Una conversación o comentario puede ser visto por un innumerable número de "*amigos virtuales*" que, a su vez pueden copiar o "*retwittear*" esa información. Cuando se popularizara "*la vida on line*" todos los usuarios se convierten en radiotelegrafistas y sin haber jurado el secreto de las telecomunicaciones[101].

[100] Indica la clase de conversación "*virtual*" informal entre el personal de una empresa, como las que transcurrían durante un descanso en el trabajo alrededor del dispensador de agua.

[101] MECA SOLANA, D. (2013, 7 de diciembre), «La vida *on line*», *http://elpais.com/elpais/2013/12/06/opinion/1386350434_374038.html*

2. Conflictos laborales por el uso de las TICs

"*Tu empleador puede estar viéndote y escuchándote*", esta afirmación se ha convertido en un recurso muy utilizado en los países anglosajones para forzar, aún más, la controversia de la obra *1984*[102] de George Orwell[103] del "*Big brother is watching you*[104]*"*, tras la irrupción generalizada de las nuevas tecnologías de la información y, en concreto, de Internet y del correo electrónico.

Se ha llegado a afirmar que la monitorización hoy día es incluso mayor que como la describió Orwell, vivimos "*en la edad de oro de la vigilancia*"[105]; estos medios, permiten formas de control nuevas y "*casi ilimitadas*" que, de *facto*, están siendo

[102] *Nineteen Eighty-Four*, en su versión original, es una novela política de ficción distópica, escrita entre 1947 y 1948 y publicada el 8 de junio de 1949. El mundo totalitario del protagonista de la novela, Winston Smith, se caracterizaba por una lucha por proteger la privacidad. La telepantalla vigilaba sus movimientos durante las 24 horas, Smith no estaba seguro de si siempre lo escuchaban por lo que debía actuar como si lo hicieran. Cualquiera podría ser el observador que lo llevara a la cárcel, al dolor o a la muerte en nombre del partido. La vigilancia era tan intensa que los padres temían que sus hijos les delatasen. La novela introdujo los conceptos del omnipresente y vigilante Gran Hermano o Hermano Mayor, de la notoria habitación *101*, de la ubicua policía del Pensamiento y de la neolengua (adaptación del inglés en la que se reduce y se transforma el léxico con fines represivos, basándose en el principio de que lo que no forma parte de la lengua, no puede ser pensado).

[103] Eric Arthur Blair, conocido bajo el pseudónimo George Orwell, escritor y periodista británico (25 de junio de 1903-21 de enero de 1950), cuya obra lleva la marca de las experiencias personales vividas por el autor en tres etapas de su vida: su posición en contra del imperialismo británico lo llevó al compromiso como representante de las fuerzas del orden colonial en Birmania durante su juventud; a favor de la justicia social, después de haber observado y sufrido las condiciones de vida de las clases sociales de los trabajadores de Londres y París; en contra de los totalitarismos nazi y estalinista tras su participación en la Guerra Civil Española.

[104] Es el ente que gobierna, si bien nadie lo conoce, la presencia del Hermano Mayor o Gran Hermano es una constante a lo largo de toda la novela, aparece constantemente a través de las telepantallas en la fuerte propaganda de "*El Partido*", y en enormes murales en cada rincón de la sociedad descrita por Orwell. Su existencia es enigmática, pues nunca llega a aparecer en persona ni a decirse su nombre real. Para crear este personaje, el escritor, se inspiró en líderes totalitarios caracterizados por infundir una política de miedo y de extremada reverencia hacia sus personas, educando a la población a través de una propaganda gubernamental intensiva en valores colectivistas donde pensar individualmente fuera visto como una traición a la sociedad.

[105] ARIZA VICTORIA, M. (2015, 9 de diciembre) «Lo saben todo sobre usted». *http://elpais.com/elpais/2015/12/04/eps/1449252033_849371.html*

utilizadas por los empresarios para intensificar las formas de conocimiento del comportamiento de los trabajadores, creando centros de "*trabajo virtuales*" en los cuales la profecía orweliana del gran hermano adquiere dimensiones laboralizadas, "*el inmenso poder del ojo mecánico empresarial*", en las que la realidad vuelve a superar la ficción.

A) Las TICs: elenco

Las potencialidades tecnológicas de control por parte del empresario constituyen un conjunto, que va en una lista que por fuerza ha de ser *numerus apertus*[106]. Desde el relativamente más tradicional sistema de videovigilancia en sus múltiples posibilidades, hasta los más sofisticados mecanismos de control de acceso y localización dentro de la empresa, mediante tarjetas de identificación personal o, incluso, datos biométricos fuera de ella, por sistemas de localización GPS. Pasando por los cada vez más habituales registros del ordenador utilizado por el trabajador y su correo electrónico o los rastros de la navegación en Internet, ya de forma física o mediante la instalación de *software* "*espía"* capaz de revelar un amplio espectro de informaciones desde los programas utilizados hasta el número de pulsaciones practicadas por minuto[107], o la información recabada en las distintas redes sociales, que va desde la posibilidad de que se indague en ellas aspectos personales de los candidatos a la hora de decidir la contratación, hasta la posibilidad de que determinadas descalificaciones o comentarios de los trabajadores sobre sus empresas, vertidas en las redes sociales, puedan considerarse como lícito motivo de despido disciplinario[108].

---

[106] TASCÓN LÓPEZ, R.: «El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica», *Revista Doctrinal Aranzadi Social* núm. 17, 2007 (BIB 2007\3032).

[107] *Ibidem.*

[108] STSJ Asturias de 19 de abril de 2013 (AS 2013\1595). Esta sentencia resulta cuando menos curiosa, al confirmar el fallo de la Instancia, absolviendo a la empresa por considerar el despido procedente, al haberse declarado probado lo imputado en la carta de despido, lo siguiente: "*La mañana del martes 4 de mayo, presentó parte médico de urgencias y dijo que le habían recomendado reposo , por lo que tampoco fue a trabajar el día 5 de mayo. Pues bien, con ocasión de la conversación mantenida el 4 de julio con la Srta. Erica, la empresa tuvo conocimiento que en realidad todo aquello fue un engaño a la empresa para poder ir a Madrid a un concierto de Jon; como efectivamente hizo, y respecto de lo que no ha tenido pudor*

En un intento por sistematizar las diversas formas posibles de control tecnológico, podemos identificar tres tipos:

- Un control directo o "*intencional*" del trabajador que tiene como objetivo recabar información directa del comportamiento laboral del mismo; presencia, desplazamientos, cumplimiento, etc. La cuestión aquí es dilucidar dónde está el límite, pues existen garantías a favor del empleado.
- Un control indirecto o difuso, destinado a satisfacer cualquier exigencia técnico organizativa o de seguridad en el trabajo. El tratamiento de datos tomados circunstancialmente, respecto a un concreto trabajador, es discutido que pueda ser usado como medio de prueba del incumplimiento del mismo, por poder vulnerar el derecho a la autodeterminación informativa.
- Un control defensivo que tiene por objeto directo el verificar la comisión de algún ataque o atentado contra la persona o bienes[109].

B) Aumento de la dependencia

Cierto sector de la doctrina afirma que las nuevas tecnologías han dado paso a lo que se ha identificado como "*nuevas formas de subordinación*" que no son otra cosa que novedosas maneras de concretar la dependencia del trabajador. Se habla de "*dependencia tecnológica*" ,"*subordinación informática*", o "*presencia virtual del trabajador en el centro de trabajo*"; existe una mayor disponibilidad del empleado por su fácil localización y, además, cualquier estancia se puede convertir en el lugar de trabajo mediante conexión informática[110], es un trabajador de cristal en el doble sentido de sufrir mayor vulneración

alguno al dar publicidad de ello mediante la red social Facebook, según nos refieren sus compañeras de tienda y se puede ver en las fotos que Vd. misma colgó en esa red social presenciando el concierto. Luego se trata de ausencias injustificadas, agravadas por ocultar un engaño manifiesto a su empresa".

[109] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *op. cit.*, págs. 13-14.

[110] PÉREZ DE LOS COBOS ORIHUEL, F.: «La subordinación jurídica frente a la innovación tecnológica», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 1, 2005, págs. 1315-1338.

de sus derechos fundamentales y de que ningún aspecto esté a salvo del conocimiento del empleador[111].

La irrupción de las nuevas tecnologías de la información y la comunicación ha puesto en crisis la manera tradicional de interpretar los rasgos característicos de la relación laboral, ha generado nuevos tipos de empresas y de empleados[112] y ha contribuido a diseñar otros nuevos indicios más acordes con las profundas transformaciones que ha experimentado el sistema de las relaciones laborales. Esta aparición de manera brusca y casi generalizada en la sociedad ha convertido a las nuevas tecnologías en un fenómeno omnipresente y que como consecuencia de lo anterior, aparecen súbitamente también en el Derecho.

Hace ya años PÉREZ DE LOS COBOS destacó que el aumento de poder del empresario sobre el trabajador se fundaba en la sustitución de un control periférico y discontinuo realizado por personas, por un control centralizado y objetivo, iniciado a raíz de las nuevas tecnologías y en la aparición de un novedoso y sofisticado tipo de control que consiste en la reconstrucción del perfil del trabajador, a través del almacenamiento de datos, aparentemente inocuos[113].

Al regular la materia, en un primer momento la Ley de Procedimiento Laboral, y posteriormente, la Ley de Enjuiciamiento Civil, introdujeron la posibilidad de incorporarlas al proceso, tal y como habían venido manteniendo la jurisprudencia y la doctrina.

---

[111] HOLGADO GONZÁLEZ, M.: «La protección constitucional de la intimidad de los trabajadores frente a el uso de las nuevas tecnologías de la comunicación» en AA.VV.: GALÁN MUÑOZ, A. (Coord.) *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación*, ed. Tirant Lo Blanch,2014, pág. 82.

[112] MOLINA NAVARRETE, C.: «Expectativa razonable de privacidad y poder de vigilancia empresarial. ¿*Quo vadis* Justicia Laboral?», *CEFLegal: revista práctica de derecho, Comentarios y casos prácticos*, núm. 399, 2016.

[113] PÉREZ DE LOS COBOS ORIHUEL, F.: *Nuevas tecnologías y relación de trabajo*, ed. Tirant Lo Blanch, 1980, pág.72.

C) Inevitabilidad

¿Hemos de rendirnos ante el carácter inevitable de las tecnologías? Señala RODOTÁ que "*todo lo tecnológicamente posible es al mismo tiempo éticamente admisible, socialmente aceptable y jurídicamente legítimo*"[114]. Por el contrario, nuestro TC ha precisado que existen límites y garantías, diferenciando un espacio legítimo de control empresarial y otro que no lo es. En este sentido, cabe traer a colación que en Francia el proyecto de Ley de reforma laboral, actualmente en tramitación, contiene algunas interesantes novedades en materia de adaptación del mercado laboral al entorno digital incluyendo el nuevo derecho a la desconexión con la finalidad de evitar la presión que los dispositivos digitales proporcionados por el empresario imponen sobre los trabajadores, aumentando su riesgo de stress y de bourn out[115].

Al respecto, pero mucho después, cabe citar la STC 173/2011, de 7 de noviembre[116] que postula que: "*es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona*"(FJ 3º).

---

[114] RODOTÁ, S. :«Democracia y protección de datos. (Traducción de PIÑAR, J.L.), Disponible en *http:// www. agdp.es*

[115] MIRÓ MORROS, D.: «El control de la jornada y el teletrabajo», *Actualidad Jurídica Aranzadi* núm. 920, 2016 (BIB 2016\3966).

[116] STC 173/2011 de 7 noviembre (RTC 2011\173).

D) Enfoque conflictivista

Las tecnologías de la información y de la comunicación han puesto en un primer plano la necesidad de que en el desarrollo del contrato de trabajo se respeten los derechos fundamentales de dignidad e intimidad del trabajador y asimismo su derecho a la autodeterminación informativa. Las nuevas tecnologías generan profundas transformaciones en la organización de las empresas[117] y cambios de principios en la práctica laboral, y asimismo llevan a los jueces a adoptar nuevos cánones, gestados y madurados (al menos en nuestro sistema jurídico) extramuros de las salas en las que los pleitos se convierten en *litis.*

El debate judicial se centra en el conflicto entre los diversos derechos constitucionales del empleado que pueden quedar afectados por el uso de las nuevas tecnologías[118] y que, en su mayoría, pertenecen a la primera generación de derechos fundamentales, que quedó plasmada en las manifestaciones más incipientes del constitucionalismo moderno, aparecidas a lo largo del siglo XIX, como derechos que se caracterizan por reunir el doble requisito de ser de la persona o de la personalidad. Por una parte, pertenecen al trabajador en su condición de tal, aun cuando se ejerzan en el marco del contrato de trabajo, y de otra por ser derechos de libertad, ya que su objeto consiste en la expectativa de la ausencia de intromisiones o interferencias.

Y en el lado contrapuesto, por parte del empleador se encuentran el derecho a la libertad de empresa y el derecho de propiedad, de aparición más tardía, pues surgen ya en el siglo XX a resultas del nuevo pacto social que refundó las relaciones entre Estado y Sociedad.

Los equilibrios y limitaciones que conlleva el contrato de trabajo, para el empresario y el trabajador, suponen que las facultades organizativas empresariales se

---

[117] Las nuevas tecnologías han propiciado, la descentralización productiva, la posibilidad de dividir el proceso de producción en distintas unidades o menos autónomas, y así atribuir cada una de ellas a diferentes sujetos productivos, estén o no relacionados entre sí creando una nueva red de empresas , externalizando de este modo una o varias fases del proceso productivo. Pues, la utilización de las nuevas tecnologías de la comunicación permite que se pueda intercambiar información sin necesidad de un intercambio o traslado físico, esto es, posibilitan la conexión inmediata entre distintas empresas que desarrollen las diferentes fases del proceso productivo. Sobre el fenómeno de descentralización productiva véase RIVERO LAMAS, J.: «La descentralización productiva y las nuevas formas organizativas del trabajo», en AA. VV. *Descentralización productiva y nuevas formas de organizar la producción*, X Congreso Nacional de Derecho del Trabajo, MTSS, 2000, pág. 30.

[118] VALDÉS DAL-RÉ, F.: «Presentación del Seminario Internacional sobre medios de comunicación y control empresarial» *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 30, 2009, núm. 30, págs. 1-8.

encuentran restringidas por los derechos fundamentales del trabajador, quedando el empleador obligado a respetarlos.

Partiendo de la prevalencia de los derechos del trabajador, los límites que quiera poner la empresa. Solo se pueden derivar del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho; de tal forma que el ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso de sustento a la producción de resultados inconstitucionales. Y ello porque los derechos constitucionales de cualquier ciudadano "*acompañan al trabajador durante toda la vida de la relación laboral, como un veto ínsito a las prerrogativas empresariales*"[119]. La entrada del trabajador en la fábrica, no entraña despojo ni paralización de aquellos derechos que el ordenamiento jurídico y la CE, reconoce a todas las personas[120].

E) Solución armónica

El Tribunal Constitucional destaca la necesidad de que las resoluciones judiciales preserven "*el necesario equilibrio entre las obligaciones dimanantes del contrato de trabajo y el ámbito modulado de su libertad constitucional*"[121].

En igual sentido, MONEREO PÉREZ y LÓPEZ INSUA, inciden en que precisamente allí donde se plantea una "*fuerte tensión dialéctica*" es el lugar de fricción entre los derechos constitucionales del empresario y los fundamentales del trabajador, que disfrutan de una dimensión constitucional diferente[122].

---

[119] STC 88/1985, de 19 de julio (RTC 1985\88). En relación con la vulneración del derecho a la libertad de expresión del jefe clínico de un psiquiátrico por "*verter*" críticas sobre en la televisión autonómica gallega sobre la prestación de los servicios médicos en el centro en el que trabajaba.

[120] GARCÍA MURCIA, J.: «Presentación» en AA. VV. (Dir.) GARCÍA MURCIA, J.: *Derechos del Trabajador y Libertad de Empresa*, ed. Aranzadi, 2013, pág. 29.

[121] STC 185/1996, de 25 de noviembre (RTC 1996\185).

[122] MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B. M. :«El control empresarial del correo electrónico tras las STC 170/2013», *Revista Doctrinal Aranzadi Social* núm. 11, 2014 (BIB 2014\122).

3. Ausencia de regulación específica

Nuestro ordenamiento se caracteriza por la ausencia de reglas especiales aplicables a la actividad de control empresarial. Podemos afirmar, sin ningún tipo de reservas, que nos encontramos en un terreno anómico[123]. Por este motivo en más de una ocasión, habrá que recurrir a la doctrina constitucional para resolver las cuestiones que se planteen. Por esta razón, algún autor ha llegado a afirmar que nos encontramos en esta materia ante "*un mal envejecimiento"* de la legislación laboral[124].

A) Caracterización general

En la regulación de las nuevas tecnologías, el Derecho del Trabajo español, es básicamente un *Derecho Jurisprudencial*[125]; a partir de los pronunciamientos judiciales, se comienza a construir doctrina general sobre el uso y control de los medios tecnológicos de información y comunicación en la empresa.

Dada la escasa normativa legal existente entre el contrato de trabajo y la Constitución Española, la repercusión, supone una mayor y más directa irradiación constitucional sobre la relación laboral en conexión con los derechos fundamentales. Esto ha permitido que las Sentencias del Tribunal Constitucional sienten una valiosísima doctrina no ya constitucional sino también *fundacional;* en esta materia un tercio del total de la doctrina del TC es social[126].

La solución al problema, pues, radica en la judicialización de los conflictos pero no solo a nivel nacional, sino también elevados a rango comunitario e internacional; pues esta protección constitucional constituye una garantía de compromiso que habrán de

---

[123] Proviene de la palabra griega *anomia* (de anomía: prefijo «ausencia de» y nómos «ley, orden, estructura»).

[124] CALVO GALLEGO, F.J.: «TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales», *op.cit*.

[125] TASCÓN LÓPEZ. R.: «Sobre la evolución de los límites del poder tecnológico de control empresarial en el caso español», disponible en *http://www.bit.ly/vMraGu*, *cit*, pág. 10 del original impreso.

[126] SEMPERE NAVARRO, A.V.: «La Constitución y la doctrina constitucional», *Revista Actualidad Jurídica Aranzadi* núm. 737, 2007.

superar todos los Estados que forman parte de la UE[127], fundamentalmente a partir de la doctrina del TEDH, como veremos.

B) Funcionalidad del artículo 20.3 ET

En todo el ordenamiento, existe una previsión general y de amplio alcance: el artículo 20.3 ET autoriza al empresario a adoptar "*las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad de los trabajadores disminuidos".*

Ya en la propia dicción de la norma del 20.3 ET, se apunta la íntima relación existente entre las genéricas facultades empresariales de dirección y de organización que permiten adoptar medidas de supervisión o vigilancia de la actividad laboral al empresario, y la atribución de tales facultades sobre el trabajador; lo que se justifica en las potestades derivadas del contrato de trabajo, cuyo fundamento se encuentra en la libertad de empresa, reconocida en el artículo 38 CE. El artículo 20.3 ET es duramente criticado de manera casi unánime por la doctrina.

- Para THIBAULT ARANDA, resulta abstracto y ambiguo, tanto por la ausencia de normativa *ad hoc* que regule la cuestión, como por la falta de referencia alguna a los procedimientos de control. Con la referencia ambigua en dicho artículo a "*las medidas que estime oportunas*" y a la " *dignidad humana*" como límite genérico a las facultades de control del empresario; lo cual equivale a llegar a la rápida conclusión de que es una cuestión a resolver esencialmente por la vía jurisdiccional. La falta de soluciones generales y rotundas en la ley ha judicializado la cuestión, poniendo en manos de los jueces y tribunales la delicada tarea de adecuar los derechos fundamentales a poderes del empresario, que este ejerce con fundamento en el contrato de trabajo[128].

[127] MONEREO PÉREZ, J.L y LÓPEZ INSUA , B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit.*

[128] THIBAULT ARANDA, J.: *Control Multimedia de la Actividad Laboral*, ed. Tirant Lo Blach, 2006, pág.15.

- SALA FRANCO critica la imprecisión legislativa y acuña por primera vez el término en esta materia de labor creadora, "*quasi legislativa"*, de los tribunales, capaz de propiciar, en ocasiones, notables contradicciones, lo cual provocará, a la postre, un evidente grado de inseguridad jurídica[129].
- Con las expresiones, "*claro ejemplo de raquitismo jurídico", y "una previsión huérfana de toda referencia al uso de los sistemas de control audiovisual en el lugar de trabajo*" GOÑI SEIN califica al referido artículo del ET, aunque también reconoce que constituye el principal anclaje legal del ejercicio del control empresarial a través de las nuevas tecnologías. Afirma este autor, que contrasta la parca regulación, con la minuciosa y detallada normativa sobre la videovigilancia en el ámbito de la seguridad pública contenida en la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Seguridad del Estado en los lugares públicos[130].
- En otra línea distinta, MONTOYA MELGAR, configura el art. 20.3 ET como un conjunto de facultades jurídicas por las que el empresario dispone del trabajo realizado, ordena las prestaciones laborales y organiza el trabajo en la empresa. Dentro de esas facultades se encontrarían también las de control y vigilancia[131].

C) Otros preceptos laborales relevantes

Pese a la omisión legislativa existente, o precisamente por ella, junto al artículo 20.3 ET aparecen otros preceptos que también son tomados en consideración como bases remotas de las soluciones acogidas:

- El 4.2.e ET, que reconoce el respeto a la intimidad del trabajador y a la consideración debida a su dignidad. En su realización se respetará al

---

[129] 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*, ed. La Ley, 1999, pág. 205.

[130] GOÑI SEIN, J.L:. *La videovigilancia empresarial y la protección de datos personales*, ed. Aranzadi, 2007, pág. 21.

[131] MONTOYA MELGAR, A.: «Nuevas dimensiones jurídicas de la organización del trabajo en la empresa», *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. 23, 2000, pág. 38.

máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello sea posible, frente al art. 20.3 ET, ya comentado.

- El 18 ET recoge que: "*solo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo*".

En un primer momento, la jurisprudencia española más consolidada consideró que había de equipararse el uso privado de Internet y de los ordenadores al resto de medios de producción, y en consecuencia, aplicar por analogía, en este caso, las mismas reglas que para el uso de las taquillas; por lo cual consideraban plenamente aplicable el art. 18 ET, y se supeditaba ese control a un interés empresarial[132].

Esta doctrina, que quedó superada con la STS de 26 de septiembre de 2007[133], la cual excluyó de manera directa el art. 18 ET, para justificar el control empresarial sobre los medios tecnológicos puestos a disposición del trabajador, al ser esta una facultad que deriva directamente del art. 20.3 ET. Así, en la actualidad, " el *útil del trabajo, no puede considerarse como un efecto personal*".

[132] MONEREO PÉREZ, J. L. y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit.*

[133] STS 26 de septiembre de 2007 (RJ 2007\7514).

D) La protección penal y su proyección

Otro extremo distinto y necesario de análisis es el de la protección de la información confidencial que en ocasiones maneja la empresa y que robustece su capacidad para competir. Buena parte de esta tecnología de vanguardia se conoce como el "know-how"[134], que resulta absolutamente crucial conservar[135]. Así, el secreto de empresa se muestra como un instrumento apto para amoldarse a un escenario en el que la adquisición de conocimientos es costosa[136], así el art. 197[137] CP, que se ha visto modificado recientemente[138], establece lo siguiente:

> *"1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*
>
> *2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."*

---

[134] *"Saber-cómo";* expresión anglosajona utilizada en los últimos tiempos en el comercio internacional para denominar los conocimientos preexistentes no siempre académicos, que incluyen: técnicas, información secreta, teorías e incluso datos privados (como clientes o proveedores).

[135] MORÓN LERMA, E.: *El secreto de empresa: Protección Penal y Retos que plantea ante las Nuevas Tecnologías*, ed. Aranzadi, 2002, pág. 28.

[136] *Ibídem, p*ág. 34.

[137] El artículo 197.1 CP, en el que tradicionalmente se han subsumido los accesos ilegales a sistemas circunscribía la punición del acceso ilegal a aquellos casos en que se hubiere llevado a cabo con la finalidad de vulnerar la intimidad o descubrir los secretos de otro; secretos que, caso de que tuvieran naturaleza empresarial, remitirían a lo dispuesto en el artículo 278 CP. En definitiva, el legislador tomó la opción, en un momento determinado, de restringir el alcance del acceso ilegal a sistemas informáticos mediante la introducción de un elemento subjetivo del injusto que determina una singular estructura de la norma, como delito de resultado cortado: por un lado, es necesario que el dolo del autor abarque la voluntad de acceder al sistema informático; por otra parte, sin embargo, esa voluntad de acceso requiere una voluntad ulterior, cual es la de vulnerar la intimidad o secretos ajenos, voluntad esta que, si bien puede materializarse en un resultado concreto (el efectivo descubrimiento de secretos o vulneración de la intimidad), no es necesario que así suceda para entender perfeccionado el tipo.

[138] LO 1/2015, de 30 de marzo, por la que se modifica la L.O 10/1995, de 23 de noviembre, del Código Penal.

Asimismo, se han añadido los artículos 197 bis[139], 197 ter[140], 197 quarter[141], y 197 quinquies[142].

La literatura jurídica señala que una información constituye secreto de empresa cuando tiene carácter reservado, posee valor competitivo y existe voluntad de mantenerla en secreto por parte de su titular[143].

Estas conductas delictivas por parte de los empleados, conllevan exigencias de organización empresarial que obliguen al trabajador a cumplir con una serie de conductas no vinculadas directamente con lo estipulado en su contrato, pero sí necesarias para preservar los bienes del empresario, como las cuestiones relacionadas con la protección de la integridad de los bienes y personas dentro de la empresa. Consecuencia de lo anterior

---

[139] Artículo 197 *bis.* Acceso no permitido a información electrónica.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

[140] Artículo 197 *ter*. Penas a imponer.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del art. 197 o el art. 197 *bis*:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

[141] Artículo 197 *quater*. Organización o grupo criminal. Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

[142] Artículo 197 quinquies. Responsabilidad de persona jurídica.

Cuando de acuerdo con lo establecido en el art. 33 bis, una persona jurídica sea responsable de los delitos comprendidos en los arts. 197, 197 bis y 197 ter , se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el art.66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del art.33.

[143] MORÓN LERMA, E.: *El secreto de empresa: Protección Penal y Retos que plantea ante las Nuevas Tecnologías, op. cit*., pág. 50.

es que, por un lado, el empresario podrá alcanzar extremos no estrictamente relacionados con la prestación laboral, aunque sí con las exigencias de la organización; por otro lado, no podrá extenderse a los aspectos extralaborales de la conducta del trabajador[144]. Cabe precisar en este punto, que la aptitud del empresario no deberá orientarse a la captación de la vida que el empleado lleve fuera de ese ámbito rector y organizativo[145].

E) Proyección de los derechos constitucionales

El control de la prestación laboral se incardinaría dentro del poder de dirección empresarial con una doble circunstancia, la propia especialidad de la relación de trabajo, que determina que el trabajador no solo está obligado a desarrollar una tarea, sino a realizarla conforme a las instrucciones del empresario, pero el interés de este no se satisface con la mera comprobación del resultado de la prestación, sino que precisa la vigilancia y control de la actividad durante su desarrollo a fin de comprobar que se desempeña de acuerdo a lo convenido.

A la vista de lo argumentado, la posibilidad de una proyección laboral de los derechos fundamentales de la persona parece indiscutible, pero no puede predicarse lo mismo respecto a las injerencias del empresario en su facultad de controlar al trabajador, pues los límites entre control empresarial y derechos fundamentales no están delimitados por normas legales, existe lo que podríamos denominar *una demarcación harto sutil entre ambos puntos de fricción*, y esto significa para el empresario una forma de poder abierta a muchos usos y potencialmente amenazadora.

A esta importante materia es imprescindible dedicarle atención detallada, lo que se hace de inmediato en el capítulo siguiente.

---

[144] FERNÁNDEZ VILLAZÓN, L.A.: *Las facultades empresariales de control de la actividad laboral*, ed. Thomson- Aranzadi, 2003, pág. 23

[145] GOÑI SEIN, J.L.: *El respeto a la esfera privada del trabajador*, ed. Civitas,1988, pág. 113.

II. EL RESPETO A LOS DERECHOS CONSTITUCIONALES

1. Poderes y derechos laborales en la Constitución

Los poderes empresariales, hunden sus raíces en el principio de libertad de empresa y se desgranan en una serie de facultades de contenido muy variado que principalmente se encaminan a la ordenación, al control y la disciplina en el trabajo[146].

Las facultades de control y vigilancia empresarial, que se reconocen al empleador, exceden con mucho a las de normal comprobación de que se ejecuta lo convenido, que pueden observarse en cualquier otra relación jurídica; este carácter, en cierto modo exorbitado, se suele justificar por las peculiaridades de la relación laboral.

Todo lo cual guarda relación directa con los derechos fundamentales del trabajador, que ejercen como una "*barrera*" frente a esta potestad empresarial. Ante el progresivo debilitamiento del Derecho Laboral y sus instituciones por las sucesivas reformas neoliberales, que han alterado el equilibrio de la relación laboral e inclinado la balanza a favor de los intereses empresariales, los derechos fundamentales han adquirido protagonismo como núcleo irreductible de derechos, frente a todo abuso de poder y también frente al empresarial[147].

A) Niveles de preceptos constitucionales

De acuerdo con su ubicación en el texto constitucional, podemos diferenciar: derechos fundamentales, derechos ordinarios de los ciudadanos y principios económicos y sociales.

---

[146] GARCÍA MURCIA, J.: «Presentación» en AA.VV. (Dir.) GARCÍA MURCIA, J.: *Derechos del Trabajador y Libertad de Empresa*, *op. cit*., pág. 27.

[147] GOÑI SEIN, J.L.: «Los Derechos Fundamentales Inespecíficos en la Relación Laboral Individual: ¿Necesidad de Reformulación?» 1ª Ponencia del XXIV Congreso Nacional Del Trabajo y de la Seguridad Social sobre Los Derechos Fundamentales Inespecíficos en la Relación Laboral y en Materia de Protección Social. Universidad de Navarra, 2014, pág. 11 del original impreso. *http://www.aedtss.com/images/stories/documentos/XXIII_Congreso_Nacional/01_Jose_Luis_Goñi.pdf*

Tanto los derechos fundamentales como los ordinarios (arts. 30 a 38) son susceptibles de aplicación directa, sin necesidad de desarrollo legal previo, mientras que los principios económicos y sociales (arts. 39 a 52) requieren una regulación previa.

Por su parte, los derechos fundamentales son los reconocidos en el Título I, Capítulo II, Sección I de la Constitución Española, todos los cuales están amparados por el máximo nivel de protección constitucional, artículos 14 a 29. Dentro este amplio elenco de derechos fundamentales, y siguiendo a PALOMEQUE LÓPEZ[148], cabe a su vez distinguir entre dos tipos, por un lado, los que son reconocidos a cualquier persona, conocidos como derechos fundamentales "*inespecíficos*", y por otro lado, aquellos que precisan titularidad o contenido laboral, llamados derechos fundamentales "*específicos o laborales*".

Los derechos fundamentales *específicamente laborales* se conciben para desplegar sus efectos principales en el marco de las relaciones de trabajo: libertad sindical (art. 28.1 CE), derecho de huelga (art. 28.2 CE). Únicamente subsisten mientras lo haga la condición de su titular, siendo este "*el presupuesto inesquivable de su nacimiento y ejercicio*"[149].

Junto a esta clase de derechos, la Constitución reconoce lo que podríamos definir como derechos laborales *inespecíficos,* que son toda una gama de derechos igualmente fundamentales que, aunque puedan tener una proyección en el ámbito laboral, pertenecen a todos, con independencia de su condición de trabajador[150].

Los derechos laborales *inespecíficos* son los que el trabajador ya ostentaba por su condición de persona, siendo su nacimiento anterior al de la relación laboral[151]. Son aquellos que el trabajador disfruta no en cuanto a su condición de trabajador , sino en cuanto ciudadano; de los cuales no puede ser despojado en modo alguno a partir de su incorporación en el seno de la empresa por mor de la celebración de un contrato de

---

[148] PALOMEQUE LÓPEZ, M.C.: *Los derechos laborales en la Constitución Española*, ed. Centro de Estudios Constitucionales (CEC),1991, pág. 31.

[149] VALDÉS DAL-RÉ, F.: «Derechos fundamentales de la persona del trabajador: un ensayo de noción lógico- formal», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 18, 2003, pág. 54.

[150] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: «Sobre el control empresarial de los ordenadores», *Revista Doctrinal Aranzadi Social* núm. 3, 2012 (BIB 2012\984).

[151] PEDRAJAS QUILES, A.: «Derechos fundamentales de la persona, del trabajador y autonomía privada» en AA.VV. (Coor). SALA FRANCO, T.: *Libro Homenaje a Abdón Pedrajas Moreno*, ed. Tirant Lo Blanch. 2012, pág. 409.

trabajo, adquiriendo una "*versión laboral*" e "*impregnando de manera esencial el desarrollo de la relación de trabajo*"[152].

Los derechos fundamentales *inespecíficos* recogidos en la CE que entran en colisión respecto del trabajador; art. 15 CE derecho a la vida y a la integridad física, art. 16 libertad ideológica, religiosa y de culto, art. 18. 3 y 4: derecho a la intimidad personal, a la propia imagen, al secreto de las comunicaciones y derecho de autodeterminación, art. 19 libertad de residencia, art. 20 libertad de expresión e información, art. 23 derecho de participación. Y en relación con el empleador; arts. 33 y 38: derecho a la libertad empresarial y derecho a controlar el patrimonio empresarial. Cierto sector de la doctrina califica todos estos derechos como *neutros*[153]. En cualquier caso, ambos tipos de claúsulas se integran en lo que se viene denominando Derecho Constitucional del Trabajo[154].

La doctrina no ha dudado en utilizar una terminología sintomática de la aceptación del superior rango de los derechos fundamentales, distinguiendo entre un "*derecho fundamental pleno y otro menos pleno*", en clara alusión a los derechos fundamentales inespecíficos por un lado, y por otro, a la libertad de empresa, sin perjuicio de reconocer que la consideración de este último puede ser incluso mayor[155].

Por lo cual con respecto a estos derechos, la relación de trabajo constituye un ámbito muy peculiar desde el punto de vista de determinados derechos de la persona; estos rigen en cuanto tengan virtualidad para la relación de trabajo y en particular para las personas que trabajan, de ahí que se hable de *versión laboral de los derechos y deberes de los ciudadanos*[156].

Es evidente que el realce de los derechos fundamentales no les otorga prioridad absoluta sobre otros valores. El rango no debe ser tomado en consideración cuando haya

---

[152] TASCÓN LÓPEZ, R.: «La protección de datos personales de los trabajadores» *Revista Jurídica de Castilla y León.* Ejemplar dedicado a Protección de datos de carácter personal núm. 16, 2008, págs. 447-499.

[153] SEGOVIANO ASTABURUAGA, M.L:. «El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores», *Revista jurídica de Castilla y León*, Núm. 2, 2004, pág. 150.

[154] ALONSO OLEA, M.: *Las fuentes del derecho, en especial del derecho del Trabajo según la Constitución*, ed. RAJL. 1981,pág. 29.

[155] OJEDA AVILÉS,.A.: «Equilibrio de intereses y bloque de constitucionalidad personal en la empresa», *Revista de derecho social*, núm. 35, 2006, pág. 18.

[156] GARCÍA MURCIA, J.: «Presentación» en AA. VV. GARCÍA MURCIA, J. (Dir.) *Derechos del Trabajador y Libertad de Empresa, op.cit.,* pág. 39.

una colisión entre derechos fundamentales o valores jurídicos protegidos a nivel constitucional, porque no hay jerarquía entre ellos, sino la ponderación de intereses en conflicto, que es lo que justifica que una vez acreditado el interés empresarial sea legítimo el sacrificio de un derecho fundamental[157]. Por tanto, se exige una relectura de los derechos fundamentales proclamados por la CE, menos condicionada desde el punto de vista interpretativo de las garantías que el art. 53 CE establece[158].

B) Eficacia de los derechos constitucionales

Hoy es una cuestión generalmente aceptada que los derechos de la persona pueden también proyectarse en el ámbito laboral, si bien ha sido necesario un largo y arduo proceso de afirmación para superar la clásica concepción como derechos públicos subjetivos, únicamente oponibles frente al poder del Estado[159]. La CE no puede quedarse a las puertas de los centros de trabajo, como de manera gráfica se ha expresado ya[160].

La llamada eficacia horizontal de los derechos fundamentales entre particulares, y en concreto en la relación laboral, ha sido avalada en nuestro sistema por una consolidada jurisprudencia constitucional, cuyo arranque se podría situar en la STC 88/1985 de 19 de julio[161], según la cual *" la celebración de un contrato de trabajo no*

---

[157] GOÑI SEIN, J.L.: «Los Derechos Fundamentales Inespecíficos en la Relación Laboral Individual: ¿Necesidad de Reformulación?» 1ª Ponencia del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social de la AEDSS 2014. *Los Derechos Fundamentales Inespecíficos en la Relación Laboral y en Materia de Protección Social*, pág. 14 del original impreso.

http://www.aedtss.com/images/stories/documentos/XXIII_Congreso_Nacional/01_Jose_Luis_Goñi.pdf

[158] *Ibídem*, pág. 15.

[159] Esta afirmación deriva de la aceptación generalizada de la terminología alemana, *Drittwirkung der Grundrechte* o "eficacia horizontal de los derechos fundamentales"; no sólo pueden ejercitarse los derechos fundamentales, frente al poder público, sino también frente a particulares en todos los ámbitos de la vida social, incluido el trabajo. La tesis de la *Drittwirkung* fue elaborada por el iuslaboralista NIPPERDEY *vid. Grundrechte und Privatrecht*, Mónaco, 1961 y aceptada por el Tribunal Federal de Trabajo de la República Federal Alemana en 1954.

[160] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: «Derechos fundamentales inespecíficos y negociación colectiva». *Cuadernos Aranzadi Social* núm. 40, 2011, pág. 21 (BIB 2011\491).

[161] STC 88/1985, 19 de Julio (RTC 1985\88).

implica en modo alguno la privación para una de las partes de los derechos que la Constitución le reconoce como ciudadano ".

La sentencia que marcará un punto de inflexión en la nueva orientación, años después, es la STC 99/1994 de 11 de abril[162] que estima lesivo el derecho al uso de la propia imagen (artículo 18 CE). Un trabajador es despedido por su negativa a obedecer la orden empresarial que le obligaba a exhibir en público su habilidad profesional como deshuesador de jamones en un acto promocional con presencia de los medios de comunicación.

En la referida sentencia se declara el carácter insoslayable del juicio de ponderación y se afirma que "*el contrato de trabajo no puede considerarse como título legitimador de recortes en el ejercicio de los derechos fundamentales que incumben al trabajador como ciudadano, que no pierde su condición de tal por insertarse en el ámbito de una organización privada*". Se aplica el llamado principio de indispensabilidad o de estricta necesidad de la limitación, en base al cual el equilibrio entre las obligaciones derivadas del contrato para el trabajador y el ámbito de su libertad constitucional ha de producirse "*en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva".*

Finalmente, este giro de la doctrina constitucional alcanza su punto culminante con la consagración del principio de proporcionalidad, como criterio para valorar lo imprescindible o no de las medidas empresariales que impliquen "*modulación*" de los derechos fundamentales, lo que sucede con las SSTC 98/2000[163] y 186/2000[164].

C) Protección procesal

Desde el punto de vista procesal, la Ley 36/2011 de 30 de octubre Reguladora de la Jurisdicción Social responde mejor que la anterior al mandato constitucional que exige la existencia de un procedimiento preferente y sumario a través del cual cualquier ciudadano pueda recabar la tutela de los derechos fundamentales, a través de un proceso específico y autónomo *ex* arts. 177 a 183 LRJS.

---

[162] STC 99/1994, de 11 de abril (EDJ 1994/3085).

[163] STC 98/2000, de 10 de abril (RTC 2000\98).

[164] STC 186/2000, de 10 de julio (RTC 2000\186).

Se corrige la confusa denominación que el proceso tenía en la anterior normativa, la rúbrica anterior en la LPL era "*tutela de los derechos de la libertad sindical"*, se produjo de manera posterior una ampliación del procedimiento al resto de derechos fundamentales, en virtud del derogado art. 181 LPL. Y existen diversas mejoras que incorpora la LRJS, para alcanzar una completa tutela: se amplía la legitimación pasiva, se podrá recabar la tutela contra terceros vinculados al empresario por cualquier título, se contempla expresamente la eficacia *erga omnes*, determinando que la víctima de la lesión puede recabar tutela contra el titular de la relación laboral y contra cualquier otro sujeto que resulte responsable[165].

D) Recapitulación

Llegado a este punto de la exposición, a modo de síntesis, se pueden establecer algunas pautas generales:

- El trabajador no ve suprimido ni negado ningún derecho fundamental por el hecho de la firma de un contrato de trabajo. Los derechos fundamentales de los trabajadores disfrutan de una especial garantía frente al derecho de control contenido en la libertad de empresa.
- No puede desconocerse que la inserción en la organización ajena que supone el contrato de trabajo modula los derechos fundamentales en la medida "*estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva*". Al ser contratado, queda sometido a las instrucciones y controles del empresario, lo que supone una limitación o modulación de sus derechos fundamentales.
- La relación laboral, en cuanto tiene como efecto típico la sumisión de ciertos aspectos de la actividad humana a los poderes empresariales, es el marco que ha de tomarse en consideración a la hora de valorar hasta qué punto ha de producirse la coordinación entre el interés del trabajador y el de la empresa que pueda entrar en colisión.

[165] MARÍN ALONSO, I. y GUTIÉRREZ PÉREZ, M.: «La práctica de la prueba en materia de derechos fundamentales tras la Ley de Jurisdicción Social», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 21, 2012, págs. 8 y 9.

2. La "*modulación*" de los derechos fundamentales

La CE no establece ninguna preferencia entre los intereses y derechos del empresario y los derechos constitucionalmente protegidos del trabajador. Comúnmente se expresa, como hemos aludido, que los derechos constitucionales expresan una modulación en el seno del contrato de trabajo, idea que ha sido difundida por la propia jurisprudencia constitucional. Estos derechos han de adaptarse desde el contexto del Derecho Público a la realidad de la empresa y del trabajo asalariado.

A) Idea general

El marco normativo del contrato de trabajo (leyes, convenios colectivos e incluso, estipulaciones contractuales) configura una institución social específica que no puede desaparecer simplemente porque los derechos fundamentales se proyecten sobre ella. Esto implica, en primer lugar, que la propia definición de los derechos debe conjugarse de manera lógica con las obligaciones contractuales del trabajador. Los derechos fundamentales deben ejercerse de un modo adecuado a las instituciones sociales en las que se desenvuelven y su contenido tiene límites.

La inserción en la organización ajena modula aquellos derechos, en la medida estrictamente imprescindible para que el correcto y ordenado desenvolvimiento de la actividad productiva; reflejo, a su vez, de derechos que han recibido consagración en el texto de nuestra norma fundamental (arts. 38 y 33 CE). Como en todo caso de colisión de derechos fundamentales o bienes constitucionalmente protegidos deben apreciarse "los intereses en presencia, mediante una adecuada ponderación de las circunstancias concurrentes" [166] STC 99/1994, de 11 de abril[167].

La idea de modulación entraña un proceso de reflexión que ha de desarrollarse en tres pasos sucesivos: la delimitación del derecho en cuestión, la identificación de los bienes o derechos afectados por su ejercicio y la búsqueda en su caso de criterios

[166] SEMPERE NAVARRO, A.V. :«Apuntes sobre la libertad de conciencia en el ámbito laboral», *Revista Aranzadi Doctrinal* núm. 10, 2015 (BIB 2015\16773).

[167] STC 99/1994, de 11 abril (RTC 1994\99).

razonables y proporcionados para la adecuada resolución de eventuales situaciones de conflicto[168].

B) Ponderación de derechos

El modo jurídico en que se solventa este dilema, puesto que el legislador no tiene obligación reconocida legalmente de regular con mayor o menor detalle las distintas esferas de los derechos constitucionales, ha sido establecido por la jurisprudencia a través de la técnica de la ponderación (que se analizará más adelante) entre derechos y bienes constitucionales y la modulación de su ejercicio conforme al criterio de la buena fe[169].

Respecto a esta cuestión, conviene realizar una primera precisión, y es que no suele hablarse de modulación con respecto a los derechos laborales ordinarios o específicos, seguramente porque juegan en el ámbito que resulta más propio o característico[170].

La modulación trata de articular un sistema que permita al trabajador ejercitar, sin desvirtuarlos, sus derechos fundamentales y libertades públicas aun en el seno de la relación de trabajo; que habrá de respetar, porque los deberes contractuales que ahora chocan con sus derechos fundamentales han sido asumidos voluntariamente por él (artículo 5. a) ET). En ese forcejeo se busca evitar que los derechos constitucionales cedan absoluta y desproporcionadamente ante los deberes laborales, puesto que aquellos son inherentes a la dignidad de la persona, y constituyen el fundamento del orden público y la paz social (artículo 10.1 CE)[171].

Por todo ello, el Tribunal Constitucional se ha pronunciado a favor de que las resoluciones judiciales preserven el necesario equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito modulado por el contrato. Dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, esa modulación solo deberá producirse en la medida estrictamente imprescindible para el

---

[168] GARCÍA MURCIA, J.: «Presentación» en AA. VV. GARCÍA MURCIA, J. (Dir.) *Derechos del Trabajador y Libertad de Empresa*, *op.cit.*, pág. 47.

[169] SALAS PORRAS, M.: «Ponderación y modulación del ejercicio del derecho a la libertad religiosa en el contexto obligacional laboral: una mirada a la jurisprudencia española», *Revista Crítica de la Historia de las Relaciones Laborales y de la Política Social*, núm. 9, 2014.

[170] *Ibídem*, pág. 35.

[171] SALAS PORRAS, M.: «Ponderación y modulación del ejercicio del derecho a la libertad religiosa en el contexto obligacional laboral: una mirada a la jurisprudencia española». *op. cit.*, pág. 45.

correcto y ordenado respeto de los derechos fundamentales del trabajador. Ello significa que, aunque el empresario pueda controlar el cumplimiento por los trabajadores de sus obligaciones laborales, deberá atenerse siempre a los límites que le vienen impuestos con respecto a los derechos constitucionales de aquellos[172].

Citemos un par de pronunciamientos del TC a título ilustrativo:

- La modulación que el contrato de trabajo puede producir en el ejercicio de los derechos fundamentales ha de ser la estrictamente imprescindible para el logro de los legítimos intereses empresariales, así como proporcional y adecuada a la consecución de tal fin[173].
- La omisión de tutela jurisdiccional de los derechos fundamentales del trabajador frente a lesiones padecidas en el ámbito de la relación laboral puede ser impugnada a través del recurso de amparo constitucional, como si fuese la resolución judicial la que incurriese en la vulneración de aquellos[174].

C) Recapitulación

Es cierto que el hecho de que se deje a la casuística una temática tan delicada como el ejercicio de los derechos fundamentales en un contexto de dependencia jurídica tiene como resultado que, de entre los diversos derechos inespecíficos, se hayan producido protecciones de distinto grado, según si el derecho en cuestión es de los más próximos al núcleo de la relación laboral -como es el caso del derecho a la libertad ideológica, de expresión e información- que tradicionalmente en la jurisprudencia ha recibido con una mayor protección constitucional. O cuando quedaba más lejano, como es el caso del derecho a la intimidad, que se han mantenido preteridos en unas zonas más frías o de mínima "constitucionalización"[175].

---

[172] VICEDO CAÑADA, L. y VIDAL VIDAL, J.: «Límites a los Derechos Fundamentales del Trabajador: intimidad y dignidad». *Revista Doctrinal Aranzadi Social* núm. 55, 2012 (BIB 2012\3061).

[173] STC 20/2002, de 28 enero (FJ 4º) (RTC 2002\20).

[174] STC 129/1989, de 17 julio (FJ 2º) (EDJ 1989/7392).

[175] SALAS PORRAS, M.: «Ponderación y modulación del ejercicio del derecho a la libertad religiosa en el contexto obligacional laboral: una mirada a la jurisprudencia española», *op.cit.*, págs. 45-46.

A modo de conclusión, podemos afirmar que la modulación implica una relativización del planteamiento; hay derechos constitucionales, pero modalizados. Todo ello, en suma, desemboca en un juicio de razonabilidad; y sabido es que tal campo nos lleva al ámbito de la subjetividad[176].

3. Doctrina constitucional concordante: evolución

Más atrás queda advertida la enorme relevancia que los criterios emanados de los grandes Tribunales poseen en una materia escasamente abordada por las leyes. El problema surge porque el enfoque que la jurisprudencia ha asumido no permanece estático sino que ha evolucionado. Por exclusiva referencia a la doctrina de nuestro Tribunal Constitucional acerca del control de la prestación del trabajador a través de las nuevas tecnologías en relación al derecho a la intimidad podemos diferenciar tres grandes etapas.

A) Primera etapa

La denominada eficacia horizontal de los derechos fundamentales o "eficacia entre particulares" fue desde muy pronto reconocida por el Tribunal Constitucional, precisamente en el ámbito laboral; donde uno de los particulares, el empleador, ocupa una posición de cierto poder respecto al otro, el empleado (SSTC 78/1982, de 20 de diciembre [177] y 47/1985, de 27 de marzo[178].).

---

[176] SEMPERE NAVARRO, A.V.: «Modulación laboral de los derechos cívicos: STC 99/1994, de 11 de abril», *Persona y derecho*. *Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos*, núm. 54, 2006, pág. 490.

[177] STC 78/1982, de 20 de diciembre (RTC 1988\6).

[178] STC 47/1985, de 23 marzo (EDJ 1985\47) recoge " sin entrar a delimitar aquí hasta dónde alcanza la dimensión entre particulares de los derechos fundamentales y libertades públicas, esto es, la denominada eficacia respecto de terceros, es claro que el presente recurso no podría ni siquiera existir si en el caso no estuviera involucrado, además y después del Centro docente y su Profesora, algún poder público al cual se le pudiera atribuir la violación del derecho fundamental invocado, que en este caso es el de la libertad ideológica".

El TC sostiene en este período, en relación con las modulaciones que los derechos fundamentales experimentan en el marco del contrato de trabajo, la idea de equilibrio o ponderación de intereses en juego; más propia de las relaciones privadas. Destacan las SSTC 6/1988 de 21 de enero[179], 186/1996 de 25 de noviembre[180], y la 1/1998 de 12 de enero[181].

La idea de criterio de proporcionalidad ya se había anticipado en algunos pronunciamientos, en los que se alude la exigencia de "*una racionalidad específica*", basada en los requerimientos organizativos y productivos de la empresa, en este sentido STC 99/1994 de 11 de abril[182]. Encontramos afirmaciones tales como " *el control a través de las cámaras de vídeo es tan lícito como el que pudiera realizar el director gerente*" [183].

Los criterios fundamentales son, por una parte, la limitación del control al ámbito del trabajo, sin extenderse a los lugares afectados a finalidades de orden personal de los trabajadores, como pueden ser los vestuarios, servicios, salas de descanso, lugares de esparcimiento, etc. y, por otra parte, la finalidad de ese control ha de ser estrictamente laboral. En definitiva, esta fase, se caracteriza por una permisividad en el control al trabajador por parte del empresario.

B) Segunda etapa

Esta fase está marcada por la doctrina de las SSTC 98/2000, de 10 de abril[184] y 186/2000 de 10 de julio[185], resolviendo los casos del Casino de La Toja y del Economato de Ensidesa, que supusieron la declaración en el orden constitucional de que en el centro de trabajo pueden producirse actuaciones lesivas a la intimidad del trabajador; lo que provocó el posterior cambio en la doctrina social. Estas sentencias, constituyen doctrina constitucional de referencia en lo que respecta a la extensión de los poderes de control de las nuevas tecnologías por el empresario.

---

[179] STC 6/1988, de 21 de enero (RTC 1988\6).

[180] STC 186/1996, de 25 de noviembre (RTC 1996\186).

[181] STC 1/1998, de 12 de enero (RTC 1998\1).

[182] STC 99/1994, de 11 abril (RTC 1994\99).

[183] STSJ Andalucía de 17 de enero de 1994 (ID CENDOJ 41091340011994100004).

[184] STC 98/2000, de 10 de abril (RTC 2000\98).

[185] STC 186/2000, de 10 de julio (RTC 2000\186).

Ambas sentencias definen toda una pauta de resolución de conflictos en el ámbito laboral, habiéndose convertido en el canon prevalentemente utilizado en la práctica constitucional y judicial para valorar la legitimidad de cualquier medida restrictiva de derechos fundamentales; pues hasta ese momento existían distintos pronunciamientos de los tribunales laborales, que no siempre eran coincidentes. Suponen un cambio de método, o de enfoque, a la hora de enjuiciar el problema, puesto que parten de que la instalación de los medios es *a priori* una medida restrictiva de los derechos del trabajador; y por tanto, se ha de considerar también de modo restrictivo la posibilidad de recurrir a tal medida.

Pese al sentido opuesto de los pronunciamientos, debido a que se trata de casos distintos, el fundamento de ambas sentencias es el mismo; se resuelve el conflicto entre el interés empresarial y el derecho a la intimidad del trabajador. Respecto a la afectación a la intimidad deben ceder las facultades de control de la empresa en la STC 98/2000, de 10 de abril[186] o bien ceder una parte del derecho a la intimidad del trabajador en la STC186/2000, de 10 de julio[187], dependiendo del juicio de ponderación.

Si acaso, anotemos que la STC 29/2013, de 11 febrero, caso del Profesor de la Universidad de Sevilla marca el cénit de la protección constitucional, negando la posibilidad de que el empleador utilice imágenes grabadas por las cámaras de seguridad existentes en sus instalaciones cuando previamente no lo ha advertido. Se afirma que el poder de control sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin: por ello se precisa una "información previa y expresa, precisa, clara e inequívoca (…) de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida"

C) Tercera etapa

Esta etapa viene marcada por la STC 170/2013, de 7 de octubre[188], que supuso un punto de inflexión, una gran novedad con respecto a la doctrina anterior constitucional del punto anterior, fijando importantes directrices[189]. Sienta que la prohibición de uso de

[186] STC 98/2000, de 10 de abril (RTC 2000\98).

[187] STC 186/2000, de 10 de julio (RTC 2000\186).

[188] STC 170/2013, de 7 de octubre (RTC 2013\170).

[189] MIRÓ MORROS, D.: «El uso del correo electrónico en la empresa: protocolos internos»,*op.cit.*

las tecnologías para un empleo particular, a través de Convenio Colectivo, permite lo siguiente:

- Que la empresa fiscalice el contenido de los correos electrónicos enviados y recibidos por el trabajador, sin advertencia previa al trabajador.
- Enervar la expectativa razonable de confidencialidad, razón por la cual no se consideran vulnerados derechos constitucional a la intimidad.

Por tanto, el principal cambio de esta doctrina, reside en que sea considerado por parte del Tribunal Constitucional que el requerimiento previo a una posible intervención del correo corporativo por parte de la empresa que es la promulgación de una política empresarial sobre el uso del correo electrónico, puede sustituirse, por un artículo en el Convenio Colectivo, que sanciona el uso desviado de tal medio. Incluso en este caso concreto que se tipificaba como leve, la conducta imputada, por incumplir el trabajador, se deriva la responsabilidad de manera implícita a lo establecido en el Convenio[190]. El razonamiento de la STC 170/2013, es del todo cuestionable pues de él se extraen dos conclusiones con las que estamos, en total desacuerdo:

1) El hecho de que un Convenio Colectivo tipifique una conducta como sancionable equivale a prohibirla, aunque no lo anuncie expresamente.

2) Un Convenio Colectivo podrá limitar decisivamente el ejercicio de derechos fundamentales[191].

La aplicación correcta del principio de proporcionalidad de manera debida para MONEREO PÉREZ y LÓPEZ INSUA no hubiera llevado a la misma solución sostenida en la STC 170/2013; el Alto Tribunal parece haber olvidado una cuestión trascendental y es que la proporcionalidad de una medida se pondera en el momento de autorizar una violación de derechos fundamentales y no *a posteriori*, a la vista de los resultados obtenidos. Se confunde la legitimidad del fin con la constitucionalidad del acto (legitimidad de origen), lesionándose gravemente los derechos contenidos en los artículos 18.1 y 18. 3 CE desde el inicio de la actuación empresarial[192].

---

[190] CARRASCO DURÁN, M.: «El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa», *Revista Aranzadi Doctrinal* núm. 9, 2014 (BIB 2013\2695).

[191] MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit.*

[192]MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit.*

Del mismo modo que en la etapa precedente, el cénit de la doctrina se logra con otra resolución posterior: en este caso la STC 39/2016, de 3 de marzo, caso Bershka, advirtiendo que suscribir el CT implica consentir el tratamiento de datos para control de la relación laboral; basta el mero conocimiento por el trabajador, pues son datos necesarios para el cumplimiento del contrato (art. 6.2 LOPD) y la falta de conocimiento vulnera la PD sólo si la medida empresarial es desproporcionada. Además, hay conocimiento si la empresa coloca información sobre vigilancia en lugar visible (distintivo Instrucción 1/2006 AEPD).

4. El principio de proporcionalidad

El principio de proporcionalidad es un criterio metodológico que cumple la función de estructurar el procedimiento interpretativo para la determinación del contenido de los derechos fundamentales. Sirve para controlar cualesquiera actos que inciden sobre los intereses de los particulares.

En las alusiones jurisprudenciales más representativas, este principio aparece articulado de tres subprincipios: idoneidad, necesidad y proporcionalidad en sentido estricto. Cada uno expresa determinada exigencia que toda intervención en derechos fundamentales debe cumplir.

A) Origen y evolución

Los primeros antecedentes del principio de proporcionalidad en el Derecho Público español datan de mediados del S. XX, cuando comenzó a ser utilizado en la jurisdicción contencioso-administrativa para la fundamentación de sus decisiones .La Sentencia del Tribunal Supremo de la Sala V de 20 de febrero de 1959, fue pionera de esta corriente jurisprudencial sostuvo que los principios generales del Derecho constituían un límite a la potestad reglamentaria, aplicando el principio de proporcionalidad[193].

Tras la promulgación de la Constitución Española y, posteriormente, con la (hoy derogada) Ley 30/1992, esta tendencia se propagó a otros campos del control de la

[193] UREÑA SALCEDO, J. A.: «El principio de servicio objetivo a los intereses generales y su control por los tribunales», *D. A. Revista Documentación Administrativa* núm. 289, 2011, pág. 66.

actividad administrativa: urbanismo, medio ambiente, liquidación de impuestos municipales, construcción, imposición de medidas cautelares, sanciones administrativas, etc. y en general, al ejercicio de los poderes discrecionales. El propio Tribunal Supremo ha señalado la sorprendente difusión del principio de proporcionalidad a lo largo y ancho de su jurisprudencia administrativa.

El principio de proporcionalidad también ha sido adoptado por el Tribunal Constitucional como uno de sus criterios estelares, para la fundamentación de sus decisiones. En esta jurisdicción se ha aplicado en los asuntos de la más variada índole. La principal novedad de los últimos años radica, en el intento del Tribunal Constitucional español "*de formalizar este principio*", es decir, llenarlo de contenido mediante diversos criterios que permitan disminuir, en la medida de lo posible, su indeterminación[194].

La utilización formal, a partir de mediados de la década de los noventa del "*test alemán*" de la proporcionalidad, esto es, de los requisitos de idoneidad, necesidad y proporcionalidad en sentido estricto, ha convertido a este principio en uno de los protagonistas de la jurisprudencia constitucional de los últimos años.

En Alemania el principio de proporcionalidad viene siendo empleado tanto en Derecho Administrativo como en Derecho Constitucional, y se ha extendido durante estos años por Europa, gracias al Tribunal Europeo de Derechos Humanos, y sobre todo, por el Tribunal de Justicia de la Unión Europea, cuya jurisprudencia ha sido emulada por otros Tribunales Constitucionales Europeos, el francés, el italiano, el portugués, el austriaco, el húngaro, el checo , el esloveno, el estonio, el español y por la Jurisdicción Constitucional Suiza[195].

B) Alcance

Con arreglo a este relevante principio, los actos del empresario solo podrán reputarse proporcionados, y por tanto válidos, cuando respeten cumulativamente tres requisitos:

---

[194] GONZÁLEZ BEILFUSS, M.: «El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional», *Cuadernos Aranzadi del Tribunal Constitucional*, núm. 11, 2003 (BIB 2003\1632).

[195] BERNAL PULIDO, C.: *El Principio de proporcionalidad y los derechos fundamentales*, Centro de Estudios Políticos y Constitucionales 2007, págs. 55-56.

- Que la intervención sea adecuada para alcanzar el fin que se propone.
- Que sea necesaria, en cuanto que no quepa una medida alternativa, menos gravosa para el interesado.
- Que sea proporcionada en sentido estricto; que en ningún caso suponga un sacrificio excesivo del derecho. Este último requisito significa que aun cuando la medida sea adecuada y necesaria, deberá considerarse inválida si implica el vaciamiento del derecho en juego.

El principio de proporcionalidad no está expresamente previsto en nuestra Constitución, con todo la jurisprudencia viene haciendo un uso cada vez más frecuente del mismo. Desde el punto de vista del Derecho del Trabajo, la proporcionalidad es una técnica tendente a que los intereses del empresario no se logren a costa de los derechos e intereses del trabajador, sino que se busque un punto de equilibrio entre ambos. No se trata pues de enjuiciar la corrección de la conducta del empresario, sino de realizar un juicio ponderativo[196].

El principio de proporcionalidad fue enunciado en la STC 37/1998, de 17 de febrero[197], en relación con la vulneración del derecho de huelga por la grabación de imágenes realizada por la Ertzaintza a un piquete de huelga informativo. Asimismo también había sido utilizado para valorar diversas medidas que afectaban a derechos fundamentales, entre los que podemos citar, a título de ejemplo, la libertad de expresión[198]

[196] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op.cit*., pág.49.

[197] STC 37/1998, de 17 de febrero (RTC 1998\37).

[198] Se cuestiona en el recurso de amparo si la filmación en vídeo por la Ertzaintza de un piquete de huelga informativo vulneró los derechos de libertad sindical y de huelga. El TC considera que la captación ininterrumpida de imágenes fue una medida desproporcionada para conseguir la finalidad que se pretendía con la misma -prevenir situaciones de desorden y contrarias a otros derechos y libertades- toda vez que existían medidas menos restrictivas para el derecho fundamental de huelga. Así otorga el amparo y anula las sentencias impugnadas en la medida que no han reparado la lesión invocada.

de la STC 1/1998 de 12 enero [199] y el derecho de reunión[200] de la STC 66/1995 de 8 de mayo[201].

C) La técnica del "triple test"

El Tribunal Constitucional ha tratado de precisar la técnica que ha de emplearse para medir la licitud de las medidas empresariales, restrictivas de los derechos fundamentales de los trabajadores en el ámbito laboral; pero, pese a todo, no se pueden realizar generalizaciones existen algunas contradicciones y no es fácil determinar cómo puede hacer uso el empresario del control al trabajador, ni en qué medida quedan afectados los derechos de los trabajadores.

La formulación del principio de proporcionalidad, puede servir para dar respuesta a problemas interpretativos que se pudieran plantear, con el llamado "*triple test*". Es necesario comprobar si se cumplen los tres requisitos o condiciones siguientes:

a) Juicio de idoneidad

El subprincipio de idoneidad, es también conocido con el nombre de "*subprincipio de adecuación"*. De acuerdo con el concepto juicio de *idoneidad*, toda intervención en los derechos fundamentales debe ser adecuada para contribuir a la obtención de un fin constitucionalmente legítimo. Y aplicándolo al control empresarial, si la medida del empleador es susceptible de conseguir el objetivo propuesto, supera la idoneidad. De

---

[199] STC 1/1998, de 12 enero (RTC 1998\1).

[200] El demandante de amparo fue despedido a consecuencia de la denuncia que realizó al Ayuntamiento de Oviedo, titular del servicio público cuya prestación es objeto único de la empleadora, en régimen de concesión, de determinadas irregularidades que, a juicio del recurrente, debían conducir a la caducidad de la referida concesión. Estima el TC que en la ponderación realizada por las resoluciones impugnadas entre el derecho a la libertad de expresión del solicitante de amparo y las modulaciones que a su contenido impone el deber de buena fe, no se tuvo en cuenta, tratándose de una empresa que presta un servicio público, el interés público del contenido de las manifestaciones realizadas por el recurrente, por lo que no fue constitucionalmente adecuada.

[201] STC 66/1995, de 8 de mayo (RTC 1995\66).

modo que se convierte, de inicio, en legítimo cualquier interés empresarial que pueda ser satisfecho por la medida de control; lo único que se precisa es adecuación.

La idoneidad es que la medida "*no sea manifiestamente irracional, arbitraria ni caprichosa*"[202], pero prácticamente, cualquier medida en este sentido funcionalmente enlaza con un interés empresarial.

b) Juicio de necesidad

El subprincipio de *necesidad* se denomina también subprincipio de "*indispensabilidad*" en la doctrina alemana, pero en la española se ha acuñado de forma unánime el concepto *necesidad* [203]. El juicio de necesidad implica la comparación entre la medida adoptada por la empresa, y otros medios alternativos que se pudieran haber escogido. En esta comparación se examina si alguno de los medios opcionales logra cumplir dos exigencias: en primer lugar, si reviste el grado de idoneidad para contribuir a alcanzar el objetivo inmediato de esta última; y en segundo lugar, si afecta al derecho fundamental en un grado menor. Es decir, que no exista otra medida más moderada para la consecución del propósito perseguido por la empresa con igual eficacia.

Con la expresión "*igual eficacia*" se hace referencia al parámetro para verificar, el carácter necesario o indispensable de la instalación de una cámara en un determinado lugar del trabajo, por ejemplo, para lo cual se ha de realizar una atenta valoración de otros medios posibles, el examen de su idoneidad y de la intensidad con que afecta negativamente al derecho fundamental; pues estos son los aspectos determinantes del juicio de necesidad.

Los subprincipios de idoneidad y de necesidad expresan el mandato de optimización relativo a las posibilidades fácticas. En ellos la ponderación no juega ningún papel. Se trata de impedir ciertas intervenciones en los derechos fundamentales, que sean

---

[202] VALDÉS DAL- RÉ, F.: «Contrato de trabajo, derechos fundamentales de la persona del trabajador y poderes empresariales, una difícil convivencia», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 2, 2003, pág. 100.

[203] BERNAL PULIDO, C.: *El Principio de proporcionalidad y los derechos fundamentales*, *op.cit.*, pág. 740.

evitables, sin menoscabo de otros principios[204], se trata, en definitiva del "*óptimo de Pareto*"[205].

c) Juicio de proporcionalidad, en sentido estricto

Conforme al subprincipio de proporcionalidad en sentido estricto, también conocido como *juicio de ponderación* en nuestro país, y en la doctrina alemana, como *juicio de adecuación*, nos referimos a la optimización relativa a las posibilidades jurídicas. Existen autores que utilizan el principio de proporcionalidad y el principio de ponderación como sinónimos, también hay otros que opinan que su coincidencia solo es parcial. La posición más coherente, nos parece la de BERNAL PULIDO, que identifica la ponderación con el principio de proporcionalidad en sentido estricto, por lo que es considerado cuna parte de principio de proporcionalidad, ya que la ponderación es el procedimiento de aplicación jurídica mediante el cual se establecen las relaciones de prelación entre principios en colisión[206].

La importancia de la intervención del derecho fundamental debe estar justificada por la magnitud del fin perseguido por el empleador; las ventajas que se obtienen mediante la intervención del empresario en el derecho fundamental deben compensar los sacrificios que ésta implica para el trabajador. En resumen, si la medida es ponderada o equilibrada, porque derivan de ella más beneficios o ventajas para el interés general que perjuicios o valores en conflicto. El decurso argumentativo del principio de proporcionalidad, en sentido estricto, debe estructurarse en tres pasos:

---

[204] ALEXY, R.: «La fórmula del peso» en AA. VV. CARBONEL, M. (Coor.): *El principio de proporcionalidad y la interpretación constituciona*l, págs. 13-42. Ministerio de Justicia y Derechos Humanos, ed. Carbonell. 2008, (Traducción al castellano de Carlos Bernal Pulido del texto alemán original publicado en: "Die Gewichtsformel", en Joachim Jickeli et al. eds., Gedächtnisschrift für Jürgen Sonnenschein, De Gruyter, Berlín, 2003, págs. 771 –792).

[205] Concepto de la economía que consiste en que partiendo de una asignación inicial de bienes entre un conjunto de individuos, si se realiza un cambio nueva asignación que al menos mejore la situación de un individuo sin hacer que empeore la situación de los demás, se denominaría mejora de Pareto. Una asignación se define como "*pareto-eficiente*" o "*pareto-óptima*" cuando no pueden lograrse nuevas mejoras de Pareto. Término que tiene aplicaciones en ingeniería y diferentes ciencias sociales y que recibe su nombre a partir del economista italiano Vilfredo Pareto, quien utilizó este concepto en sus estudios sobre eficiencia económica y distribución de la renta.

[206] BERNAL PULIDO, C.: *El Principio de proporcionalidad y los derechos fundamentales, op. cit.*, pág. 581.

1º. El primer paso supone determinar las magnitudes que deben ser ponderadas, es decir, la importancia de la intervención del derecho fundamental y la relevancia de la realización del fin perseguido por el empresario. Los objetivos que concurren en la ponderación son, de un lado, determinar el alcance de la lesión del derecho fundamental afectado y, de otro, la magnitud de la medida de control empresarial.

2º. El segundo paso compara dichas magnitudes, a fin de determinar si la importancia del fin perseguido por el empresario es mayor que la importancia de la intervención en el derecho fundamental. Para llevar a cabo esta comparación es imprescindible haber fijado la magnitud de la importancia de los dos objetivos perseguidos, respectivamente, de manera positiva y de manera negativa. Por un lado, proteger los derechos fundamentales del trabajador y; por otro lado lo que se obtendría con la intervención empresarial. De acuerdo con la nomenclatura, ya usual en la doctrina, dicha magnitud se conoce como "*el peso*"; se tiende a reducir el enjuiciamiento de las pretensiones a un problema de *peso*[207], cuanto más intensa sea la intervención en el derecho fundamental, mayor será el peso del derecho de la ponderación.

Correlativamente, cuanto más intensa sea la realización de la finalidad perseguida por el empresario y que fundamenta la medida de control, mayor será su peso en la ponderación. En estos casos, según ALEXY, "*uno de los principios tiene que ceder ante el otro*"[208]. Por tanto, no cabe confundir el valor o peso específico del bien jurídico con la técnica o garantía de protección, de tal forma que no existe de antemano una jerarquía que haga prevalecer automáticamente unos derechos sobre otros.

Llegados a este término, como ya hemos apuntado anteriormente, el punto débil de la referida técnica consiste en que la ponderación actúa como un "*mandato de optimización*", los intereses a ponderar se convierten en un problema de peso; el reproche a la teoría de los principios se centra en señalar que es incapaz de determinar de forma adecuada, por un lado, la relación entre los derechos fundamentales y el control constitucional, y, por otro lado, de éstos con la democracia[209] .

---

[207] ALEXY, R.: *Teoría de los derechos fundamentales*, ed. Centro de Estudios Constitucionales, 1993, pág. 89.

[208] *Ibídem*, pág. 88.

[209] ALEXY, R.: «Principios formales», *DOXA, cuadernos de Filosofía del Derecho*, núm.37, 2014, pág. 16.

El referido margen de discrecionalidad puede ser muy amplio, y, por tanto, la decisión impredecible, el equilibrio de la balanza puede inclinarse a uno u otro lado en base a apreciaciones subjetivas: se magnifica la lesión de un derecho y se minimiza la restricción del otro con medidas que pueden variar en uno y otro caso[210]. Por lo que la doctrina científica exige que la comparación entre bienes jurídicos en seno el juicio de proporcionalidad en sentido estricto "no se realice en términos abstractos y generales, sino a partir de una ponderación de carácter necesariamente concreto, es decir, a partir de las específicas circunstancias del caso, lo que impide extraer pautas axiológicas constitucionalmente indiscutibles". Extendiendo determinados sectores de la doctrina este requisito al juicio de necesidad, "cuyo resultado debe ceñirse exclusivamente al caso concreto, sin que puedan desprenderse tampoco en este caso prohibiciones abstractas o absolutas" [211].

3.º El tercer paso construye una relación de precedencia condicionada entre el derecho fundamental y el fin del empresario, con base en el resultado de la comparación llevada a cabo en el segundo paso. Una vez se ha determinado la intensidad de la intervención en el derecho fundamental y la intensidad de la realización del principio constitucional que fundamenta la medida empresarial, debe llevarse a cabo la ponderación, propiamente dicho en sentido estricto; consiste en una comparación entre el grado de intensidad de la intervención en el derecho fundamental y el grado de la realización del principio que fundamenta la medida empresarial que se controla, para establecer una relación de precedencia condicionada entre aquel derecho y la medida de control empresarial.

La regla argumentativa que define la ponderación en sentido estricto, ha sido esbozada por el Tribunal Constitucional Alemán y ha sido enunciada doctrinalmente por ALEXY, según la ley de la ponderación: "*cuanto mayor sea el grado de no satisfacción o restricción de uno de los principios, tanto mayor deberá ser el grado de la importancia de la satisfacción del otro"*[212]. Esto quiere decir que la combinación entre la "*no satisfacción*" y la "*afectación*" conforma un doble concepto: la dicotomía entre los

[210] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op.cit.*, pág. 23.

[211] LLOBERA VILA, M.: «El efecto sustitución del legislador laboral y de la autonomía colectiva en la aplicación del juicio de proporcionalidad por parte del TJUE», *Lex Social: revista de los derechos sociales,* núm. 2, 2016, pág. 54.

[212] ALEXY, R.: «Teoría de los derechos fundamentales», *op. cit.*, pág. 146.

derechos de defensa y los derechos de protección. Cuando se trata de un derecho fundamental como el derecho de defensa, entonces la medida *sub judice* representa una intervención. Las intervenciones son restricciones. La expresión "*no satisfacción"* opera de una manera natural, cuando se trata de los derechos de protección. A diferencia de los derechos de defensa, estos derechos no exigen una omisión, sino un actuar positivo. Aquí también puede hablarse de "*restricción"* y, por tanto, de "*intervención",* lo cual de nuevo es un indicador de la flexibilidad del lenguaje. Cuando un principio exige protección, pero no ha sido garantizado, no solo puede hablarse de una "*no satisfacción*" de ese principio, sino también de una intervención en el mismo, y, por tanto, de una "intervención por medio de una no satisfacción".

En el primer paso, es preciso definir el grado de la no satisfacción o de afectación de uno de los principios. Luego, en un segundo paso, se define la importancia de la satisfacción del principio que juega en sentido contrario. Finalmente, en un tercer paso, debe definirse si la importancia de la satisfacción del principio contrario justifica la restricción o la no satisfacción del otro.

El resultado del examen de ponderación consiste en una relación de precedencia condicionada, porque uno de los dos intereses en pugna adquiere prioridad. En este sentido, el Tribunal Constitucional ha establecido en la STC 320/1994 de 28 de noviembre[213], que en caso de colisión de derechos fundamentales:

> *"La solución consistirá en otorgar la preferencia de su respeto a uno de ellos, justamente aquel que lo merezca, tanto por su propia naturaleza, como por las circunstancias concurrentes en su ejercicio. No se trata, sin embargo, de establecer jerarquía de derechos ni prevalencias a priori, sino de conjugar, desdén la situación jurídica creada, ambos derechos o libertades ponderando, pesando cada uno de ellos, en su eficacia recíproca para terminar decidiendo y dar preeminencia al que se ajuste más al sentido y finalidad que la Constitución señala, explícita o implícitamente" (FJ 2º).*

D) Otros requisitos

a) Necesidad de justificación suficiente

Tras la regla del triple test, SEMPERE NAVARRO y SAN MARTÍN MAZZUCCONI afirman que adicionalmente se exige también que la restricción o medida sea necesaria; ha de revelarse como indispensable para el correcto y ordenado

[213] STC 320/1994, de 28 de noviembre de 1994 (EDJ 1994/8971).

desenvolvimiento de la actividad productiva, lo cual significa que responda a motivaciones objetivas, distintas del mero interés empresarial[214]; como recoge la STC 98/2000 con la siguiente alusión: "*la mera utilidad o conveniencia no legitima sin más*".

b) Autodeterminación informativa

Algún autor sostiene que la regla del triple test es insuficiente por su escaso grado de efectividad, y que la autotutela informativa constituye un elemento de cierre del juicio de legitimidad de la actividad de control empresarial, que integra las reglas y requisitos que conciernen a las actividades de recogida de información, e incorpora las condiciones de licitud del tratamiento de datos del trabajador[215]. Quizás este requisito tras la STC 39/2016 de 3 de marzo[216], haya perdido vigencia.

E) Debate sobre su virtualidad

El constitucionalista DÍEZ PICAZO reconoce que el principio de proporcionalidad ha tenido el mérito innegable de vindicar la importancia del legislador democrático, para la definitiva configuración de los derechos fundamentales; aunque subraya que es particularmente "*sensible*" hacia un fenómeno crucial como es la variabilidad histórica del significado de los distintos derechos. Considera que en el fondo, el principio de proporcionalidad es una nueva y sofisticada concepción estricta de los derechos fundamentales. Argumenta que ante una situación que aspira a ser comprendida dentro del contenido de un derecho fundamental, la respuesta solo podría ser afirmativa o negativa, "*sin dejar espacio intermedio de protección prima facie*". Si no se distinguen estas dos posibilidades en el contenido de los derechos fundamentales, nada sería verdaderamente esencial. El problema estriba, pues, en que si se razona de esta forma, no se deja espacio para el principio de proporcionalidad. La objeción que cabe hacerse es la

---

[214] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI. C. : *Nuevas tecnologías y Relaciones Laborales, op, cit*., pág. 46.

[215] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *op. cit.*, pág. 19

[216] STC 39/2016, de 3 marzo (RTC 2016\39).

visión diacrónica del contenido esencial, que no exige que las intervenciones sobre los derechos fundamentales sean adecuadas y necesarias[217].

El constitucionalista BERNAL PULIDO recoge las críticas en el ámbito internacional de E. FORSTHOFF y de A. ALEINIKOFF, sobre el principio de proporcionalidad, que se sintetizan en lo siguiente: llegan a afirmar que el Tribunal Constitucional Alemán, en el caso del primero, y el Tribunal Supremo Federal de Estados Unidos, en el caso del segundo, carecen de legitimidad para aplicar el principio de proporcionalidad, dado que la aplicación de este principio no puede orientarse por criterios jurídicos completamente certeros; el intérprete se ve compelido a llevar a cabo valoraciones subjetivas, por lo que cada aplicación de este principio constituye una intervención ilegítima del Alto Tribunal[218].

Cada vez que el Tribunal actúa, y soluciona los problemas jurídicos que conoce, en términos de ponderación de derechos fundamentales y bienes constitucionales, lo que hace es aumentar ilegítimamente su propio ámbito competencial y reduce la esfera que le corresponde al legislador, pues define las relaciones de predominancia entre derechos bienes e intereses, que en una democracia le corresponde al Parlamento[219]. El propio BERNAL PULIDO admite en las conclusiones de su amplia monografía sobre el principio de proporcionalidad, que si bien es cierto que no constituye un procedimiento objetivo para la determinación del contenido de los derechos fundamentales, sí cumple en la mayor medida de lo posible y en comparación con otros criterios alternativos (que resultan simplistas), las exigencias de racionalidad y respeto de las competencias del Parlamento. Recomienda, no obstante, refinar la estructura del principio de proporcionalidad, o intentar construir una mejor alternativa metodológica[220].

Dentro de la doctrina social, SEMPERE NAVARRO y SAN MARTÍN MAZZUCCONI señalan que no cabe más remedio que reconocer que la solución

---

[217] DÍEZ PICAZO, L.M.: Sistema de Derechos Fundamentales. Serie Derechos Fundamentales y Libertades Públicas, *op. cit*., pág. 121.

[218] Forsthoff arremete en contra de la extrapolación del derecho administrativo hasta el derecho constitucional, que expropia su verdadero carácter y lo convierte en un peligroso instrumento de intervención del Tribunal Constitucional, en la órbita que la Constitución atribuye al legislador. Aleininikoff señala que cuando el Juez Constitucional, lleva a cabo una ponderación, termina inevitablemente ejerciendo la función de armonizarlos intereses sociales que en todo Estado Democrático está atribuido al poder legislativo.

[219] BERNAL PULIDO, C.: *El Principio de proporcionalidad y los derechos fundamentales*, *op. cit*., págs. 199-202.

[220] *Ibídem*, págs. 815-816.

alcanzada por el Tribunal Constitucional, en la formulación del principio de proporcionalidad, adolece de notables dosis de imprecisión, pues faltan soluciones generales, rotundas y diáfanas. Admiten que la problemática es bastante compleja, debido a que se exige la presencia de varios elementos que han de concurrir para entender que estamos ante medidas ajustadas a Derecho, y no vulneradoras de derechos fundamentales. El problema reside en que tales elementos son de carácter acumulativo, por lo que la ausencia de uno de ellos trae consigo la tacha de inconstitucionalidad. Por esta razón, en muchos pronunciamientos no se despliega la totalidad de la doctrina de la proporcionalidad, pues es suficiente que falte uno de sus requisitos para que resulte innecesario proseguir el análisis del resto[221].

MONEREO PÉREZ y LÓPEZ INSUA, respecto al principio de proporcionalidad afirman que deben estar equiparados los diferentes intereses en conflicto; de un lado el general, que pretende defender el patrimonio empresarial, y de otro el particular, la *privacy* del trabajador[222].

FERNÁNDEZ VILLAZÓN afirma *"que bajo la aparente asunción del principio de proporcionalidad, en los fundamentos de las sentencias, todavía persisten en los subconscientes de algunos juzgadores criterios caducos que pudieran interferir en la adecuada comprensión y correcta aplicación de dicho principio*"[223].

THIBAULT ARANDA señala como punto positivo que la doctrina de la proporcionalidad constituye un sólido anclaje, pero a pesar de esta labor cuasireguladora de los tribunales, la conclusión que se ha de extraer es negativa, pues la modernidad y complejidad de este principio, aboca en ocasiones en contradicciones y fisuras judiciales que provocan incertidumbre e inseguridad jurídica[224].

GOÑI SEIN reconoce que aunque, la regla de la proporcionalidad pueda en muchas ocasiones esclarecer, no deja de ser un principio interpretativo, que está siendo

---

[221] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C. : *Nuevas tecnologías y Relaciones Laborales*, *op., cit*. págs.47 y 146.

[222] MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit*.

[223] FERNÁNDEZ VILLAZÓN, 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.37.

[224] THIBAULT ARANDA, J.: *Control Multimedia de la Actividad Laboral*, ed. Tirant Lo Blanch, 2006, pág.139.

aplicado por los jueces y tribunales ordinarios con resultados no siempre satisfactorios, porque lo que pone de manifiesto su uso a la postre más formal que real; el principio de proporcionalidad se va erosionando ya que los tribunales vienen adoptando un sentido muy laxo del término idoneidad, con la consiguiente inseguridad jurídica que ello provoca[225].

TASCÓN LÓPEZ afirma que no deja de sorprender que, a partir de la doctrina constitucional de la proporcionalidad, la mayor parte de las veces en que los Tribunales Superiores de Justicia de las distintas Comunidades Autónomas han entrado a conocer acerca de la licitud de la instalación de sistemas de control a través de videovigilancia hayan considerado tal medida proporcionada y ajustada a las circunstancias del caso. Incluso, "*forzando sobremanera*" la interpretación razonable de la tesis del máximo intérprete constitucional, se ha admitido su instalación aun cuando la finalidad perseguida por la empresa fuera algo tan genérico como "*la verificación del cumplimiento de las obligaciones laborales por parte de los trabajadores de la misma y dotar de mayor seguridad a las instalaciones y material de la misma*"[226].

F) Aplicación judicial

Como botón de muestra, analizamos a continuación unas pocas sentencias de premisas similares, en las que la conducta merecedora del despido es la misma; una apropiación indebida, pero los resultados son distintos a la hora calificar los despidos.

- Noticiemos primero la STSJ de Madrid de12 de marzo de 2012[227]. El trabajador recurre en suplicación la sentencia que declaró procedente su despido disciplinario. El TSJ estima el recurso y declara improcedente la extinción, al apreciar que la instalación de la cámara de vigilancia en el puesto de trabajo no observó los criterios constitucionales, lo que determina la nulidad de la prueba videográfica obtenida, que servía de base a la prueba de la apropiación de objetos, imputada al recurrente.

---

[225] GOÑI SEIN, J.L.: *La Videovigilancia empresarial y la protección de datos personales*. *op. cit*., págs 47-48.

[226] TASCÓN LÓPEZ, R.: «El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica», *op.cit.*

[227] STSJ de Madrid de 12 de marzo de 2012 (AS 2012\2426).

Señala la Sala que la instalación de la cámara no estaba justificada, pues se instaló como una vigilancia inicial, al no acreditarse que existieran desapariciones de objetos en la empresa, ni que el actor en particular fuera sospechoso de este tipo de comportamiento por algún motivo. La medida no es tampoco necesaria, ni idónea, ni proporcionada, ya que la normativa legal exige la previa comunicación al comité de empresa e incluso la colocación visible de un distintivo informativo de conformidad con lo establecido en la normativa de protección de datos, todo ello como elementos de equilibrio para preservar lo más posible la integridad de los derechos fundamentales, sin que ninguna de esas circunstancias concurran en el caso enjuiciado:

> *"Como se ha dicho, la doctrina constitucional exige que la medida restrictiva del derecho fundamental debe cumplir los tres requisitos siguientes: que sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad); que sea necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, que sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto). Pues bien, a diferencia de lo apreciado en la STC 186/2000 antes transcrita, en el presente caso no se puede estimar que la instalación de la cámara grabando los alrededores de una mesa en el centro de trabajo estuviera justificada, pues se instala como una vigilancia inicial, ya que no se ha acreditado que existieran desapariciones de objetos en la empresa, ni que el actor en particular fuera sospechoso de este tipo de comportamiento por algún motivo. Por otra parte la medida no aparece como necesaria, pues resulta extraño que se coloquen determinados objetos en una mesa en un lugar de paso dentro de cajas que se abren sin dificultad alguna, y luego se instale una cámara para vigilar esa mesa, como si no pudieran existir en la empresa medios habituales (locales cerrados, cajas cerradas) de proteger los objetos cuya sustracción se quiere evitar. Tampoco parece idónea, pues la carta de despido no llega a imputar al trabajador la apropiación de algún objeto, pese a lo cual la sentencia indebidamente ha considerado acreditado, en la fundamentación jurídica, que el actor se llevó un reloj. Ni tampoco es posible apreciar la proporcionalidad de la medida, pues la normativa legal exige la previa comunicación*
>
> *al comité de empresa e incluso la colocación visible de un distintivo informativo, como elementos de equilibrio para preservar lo más posible la integridad de los derechos fundamentales. Sin embargo, en este caso la instalación no fue objeto de publicidad alguna, no dándose cuenta a los representantes de los trabajadores ni instalando dispositivo informativo alguno.*
>
> *Como conclusión de lo razonado se ha de estimar que la instalación de la cámara de vigilancia no observó los criterios constitucionales, lo que determina la invalidez de la prueba conforme"* (FJ 5º).

- En segundo lugar hay que aludir a la STSJ de Castilla-León de 24 de julio de 2013[228]. La trabajadora recurre en suplicación la sentencia que declaró procedente su despido disciplinario. El TSJ desestima su recurso y declara procedente la extinción, al apreciar que la instalación de la cámara de vigilancia en el puesto de trabajo observó los criterios constitucionales, no

[228] STSJ de Castilla-León de 24 de julio de 2013 (JUR 2013\276661).

comunicando a los trabajadores dicha instalación, si bien en el escaparate del establecimiento, en un lugar visible, se había colocado el distintivo informativo.

Se declara probado en base a la prueba videográfica, la apropiación indebida de la actora, y por tanto su despido procedente:

> *"La decisión empresarial de colocar una cámara de video vigilancia en el centro de trabajo en el que laboraba la Sra. Florencia satisfizo el juicio de proporcionalidad constitucionalmente exigido para poder afirmar su legalidad y legitimidad en sede de tutela de los derechos fundamentales y libertades públicas de los que son titulares los trabajadores en el ámbito del contrato de trabajo En segundo lugar, la instalación de la cámara de video vigilancia se revelaba necesaria para aquilatar las irregularidades o anomalías que pudieren estar relacionadas con el uso o con la gestión de la caja del centro comercial, puesto que se trataba de verificar a través de aquella instalación eventuales operaciones o maniobras de apropiación dineraria, esto es, de maniobras de trasiego físico del dinero obrante en la caja a otro lugar distinto en el que ese dinero se depositaba. Y, en tercer término, la medida era estrictamente proporcional, en tanto que su adopción tenía como exclusivo destino la dependencia de caja de la tienda, esto es, un espacio destinado a la permanente interrelación personal y en el que se llevan a cabo conductas escasamente exigentes de la preservación de la injerencia o del conocimiento de las mismas por terceras personas; en tanto que la video vigilancia afectaba exclusivamente a uno de esos ámbitos, cual el de la recaudación dineraria, en los que se expresa de forma primordial el interés de empresa; en tanto que la instalación de la cámara estuvo acompañada de la colocación de un anuncio informativo de que el centro de trabajo estaba video vigilado"(FJ 2º).*

- Por todo ello se puede afirmar lo que parece ser unánime en la doctrina, que existe una cierta desconfianza hacia la aplicación del principio de proporcionalidad por nuestro Alto Tribunal. Y además existen algunos pronunciamientos en los que se aprecia una aplicación algo defectuosa o meramente proforma del principio de proporcionalidad, que puede ensombrecer otros posibles parámetros de enjuiciamiento; lo que lleva a validar con enorme laxitud cualquier tipo actuación de empresarial de control[229]. Mencionemos, sobre el recurso a la prueba de los detectives privados, las STSJ Cataluña de 13 octubre de 2008[230], la STSJ Extremadura de 1 de diciembre de 2009[231] y la STSJ Extremadura de 23 de diciembre 2009[232].

---

[229] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *op. cit.*

[230] STSJ de Cataluña de 13 de octubre de 2008 (AS 2008\3128).

[231] STSJ de Extremadura de 1 de diciembre de 2009 (AS 2010\467).

[232] STSJ de Extremadura de 23 de diciembre de 2010 (AS 2010\685).

- Respecto a la monitorización de equipos informáticos en la STSJ Castilla y León de 8 de noviembre de 2004[233], que recoge con respecto al mencionado principio de proporcionalidad, tan solo lo siguiente:

"El Juzgador "a quo" ha ponderado con acierto todos los elementos que concurren en la situación enjuiciada, respetando la proporcionalidad y la adecuación necesarias entre el hecho imputado, la sanción y el comportamiento tanto del trabajador como del empresario y ha realizado un correcto juicio de valor sobre la gravedad y culpabilidad de la falta alegada sin poder rectificar la sanción impuesta ya que, de acuerdo con el artículo 58 del Estatuto de los Trabajadores".

G) Comentario a la STC 39/2016

No puede dejar de criticarse aquí la ya reseñada STC 39/2016, de 3 de marzo[234], caso Bershka; desde nuestro punto de vista se equivoca, a todas luces el Alto Tribunal, cuando somete a un juicio de proporcionalidad el derecho del art. 18. 4 CE. En primer lugar manifestar que es la primera vez que en sede constitucional el referido principio se aplica respecto al derecho a la autodeterminación informativa, es *una extravagante vuelta de tuerca*[235], pues la cuestión creíamos que era de delimitación previa; cabía preguntarse si para entender cumplido este derecho la información anterior a la medida restrictiva había sido suficiente o no; si había sido la información suficiente no había vulneración y si no por el contrario la información proporcionada era inexistente o insuficiente había vulneración del art. 18.4 CE. Se trata, por tanto, de una colisión de derechos ficticia, pues el problema es de delimitación. y no existe sólo colisión.

Ahora la STC 39/2016,de 3 de marzo, al intentar someter la técnica del triple test al 18.4 CE el TC se equivoca confundiendo los términos del debate, al afirmar lo siguiente: "*El incumplimiento del deber de requerir el consentimiento del afectado para el tratamiento de datos o del deber de información previa sólo supondrá una vulneración del derecho fundamental a la*

[233] STSJ de Castilla-León de 8 de noviembre de 2004 (AS 2004\3073).

[234] STC 39/2016, de 3 marzo (RTC 2016\39).

[235] En semejantes términos se pronuncia el VOTO PARTICULAR que formula el magistrado VALDÉS DAL- RÉ: "*la Sentencia procede a dar una extravagante vuelta de tuerca, sosteniendo la tesis de que el escenario de confrontación entre derechos – y, por tanto, la necesidad de utilizar juicios de ponderación y proporcionalidad – concurre incluso si los poderes empresariales se ejercitan con manifiesta irregularidad o exceso; esto es, fuera del marco de la ley"(…) "en el decir de la Sentencia hay conflicto de derechos y necesidad de ponderación en clave de proporcionalidad incluso si el empresario manifiestamente no atiende e inobserva, sea cual fuere la causa, el deber legal de informar a los trabajadores ex art. 5 LOPD".*

protección de datos tras una ponderación de la proporcionalidad de la medida adoptada" (FJ 3º último inciso). ¿No existirá un error de terminología queriendo decir el TC información previa del trabajador en lugar de consentimiento? Si no existe tal error, francamente, no se entiende nada.

¿Tal aseveración de la sentencia, quiere decir que al someter la medida de videovigilancia al juicio de proporcionalidad en sentido estricto, prima la relevancia de la realización del fin perseguido por el empresario, frente a lo reconocido al trabajador en el art. 18.4 CE? Por tanto, al contestar a la pregunta anterior en sentido afirmativo, al haber superado la medida el juicio de proporcionalidad en sentido estricto, se considera justificado y constitucional prescindir del consentimiento del trabajador afectado respecto a la videovigilancia: "*En consecuencia, teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el art. 18.4 CE" (FJ 4º último inciso).*

En nuestra opinión, no puede equipararse el respeto al contenido esencial del derecho del art. 18. 4 CE con los principios de ponderación y proporcionalidad de la decisión adoptada, el resultado de la aplicación del principio es erróneo pero es que el fallo es aplicar el referido principio al art. 18. 4 cuando no hay colisión.

El error de aplicar el principio de proporcionalidad al art. 18. 4 CE es tal magnitud que, a efectos de expresarlo de una manera gráfica permítasenos recurrir a la analogía, es como si para comprobar el ilícito penal del delito contra la seguridad vial por conducir bajo la influencia de drogas tóxicas, estupefacientes o sustancias psicotrópicas la policía usase un alcoholímetro y no un análisis de sangre. Por todos es sabido, que la presencia de drogas no se detecta con un etilómetro sino con un análisis de sangre, otro tanto de lo mismo sucede con la vulneración del 18.4 CE no se constata con la aplicación del principio de proporcionalidad sino con la verificación de la existencia de información suficiente o no, en definitiva, con una delimitación. Cabe concluir, pues la referencia a este intento artificioso de la STC 39 /2016, de 3 de marzo, haciendo nuestras las palabras del Voto Particular: "*una tesis semejante constituiría, sencillamente, un despropósito jurídico-constitucional, pudiendo arrastrar un caudal de consecuencias prácticas de imposible aceptación en nuestro Estado social*".

H) Recapitulación

Pese a los errores manifiestos en la aplicación del principio de proporcionalidad en las SSTC 170/2013 de 7 de octubre y 39/2016 de 3 de marzo, se debe concluir este apartado afirmando que la práctica judicial muestra, mayoritariamente, una recepción adecuada de la doctrina judicial de la ponderación, al menos en lo que concierne a la articulación recíproca entre el legítimo ejercicio del poder empresarial y la protección del derecho a la intimidad de los trabajadores.

Con todo, el principio de proporcionalidad comporta cierta inseguridad jurídica, pues, en definitiva, se basa en juicios de subjetividad. En consecuencia, queda patente la necesidad de que se definan por el legislador "*lege ferenda*" los criterios que delimiten los requisitos de idoneidad, necesidad y proporcionalidad cuando entren en conflicto con los derechos fundamentales, tarea, que ciertamente, no se supone fácil. Se hace necesario partir de unos parámetros claros, tras esto establecer una proporcionalidad y ponderación entre los intereses y bienes jurídicos en conflicto, siempre que no quede otro medio para esclarecer los hechos de manera menos lesiva con los derechos fundamentales.

5. La expectativa razonable de intimidad

Examinemos ahora un concepto que pone de relieve la necesidad de hallar un equilibrio entre el derecho del trabajador a su intimidad y el interés del empleador en disponer cada vez de un mayor control sobre el desarrollo de la actividad productiva.

A) El paradigma estadounidense

Hay que aludir primero a la interpretación dada por la *Supreme Court* a la Cuarta Enmienda de la Constitución Americana, que contempla la protección contra persecuciones e investigaciones irracionales[236], y sirvió de base para sentar el criterio de

[236] El Tribunal Supremo estadounidense, a lo largo de una extensa y gradual jurisprudencia, ha considerado implícito un "*right to privacy*" en la garantía de la Cuarta Enmienda frente a registros y requisas

la expectativa razonable de intimidad[237], conocido también como *expectation of privacy test*[238] o Katz-test. El referido criterio podría resumirse en la siguiente máxima: un ciudadano no puede ser sometido a una injerencia sobre su privacidad con la que no pudiera contar en términos razonables[239].

La Administración estadounidense alegó que la actividad de investigación no debía pasar por el examen de la Cuarta Enmienda Constitucional, debido a que la técnica de vigilancia empleada no implicaba ingreso físico a la cabina desde donde se realizaron las llamadas. No obstante, la Corte decidió en este caso abandonar dicho criterio y extendió el contenido de la Cuarta Enmienda Constitucional no sólo a la incautación de cosas tangibles, sino también a la grabación de conversaciones. Fue justamente a partir de un voto concurrente de un magistrado llamado Harlan, cuando surgió la categoría y el test de protección[240], que en adelante resulta aplicable, al afirmar:

> *"(...) yo comparto la opinión de la Corte en la cual se sostiene: a) que una cabina telefónica es un área en la cual tal como en la casa y a diferencia del campo una persona tiene*

---

arbitrarias (*unreasonable searches and seizures*), que limita la intrusión del gobierno en las personas, domicilios, documentos y efectos personales, incluyéndose no sólo los supuestos de invasión material (*physical trespass*) sino también de vigilancia electrónica.

[237] El caso *Katz v. United States, 389. Vs. 347,* resuelve la legalidad del seguimiento del ciudadano estadounienese Charles Katz por agentes del FBI, con motivo de ser sospechoso de traficar de manera ilegal con información confidencial sobre apuestas, se sabía que solía hacer uso siempre de una misma cabina telefónica de los Ángeles para llamar a sus contactos de Miami y Boston, el FBI en las inmediaciones de la red telefónica colocó un micrófono para grabar las conversaciones, material que se convirtió en la base esencial de su posterior condena. El gobierno presentó como prueba el registro magnetofónico de las conversaciones de Katz sobre las apuestas y la Suprema Corte en un recurso extraordinario aceptó analizar si las grabaciones habían sido realizadas infringiendo la cuarta enmienda constitucional, que prevé el derecho a la privacidad de las personas, teniendo en cuenta que con la jurisprudencia vigente no existía intromisión en el área ocupada por el acusado. Basándose en la opinión mayoritaria el Alto, el Juez Harlan ofreció en su voto concurrente la noción de "expectativa razonable de privacidad", un nuevo juicio de valor, según el cual sólo existe una zona de privacidad garantizada por la Cuarta Enmienda si la persona ha actuado conforme a una real expectativa de privacidad, y si tal expectativa la sociedad está preparada para reconocerla como "razonable".

[238] Juicio de expectativa razonable de privacidad.

[239] RODRÍGUEZ LAINZ, J.L: «Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013 de 7 de octubre)», *Diario La Ley*, núm. 8271, 2014, págs. 2 y 3.

[240] GUERRERO PERALTA, O.J.: «La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal», *Revista de Derecho Penal y Criminología*, núm. 92, 2011, pág. 59.

expectativa razonable de intimidad; b) que la intromisión física así como la electrónica en un lugar que en este sentido es privado puede constituir una violación de la cuarta enmienda, y c) que la invasión de un área constitucionalmente protegida por las autoridades federales es presumiblemente irrazonable en ausencia de una orden judicial, como se ha sostenido desde hace tiempo.

Como lo afirmó la opinión mayoritaria la Cuarta Enmienda protege personas, no lugares. sin embargo, la cuestión es qué tipo de protección requiere la ciudadanía. generalmente, la respuesta a esta pregunta va a estar relacionada con un lugar. mi comprensión de la regla que surge de la anterior decisión es que existe un doble requerimiento, esto es, primero que la persona haya exhibido una expectativa actual (subjetiva) de intimidad y segundo que la sociedad esté preparada para reconocer tal expectativa como razonable. en tal sentido, la casa de habitación es para la mayoría de los propósitos, un lugar donde normalmente se espera privacidad, de tal manera que los objetos, actividades o afirmaciones que resulten expuestas a la vista de terceros no están protegidos debido a que no existe una intención de preservarlos una vez han sido exhibidos[241]*."*

Pese a que en el referido supuesto, desde el punto de vista de un jurista de la Corte Europea, supondría un ejemplo de libro de violación de las comunicaciones, el fallo fue desestimatorio para el señor Katz; porque la esencialidad de la Cuarta Enmienda exigía la existencia de contacto físico, bien con la persona objeto de investigación[242], bien con cualesquiera bienes u objetos que fueran de su propiedad[243].

Desde este renombrado caso, el interés central de la Cuarta Enmienda ha sido la protección de la privacidad individual, de aquellos ámbitos de la esfera privada que tienden a preservar esos intereses de "*secreto*", "*santuario*" o "*soledad*" individual, frente a la ilegítima intromisión estatal, que han fundamentado su protección constitucional y que están implícitos en la centenaria formulación del derecho a la privacidad como "*the right to be let alone*" [244]. A partir de ahí, se ha reconocido una expectativa razonable de privacidad en diversos ámbitos y con distintas graduaciones; así respecto de la utilización de mecanismos de interceptación y grabación en los supuestos de registros administrativos de casas y oficinas, en los registros de equipajes y taquillas, así como en los supuestos de inspección de licencia de circulación y registro de vehículos en los controles policiales de tráfico, etc.

---

[241] *Ibídem.*

[242] RODRÍGUEZ LAINZ, J.L.: «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre», *Diario La Ley*, núm. 8271, 2014, pág. 2.

[243] Como el lugar donde se ejecutó el acto e injerencia era una caja de registro de propiedad de la compañía telefónica que le prestaba el servicio de telefonía al recurrente, propiedad de un tercero, y que además se encontraba en la vía pública a la vista de otros, el Alto Tribunal consideró que no existía injerencia alguna.

[244] *El derecho a estar solo.*

B) Ámbito Europeo

La penetración de la doctrina de la expectativa razonable de privacidad, puede residenciarse en alguno de los derechos protegidos por el art. 8 del Convenio Europeo para la salvaguardia de los Derechos Humanos y las Libertades Fundamentales (CEDH) [245] ,y en algunos arranques puntuales de esta doctrina jurisprudencial en los casos *Huvig y Krsuling v. Francia*[246] de 24 de abril de 1.990[247].

El criterio de la expectativa razonable de privacidad, fue incorporado de manera expresa, por el Tribunal Europeo de Derechos Humanos, en los términos que establecen las SSTDH de 25 de junio de 1997 -caso HALFORD[248]- y de 3 de abril de 2007 -sentencia COPLAND[249]- para valorar la existencia de una lesión del art. 8 del Convenio Europeo para la Protección de los Derechos Humanos; y a través de este ha pasado a formar parte de la jurisprudencia de la Sala IV del Tribunal Supremo y posteriormente de la del Tribunal Constitucional.

El *caso Halford contra el Reino Unido,* como ya hemos apuntado, constituye el primero en el que se llevó acabo una utilización explícita de la doctrina de la expectativa de privacidad. Los hechos que se declararon probados en la sentencia son los siguientes :

- La demandante, llamada Alinson Halford, era inspectora general de la policía británica de Merseyside.
- Antes del proceso ante el TEDH, presentó una demanda por vulneración del principio de igualdad ante un tribunal de trabajo, debido a que se rechazó en sucesivas ocasiones su candidatura a un ascenso; y, sin embargo, según sostenía, se concedió a colegas con menos méritos pero todos de sexo masculino.

---

[245] Artículo 8 sobre el derecho al respeto a la vida privada y familiar, cuya literalidad es la siguiente: «1. Toda persona tiene derecho al respeto a su vida privada y familiar, de su domicilio y de su correspondencia; 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho , sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida, que en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás».

[246] STDH 24 de abril de 1999 (TEDH 1990\2).

[247] RODRÍGUEZ LAINZ, J.L.: «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre», *op.cit.*

[248] STDH de 25 de junio de 1997 (TEDH 1997\37).

[249] STDH de 3 de abril de 2007 (TEDH 2007\23).

- Halford tenía derecho a un despacho para su uso exclusivo y en él hacía uso de dos teléfonos, uno de los cuales era para sus comunicaciones privadas y otro de trabajo (Estos teléfonos formaban parte de un sistema interno de comunicaciones de la policía, independiente de la red pública).
- La inspectora tuvo conocimiento de que se habían interceptado sus llamadas telefónicas y solicitó a la comisión competente en su país, en materia de interceptaciones de comunicaciones que abriera una investigación puesto que consideraba que tal medida se había realizado para obtener información que sería utilizada contra ella en el curso del procedimiento en materia de discriminación. Como el amparo se le denegó en el país inglés agotadas todas la vías legales en el mismo, acudió al TEDH.

El TEDH consideró que la intercepción de las llamadas de la demandante representaba una violación del art. 8 del Convenio Europeo para la Protección de los Derechos Humanos (CEDH). Para el Tribunal[250] "*se desprende claramente de su jurisprudencia que las llamadas telefónicas que proceden de locales profesionales, al igual que las procedentes del domicilio, pueden incluirse en los* conceptos de "*vida privada*" y de "*correspondencia*" citados en el apartado 1 del artículo 8 del Convenio de Roma. No hay pruebas de que a la Sra. Halford se le hubiera avisado, en calidad de usuaria de la red interna de telecomunicaciones de la policía, de que las llamadas efectuadas mediante la misma podían ser interceptadas. El Tribunal considera que "*ella podía razonablemente esperar que se reconociera el carácter privado de este tipo de llamadas"* [251].

En el caso *Copland contra el Reino Unido*[252] , el TEDH estima que el almacenamiento de la información personal sobre el teléfono de la demandante, su email

[250] Asimismo declara la violación del art.13 al no poder la demandante obtener una rectificación.

[251] Se condena a pagar a la cantidad de 10.600 libras esterlinas en concepto de daños materiales y morales, 25.000 libras por costas y gastos, más toda cantidad que pudiera deberse en concepto de IVA y que esta cantidad debía aumentarse con un interés simple del 8% al año a contar desde la expiración del plazo y hasta su pago.Se unió a esta sentencia la opinión disidente del juez Russo.

252 En el año 1991 la Sra. Copland estaba empleada en un colegio estatal.En el año 1995 la demandante se convirtió en asistente personal del director y desde finales de 1995 la demandante fue requerida para trabajar junto a otro director asignado.Sobre julio de 1998 Sra. Copland visitó otro campus. Posteriormente se enteró que se había preguntado por su visita y que se había sugerido una relación personal

y el uso que hace de Internet sin su consentimiento suponía una interferencia con su derecho a la vida privada del art. 8 de la CEDH. Durante su empleo en un colegio estatal, el teléfono de la demandante, su email y el uso de internet estuvo sujeto a monitorización por parte de una institución británica ante las sospechas de que la recurrente estaba realizando un abuso de tarificación desde los terminales telefónico e informático. El TEDH declara el quebranto de la expectativa razonable de privacidad, porque la recurrente vivía en un ambiente de permisividad con el que se manejaba en su puesto de trabajo, lo que la había llevado a la creencia de que estaba libre del escrutinio de sus comunicaciones por parte del empleador.

En suma: existe un hábito social generalizado de cierta tolerancia con el usos moderado de los medios informáticos y de comunicación, facilitados por la empresa, que crea una expectativa general de confidencialidad que puede entrar en conflicto con el control empresarial, de ahí la necesidad de regulación mediante convenio colectivo[253]; se hace necesario que los representantes de los trabajadores negocien previamente unas reglas de uso que puedan ser asumidas por las partes[254].

En este sentido, el Grupo de Trabajo del "*Artículo 29*", considera que una prohibición absoluta de la utilización de Internet con fines privados por los trabajadores podría considerarse inaplicable y un tanto irrealista, ya que no se tendría en cuenta el apoyo que Internet puede brindar a los trabajadores en su vida diaria[255]. Cabe añadir que la tolerancia de un uso moderado es en parte debida a la progresiva informatización de

entre la demandante y el director del otro campus.Durante su empleo, el teléfono de la demandante, su email y el uso de Internet estuvo sujeto a monitorización.Sobre marzo o abril de 2000 la demandante fue informada por otro miembro del colegio que entre los años 1996 y 1999 muchas de sus actividades habían sido monitorizadas por la dirección.El TEDH tiene que fallar sobre el ajuste a la ley y a necesidad social, el TEDH observa que no hay ley que regule la monitorización en el momento de los hechos por lo que falla que ha habido violación del art. 8 de la CEDH. El TEDH otorga 3.000 euros por daños morales a la demandante y 6.000 euros por costas y gastos procesales.

[253] *Ibídem*, pág. 79.

[254] SEMPERE NAVARRO, A.V y MATEOS y de CABO, O.: «Uso y control de herramientas informáticas en el trabajo. (Marco legal, pautas judiciales y convencionales.)» *op. cit.*, pág.79.

[255] Véase pág. 24 del Documento del grupo de Trabajo de la UE relativo a la vigilancia de las comunicaciones electrónicas en al lugar de trabajo, aprobado el 29 de mayo de 2002. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/B.2.52-cp--wp55---vigilancia-comunicaciones-electr-oo-nicas-trabajadores.pdf*. Pág. 24.

muchas de las transacciones que diariamente realizan las personas tanto a nivel laboral como personal[256].

C) Tribunal Supremo: la STS 26 septiembre 2007

La primera aproximación a estos problemas por parte de la Sala 4ª del Tribunal Supremo se produjo con la STS de 26 de septiembre de 2007[257], que se puede considerar un *leading case*[258], por su relevancia y trascendencia. En ella se sienta doctrina sobre el controvertido tema de control empresarial respecto al uso del ordenador facilitado por la empresa como mecanismo de trabajo. La sentencia no se limita a resolver la cuestión de hecho planteada, sino también construye una técnica argumental de razonamiento genérico para enfrentarse a este tipo de problemas[259] y entre ellos el relativo al derecho a la intimidad.

Los antecedentes del caso son los siguientes: durante la reparación rutinaria de un ordenador de empresa infectado por un virus, el informático que lo repara, en su afán indagatorio, descubre a través de los archivos temporales[260], que ha resultado averiado por acceder a páginas web no seguras que eran de contenido pornográfico, lo que comunica de manera oportuna. Se realiza una copia de la información en un puerto USB, se imprime y se entrega a un notario, posteriormente se repite la fiscalización del ordenador, delante de los delegados de personal, y se entrega carta de despido disciplinario al trabajador que resultó afectado.

La sentencia razona que se debe respetar la dignidad del trabajador, para ello previamente se han de establecer unas reglas de uso de los sistemas informáticos en la empresa, y se debe informar a los trabajadores de la existencia de un control. En lo que

---

[256] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013»,*op.cit.*

[257] STS 26 de septiembre de 2007 (RJ 2007\7514).

[258] En el sistema del *common law,* el concepto de *leanding case*, es una expresión comúnmente utilizada, la palabra *leading* es un gerundio que procede de *leader* e implica avance y está referido a algo que actúa en forma permanente, como dirigente o conductor de algo. En el inglés jurídico, *case* es litigio, cuando se hace alusión a esta expresión es para hacer referencia a una respuesta judicial nueva, creadora, que deja atrás todo lo existente; es una resolución verdaderamente importante.

[259] MERCADER UGUINA, J.: «Límites del control empresarial sobre el uso del trabajador del ordenador facilitado por la empresa como instrumento de trabajo: TS 26/9/07 como "*leading case*"», en AA. VV. GIL SUÁREZ.L. y SARGADOY DE SIMÓN, I. (Coors): *Jurisprudencia y grandes cuestiones laborales*, ed. Francis Lefebvre, 2010, págs. 170-173.

[260] Copias que se guardan automáticamente en el disco duro de los sitios visitados a través de Internet.

se refiere a la obtención de la prueba es donde se vulneró la expectativa razonable de intimidad del trabajador, pues no había política empresarial establecida, lo que generó una expectativa de tolerancia que es necesario proteger a nivel constitucional. Por lo cual se confirma la decisión de la instancia, y se desautoriza la actuación de la empresa.

El Tribunal Supremo afirma que la protección a la intimidad incluye el correo electrónico, y no solo los archivos personales del ordenador, sino también los temporales. Estos son los que pueden contener datos más sensibles, pues incorporan informaciones reveladores sobre determinados aspectos de la vida privada (ideología, orientación sexual, aficiones personales, etc.). En este caso se accedió al ordenador del trabajador para borrar un virus, pero se apoderó de un archivo cuyo examen o control no puede reputarse que fuera necesario para la reparación interesada, de esta forma, no cabe entenderse que estemos ante lo que en el ámbito penal se califica como un "*hallazgo casual*", pues se ha ido más allá de lo que la entrada regular para la reparación justificaba. La medida no resultaba indispensable, se ha vulnerado con ello la expectativa razonable de intimidad, que legítimamente le corresponde al trabajador.

Claramente se extrae del argumento del TS el criterio del respeto a la expectativa razonable de intimidad del trabajador; consiste en que, si la herramienta tecnológica del trabajador se usó para fines privados, en contra de las prohibiciones y con conocimiento de los controles efectuados por la empresa, y en su caso de las medidas aplicables, no puede entenderse que, al realizarse el control empresarial, se haya vulnerado una expectativa razonable de intimidad.

Por lo que si el empresario ha establecido una prohibición de uso para fines privados y ha avisado a los trabajadores de la posibilidad de hacer controles, podrá entenderse que, al registrar el ordenador, no ha vulnerado esa expectativa razonable de intimidad. Así se ha venido considerando respecto de la posibilidad de las empresas para vigilar y monitorizar las conversaciones que mantiene el personal comercial que presta su actividad por teléfono si previamente lo ha anunciado y existe una línea telefónica diferenciada para conversaciones extralaborales[261] (STS de 5 de diciembre de

[261] El TS desestima el recurso de casación interpuesto por la unión sindical codemandante frente a sentencia que rechazó su pretensión de que se declarase la ilegalidad de las escuchas telefónicas practicadas por la empresa. La Sala señala que la "monitorización" o control empresarial se realizó en condiciones de respeto a la legislación vigente, por cuanto tenía como único objeto controlar la actividad laboral del

2003[262]).Desmenuzando el contenido de la sentencia, podemos establecer las pautas generales que marca, que son las siguientes:

- El control empresarial se funda en el art. 20.3 ET y no en el art. 18 ET, el ordenador es un medio de trabajo y el titular es el empresario.
- No es necesario que la fiscalización empresarial se practique en el centro y en horario de trabajo ni ante la presencia del trabajador afectado.
- La expectativa de confidencialidad no es absoluta, está sometida a las reglas de la buena fe, se ha de informar al trabajador de las reglas de uso de las nuevas tecnologías, de los posibles controles.
- La falta de autorización para el uso de las nuevas tecnologías no implica prohibición, sino tolerancia.

D) La STS 8 marzo 2011

Una confirmación de la expuesta doctrina la constituye la STS de 8 de marzo de 2011[263], que desestima el recurso de la empresa que había vulnerado el derecho a la intimidad del trabajador por registrar el ordenador, sin existir advertencia previa sobre posibles límites de utilización y de realización de controles al efecto. La empresa debía haber delimitado previamente las reglas de uso de los medios informáticos puestos a disposición de los trabajadores, para garantizar la expectativa razonable de intimidad:

> *"En este punto es necesario recordar la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza*

---

trabajador en condiciones de respeto a su esfera íntima inatacable. El teléfono controlado se puso a disposición de los trabajadores como herramienta de trabajo para que llevasen a cabo sus funciones de telemarketing disponiendo de otro teléfono para sus conversaciones particulares y los trabajadores conocían que podía ser intervenido por la empresa, En consecuencia, concluye el Tribunal, era un control necesario, ya que no se conoce otro medio más moderado para obtener la finalidad que se pretendía - juicio de necesidad-, era idóneo para el mismo fin -juicio de idoneidad- y ponderado o equilibrado porque de ese control se podían derivar beneficios para el servicio que presta la empresa y no parece que del mismo se pudieran derivar perjuicios para el derecho fundamental de los trabajadores -proporcionalidad en sentido estricto.

[262] STS 5 de diciembre de 2003 (RJ 2004\313).

[263] STS 8 de marzo de 2011 (RJ 2011\932).

un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio "(FJ 3º).

Por lo que concluye lo siguiente:

"En el presente caso sin duda que la decisión de la sentencia recurrida se ajusta a la doctrina trascrita. En efecto, como ya se ha señalado, la prueba ha sido obtenida por la empresa a partir de una auditoría interna en las redes de información con el objetivo de revisar la seguridad del sistema y detectar posibles anomalías en la utilización de los medios informáticos puestos a disposición de los empleados. No consta que, de acuerdo con las exigencias de la buena fe, la empresa hubiera establecido previamente algún tipo de reglas para el uso de dichos medios -con aplicación de prohibiciones absolutas o parciales- ni tampoco que se hubiera informado a los trabajadores de que se iba a proceder al control y de los medios a aplicar en orden a comprobar su correcto uso, así como las medidas a adoptar para garantizar la efectiva laboral del medio informático cuando fuere preciso"(FJ 4º).

E) La STS 6 octubre 2011

La doctrina anterior fue ratificada posteriormente por la STS de 6 de octubre de 2011[264]; en ella se desestima el recurso planteado por la trabajadora, que fue despedida de manera disciplinaria pues su ordenador fue monitorizado a través de un programa espía, mediante el que se constató, el uso del mismo para fines particulares, pese a tenerlo prohibido de manera expresa.

Los hechos del caso son los siguientes: La empresa demandada entregó a todos los trabajadores una carta que la actora recibió y firmó en la que se comunicaba que quedaba terminantemente prohibido el uso de medios de la empresa (ordenadores, móviles, Internet, etc.) para fines propios tanto dentro como fuera del horario de trabajo. Decidió hacer una comprobación sobre el uso de sus medios de trabajo para lo que procedió a la motorización de los ordenadores de la demandante y de otra trabajadora. Se trataba de un sistema "*pasivo*", es decir, poco agresivo que no permitía acceder a los archivos del ordenador que están protegidos por contraseñas de cada uno de los usuarios.

Se procedió a visualizar el proceso de monitorización del ordenador de la demandante en presencia de ésta, de las dos personas que habían procedido a la monitorización, de representantes de la empresa y de los trabajadores y de otros dos trabajadores, firmando los comparecientes el acta levantada al efecto, con excepción de la actora. La sentencia recurrida entiende que la prueba que ha servido para acreditar la

[264] STS 6 de octubre de 2011 (RJ 2011\7699).

causa del despido se ha obtenido de forma lícita y ello aunque el "software" espía se instaló sin darlo a conocer expresamente a la actora, por cuanto existía previamente una prohibición absoluta de usar el ordenador para fines ajenos a la actividad laboral; valora la sentencia que se trataba de un sistema pasivo o poco agresivo, que capturaba lo que estaba en pantalla pero que no invadía la intimidad de la trabajadora, toda vez que la contraseña usada por ella impedía el acceso a sus archivos. El TS declara que la prohibición absoluta de uso del ordenador neutraliza la expectativa de intimidad que hasta ahora constituía el elemento básico sobre el que pivotaba la protección del derecho a la intimidad: "*La cuestión clave -admitida la facultad de control del empresario y la licitud de una prohibición absoluta de los usos personales- consiste en determinar si existe o no un derecho del trabajador a que se respete su intimidad cuando, en contra de la prohibición del empresario o con una advertencia expresa o implícita de control, utiliza el ordenador para fines personales"* (FJ 4º).

La STS de 6 de octubre de 2011[265], viene a decir a modo de síntesis, que no puede existir un conflicto de derechos cuando hay una prohibición válida[266]. La respuesta parece clara: 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 existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo. La sentencia desestima el recurso de casación para la unificación de doctrina, interpuesto por la trabajadora despedida contra la sentencia que declaró procedente su despido: "*existía una prohibición absoluta de usar el ordenador para fines ajenos a la actividad laboral, de forma que la instalación del sistema de control sin conocimiento de la recurrente no conlleva que la prueba así obtenida para justificar el despido sea ilícita*".

Y en base a esa prohibición concluye la Sala que válidamente impuso el empresario una prohibición absoluta sobre el uso de medios de la empresa (ordenadores, móviles, Internet, etc.) para fines propios, tanto dentro como fuera del horario de trabajo;

---

[265] STS 6 de octubre de 2011 (RJ 2011\7699).

[266] CEFGESTIÓN: «El control por la empresa de las herramientas puestas a disposición del trabajador o el derrumbe del derecho a la intimidad», *CEF Gestión: Revista de actualización empresarial*, núm. 162, 2012, pág. 64.

no de manera arbitraria, sino entre sospechas fundadas de que se estaban desobedeciendo las órdenes impartidas al respecto. Y, sentada la validez de prohibición tan terminante, que lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador, no es posible admitir que surja un derecho del trabajador a que se respete su intimidad en el uso del medio informático puesto a su disposición. Tal entendimiento equivaldría a admitir que el trabajador podría crear, a su voluntad y libre albedrío, un reducto de intimidad, utilizando un medio cuya propiedad no le pertenece y en cuyo uso está sujeto a las instrucciones del empresario de acuerdo con lo dispuesto en el art. 20 ET.

Esta sentencia, contiene un voto particular el de una Magistrada[267], al que se le unen cuatro Magistrados más, pues la discrepancia se fundamenta en que la decisión adoptada en la sentencia mayoritaria comporta un retroceso en la protección de los derechos fundamentales, concretamente del derecho a la intimidad del trabajador, pues entiende y afirma que si no hay derecho al uso del ordenador para asuntos personales, por existir esa prohibición, tampoco puede exigir el derecho a que se respete la intimidad del trabajador ni tiene expectativa razonable de confidencialidad e intimidad en la utilización dichos medios[268].

La conclusión que cabe obtener de la STS de 6 de octubre de 2011[269] es que, una vez establecida la prohibición expresa, cabe distinguir si el empresario informa antes de

[267] El voto particular es de Segoviano Astaburuaga al que se adhieren los magistrados de Castro Fernández, Agustí Julia, Viroles Piñol y Alarcón Caracuel.

[268] El voto particular recoge: " *(...) es necesario recordar lo que ya se dijo sobre la existencia de un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esa tolerancia crea una expectativa también general de confidencialidad en esos usos; expectativa que no puede ser desconocida, aunque tampoco convertirse en un impedimento permanente del control empresarial, porque, aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio. Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir contro*l ".

[269] STS de 6 de octubre de 2011 (RJ 2011\7699).

los controles que va a llevar a cabo una inspección de las herramientas de trabajo puestas a disposición de los trabajadores o por el contario, no lo hace.

En este sentido la doctrina se halla dividida. De un lado se encuentra la opinión de quienes piensan que con independencia de si el empresario ha informado o no de posibles controles, previamente, existe la posibilidad de inspeccionar el contenido de las comunicaciones; pues la mera prohibición equivale a la información a los trabajadores sobre la posibilidad de inspeccionarlos, sin vulnerar derechos fundamentales[270]. De otro lado se encuentra la postura más amplia y menos restrictiva que no es la la mantenida por el TC en la actualidad, defendida por cierto sector de la doctrina que sostiene que pese a existir prohibición si no hay información, se produce una violación de derechos fundamentales[271].

Por tanto, la existencia o no de esa orden por parte del empresario o la existencia de una regulación o no, sería la pieza clave a la hora de permitir que se produzca legal y constitucionalmente el control empresarial. Y ello porque, en primer lugar, si no existe dicha limitación, la doctrina tradicional del Tribunal Supremo parte de la imposibilidad de tal control ante la expectativa de privacidad generada por la inactividad empresarial.

D) Asunción del criterio por el Tribunal Constitucional

El arranque en la doctrina de la expectativa en la jurisprudencia constitucional fue más tardío, pues no tuvo lugar hasta la publicación de las SSTC 12/2012 de 30 de enero[272] y 74/2012 de 16 de abril[273], referidas ambas a un reportaje periodístico de investigación

---

[270] MONTOYA MELGAR, A.: «Nuevas tecnologías y buena fe contractual (buenos y malos usos del ordenador en la empresa)», *Relaciones laborales: revista crítica de teoría y práctica*, núm. 1, 2009, pág. 113.

[271] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B.M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op. cit.*

[272] STC 12/2012, de 30 de enero (RTC 2012\12). Versa sobre un reportaje que la televisión autonómica valenciana emitió, que fue producido por Canal Mundo Producciones, en el que se utilizaban imágenes obtenidas mediante cámara oculta. El canal de televisión y la productora fueron condenados por intromisión a la intimidad y vulneración del derecho a la propia imagen. La sentencia recoge la jurisprudencia del Tribunal Europeo de Derechos Humanos, haciéndose eco de la teoría de la expectativa razonable. De este modo, concluye que la conversación mantenida en un lugar específicamente ordenado a asegurar la discrecionalidad de lo hablado -en este caso concreto una consulta profesional- pertenece al ámbito de la intimidad. En consecuencia, se desestima el recurso de amparo interpuesto.

[273] STC 74/2012, de 16 de abril (RTC 2012\74).

oculta, rodado en el interior de una clínica sospechosa de intrusismo profesional[274]. Se resolvió el caso concreto dando la razón al titular del derecho a la intimidad: "*Conforme al criterio de expectativa razonable de no ser escuchado u observado por terceras personas, resulta patente que una conversación mantenida en un lugar específicamente ordenado a asegurar la discreción de lo hablado, como ocurre por ejemplo en el despacho donde se realizan las consultas profesionales, pertenece al ámbito de la intimidad*".

De este modo, el TC hace propia la esencia misma del concepto de "*expectativa razonable de privacidad*"; reside en derivar los contornos mismos del derecho fundamental concernido del entorno de la privacidad, no tanto en su configuración formal, como en ese poder que todo ciudadano tiene de hacerlo valer, frente a los poderes públicos o al resto de la sociedad, el llamado derecho de exclusión[275].

E) La STC 241/2012 de 17 diciembre

En el ámbito laboral la primera sentencia del Tribunal Constitucional, en la que se recoge el mismo criterio de *expectativa razonable de confidencialidad*, es la importante STC 241/2012, de 17 de diciembre[276] . Los antecedentes del caso son los siguientes:

- Dos empleadas mantienen conversaciones con un programa de mensajería instantánea en sus respectivos ordenadores de la empresa.
- En dichos diálogos vierten críticas hacia sus compañeros y a sus superiores.
- No hay ordenador de uso exclusivo para cada empleado, sino que el uso era común.
- Existía una prohibición expresa de uso de las herramientas de trabajo para fines propios.
- Pese a tal prohibición instalaron un programa de mensajería instantánea con el que se comunicaban.
- De manera casual un compañero de trabajo accede al contenido de los mensajes, lo transmite a los superiores y las empleadas fueron amonestadas de manera verbal.

Sorprende sobremanera, que ante la escasa trascendencia de la sanción, una de las dos trabajadoras llegara a solicitar amparo ante el TC. Se planteó el recurso alegando

[274] RODRÍGUEZ LAINZ, J.L.: «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre» *op. cit.*, pág. 6.
[275] *Ibídem*, pág. 7.
[276] STC 241/2012, de 17 de diciembre (RTC 2012\241).

vulneración de los arts. 18.1 y 18.3 CE. Respecto a la violación del derecho a la intimidad, el TC resuelve que desde el momento en que las trabajadoras dispusieron la instalación del programa de mensajería instantánea e hicieron uso del mimo, contravinieron las ordenes de la empresa, por lo que la protección del derecho a la intimidad queda enervada. Otro tanto de lo mismo sucede con el secreto de las comunicaciones, al incluir las empleadas sus conversaciones en el disco duro de los ordenadores donde cualquier colega podía leerlas, pues como se ha dicho eran de uso común; con lo que ellas eliminaron de manera voluntaria la privacidad. Además, el uso compartido de los terminales informáticos que no presentaban ningún tipo de restricción para poder acceder a ellos: los convertía en un canal abierto, (no se da por tanto cobertura constitucional a aquellas comunicaciones de las que no puede predicarse su confidencialidad). Y en segundo lugar, corresponde al empresario fijar las condiciones de uso de los medios informáticos de su titularidad, y en el caso enjuiciado, existía una prohibición absoluta, por lo que en base a este imperativo se hace perder la inmunidad de la protección formal de la que goza a tenor del art. 18.3 CE[277]: *"Por otra parte, la prohibición expresa de instalar programas en el ordenador de uso común se conculca por la recurrente y otra trabajadora, quienes instalaron el programa de mensajería instantánea denominado "Trillian". Por tanto, no existiendo una situación de tolerancia a la instalación de programas y, por ende, al uso personal del ordenador, no podía existir una expectativa razonable de confidencialidad derivada de la utilización del programa instalado, que era de acceso totalmente abierto y además incurría en contravención de la orden empresarial"*(FJ 6º).

Es importante destacar el avance que realiza el TC, que supone acuñar el término *expectativa razonable de confidencialidad*, aplicado a enervar la eficacia de la inmunidad de la protección formal del art. 18.3 CE. Esto nos viene a decir que en la medida que hagamos permeable una determinada comunicación al conocimiento ajeno, dejará de ampararnos la protección formal del secreto de las comunicaciones[278].

Por tanto, no pueden abrigarse expectativas razonables al respecto, cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean pueden ser objeto de registro[279], contravienen las órdenes del empleador. Queda, pues, configurada la *expectativa razonable de confidencialidad*

[277] RODRÍGUEZ LAINZ, J.L: «Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013 de 7 de octubre)», *op cit*. ,pág.9.

[278] *Ibídem,* pág. 9.

[279] GARCÍA ORTIZ, S. y SALAS DARROCHA, J.T.: «STC 170/2013 y nueva doctrina sobre el derecho a la intimidad del trabajador», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 30, 2014, pág. 464.

como un derecho de exclusión, en virtud del cual podemos excluir del conocimiento ajeno aquello que transmitimos a través de determinados canales de comunicación.

Esta sentencia contiene un voto particular que discrepa frontalmente de la misma; tanto de los datos de hecho de los que parte, como de las conclusiones obtenidas. En ese orden de cosas, se llega a afirmar que la tesis aquí expuesta pone en cuestión el modelo de relaciones laborales que constitucionalmente se venía aceptando hasta ahora. Así indica que dicha sentencia y en contra de tal modelo, atribuye al empresario facultades de las que carece; soslaya los condicionantes que en un juicio como el actual impone la libertad de las comunicaciones y el derecho al secreto de las mismas, con su carácter formal; y, en última instancia, opta por avalar los instrumentos de fiscalización incluso cuando se actualizan en términos abiertamente invasivos, lo que, al margen de acentuar la dependencia jurídica y la presión psicológica a los trabajadores, repercute negativamente en la efectividad de los derechos fundamentales que son constitucionalmente reconocidos a los mismos.

F) La STC 170/2013: remisión

Posteriormente, la STC 170/2013 de 7 de octubre[280], que se analizará de manera más detallada en otro apartado, también, recoge este criterio de *expectativa razonable de privacidad*: "*Nuestra doctrina ha establecido también ciertas matizaciones en cuanto al alcance de la protección del derecho a la intimidad reconocido en el art. 18.1 CE. Hemos tenido ocasión de precisar que el ámbito de cobertura de este derecho fundamental viene determinado por la existencia en el caso de una expectativa razonable de privacidad o confidencialidad. En concreto, hemos afirmado que un -criterio a tener en cuenta para determinar cuándo nos encontramos ante manifestaciones de la vida privada protegible frente a intromisiones ilegítimas es el de las expectativas razonables que la propia persona, o cualquier otra en su lugar en esa circunstancia, pueda tener de encontrarse al resguardo de la observación o del escrutinio ajeno. Así por ejemplo cuando se encuentra en un paraje inaccesible o en un lugar solitario debido a la hora del día, puede conducirse con plena espontaneidad en la confianza fundada de la ausencia de observadores. Por el contrario, no pueden abrigarse expectativas razonables al respecto cuando de forma intencional, o al menos de forma consciente, se participa en actividades que por las circunstancias que las rodean, claramente pueden ser objeto de registro o de información pública* "(FJ 4º).

[280] STC 170/2013, de 7 de octubre (RTC 2013\170).

G) Recepción judicial

Siguiendo los criterios establecidos en estas sentencias, los Tribunales Superiores de Justicia han ido abordando los diferentes problemas que se han planteado tanto en relación con la licitud de los medios empleados por las empresas para controlar el uso de los ordenadores por parte de sus trabajadores, como en la valoración de la gravedad de determinadas conductas relacionadas con el uso de tales medios para fines privados. A título de ejemplo citamos, STSJ de Asturias de 25 de octubre de 2013[281], STSJ de Cataluña de 21 de octubre de 2013[282] y STSJ de Madrid de 20 de mayo de 2013[283].

En un momento en que las nuevas tecnologías, y en particular las herramientas informáticas, están plenamente extendidas en los procesos productivos de las empresas, se plantea la necesidad de determinar no solo lo que se debe considerar como un uso adecuado por parte de los trabajadores de tales instrumentos de trabajo, sino también el alcance del control empresarial de ese uso y la manera en que debe llevarse a cabo. Si el medio se utiliza para usos privados en contra de las prohibiciones del empleador y con

---

[281] STSJ de Asturias de 25 de octubre de 2013 (JUR 2013\344267). El TSJ desestima el rec. de suplicación del trabajador y confirma la procedencia del despido. La utilización por el trabajador del ordenador de la empresa en tiempo y lugar de trabajo para usos personales, burlando los dispositivos de seguridad de la red inalámbrica de la empresa, constituye grave transgresión de la buena fe y abuso de confianza con entidad suficiente para justificar el despido (FJ 4º).

[282] STSJ de Cataluña de 21 de octubre de 2013 (JUR 2013\359792). Se revoca la sentencia de instancia que declaró procedente el despido del trabajador que confía en la apariencia de tolerancia creada por el empresario, y éste lo aprovecha para realizar un seguimiento del concreto uso de su equipo, y no de forma aleatoria, o general, sino selectiva, para sorprenderlo e imputarle indebido uso de elemento productivo o pérdida del tiempo que debe dedicarse a la prestación de servicios porque, entonces, la mala fe no es del trabajador que confía en la expectativa de racionalidad creada (FJ 6º).

[283] STSJ de Madrid de 20 de mayo de 2013 (EDJ 2013/167191). Se estima en parte el recurso de la empresa, con respecto a la cuantía de la indemnización, el resto de pronunciamientos se mantienen, confirmando así el despido improcedente. La prohibición absoluta de la recurrente, determina que no exista una situación de tolerancia con el uso personal del ordenador y que tampoco exista lógicamente una "expectativa razonable de confidencialidad". En estas condiciones el trabajador afectado sabe que su acción de utilizar para fines personales el ordenador no es correcta y sabe también que está utilizando un medio que, al estar lícitamente sometido a la vigilancia de otro, ya no constituye un ámbito protegido para su intimidad ",y existiendo en la empresa tal y como relata el ordinal tercero de la sentencia impugnada, una prohibición expresa de la demandada de utilización de Internet exclusivamente para fines laborales, lo que determinaría de conformidad con la doctrina expuesta la inexistencia de una situación de tolerancia, lo cierto es que en el supuesto de autos, no consta la conexión masiva del actor.

conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se haya vulnerado "*una expectativa razonable de intimidad* "

El criterio de la expectativa razonable de intimidad también llamado, criterio de la expectativa de confidencialidad o de privacidad, ha de cumplir un doble requisito. Uno, de carácter subjetivo relativo a que un individuo exhiba una real expectativa de intimidad; y otro, de carácter objetivo, la expectativa ha de ser de tal índole que la sociedad la reconozca como favorable.

El elemento clave, a tomar en consideración al tratar los límites entre los derechos fundamentales y el control de la actividad laboral del empresario, es la existencia o no de la orden de prohibición de uso de los instrumentos de la empresa para fines particulares; lo cual sería la pieza fundamental a la hora de permitir que se produzca o no, legal y constitucionalmente el control empresarial. Y ello porque, si no existe dicha limitación, la doctrina tradicional del Tribunal Supremo parte de la imposibilidad de tal control ante la expectativa de privacidad generada por la inactividad empresarial, como vamos a analizar a continuación.

H) Recepción doctrinal

Existe una parte de la doctrina que flexibiliza el uso de las nuevas tecnologías y de Internet en particular, apelando siempre al sentido común. Se arguye desde esta perspectiva, que, la utilización de la Red para uso personal, en casos concretos no debe necesariamente suponer un quebrantamiento grave a la confianza del empresario y a la lealtad[284]; más bien supone una ayuda para permitir atender a aspectos tan necesarios como cotidianos[285], como las responsabilidades familiares y con ello la posibilidad de conciliar vida profesional y personal.

Una vez establecida la prohibición a los trabajadores, la empresa ha de avisar previamente a sus empleados de la fiscalización de su prestación de servicios, lo que emparenta así con el principio de buena fe, según el cual se ha de preservar la expectativa

[284] TOSCANI JIMÉNEZ, D. y CALVO MORALES, D.: «El uso de Internet y el correo electrónico en la empresa: límites y garantías», *op.cit.*

[285] SAN MARTIN MAZZUCONI, C.: «El uso y el control empresarial de las nuevas tecnologías en el ámbito laboral. Algunas pautas recurrentes en la doctrina judicial para tener en cuenta», *Aranzadi Social* núm. 26, 2007 (BIB 2007. 997).

de los trabajadores de respeto a la intimidad[286]. El art. 20.2 ET declara el sometimiento tanto del trabajador como del empresario a las exigencias de buena fe.

En este sentido, MONEREO PÉREZ y LÓPEZ INSUA afirman que es necesario que el empresario disponga de los pertinentes instrumentos jurídicos, ya sean pactados o unilaterales, que le permitan prohibir o autorizar el empleo de los medios tecnológicos para fines personales o no; y en su caso, sancionar o no los incumplimientos en esta materia; de esta forma no se podrá considerar que se vulnera "*una expectativa razonable de intimidad*"[287].

FOLGUERA CRESPO afirma que para que el control empresarial o *monotoring* sea adecuado debe existir una previa advertencia (*warning*) que el trabajador afectado tiene que recibir; lo cual destruye la expectativa razonable de intimidad[288].

I) Recapitulación

En el supuesto de no existir ninguna proscripción sobre el manejo de los medios de la empresa, se da una situación de tolerancia con una expectativa razonable de confidencialidad y un desconocimiento de la prohibición absoluta. El trabajador actúa creyendo que la utilización que está haciendo es adecuada y confía en el carácter íntimo y secreto del contenido del medio; si se fiscalizase, se vulnerarían sus derechos constitucionales.

Situación contraria a la del supuesto anterior sería la del trabajador que desoye una prohibición expresa del empresario. Puesto que existen unas reglas de uso y manejo de los equipos de la empresa, y el operario puede fácilmente prever una posible fiscalización por parte del empleador, no se está dando una situación de tolerancia, ni tampoco cabe una expectativa razonable de confidencialidad, no se vulnera ningún derecho.

Por lo tanto, lo que se debe proteger es una expectativa de secreto, y no así el efectivo secreto o contenido del mensaje. De este modo cuando se quiebra la expectativa

---

[286] SEMPERE NAVARRO, A. V.: «Tras el pronunciamiento del Tribunal Supremo, ¿cabe controlar el ordenador de los trabajadores?» , *Actualidad Jurídica Aranzadi*, núm. 741, 2007 (BIB 2008/2115).

[287] MONEREO PÉREZ, J.L. y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op. cit.*

[288] FOLGUERA CRESPO, J.A.: «¿Puede el empresario controlar los ordenadores y correos electrónicos de sus empleados? (STC 170/2013, as."ALCALIBER")», *Revista Otrosí* núm. 3, 2013, págs. 51-53.

razonable de confidencialidad por contravenirse una orden empresarial, no puede hablarse de vulneración de ningún derecho constitucional[289].

Para concluir, un apunte; cabe subrayar que esta doctrina de la expectativa razonable de confidencialidad, no es proyectable al ámbito penal, en el que por expresa advertencia del Tribunal Supremo (STS 16 de junio de 2014[290]), el registro electrónico del correo corporativo de un trabajador, solo tendrá validez probatoria si media autorización judicial, pues en caso contrario, se está vulnerando el secreto de las telecomunicaciones[291].

6. Los tres derechos principalmente afectados (intimidad, honor, propia imagen)

Son numerosos los pronunciamientos del Tribunal Constitucional que califican el honor, la intimidad y la propia imagen como derechos estrictamente vinculados a la personalidad y derivados de la dignidad de la persona.

A) Plano internacional

El artículo 12 de la Declaración Universal de Derechos del Hombre y el artículo 17 del Pacto Internacional de Derechos Humanos de 1966 sobre Derechos Económicos y Sociales y Culturales[292] disponen que:

> *1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación.*
> *2. Toda persona tiene derecho a la protección de la ley contra estas injerencias o esos ataques.*

En sus Observaciones sobre este artículo, el Comité de Derechos Humanos, indica que este derecho debe estar garantizado respecto a cualquier ataque, venga de donde venga, bien de autoridades estatales, o bien de personas físicas o de personas jurídicas.

---

[289] TALENS VISCONTI, E.E.: «La expectativa razonable de confidencialidad como presupuesto de la vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario», *Revista doctrinal Aranzadi* núm. 51, 2013 (BIB 2013/2377).

[290] STS de 16 junio de 2014 (RJ 2014\3451)

[291] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*. *Op.cit*,. pág. 44.

[292] BOE 103/1977, de 30 de abril de 1977. Ref. Boletín: 77/10734.

Con la expresión "*injerencias arbitrarias"* se pretende garantizar que incluso cualquier injerencia prevista en la ley, debe ser en todo caso, puesta en consonancia con las disposiciones del Pacto y valorarse, en todo caso, como razonable respecto a las circunstancias particulares del caso[293].

El Convenio de Roma de 4 de noviembre de 1950, para la Protección de los Derechos Humanos y de las Libertades Fundamentales[294], recoge lo siguiente en su artículo 8, sobre el Derecho al respeto a la vida privada y familiar:

> *1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*
>
> *2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*.

El Tribunal Europeo de Derechos Humanos se ha pronunciado en algún caso sobre ciertas medidas de control o intercepción de comunicaciones en el lugar del trabajo, que pueden considerarse lesivas del derecho de la vida privada de los empleados, en concreto de su derecho a la intimidad. Ciertamente ello podría resultar sorprendente porque de la literalidad del art. 8 del Convenio de Roma, cabría inferir un ámbito de aplicación circunscrito a las injerencias de los poderes públicos, dejando al margen la vigilancia ejercida por los empresarios en el contexto laboral; sin embargo, no es esa la interpretación de la Corte de Estrasburgo.

Se ha declarado la existencia de lesión del derecho al respeto de la vida privada en diversos supuestos de utilización de medios técnicos de control a distancia en ámbitos profesionales; también incluso cuando son los propios empleadores o superiores jerárquicos los que ordenan la intercepción, la grabación o registro de las llamadas telefónicas desde su puesto de trabajo. Dos ejemplos de este tipo de acciones, los encontramos en el Tribunal Europeo de Derechos Humanos en las sentencias ya comentadas de fecha 25 de junio 1997, caso *Halford*[295],y en sentencia de fecha 3 de abril de 2007, caso *Copland*[296].

---

[293] BOU FRANCH, V. y CASTILLO DAUDÍ, M.: *Curso de Derecho Internacional de los Derechos Humanos*, ed. Tirant Lo Blanch, 2008, pág. 85.

[294] BOE 243/1979, de 10 de octubre de 1979. Ref. Boletín: 79/24010.

[295] STEDH 25 de junio de 1997 (TEDH 1997\37).

[296] STEDH 3 de abril de 2007 (TEDH 2007\23).

B) Plano constitucional

El art. 18 CE, por su parte, consagra una pluralidad de derechos cuya finalidad última es proteger la vida privada; pero, propiamente, no podemos encontrar un concepto de intimidad y tampoco están regulados todos sus posibles contenidos, así dice su primer apartado: *"se garantiza el derecho al honor a la intimidad personal y familiar y a la propia imagen"*.

Los conceptos de intimidad y propia imagen serán desarrollados *ut infra*; por su parte, el honor es un concepto jurídico indeterminado y el denominador común de todos los ataques al mismo es "el desmerecimiento en la consideración ajena" (STC 223/1992, de 14 de diciembre[297]).

Doctrina solvente explica que el TC en su evolución sobre la interpretación del art 18 CE tiene claramente tres fases: una primera, en la que se otorga una tutela hegemónica de los derechos al honor, intimidad y propia imagen; una segunda, en la que se produce una inversión, dándose prioridad a los derechos a la libertad de información y expresión[298] , de manera que estos derechos se relativizan; y una última, en la que estos derechos resultan claramente erosionados[299]. Incluso se ha llegado a afirmar que en Internet, resultan aniquilados[300].

C) Plano legal

La Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del derecho al Honor, la Intimidad Personal y Familiar y a la Propia Imagen regula importantes aspectos del ejercicio de estos derechos. Según el Preámbulo de este cuerpo legal, el derecho al honor, el derecho a la intimidad y el derecho a la propia imagen deben considerarse como tres

---

[297] STC 223/1992, de 14 de diciembre (EDJ 1992/12332).

[298] Tras la resolución del caso «*José María García*» (El Tribunal Constitucional desestimó el recurso de amparo del conocido periodista deportivo, interpuesto contra una sentencia de la Audiencia Provincial de Zaragoza a raíz de unas informaciones sobre una persona llamada, José Luis Roca, quien entonces -en el año 1987- era presidente de la Federación Española de Fútbol y diputado regional de Aragón, el motivo fundamental de esta condena fue la afirmación de que Roca "*había robado al pueblo de Zaragoza 219.000 pesetas*" en dietas y gastos) surge la llamada tesis «*la tutela condicionada de los derechos a la libertad de expresión e información*».

[299] HERRERO-TEJEDOR ALGAR, F.: «La protección del honor y de la intimidad en el ámbito de las telecomunicaciones» en AA. VV. PÉREZ-UGENA COROMINA, M. (Coor.): *Régimen de las telecomunicaciones*, ed. Tecnos, 1998.

[300] LOZANO GAGO, M, L.: «Los derechos al honor, intimidad e imagen en la Constitución Española y en las de EEUU y Francia», *Diario La Ley*, núm. 8593, 2015.

derechos distintos. La representación gráfica de los tres derechos adopta la forma de círculos secantes, de modo que una parte de su contenido coincide pero otra parte transita por vías distintas[301]. En su art. 1.3 lo califica como irrenunciable, inalienable e imprescriptible; estableciendo también la nulidad de la renuncia a la protección establecida en la ley, en caso de que se produjera.

D) Alcance de la intimidad laboral

La intimidad es "*a concept in disarray* [302]" que abarca la libertad individual, el control sobre el propio cuerpo, la potestad de información personal, la libertad ante los sistemas de control y vigilancia, la protección al honor y a la reputación, etc[303].

El concepto actual de derecho a la intimidad personal y familiar es relativamente reciente; pues tal y como viene manteniendo el Tribunal Constitucional, el respeto a la vida privada que deriva de la dignidad humana, dentro de los derechos de la personalidad, se encuentra en algunos de los derechos y libertades tradicionales como el de inviolabilidad del domicilio y el secreto de la correspondencia. En el art. 8 del Convenio de Roma aparecen unidas estas y aquel[304].

Se trata de un derecho de difícil determinación "*sustantiva*". Su vinculación con la dignidad de la persona y la inviolabilidad de los derechos "*que le son inherentes*" del art. 10.1 CE le ha dado un carácter particularmente expansivo, y ha hecho que se mueva en una zona algo "*brumosa circundante al individuo*"[305]. Y es que el derecho a la intimidad comprende "*una constelación de derechos*" vinculados a la tutela de la persona,

---

[301] RODRÍGUEZ CARDO, I. A.: «Dignidad, honor e intimidad en el trabajo», *Revista del Ministerio de Empleo y Seguridad Social*, núm. 108, 2014, pág. 141.

[302] Término en desorden.

[303] LUCENA CID, I.V. :«El nuevo concepto de la intimidad en los nuevos contextos tecnológicos» en AA. VV., GALÁN MUÑOZ, A. (Coord.) *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación*, *op. cit*. , pág. 22.

[304] TORRES DEL MORAL. A.: *Principios de Derecho Constitucional Español*. Tomo I. Sistemas de Fuentes. Sistemas de los Derechos. Servicio de Publicaciones de la Facultad de Derecho de la Universidad Complutense, 2004, pág. 348.

[305] RODRÍGUEZ PIÑERO y BRAVO-FERRER, M.: «Intimidad del trabajador y contrato de trabajo», *op. cit*., págs. 93- 103.

de su libertad y dignidad[306], espacios de la vida personal y familiar, aspectos concernientes a su corporeidad e imagen, a la sexualidad, a la integridad física y moral, a la dignidad, a la libertad de conciencia, etc., materias colindantes con otros derechos fundamentales (el derecho al honor, a la libertad ideológica o de expresión, etc.) que también afectan a la dinámica del contrato de trabajo.

Según reiterada jurisprudencia constitucional, el derecho a la intimidad personal, en cuanto derivación de la libertad y dignidad de la persona, art. 10.1 CE, implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario según las pautas de nuestra cultura, para mantener una mínima calidad de vida humana. A fin de resguardar ese espacio reservado, este derecho confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido. (STC 196/2004, de 15 de noviembre)[307]. Por lo tanto, "*el atributo más importante de la intimidad, como núcleo central de personalidad, es la facultad de exclusión de los demás, de la abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de estos datos*" (STC 142/1993, de 22 de abril[308]).

El Tribunal Constitucional ha destacado en la STC 200/1999, de 8 noviembre[309], que el elemento teleológico del derecho a la intimidad del art. 18.1 CE es la "*protección de la libertad y de las posibilidades de autorrealización del individuo"* y ha considerado que "*se trata del poder de resguardar un ámbito reservado por el individuo para sí y su familia de una publicidad no querida*".

El derecho a la intimidad consiste en la facultad de excluir del conocimiento ajeno, cualesquiera hechos comprendidos dentro del ya mencionado ámbito propio y reservado. El problema reside en determinar cuál es el alcance exacto de la esfera privada, y por consiguiente qué son las intromisiones ilícitas en la intimidad. A la hora de resolver la

---

[306] RODRÍGUEZ PIÑERO y BRAVO-FERRER, M.: «Derecho a la Intimidad y Relaciones laborales», Ponencia en la Universidad de Huelva en el Seminario sobre Tendencias de la Protección Jurídica de la Intimidad "Privacidad y Relaciones Laborales" 2006, pág. 7 del original impreso. *http://www.uhu.es/intimidadyderecho/Docs/ponencia.pdf*

[307] STC 196/2004, de 15 noviembre (RTC 2004\196).

[308] STC 142/1993, de 22 abril (RTC 1993\142).

[309] STC 200/1999, de 8 noviembre (RTC 1999\2000).

cuestión, el Tribunal Constitucional ha tenido que discernir si el criterio para la definición de esa esfera privada era formal o material. Si se optase por el criterio formal, resultará ser lo que cada persona quiera excluir del ámbito de los otros; si se escogiera, en cambio, el criterio material, se trataría de lo que según las pautas sociales imperantes suela considerarse reservado o ajeno al legítimo interés de los demás. La jurisprudencia constitucional ha venido siguiendo un criterio predominantemente material a la hora de delimitar la esfera privada.

E) Recapitulación

El derecho a la intimidad configura una reserva absoluta en torno a ciertos campos considerados como el núcleo más primario y esencial de la privacidad de la persona: la intimidad espiritual, la intimidad corporal y sexual, y la intimidad doméstica o familiar[310] (STC 10/2002, de 17 enero[311]). Su función es la de proteger frente a cualquier invasión que se pueda realizar en el ámbito de la vida personal y familiar de la persona. Es un derecho objetivo o material, mediante el cual el ordenamiento jurídico designa y otorga protección al área que cada uno se reserva para sí o para sus íntimos, un *"ámbito reservado de las vida de las personas excluido el conocimiento de terceros*" en contra de su voluntad (SSTC 127/2003, de 30 junio[312] y 189/2004[313], de 2 de noviembre).

"El conflicto entre la libertad de expresión y la intimidad personal es sin duda el tema de nuestro tiempo en materia de derechos fundamentales"[314], esta afirmación goza de actualidad a pesar de que estas palabras fueron escritas por PENDÁS DÍAZ en el año

---

[310] ÁLVAREZ ALONSO, D.: «Medios audiovisuales de vigilancia empresarial y derechos fundamentales del trabajador», Comunicación a la ponencia temática: El Derecho del Trabajo y las Relaciones Laborales ante los cambios económicos y sociales del X Congreso Europeo de Derecho del Trabajo y de la Seguridad Social de la AEDTSS, septiembre 2011, pág. 3 del original impreso. *http://www.aedtss.com/images/stories/documentos/congresoeuropeocomunicaciones/1/123alvarez_alonso.pdf*

[311] STC 10/2002, de 17 enero (RTC 2002\10).

[312] STC 127/2003, de 30 junio (RTC 2003\127).

[313] STC 189/2004, de 2 noviembre (RTC 2004\189).

[314] PENDÁS DÍAZ, B.: «Prólogo» en WARREN, S. y BANDREIS, L.: *El Derecho a la Intimidad*. ed. Civitas, 1995, pág. 11.

1995. El honor y la intimidad son derechos inextricablemente unidos a la dignidad, que han sido invocados en múltiples ocasiones en los Juzgados de lo Social por los trabajadores frente a la libertad de expresión y al derecho a transmitir información como argumentos en contra esgrimidos por la empresa[315].

Con el fin de delimitar mejor la cuestión objeto de debate, podemos exponer una serie de afirmaciones:

- Por razones de pura lógica, la esfera de intimidad personal está en función de la disposición que de la misma realice su titular. Por ello, corresponde a cada persona delimitar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno.
- El consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad[316].
- Por lo cual podemos concluir diciendo que la intimidad acota un campo de reserva personal, definido de forma objetiva por los usos sociales, en el que puede, sin embargo, intervenir la decisión de cada persona de "*bajar las barreras"* protectoras haciendo público lo íntimo.

[315] OJEDA AVILÉS, A. e IGARTUA MIRÓ, M.T.: «La dignidad del trabajador en la doctrina del Tribunal Constitucional. Algunos apuntes», *Revista del Ministerio de Trabajo e Inmigración*, núm. 73, 2008, pág. 73.

[316] STC 173/2011, de 7 de noviembre (RTC 2011\173). En un proceso penal por delito de corrupción de menores en su modalidad de distribución de pornografía infantil, se accedió al contenido del ordenador personal del recurrente sin su consentimiento ni autorización judicial. Se trata de una conducta que persigue un fin legítimo y que se encuentra dentro de las investigaciones dirigidas al esclarecimiento de un delito; por tanto, es una medida necesaria, razonable y proporcional. El sacrificio del derecho fundamental afectado está justificado por la presencia de otros bienes jurídicos constitucionalmente relevantes y protegidos; de manera que la vulneración de la normativa constitucional es inexistente.

7. Control mediante TICs: la privacidad

La posición jurídica activa del empleador afecta a la esfera privada y personal del trabajador, dado que en la dinámica contractual se insertan facultades de vigilancia y control del empresario, connaturales a la estructura del contrato y a la configuración jurídica de la prestación de trabajo.

A) Funcionalidad constitucional genérica

La Constitución impone límites externos a los poderes de injerencia del empresario sobre datos que, por su naturaleza, exceden de la esfera del compromiso contractual del trabajador, y que no guardan cierta relación con el trabajo. El Tribunal Constitucional reconoce que la intimidad protegida por la Carta Magna no sólo se reduce al ámbito doméstico o privado, sino que también existen otros, en particular el relacionado con el trabajo o profesión, donde se desarrollan relaciones interpersonales, vínculos o actuaciones que pueden constituir manifestación de la vida privada. Es más, argumenta también que la cobertura de este derecho abarca el cúmulo de información que es almacenada por su titular; por ejemplo, en un ordenador personal, puede haber correos electrónicos guardados en la memoria del terminal informático utilizado.

La intimidad actúa como mecanismo defensor frente a ilimitaciones del empresario y; además, atribuye al empleador obligaciones o deberes positivos, que implican nuevas posiciones contractuales que enriquecen y completan el vínculo laboral. Esa dimensión constitucional y ordinaria es relativamente numerosa en relación con la incidencia del art. 18 CE en el contrato de trabajo[317].

B) Reconocimiento legal

El art. 4.2 ET afirma que los trabajadores tienen derecho a la intimidad. Ello permite al empleado disfrutar de un ámbito privado, libre de intromisiones ilegítimas,

[317] RODRÍGUEZ PIÑERO y BRAVO FERRER, M.: «Intimidad del trabajador y contrato de trabajo», *op. cit.* , págs. 93-103.

incluidas, obviamente, las que provienen del empresario. La tutela del derecho a la intimidad como derecho fundamental da base y protección constitucional a los límites contractuales de las facultades de control empresarial, para impedir el control de conductas no referidas a la actividad laboral y a la toma intrusiva o a la divulgación ilegítima de datos del trabajador.

El alcance de la protección de la intimidad afecta a los medios de trabajo cuyo control puede resultar afectado por este derecho, a saber: comunicaciones telefónicas, correo electrónico, archivos personales del ordenador, histórico de visitas a Internet, etc.

Las organizaciones productivas no son ajenas a los principios y derechos constitucionales y que la celebración del contrato de trabajo, en el que se ponen en juego la dignidad y la libertad del trabajador, no lo priva de los derechos fundamentales que la Constitución le reconoce, como trabajador y como persona que debe ser defendida frente a peligros o intrusiones provenientes del medio empresarial. Por ello, el contrato de trabajo se ha visto condicionado o influido más que ningún otro contrato privado por los derechos fundamentales, y, en particular, por el derecho a la intimidad.

C) Valoración doctrinal sobre video vigilancia

Por otro lado, la relación entre intimidad y el control a través de la videovigilancia sigue siendo una cuestión problemática. El TC nos remite a la casuística; tampoco la doctrina parece haber llegado a conclusiones definitivas en la materia; encontramos a defensores y detractores de este mecanismo de control, como analizamos a continuación.

La postura más restrictiva es la que ha mantenido GOÑI SEIN, para el cual las técnicas de captación y de reproducción de la imagen, cuando se usan por razones de seguridad, de prevención de riesgos laborales o de carácter organizativo, resultan ilegítimas "*si permiten ejercitar alguna función de control de personal*[318]". Tras la recepción de la doctrina constitucional del año 2000, este autor ha admitido de forma más amplia su utilización aunque con importantes restricciones[319].

[318] GOÑI SEIN, J. L.: *El respeto a la esfera privada del trabajador*, *op. cit*., pág. 143.

[319] GOÑI SEIN, J. L.: *La Videovigilancia empresarial y la protección de datos personales*. *op. cit*., págs. 105-141.

MERCADER UGUINA afirma que las nuevas tecnologías de la comunicación lo que hacen es contribuir a "*reforzar la visión panóptica de la sociedad de trabajo*"[320] o, dicho con otras palabras, que la privacidad queda prácticamente anulada; ya que no existe prácticamente espacio alguno para la libertad, el trabajador ya no es uno más del grupo sino un ser individualizado y controlado en todo momento.

Una parte de la doctrina ha señalado que no existe en nuestro ordenamiento una regulación general para la utilización de las nuevas tecnologías como control empresarial; y en algún caso, en la línea de la doctrina tradicional social, hasta se ha cuestionado que haya una afectación de la intimidad de los trabajadores. En este sentido MONTOYA MELGAR opina que sólo se puede considerar intromisión ilegítima, el uso de medios de videovigilancia "*destinados a captar o a conocer la vida íntima*"[321]: lo que parece dejar fuera del ámbito a la vida laboral. Para este autor la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, es validada como no aplicable al ámbito laboral, por considerar la vida íntima de las personas como un estadio necesariamente distinto al ámbito profesional de las mismas.

Según FERNÁNDEZ VILLAZÓN, estas posturas olvidan la relación existente entre el derecho a la intimidad y los otros derechos fundamentales, como la dignidad y el libre desarrollo de la persona (art. 10.1 CE), aspectos que sí se ven implicados en el mundo del trabajo como muy bien se desprende del Estatuto de los Trabajadores; es más, el propio Tribunal Europeo de Derechos Humanos ha establecido que la vida privada también se extiende al ámbito profesional[322].

Desde una posición coherente SEMPERE NAVARRO y SAN MARTÍN MAZZUCCONI afirman que lo que resulta vulnerador del derecho a la intimidad frente al control empresarial, "*es el control por el control en sí mismo, sin que exista razón objetiva que lo motive"*[323].

DESDENTADO BONETE y MUÑOZ RUIZ, afirman que el conflicto entre el control con las nuevas tecnologías por parte del empresario y el derecho a la intimidad

---

[320] MERCADER UGUINA, J.: *Derecho del Trabajo. Nuevas tecnologías y sociedad de la información*, ed. Lex Nova, 2002, pág. 101.

[321] MONTOYA MELGAR, A.: *Derecho del Trabajo*, ed. Tecnos, 2010, págs. 365-367.

[322] FERNÁNDEZ VILLAZÓN, L.A.: «Las facultades empresariales de control de la actividad laboral»,*op. cit.*, pág. 36

[323] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y Relaciones Laborales, op.cit,* pág. 92

está relacionado con el recurso al principio de proporcionalidad, a través de la técnica de la ponderación. Solamente se producirá una lesión cuando la intimidad quede realmente afectada por las formas de control aplicadas. Pero cualquier medio de control por parte del empresario no ha de rechazarse, habrá que emplear la técnica de la ponderación, y después concluir si afecta o no a la intimidad del trabajador, y por tanto hay que excluirlo[324].

En definitiva, ha señalado RODRÍGUEZ-PIÑERO que no cabe hablar en abstracto de la legitimidad o ilegitimidad del uso de las nuevas tecnologías de control del empresario al trabajador. Desde la perspectiva de la intimidad, hay que valorar el supuesto de hecho y las circunstancias concurrentes, si el empleo de una técnica de control se encuentra en el ámbito de lo privado y si lo hace justificadamente o no[325].

D) Transformaciones tecnológicas y jurídicas

El derecho a la intimidad ha sufrido una profunda transformación a consecuencia de la evolución de la tecnología informática y la consecuente recogida, almacenamiento y tratamiento de datos, y su posible transmisión por vía telemática. La intimidad incluye ahora también una vertiente activa, que se traduce en las facultades de gobierno o de control, de esas facetas en principio íntimas, de modo que "*la garantía de intimidad adopta hoy un entendimiento positivo que se traduce en el derecho de control sobre los datos relativos a la persona*" [326].

Los avances tecnológicos de las últimas décadas nos llevan a la necesidad de formular una reconceptualización del concepto de intimidad. El hecho cierto es que la noción de intimidad parece constituir una realidad en declive; su importancia es decreciente porque lo que se incentiva es una forma de relacionarse colaborativa que obliga a compartir y a salir del anonimato.

---

[324] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op. cit.,* pág. 55.

[325] RODRÍGUEZ PIÑERO y BRAVO FERRER, M.: «Intimidad del trabajador y contrato de trabajo», *op. cit.*

[326] STC 200/1999, de 8 noviembre (RTC 1999\2000).

La sociedad está ahora sensibilizada con un fenómeno más complejo que el de un ámbito de protección especifico, cual es el control de la identidad[327], en palabras de THOMPSON "la manera más prometedora de conceptualizar la privacidad es en términos de control"[328]; por tanto, el concepto actual de privacidad tiene que ver con la capacidad de los individuos de controlar las revelaciones sobre uno mismo y hasta qué punto estas pueden comunicarse con los demás[329]. Pero no debe entenderse solo como un control de la información, RÖSSLER distingue tres esferas:

1) Privacidad informativa. Control de la información sobre sí mismo y el derecho a protegerla del acceso indeseado de los demás.
2) Privacidad de decisión. Control de las decisiones y acciones.
3) Privacidad espacial. Control respecto nuestros propios espacios y el derecho a protegerlos de la intrusión indeseada de los demás

Las violaciones a la privacidad en cada una de estas dimensiones se definirían de la siguiente manera: como el acceso y uso ilícito de información sobre nosotros; como una interferencia ilícita en nuestras decisiones y actos; y como una intrusión ilícita en nuestros espacios ya sea a través de intrusión física por medio de vigilancia o a través de las nuevas tecnologías de la información y de la comunicación[330].

Algunos autores llegan a diferenciar entre privacidad e intimidad; entendiendo por esta determinados aspectos de la vida personal del trabajador que no constituyen propiamente intimidad; señalan que en esta parcela el empresario sí podría incidir para controlar a su empleado, cumpliendo los requisitos legales[331]. Pero otros autores no comparten esta distinción sirva de ejemplo TOSCANI GIMÉNEZ, que la considera del todo artificial[332] ya que sostiene que la vida personal pertenece a la intimidad siempre.

---

[327] GOÑI SEIN, J.L.: «Los límites de las potestades empresariales *vs.* Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *Actum Social* núm.95, 2015.

[328] THOMPSON, J.B.: «Los límites cambiantes de la vida pública y privada», Revista Nueva Época, núm. 15, 2011, págs. 11-42.

[329] LUCENA CID, I.V. :«El nuevo concepto de la intimidad en los nuevos contextos tecnológicos» en AA. VV., GALÁN MUÑOZ, A. (Coord.): *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación*, *op.cit.*, pág. 51.

[330] *Ibídem*, pág. 51.

[331] DÍAZ RODRÍGUEZ, J.M.: *Detectives y vigilantes privados en el ámbito laboral*, ed. Tirant Lo Blanch, 2013, pág. 94.

[332] TOSCANI JIMÉNEZ, D.: «La vulneración del derecho a la intimidad por delatores, detectives privados y medios tecnológicos», *Revista Española de Derecho Social*, núm.71, 2015, pág. 64.

8. El derecho a la propia imagen del trabajador

Tras el enorme desarrollo de la publicidad y de las técnicas de comunicación, "*está de moda*" que todo se vea, que todo sea imagen.

Podemos citar algunos ejemplos tan ilustrativos, como las campañas electorales que cada vez más se centran en la imagen de los políticos, frente a la que la propuesta o el programa electoral pierde relevancia, vaciando su contenido.

Asimismo puede traerse a colación la lamentable noticia que saltó hace poco a los medios de comunicación, en la que unos adolescentes grabaron la agresión a otro menor con el "*aliciente*" de "*rewhatsappear"* el vídeo a gran parte de sus contactos telefónicos[333]. Es también por todos conocido, que algunas personas no tienen ningún pudor en realizar los más variados sinsentidos delante de una cámara, para "*colgar*" luego el vídeo en Internet (solo hay que navegar por *YouTube* para ver que los videos más absurdos son *trending topic).* El Derecho del Trabajo no es ajeno a esta tendencia de "*adicción a la imagen*" como reflejo de la sociedad y de lo que impera en ella.

A) Delimitación

A partir de la segunda mitad del siglo pasado aparecen los procedimientos mecánicos de captación y difusión de la imagen y es cuando se comienza a hablar de un derecho a la propia imagen, que precisa protección jurídica. La Sala de lo Social del Tribunal Superior de Justicia de Madrid, declara en este sentido: "La imagen tiene, y cada vez más, un valor comercial indiscutible en nuestro tráfico económico, siendo un elemento generador de importantes beneficios e intereses" (FJ 9º) [334].

El derecho constitucional a la propia imagen, no se planteó, originariamente, para ser postulado específicamente en el ámbito de las relaciones laborales, es un derecho

[333] elmundo.es (2016, 3 de febrero) «Una escuela de Girona expulsa a tres alumnos una semana por hacer 'bullying' a otro estudiante». *http://www.elmundo.es/cataluna/2016/02/03/56b2280b22601df4468b462b.html*

[334] STSJ de Madrid de 16 de noviembre de 2012 (AS 2013\162).

fundamental inespecífico, consagrado en el art. 18.1 de la Constitución Española, junto con los derechos a la intimidad personal y familiar y al honor, contribuye a preservar la dignidad de la persona (art. 10.1 CE), salvaguardando una esfera de propia reserva personal frente a intromisiones ilegítimas provenientes de terceros.

B) Plasmación normativa

En nuestro ordenamiento el desarrollo legislativo de tales derechos se halla recogido en la LO 1/1982, de 5 de mayo, de Protección Civil al Honor, la Intimidad Personal y Familiar y Propia Imagen. El art. 2 de la citada Ley establece que la protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales y deberá atenderse al ámbito que mantenga cada persona según sus propios actos, disponiendo el art. 7 una serie de supuestos en que se considera que existen intromisiones ilegítimas de tales derechos. El art. 9.3 manifiesta que la existencia de perjuicio se presumirá siempre que exista intromisión ilegítima y para la valoración del daño moral causado por la misma deberá atenderse a las circunstancias del caso y a la gravedad de la lesión, así como a la difusión o audiencia del medio en que se ha divulgado y el beneficio que el causante de la lesión haya obtenido.

Ya dentro del Derecho del Trabajo, resulta sorprendente que nuestro Estatuto de los Trabajadores sea "*tan parco*" en palabras y se limite a dedicar sólo el art. 4 a la referencia de los derechos fundamentales de la persona del trabajador, en tanto la garantía y defensa de los derechos fundamentales la aborda sólo en tres de sus preceptos, art. 17, art. 18 y art. 19 y de manera casuística. Brilla por *"su ausencia*" una configuración global respecto a la privacidad del trabajador y su protección. Normativa inexistente, pero que entendemos, *lege ferenda*, a todas luces, necesaria.

C) Protección y vulneración

El derecho fundamental a la propia imagen concede a su titular la facultad única de difundir o publicar su imagen y por el otro lado, de evitar la incondicional difusión de su aspecto físico, sin que se pueda reproducir o publicar la propia imagen por parte de otra persona, sea cual sea su finalidad[335]. El derecho a la propia imagen pretende salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás; un ámbito necesario para poder decidir libremente el desarrollo de la propia personalidad y, en definitiva, un ámbito necesario según las pautas de nuestra cultura para mantener una calidad mínima de vida humana (STC 231/1988, de 2 de diciembre, FJ 13º).

Asimismo, tiene declarado el TC que el derecho a la propia imagen se salvaguarda reconociendo la facultad para evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como sujeto individual (SSTC 231/1988, de 2 de diciembre[336], FJ 3º y 99/1994, de 11 de abril[337] FJ 5º).

Según el TC, mediante la captación y publicación de la imagen de una persona puede vulnerarse tanto su derecho al honor como su derecho a la intimidad. Sin embargo, lo específico del derecho a la propia imagen es la protección frente a las reproducciones de la misma que, afectando a la esfera personal de su titular, no lesionan la reputación ni dan a conocer la vida íntima (STC 81/2001, de 26 de marzo[338]).

---

[335] APARICIO ALDANA, R.K.: «Derecho a la propia imagen en las relaciones laborales», *Revista Doctrinal Aranzadi Social* núm. 27, 2013 (BIB 2013\1440).

[336] STC 231/1988, de 2 de diciembre (RTC 1988\231).

[337] STC 200/1999, de 8 noviembre (RTC 1999\2000).

[338] STC 81/2001, de 23 de marzo (RTC 2001\81). El TC desestima el recurso de amparo interpuesto por un popular personaje televisivo (Emilio Aragón Álvarez) contra sentencia del TS, que desestimó su pretendido derecho a la propia imagen al permitir, y no sancionar, la apropiación y explotación inconsentida de su imagen, reproducida por una campaña publicitaria con el eslogan: "*La persona más popular de España está dejando de decir te huelen los pies",* en la que quedaba plenamente identificado por la peculiar forma de vestir en sus apariciones televisivas, y por una canción que había popularizado titulada "*me huelen los pies* ", sin necesidad de haberse reproducido su cara o utilizar su nombre. La Sala

J) Evolución conceptual

Cabe distinguir varias concepciones del derecho a la propia imagen. En un primer momento se consideró a la imagen como una manifestación del propio cuerpo, los derechos del individuo sobre su cuerpo alcanzaban igualmente a su imagen. Se propugnaba así una protección absoluta, comprensiva incluso de la legítima defensa contra quienes, sin la voluntad del titular del derecho, quisieran tomar una fotografía.

De esta configuración se pasó a considerar la imagen como una manifestación de la protección del honor, concediendo acción únicamente a aquél cuyo honor hubiera sido dañado mediante la utilización de su imagen[339].

Hoy parecen superadas ambas teorías, confiriendo al derecho a la imagen, una entidad propia. En este sentido se manifiestan, entre otros, BALLESTER PASTOR[340] y PACHECO ZERGA[341]. El ámbito del derecho a la imagen está, pues, relacionado con el derecho a la intimidad y aunque la lesión doble sea posible, en la jurisprudencia constitucional de los últimos quince años aparece ya como un derecho fundamental autónomo.

K) Conexión con la intimidad

Por otro lado, cabe resaltar que en la doctrina comparada este tratamiento autónomo no existe, ya que el derecho a la propia imagen suele ir anudado con el derecho

---

señala que nos encontramos ante la representación imaginaria de las características externas de un personaje televisivo, imagen que constituye una representación ajena al espacio de privacidad de su creador, a su propia imagen como individualidad y como persona, y a su dignidad personal. Considera además que el valor asociado a la persona de su creador por lazos jurídicos y económicos es susceptible de protección jurídica, pero no a través del derecho a la a la propia imagen, al no pertenecer a la esfera reservada y propia de aquél sino al valor patrimonial o comercial del personaje televisivo.

[339] CASTELO GARCÍA, M.: «Aproximación a la apropiación comercial de la imagen», *Base de Datos de Bibliografía El Derecho*, núm. 9, 2006, pág. 2 (EDB 2006/247628).

[340] BALLESTER PASTOR, I.: «Facultades de control empresarial sobre el aspecto exterior del trabajador: Límites a la expresión del derecho a su propia imagen en el desarrollo de la prestación laboral» *Tribuna Social: Revista de seguridad social y laboral*, núm. 169, 2005, pág. 27.

[341] PACHECO ZERGA, L.*: La dignidad humana en el Derecho del Trabajo*, ed. Thomson-Civitas, 2007, pág. 219.

a la intimidad[342]. Podemos centrarnos en la STC 156/2001 de 2 de julio[343], para analizar con un poco más de detalle las diferencias y similitudes entre el derecho a la intimidad y el derecho a la propia imagen. Se pueden contemplar tres hipótesis:

- El supuesto que mediante la captación y reproducción gráfica de una persona, se pueda vulnerar su derecho a la intimidad y no su derecho a la propia imagen.
- Cuando, a diferencia del caso anterior, se viole el derecho a la propia imagen sin menoscabar el derecho a la intimidad. Lo que sucederá cuando las imágenes permitan la identificación de la persona fotografiada pero que no presenten una intromisión en su intimidad. Será determinante que la representación de la imagen permita la identificación de la persona. Si no se puede identificar o reconocer no estaríamos ante un supuesto de intromisión ilegitima. Es lo que la doctrina denomina "*principio de recognoscibilidad*" .
- Y, por último, aquellas ocasiones en que una imagen lesione a la vez ambos derechos. Tal acontecerá en los casos en los que se revele la intimidad personal y familiar y además se permita identificar a la persona.

La STC 231/1988 de 2 de diciembre[344] recoge que solo adquiere su pleno sentido, el derecho a la propia imagen, cuando se le enmarca en la salvaguardia de "*un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las*

---

[342] FERNÁNDEZ LÓPEZ, M. F.: «La intimidad del trabajador y su tutela en el contrato de trabajo» en AA. VV. CASAS BAAMONDE, E., CRUZ VILLALÓN, J. y DURÁN LÓPEZ, F. (Coords.): *Las transformaciones del derecho del trabajo en el marco de la Constitución española: estudios en homenaje al profesor Miguel Rodríguez-Piñero y Bravo-Ferrer*, *op. cit.*, pág. 634.

[343] STC 156/2001, de 2 de julio (RTC 2001\156). El TC estima parcialmente la demanda de amparo interpuesta por la recurrente, y considera que, la publicación de ciertas fotografías en las que aparece desnuda y claramente identificable, vulnera sus derechos a la intimidad y a la propia imagen. La Sala aprecia intromisión ilegítima en el derecho a la intimidad de la demandante en el hecho de que la publicación de dichas fotografías se realizó sin su consentimiento y fueron obtenidas en un ámbito privado. Señala además que la circunstancia de que la recurrente pertenezca a una secta que fomenta la promiscuidad sexual, no conlleva que aquélla haya perdido el poder de reserva sobre partes íntimas de su cuerpo, ni puede considerarse que tal intromisión pueda ampararse en la existencia de un bien o derecho merecedor de mayor protección.

[344] STC 231/1988, de 2 de diciembre (RTC 1988\231). Versa sobre la difusión de imágenes en la enfermería del Torero Paquirri, tras la cogida mortal de un toro.

pautas de nuestra cultura, para mantener una calidad mínima de la vida humana"(FJ 3º), una valoración teleológica que, por lo demás, también ha prevalecido cuando se ha analizado la proyección del derecho en cuestión sobre la relación individual de trabajo STC 170/1987, de fecha 30 de octubre[345] (FJ 4 º).

El primer elemento a salvaguardar sería el interés del trabajador de 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 imprescindible para su propio reconocimiento como individuo. En este contexto, la captación y difusión de la imagen del trabajador, solo será admisible cuando la propia, y previa, conducta de aquél o las circunstancias en que se encuentra inmerso justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que puedan colisionar con aquél. Esta estricta vinculación con la salvaguardia de la intimidad, y la dimensión teleológica del derecho a la propia imagen, hace que la dimensión constitucional del tema quede restringida a este concreto ámbito de natural reserva de la propia esfera íntima.

L) Recapitulación

El derecho a la propia imagen, consagrado en el art. 18.1 CE junto con los derechos a la intimidad personal y familiar y al honor, contribuye a preservar la dignidad de la persona (art. 10.1 CE), salvaguardando una esfera de propia reserva personal frente a intromisiones ilegítimas provenientes de terceros. El ámbito del derecho a la imagen está ligado, de manera indisoluble al derecho a la intimidad y aunque la lesión doble sea posible, en la jurisprudencia constitucional más reciente, aparece como un derecho autónomo.

El derecho a la propia imagen atribuye a su titular la facultad de disponer de la representación de su aspecto físico que permita su identificación, lo que conlleva, tanto el derecho a determinar la información gráfica generada por los rasgos físicos que la hagan reconocible, que puede ser captada o tener difusión pública, como el derecho a impedir la obtención, reproducción o publicación de la propia imagen de un tercero no autorizado.

[345] STC 170/1987, de 30 de octubre (RTC 1987\170).

La imagen es un instrumento indispensable para la configuración de la esfera personal, ya que permite la identificación de la persona como ser individual y le proyecta socialmente hacia el exterior. Por ello, el derecho fundamental a la propia imagen otorga a su titular la facultad exclusiva de difundir o publicar su imagen y por ende, de evitar la incondicional difusión de su aspecto físico, impidiendo la reproducción o publicación de la propia imagen por parte de un tercero, sea cual sea su finalidad, comercial, informativa, científica, cultural, etc.[346]

Ya aludimos a la importante STC 99/1994, de 11 de abril [347], que reconoce el derecho a la propia imagen del trabajador deshuesador de jamones, derecho que junto con el derecho al honor contribuye a preservar la dignidad de la persona, salvaguardando una esfera de propia reserva personal frente a intromisiones ilegítimas. Reflexiona la Sentencia, que no puede deducirse, sin embargo, del art. 18 CE un derecho incondicionado al anonimato; pero la captación y difusión de la imagen del trabajador sólo será admisible cuando la conducta de aquél justifique el descenso de las barreras de reserva para que prevalezca el interés público y no consta que tuviese asignada tarea alguna de exhibición de su habilidad en la promoción del jamón.

9. El secreto de las comunicaciones

El valor o bien jurídico protegido por el secreto de las comunicaciones es la libertad de las comunicaciones, no la intimidad, su principal rasgo es que está configurado como garantía de intangibilidad. El secreto de las comunicaciones es otro campo de conflicto, así lo ha señalado el TEDH respecto a las llamadas telefónicas que proceden de locales profesionales, pues son susceptibles de incluirse en los conceptos de vida privada y de correspondencia a los efectos del art. 8 del Convenio de Roma. Del mismo modo, gozan de esa protección los correos electrónicos enviados desde el lugar de trabajo. Protección que se extiende también a los mensajes recibidos, ya sea en el servidor

[346] APARICIO ALDANA, R.K.: «Derecho a la propia imagen en las relaciones laborales», *op.cit.*

[347] STC 99/1994, de 11 de abril (RTC 1994\99).

empleado por la empresa, ya sea en el buzón del correo electrónico del trabajador, no obstante, es preciso que tales mensajes precisen la evidencia externa que permita tener la constancia objetiva de que son objeto de una comunicación secreta[348].

A) Idea general

El secreto de las comunicaciones posee un perfil mucho más definido y cierto[349] que el derecho a la intimidad, así el artículo 17 del Pacto Internacional de Derechos Humanos de 1966 sobre Derechos Civiles y Políticos, dispone que:

> *1.Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
> *2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o contra esos ataques.*

El derecho del art. 18.3 CE garantiza "*el secreto de las comunicaciones*", y en especial "*de las postales, telegráficas y telefónicas, salvo resolución judicial*", aunque el texto constitucional, obviamente, no hace referencia a las nuevas tecnologías, son un medio de comunicación interpersonal, y por ello deben ser protegidas.

El apartado segundo y tercero del art. 18 CE, proclaman respectivamente, la inviolabilidad del domicilio y el secreto de las comunicaciones, son derechos que se encuentran entre los más antiguos de los fundamentales, pues ya eran consagrados en las primeras declaraciones de derechos. En ambos casos, se trata de garantizar que un espacio o actividad sean de acceso reservado, en este sentido guarda relación con el derecho a la intimidad, pero aparte de que el reconocimiento expreso de este es mucho más reciente, como ya hemos manifestado, opera como garantía formal de intangibilidad, por lo que debe ser analizado como derecho autónomo. Estar configurado como garantía formal de intangibilidad significa que la actividad, comunicación, es de acceso reservado en cuanto tal.

---

[348] ROQUETA BUJ, R.: *Uso y control de los medios tecnológicos de información y comunicación en la empresa*, ed. Tirant lo Blanch. 2005, pág. 24.

[349] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*, *op.cit.*, pág. 25.

B) Significado instrumental

El secreto de las comunicaciones, que es lo expresamente proclamado en el art. 18.3 CE tiene un significado instrumental, respecto de la libertad, pues se garantiza el secreto de las comunicaciones para que éstas puedan desarrollarse con libertad. Así podemos realizar una serie de precisiones:

- Solo la comunicación que ha de valerse de algún medio técnico, está cubierta por el art. 18.3 C.E. No lo está, sin embargo, la directa.
- Se protege el soporte y el contenido.
- El secreto no rige entre los propios comunicantes, y en consecuencia la grabación de la propia conversación no vulnera el secreto de las comunicaciones.

Así la STC 56/2003, de 24 de marzo[350], citando el clásico precedente de la STC 114/84, de 29 de noviembre[351], tiene sentado que "*no hay secreto para aquél a quien la comunicación se dirige, ni implica contravención de lo dispuesto en el art. 18.3 CE la retención por cualquier medio, del contenido del mensaje*". Dicha retención (la grabación, en el presente caso) podrá ser, en muchos casos, el presupuesto fáctico para la comunicación a terceros, pero ni aun considerando el problema desde este punto de vista puede apreciarse la conducta del interlocutor como preparatoria del ilícito constitucional, que es el quebrantamiento del secreto de las comunicaciones".

Quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera "*íntima*" del interlocutor, pudiesen constituir atentados al derecho garantizado en el art. 18.1 CE. El secreto de las comunicaciones es un derecho de naturaleza formal, en consecuencia, quien grabe y divulgue una conversación mantenida con una persona

[350] STC 56/2003, de 24 de marzo (RTC 2003\56).

[351] STC 114/1984, de 29 de noviembre (RTC 1984\114).

atentaría, en su caso, al derecho a la intimidad del interlocutor, pero no al reconocido en el art. 18.3 CE[352].

C) Doctrina constitucional

El secreto de las comunicaciones que la Constitución garantiza, es un concepto rigurosamente formal, en el sentido de que "*se predica de lo comunicado sea cual sea su contenido*[353]", no se dispensa el secreto en virtud del contenido de la comunicación, ni se garantiza el secreto porque lo comunicado sea necesariamente íntimo o personal, sino debido a la evidente vulnerabilidad de las comunicaciones realizadas en un canal cerrado a través de la intermediación técnica de un tercero, se pretende que todas las comunicaciones, incluidas las electrónicas puedan desarrollarse con libertad. Quedan fuera de la protección constitucional aquellas formas de envío de la correspondencia que se configuran como comunicación abierta, o canal en el que no pueda predicarse su confidencialidad, por ejemplo, el acceso a un programa de mensajería entre los trabajadores sin clave de acceso, no goza de esta protección.

El objeto directo de protección del artículo 18. 3 CE es el proceso de comunicación en libertad y no el mensaje transmitido, lo que el texto constitucional garantiza es la impenetrabilidad por parte de terceros, así ya lo predicó la STC 114/1984 de 29 de noviembre[354], pero también puede verse el bien jurídico protegido como una garantía de intimidad.

La ya mencionada STC 170/2013 de 7 de octubre[355], recoge que el derecho al secreto de las comunicaciones solo tutela el proceso de comunicación pero no el mensaje en sí mismo, en ese punto se desestima el recurso de amparo, por estar ante un sistema de comunicación abierto y no cerrado, por lo que no existe vulneración del secreto de las comunicaciones[356]. Esta sentencia recoge, además, lo que se viene afirmado en la doctrina

---

[352] URBANO CASTRILLO, E.: *El Derecho al secreto de las comunicaciones*, ed. La Ley, 2011, pág. 19.

[353] SSTC 114/1984, de 29 de noviembre (EDJ 1984/114) y 34/1996, de 11 marzo (EDJ 1996/897).

[354] STC 114/1984, de 29 de noviembre (RTC 1984\114).

[355] STC170/2013, de 7 de octubre (RTC 2013\170).

[356] Este extremo no es compartido por parte de la doctrina que sí considera que existe una infracción del secreto de las comunicaciones; CARRASCO DURÁN, afirma que la STC subordina de

que es un derecho formal que garantiza la comunicación en sí con independencia de su contenido, y, esencialmente, afecta al correo electrónico: "*El objeto directo de protección del art. 18.3 CE es el proceso de comunicación en libertad y no por sí solo el mensaje transmitido, cuyo contenido puede ser banal o de notorio interés público".*

D) Doctrina judicial

Por su parte, la jurisprudencia laboral, conforme a la doctrina sentada por el Tribunal Constitucional, ha tenido oportunidad de pronunciarse en alguna ocasión sobre el carácter de la configuración del derecho al secreto de las comunicaciones, considerando al empresario como tercero ajeno a la comunicación fundamentándose en el concepto estricto de *"secreto*" mantenido por el Tribunal Constitucional[357]. Así, el empresario, pese a poseer la titularidad de las herramientas de trabajo, es un tercero ajeno a la comunicación frente al que se puede oponer el secreto, de modo que no puede fiscalizar las comunicaciones privadas o profesionales. Podemos afirmar, de modo general, que para los correos personales, estén o no prohibidos, rige la obligación de secreto, pudiéndose controlar el contenido de los mensajes de carácter profesional.

E) Doctrina científica

La doctrina explica que este derecho se configura en un doble sentido; de una parte, abarcando el derecho a comunicarse libremente, esto es, a utilizar los medios técnicos de comunicación sin ningún tipo de trabas o limitaciones. Y de otro lado, extendiéndose también en cuanto "*secreto*" que es, al contenido de lo comunicado o conservado, cualquiera que fuere este, es decir, con independencia de que fuere este, el contenido de índole personal, comercial o sin aparente trascendencia.

---

forma incondicionada el ámbito del derecho al secreto a lo que disponga en convenio colectivo, dejando a un lado la doctrina consolidada de que las intromisiones en este derecho se han de regular a través de previsión legal específica. CARRASCO DURÁN, M.: «El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa», *Revista Aranzadi Doctrinal* núm. 9, 2014 (BIB 2013\2695).

[357] MARÍN ALONSO, I.: «La utilización del correo electrónico por los sindicatos o sus secciones sindicales para transmitir noticias de interés sindical a sus afiliados o trabajadores en general», *Revista Doctrinal Aranzadi Social*, núm. 1, 2001 (BIB 2001\423).

Para DÍEZ-PICAZO lo decisivo en el secreto de las comunicaciones, "*es el continente, no lo que se dice en el mensaje*", pues cuando el titular de la comunicación consiente el acceso de otro queda excluida cualquier vulneración del art. 18 CE[358]. TORRES DEL MORAL afirma que el contenido de este clásico derecho se ha desbordado con la aparición de las nuevas tecnologías, y es por consiguiente más correcto llamarlo "*derecho a la inviolabilidad de las comunicaciones privadas*", cualquier prueba obtenida con violación de este derecho, es nula[359]. Afirma JIMÉNEZ CAMPO que "*la protección del derecho de las comunicaciones opera de forma puramente formal, de manera que toda comunicación es secreta y solo algunas comunicaciones serán íntimas*"[360].

Algunos autores parten de la existencia de un uso extra laboral del correo electrónico tolerable y un uso abusivo, pero señalan la dificultad del control por el límite con los derechos al secreto de las comunicaciones y a la intimidad, por lo que recomiendan que el control se realice de acuerdo con la doctrina constitucional[361]. Otros sectores distinguen varios supuestos de control: si el uso del correo electrónico es exclusivamente profesional, como consecuencia de una prohibición empresarial de usos personales, que se considera lícita, el acceso al correo será legítimo, porque no hay ninguna expectativa de confidencialidad, pero si el uso es estrictamente personal, como consecuencia de una cuenta a nombre del trabajador, rige plenamente el secreto de las comunicaciones y si el uso es mixto, profesional en ocasiones, personal en otras, sin "*advertencias de control*" se crea una "*expectativa de confidencialidad*" que debe ser protegida por lo que el control empresarial solo podrá desarrollarse conforme a los principios generales[362]. En ese sentido, se señala que las comunicaciones realizadas por el trabajador con un fin únicamente laboral, se deben considerar también, como propias de la empresa, al ser realizadas por el comitente en el ejercicio de la actividad encargada. Por lo que el

---

[358] DÍEZ PICAZO, L.M.: *Sistema de Derechos Fundamentales. Serie Derechos Fundamentales y Libertades Públicas, op.cit.*, pág. 316.

[359] TORRES DEL MORAL. A. *Principios de Derecho Constitucional Español, op.cit.*, pág. 353.

[360] JIMÉNEZ CAMPO, J.: «La garantía constitucional del secreto de las comunicaciones», *Revista española de Derecho Constitucional* núm. 20, 1987, pág. 41.

[361] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y Relaciones Laborales, op.cit*, págs. 73-93.

[362] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *op.cit*, págs. 32-34.

contenido de las comunicaciones que el trabajador realiza de acuerdo con las órdenes del empresario no es patrimonio exclusivo de los trabajadores sino que pasa también a ser de la empresa[363].

F) Recapitulación

Para delimitar la materia, debemos distinguir entre los correos personales y los profesionales. Las facultades de control del correo electrónico, con respecto al correo de ámbito personal están limitadas por el secreto de las comunicaciones de los trabajadores, de forma que ni la propiedad del medio ni la posición empresarial autorizan a romper el secreto, lo que implica que el empresario no puede ni comprobar ni registrar el contenido de las comunicaciones. Respecto al correo profesional, el control será admisible solo *"cuando resulte imprescindible para controlar la prestación laboral*". Son posibles lo controles externos o los filtros, que pueden suponer un sacrificio aceptable desde el punto de vista de la proporcionalidad.

En el derecho fundamental al secreto en las comunicaciones el objeto de protección por la norma constitucional es la situación de confianza entre los comunicantes, independientemente de que la comunicación en sí misma pueda ser fácilmente interceptable y de que el medio empleado para la comunicación sea o no propiedad de un tercero ajeno a la misma.

10.Libertad informática

Lo que hoy denominamos derecho fundamental a la protección de datos personales, libertad informática o autodeterminación informativa, es en el sistema español un derecho fundamental de creación jurisprudencial, obra del Tribunal Constitucional, pues el artículo 18.4 CE, que le sirve de sustento principal, establece en puridad, un mandato al legislador y no un derecho fundamental en sentido propio, así dispone lo siguiente: "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno uso de sus derechos*".

[363] GOÑI SEIN, J.L.: «Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y de archivo de datos» en AA. VV., ALARCÓN, M.R. y ESTEBAN, R. (coords.): *Nuevas tecnologías de la información y de la Comunicación y Derecho del Trabajo*, ed. Bomarzo, 2004, pág. 81.

A) Idea general

La redacción del examinado precepto constitucional no es afortunada, ya que limitar el uso de la informática, además de poco factible, es poco deseable, cosa distinta, que es sin duda lo que el constituyente quiso decir, es "*poner coto"* a los eventuales abusos en el empleo de las nuevas tecnologías[364]. El mandato constitucional es, sin duda, una garantía para la plena eficacia de otros derechos como son el honor y la intimidad. En este sentido, sobre el legislador pesa el deber de regular el tratamiento de datos de manera que dicha actividad se realice de forma respetuosa con los derechos fundamentales[365].

a) Enfoque genérico

La autodeterminación informativa es un derecho de perfil muy formalista[366], garantiza a la persona el control activo de las informaciones que le afectan, y el derecho a no ser instrumentalizado a través del conocimiento adquirido de aspectos de su personalidad, en la medida en que supone ser informado de quien posee sus datos personales, a qué uso se están sometiendo y el derecho a oponerse, en su caso, a una posesión ilegítima o uso ilícito[367]; es la potestad de control sobre el uso de los datos propios. Las vulneraciones a la autodeterminación informativa por parte de los particulares, tienen relevancia constitucional y por consiguiente también se consideran violaciones del artículo 18.4 CE y esto significa, en la práctica que son susceptibles de protección vía recurso de amparo. Así, el Tribunal Constitucional ha amparado a los trabajadores frente a la utilización empresarial no justificada de información sobre

[364] DÍEZ PICAZO, L.M.: *Sistema de Derechos Fundamentales. Serie Derechos Fundamentales y Libertades Públicas*, *op.cit.*, págs. 313- 314.

[365] De ahí que la apreciación de la licitud de las medidas de control electrónico se deba hacer desde la posible afectación a la intimidad del trabajador para enmarcarse también dentro del derecho a la autodeterminación informativa, regulado en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, de 13 de diciembre.

[366] De modo que una intromisión empresarial, por ejemplo, puede no vulnerar ni la intimidad del trabajador ni el secreto de las comunicaciones, pero, puede estar quebrando su derecho a la protección de datos personales. *Vid.* SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*, *op.cit.*, pág. 25.

[367] THIBAULT ARANDA, J.: «La vigilancia del uso de internet en la empresa y la protección de datos personales», *Relaciones Laborales: revista crítica de teoría y práctica* núm.1, 2009, pág. 215.

afiliación sindical[368] (STC 11/1998, de 12 de febrero[369]) o frente a la creación por el empresario sin el consentimiento de los afectados de un fichero sobre absentismo con baja médica (STC 202/1999 de 8 de noviembre[370]).

El TC viene a considerar este derecho como "*derecho de control sobre los datos relativos a la propia persona*", añadiendo que la llamada "*libertad informática"* es el derecho a controlar el uso de los mismos datos insertos en un programa informático, *habeas data*[371], y comprende la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

El contrato de trabajo es, sin duda, una zona "*particularmente sensible*" en orden a las amenazas que para la vida privada de los trabajadores pueden derivar del control de los datos personales. Las características propias de la relación laboral hacen que existan dificultades y excepciones a la hora de trasplantar el régimen jurídico propio de la protección de datos de carácter personal en el ámbito de la empresa. El peligro denunciado se multiplica por el desequilibrio de las posiciones de poder en la relación de trabajo, dentro de la cual, el trabajador tiene menor capacidad de resistencia a las pretensiones de control informativo:

b) Procesos de selección de personal

El Grupo de Trabajo del art. 29 ha argumentado que se pueden encontrar datos personales en las evaluaciones y en los juicios subjetivos de los candidatos, en definitiva, componentes que, en realidad, podrían incluir elementos específicos de la identidad física, fisiológica, psíquica, económica, cultural o social de los interesados[372].

El hecho de archivar un currículum en una carpeta de candidatos descartados se consideran datos personales sometidos a tratamiento. Por ese motivo, el candidato tiene derecho a conocer, previa solicitud, todos sus datos de base, los resultantes de cualquier

---

[368] DÍEZ PICAZO, L.M.: *Sistema de Derechos Fundamentales. Serie Derechos Fundamentales y Libertades Públicas , op. cit.* pág. 316.

[369] STC 11/1998, de 12 de febrero (RTC 1998\11).

[370] STC 202/1999, de 8 de noviembre de 1999 (RTC 1999\202).

[371] Se denomina *habeas data* por su función análoga en el ámbito de la libertad de información a cuanto supuso el tradicional *habeas corpus* en lo referente a la libertad personal.

[372] Recomendación 1/2001 sobre los datos de evaluación de los trabajadores. *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp42es.pdf*

elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos, todo ello en virtud del art. 15 LOPD y del art 29.3 del RPD. El responsable del fichero tiene el plazo máximo de un mes, a contar desde la recepción de la solicitud, para facilitar esos datos o indicar que no los tiene.

c) Ejecución del contrato laboral

Las informaciones operan a través de tres vías principales: en la retención del IRPF de la nómina de los trabajadores, en el pago delegado de prestaciones de seguridad social, y en menor medida, en el abono de las cotizaciones sociales.

En este punto, SEMPERE NAVARRO y SAN MARTÍN MAZZUCCONI advierten que el Tribunal Constitucional se "*afana en deslindar"* la libertad informática respecto del derecho a la intimidad, pero tácitamente, reconoce que la escisión no puede ser absoluta, porque el derecho a la protección de datos, comprende el derecho a la intimidad, aunque lo exceda[373]. Asimismo, GARCÍA NINET y VICENTE PACHÉS precisan que desde la perspectiva de la informática, el derecho a la intimidad cobra una nueva dimensión, pues "*resulta insuficiente concebir la intimidad como un derecho garantista*". Existe un *status* negativo de defensa frente a cualquier intromisión de la esfera privada, sin contemplarla, al propio tiempo, como un derecho activo de control y un *status* positivo sobre el flujo de informaciones que conciernen a cada sujeto". Identifican así un nuevo derecho, configurándolo como aquel que tiene por objeto "*garantizar la facultad de las personas para conocer y acceder a las informaciones que le conciernen archivadas en bancos de datos"* (*habeas data*); controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su transmisión.

En definitiva, la autodeterminación informativa, consiste en la facultad de disponer sobre la revelación y el uso de los datos personales, en todas las fases de

[373] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y Relaciones Laborales, op.cit,* pág. 120.

elaboración y utilización de estos datos, es decir, su acumulación, su transmisión, su modificación y cancelación[374].

Realmente, lo que está en juego es la contraposición del derecho del empresario a optimizar las posibilidades que le ofrecen las nuevas tecnologías, incluida la "*gestión de su personal"* y la privacidad entendida en este sentido como la *privacy* anglosajona, como un ámbito más amplio que el de la estricta intimidad y que comprende también todas las informaciones que el sujeto pueda mantener libre de invasión o que solo sean conocidas por determinadas personas. Este tipo de datos no íntimos, aunque aisladamente considerados parezcan no tener trascendencia, coherentemente enlazados pueden obtener un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado[375].

B) Ámbito internacional

El objeto del derecho fundamental a la protección de datos desde la perspectiva de las relaciones laborales, persigue garantizar a la persona un poder de control sobre sus datos personales, su uso y su destino, con el propósito de impedir un tráfico ilícito y lesivo para la dignidad del trabajador afectado. Su concepción abarca cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo pueda afectar a los derechos de la persona, sean o no fundamentales. Entre los instrumentos internacionales más importantes sobre la materia, se encuentran:

- El Convenio Europeo de Derechos Humanos de 4 de noviembre de 1950[376], dada la fecha de su elaboración, no consagra este derecho, pero la limitación del tratamiento de datos se considera incluida dentro de la noción de vida privada del art. 8 CEDH.
- La Recomendación del Consejo de la Organización para la Cooperación y Desarrollo Económico (OCDE) relativa a las líneas directrices que regulan la

[374] GARCÍA NINET, J.I. y VICENTE PACHÉS, F.: «El derecho valor a la dignidad humana y el derecho a la protección de datos personales en la Constitución Europea», *Revista del Ministerio de Trabajo e Inmigración*, núm. 57, 2005, págs. 137-192.

[375] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y Relaciones Laborales, op.cit*, pág.118

[376] BOE núm. 243, de 10 de octubre de 1979, páginas 23564 a 23570.

protección de la privacidad y los flujos transfronterizos de datos personales, de 23 de septiembre de 1980[377].

- El Convenio del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981[378].
- Las directrices para la regulación de ficheros automáticos de datos personales de la Organización de las Naciones Unidas (ONU), de 29 de enero de 1991[379].

C) Ámbito de la UE

La Directiva de la Unión Europea 95/46/CE[380], del Parlamento Europeo sobre protección de datos y del Consejo de 24 de octubre, relativa a la protección a las personas, en lo que respecta al tratamiento de datos personales[381]. Que más tarde dio origen a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, pues constituye su transposición al ordenamiento español.

La Carta de Derechos Fundamentales de la Unión Europea de 2 de octubre de 2000, reconoce expresamente el derecho a la protección de datos de carácter personal, en un precepto distinto al del derecho a la vida privada y familiar[382].

La Recomendación CM/rec (2015)5[383] relativa al tratamiento de datos personales en el entorno laboral, aprobada por el Comité de Ministros del Consejo de Europa adoptada el 1 de abril de 2015.

---

[377] *http://www.oecd.org/sti/ieconomy/15590267.pdf*

[378] BOE núm. 274, de 15 de noviembre de 1985, páginas 36000 a 36004.

[379] Adoptadas mediante resolución 45/95 de la Asamblea General de la ONU, de 14 de diciembre de 1990. *http://inicio.ifai.org.mx/Estudios/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf*

[380] DOUE núm. 281, de 23 de noviembre de 1995, páginas 31 a 50.

[381] Constituye un hito fundamental, pues su objetivo se orienta a eliminar los obstáculos a la circulación de los datos personales en el ámbito europeo, mediante el establecimiento de un nivel equivalente de protección de esos datos en ese ámbito.

[382] DOUE núm. 83, de 30 de marzo de 2010, páginas 389 a 403.

[383] *https://wcd.coe.int/ViewDoc.jsp?id=2306625*

El Reglamento General sobre Protección de Datos de la UE[384] que entrará en vigor el 25 de mayo de 2018, y en ese momento quedará a su vez derogada la Directiva 95/46/CE. Por su alcance y relevancia, ha de analizarse de manera exhaustiva.

D) El Grupo de Trabajo del artículo 29

En virtud del artículo 29 de la Directiva 95/46/CE de 24 de octubre de 1995 del Parlamento Europeo y del Consejo [385] se creó el Grupo de Trabajo del art. 29, que es un órgano consultivo independiente de la UE sobre protección de los datos y de la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

El Grupo de Trabajo del art. 29, recomienda que por parte de la empresa se empleen las medidas que resultan de los recursos informáticos, pues considera que la prevención debería prevalecer sobre la detección; es decir, que es mejor para el empleador prevenir la utilización abusiva de Internet [386]. Este mecanismo, es, sin duda, el menos lesivo para los derechos de los trabajadores.

En este sentido, el Grupo de Trabajo llama la atención sobre el papel del administrador del sistema, un trabajador cuyas responsabilidades en materia de protección de datos son muy importantes. Subraya que es fundamental que el administrador del sistema, así como cualquier persona que tenga acceso a datos personales de los trabajadores durante las operaciones de control, esté sometido a una obligación estricta de secreto profesional respecto a la información confidencial a la que pueda tenar acceso[387]. El deber de guardar secreto tendrá que acompañarse de la adopción

---

[384] Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos.

[385] La secretaría encargada es la siguiente: Dirección A (Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de Datos) de la DG Mercado Interior de la Comisión Europea, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.

Sitio Internet: *htp://www.europa.eu.int/comm/privacy*

[386] Véase Documento del grupo de Trabajo de la UE relativo a la vigilancia de las comunicaciones electrónicas en al lugar de trabajo, aprobado el 29 de mayo de 2002. Págs. 4-5 y 24. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/B.2.52-cp--wp55---vigilancia-comunicaciones-electr-oo-nicas-trabajadores.pdf*.

[387] *Ibídem,* pág.19

por el responsable del tratamiento de los datos de las medidas de seguridad exigibles en orden a garantizar el mismo. Así el artículo 9 de la propia LOPD se refiere a la seguridad de los datos estableciendo que:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

E) El nuevo Reglamento General sobre Protección de Datos

En un entorno globalizado como el tecnológico, la aplicación extraterritorial de las normas constituye un verdadero desafío, pues no tendría demasiado sentido limitarlas a un determinado espacio, por el principio de aplicación territorial de la Ley, o a un concreto conjunto de personas, por imperativo del principio de personalidad. Frente al nulo desarrollo que la normativa de protección datos ha experimentado en el ámbito laboral en nuestro país, a nivel europeo el Reglamento General sobre Protección de Datos (RGPD) abre la posibilidad de intervenir en este ámbito hasta ahora ignorado por la normativa estatal[388].

El RGPD establece una normativa única, válida en toda la UE y aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no[389]. El nuevo RGPD impone a los Estados de la UE que adapten su normativa a este con la fecha máxima de su entrada en vigor, a saber, en el año 2018, por lo que cabe esperar que cambios legislativos en la normativa analizada.

---

[388] GOÑI SEIN, J.L.: «Los límites de las potestades empresariales *vs.* Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *op.cit.*

[389] DÍAZ DÍAZ, E.: «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *Revista Aranzadi Doctrinal*, núm. 6, 2016 (BIB 2016\3067).

De este modo, el RGPD incorpora nuevas reglas sobre extraterritorialidad de las normas y se aplicará fuera de la Unión Europea cuando el tratamiento de datos personales de interesados residentes en la Unión se efectúe por responsables o encargados del tratamiento no establecidos en la Unión y las actividades de tratamiento estén relacionadas con dos ámbitos:

- La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte del interesado.
- El control de su conducta, en la medida en que esta tenga lugar en la Unión Europea.

En el ámbito laboral, los aspectos más relevantes del RGPD son los siguientes:

1. El tratamiento de datos está prohibido cuando revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física[390].

[390] Esta prohibición tiene algunas salvedades cuando el tratamiento, es para, art. 9.2 del RGPD:

b) es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.

(…)

d) es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

(…)

h) es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario, siempre que su tratamiento sea

2. El Reglamento da la posibilidad a los Estados miembros de establecer normas más específicas, a través de disposiciones legislativas o de convenios colectivos, para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

3. Las normas que establezcan los Estados deben incluir medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses 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. La figura del *Delegado de Protección de Datos*[391], ha sido altamente debatida en todo el proceso regulatorio. En determinados países de la Unión Europea, como Alemania o Hungría, dicha figura es a día de hoy obligatoria. En otros países como Holanda o Austria, su nombramiento es opcional y en otros, como en España, no existe tal obligación[392]. Al final, el RGPD ha optado por una solución intermedia, que es la obligatoriedad en la designación de dicha figura pero sólo para determinados casos concretos, como:

- Administraciones Públicas.
- Entidades cuya principal actividad lleve aparejada la monitorización de datos personales o el tratamiento de datos personales a gran escala.

---

realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto.

[391] *DPO* "*data protection officer* ".

[392] RODRÍGUEZ BALLANO, S. y VIDAL. M.: «*Habemus* nuevo Reglamento General de Protección de Datos», *Actualidad Jurídica Aranzadi*, núm. 919, 2016 (BIB 2016\3116).

- Entidades cuya principal actividad lleve aparejado el tratamiento de datos especialmente protegidos a gran escala, así como de antecedentes penales[393].

Con respecto a los derechos de los interesados, existen dos nuevos derechos que son reconocidos a favor de todos los ciudadanos que constituyen una de las principales novedades del RGPD; el derecho al olvido y el derecho a la portabilidad, que a su vez constituyen las dos indicaciones más interesantes que surgen respecto a la aplicación en el ámbito laboral, aspectos, que por su importancia, se analizan en un epígrafe separado.

F) Derecho al olvido y supresión de datos

En nuestra normativa interna este derecho no aparece regulado como tal, pero se puede ejercitar a través del derecho de cancelación, el art. 31.2 RPD establece que en cualquier momento un interesado puede solicitar al responsable de un fichero o tratamiento, que se cancelen los datos que le conciernen, bien porque desee revocar el consentimiento otorgado con anterioridad o bien porque entienda que el tratamiento se está efectuando sin su consentimiento previo o porque no se le ha informado de los extremos que el art. 5 de la LOPD exige, así el derecho de cancelación dará lugar a la supresión de los datos que resulten inadecuados o excesivos.

Desde que se publicó la conocida STJUE de 13 de mayo de 2014[394] en la que se estimaba la pretensión de un ciudadano español que pedía la cancelación de resultados obtenidos al buscar su nombre en Google, pues mostraba una información

[393] *Ibídem.*

[394] STJUE de 13 mayo 2014 Caso Google Spain S.L contra Agencia Española de Protección de Datos (TJCE 2014\85).

desactualizada[395], se ha ido configurando el "derecho al olvido"[396] y se ha ido concretado su ejercicio. La sentencia del TJUE, no siguiendo el criterio propuesto en las Conclusiones del Abogado General, contesta con claridad a las cuestiones presentadas por la AN:

> *"1) (…) la actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de "tratamiento de datos personales" (…), cuando esa*

[395] Los hechos que han dado lugar al pronunciamiento de esta sentencia consisten, básicamente, en lo siguiente: en el año 2010 una persona de nacionalidad española y domiciliada en España, presentó ante la AEPD una reclamación contra La Vanguardia Ediciones, S.L., y contra Google Spain y Google Inc. Esta reclamación se basaba en que, cuando un internauta introducía el nombre del reclamante en el motor de búsqueda de Google, obtenía como resultado vínculos hacia dos páginas de dicho periódico del año 1998, en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre del reclamante.

Solicitaba esta persona a la AEPD que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales, o utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos, así como que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. El reclamante entendía que el embargo al que se vio sometido en su día estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actual. La Resolución dictada por AEPD tuvo diversos pronunciamientos que detallamos a continuación:

-Desestimó la reclamación frente a la editorial del periódico pues consideró que la publicación de la información estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores.

-Estimó la reclamación en relación a Google Spain y Google Inc pues consideró que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información.

Se interpuesto recurso contencioso administrativo contra la resolución dictada por la Agencia Española de Protección de Datos tanto por Google Spain y Google Inc. la Sala de lo Contencioso de la Audiencia Nacional optó por la acumulación de ambas impugnaciones y en el curso de la tramitación del correspondiente recurso contencioso, decidió plantear la cuestión prejudicial que ha concluido con la sentencia que comentamos. *Vid.* GUERRERO ZAPLANA, J. «La sentencia del asunto Google: configuración del derecho al olvido realizada por el TJUE», *Revista Aranzadi Doctrinal* núm. 4, 2014 (BIB 2014\2154).

[396] En el sentido de «desindexación»; alude al derecho de la persona a dejar de tener un perfil *on line*, es decir, a eliminar de la Red su huella digital.

información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento (…).

2) (…) se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro, en el sentido de dicha disposición, cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro.

3) (…) para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita.

4) (…) al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado".

Efectivamente, el TJUE reconoció en esta importante sentencia *un cierto derecho a ser olvidados en Internet*[397], derecho del interesado a solicitar que la información sobre su persona no se ponga a disposición del público en general mediante su inclusión en la lista de resultados de los buscadores de Internet, pero no supone un derecho a la supresión de los datos publicados en la Red, es importante resaltar que la sentencia solo se refiere a los buscadores, no comporta el derecho a borrar información del soporte original, porque la información personal no se elimina de las webs de origen[398].

El RGPD "va un poco más allá"[399] se configura por vez primera como un derecho autónomo a los denominados "derechos ARCO" (acceso, rectificación, cancelación y oposición)[400], al reconocer en su art. 17 lo siguiente:

"1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

---

[397] GOÑI SEIN, J.L:. «Los límites de las potestades empresariales *vs.* Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *op.cit.*

[398] *Ibídem.*

[399] *Ibídem.*

[400] DIAZ DÍAZ, E.: «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *Revista Aranzadi Doctrinal*, núm. 6, 2016 (BIB 2016\3067).

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1".

Ahora bien, este derecho al olvido *no constituye un derecho ilimitado*[401] porque permite que se excluya la supresión en una serie de circunstancias que se regulan en el apto. 3 de este artículo por motivos de salud pública para ejercer el ejercicio de la libertad de expresión, etc. Asimismo, este derecho plantea dificultades importantes de origen práctico, ya que existen serias restricciones, una de ellas es la imposibilidad de modificar la información contenida en los boletines oficiales, dado que son inalterables una vez transcurrido el plazo para recurrir, otra es la imposibilidad técnica de hacer desaparecer determinadas fotos o noticias una vez que son compartidas en redes sociales, que posteriormente se difunden a otros alojamientos web.

En la práctica, este derecho tiene una dimensión dual: por una parte, para el ciudadano supone un reconocimiento de la pretensión de suprimir de inmediato la información afectada en el sitio web, así como de abstenerse de dar difusión a esta información siempre que el titular de los datos lo solicite[402]. De otra parte, también resulta relevante destacar que este derecho incide en la esfera del Responsable del tratamiento, esto es, la entidad, corporación, sitio web o red social que trata los datos. El Responsable del tratamiento deberá optar entre limitar el tratamiento art.18 RGPD, o bien suprimir sin demora la información (art.17), ponderando caso por caso el alcance de este derecho con el derecho a la libertad de expresión, la salud pública, el deber de conservación de los datos para dar cumplimiento a una obligación legal y el interés público[403].

---

[401] *Ibídem.*

[402] Los reclamantes que acuden a la Agencia Española de Protección de Datos a solicitar "el derecho al olvido" son aquellos cuyas reclamaciones han sido previamente desestimadas por Google, que en España ha recibido casi 31.000 por supuestas vulneraciones de privacidad por la indexación de contenidos personales, según la compañía. Las reclamaciones anuales a la AEPD ascienden a 325, de las cuales el 40 % han sido estimadas. *Vid*. EFE (2015, 27 de octubre) «Directora AEPD: Las denuncias por privacidad se han cuadruplicado desde 2008» *http://www.efefuturo.com/entrevista/directora-aepd-las-denuncias-por-privacidad-se-han-cuadruplicado-desde-2008/*

[403] DÍAZ DÍAZ, E.:«El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *op.cit.*

G) Derecho a oponerse a la elaboración de perfiles virtuales

Un segundo límite que no debe desconocerse en el tratamiento de los datos en el ámbito laboral es el derecho a la portabilidad de los datos, este derecho no ha tenido unos antecedentes jurisprudenciales tan amplios como los del olvido digital y se ha suscitado principalmente por razones de interoperabilidad técnica. El art 20 RGPD, atribuye al interesado la facultad de *"recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado y de uso habitual y de lectura mecánica y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos"*.

Asimismo, el art. 18 del RGPD, recoge lo siguiente:

> *"1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:*
> *a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;*
> *b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;*
> *c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;*
> *d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.*
> *2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro".*

El derecho a la portabilidad debe facilitar la transmisión de datos personales de un proveedor de servicios, como una red social, a otro en un formato estructurado y de uso habitual y de lectura mecánica. Este derecho aumentará los derechos en materia de protección de datos y también mejorará la competencia efectiva entre proveedores de servicios[404].

Este artículo permite al interesado controlar su disponibilidad *on line*, derecho perfectamente aplicable a los datos subjetivos procedentes de evaluaciones o juicios subjetivos realizados sobre los candidatos a puestos de trabajo o sobre los propios trabajadores, en la práctica el ejercicio del derecho no está exento de complejidades,

[404] *Ibídem*.

porque no es nada fácil saber por lo pronto quién posee esos análisis de datos personales (evaluaciones y juicios subjetivos)[405].

H) Normas internas

La Ley Orgánica 15/1999, de 13 de noviembre, de protección de datos de carácter personal (LOPD), obliga a todas las personas, empresas y organismos, tanto privados como públicos que dispongan de datos de carácter personal, a cumplir una serie de requisitos y aplicar determinadas medidas de seguridad en función del tipo de datos que posean. Hasta la aparición de la nueva norma, la regulación de este ámbito se basaba en una legislación de desarrollo desfasada y caduca, surgida al amparo de una Ley ya derogada, la LO 5/1992, de 24 octubre, reguladora del Tratamiento Automatizado de Datos de Carácter Personal y que el legislador había mantenido vigente de modo pretendidamente coyuntural.

El reglamento de la LOPD aprobado por RD 1720/2007, de 21 de diciembre, (RDP) se justifica porque las normas hasta hace poco subsistentes habían quedado obsoletas frente a la desbordante evolución tecnológica y social experimentada en los últimos años, lo que demandaba una adaptación a las circunstancias actuales. Además, se hacía necesario corregir las carencias que, a lo largo de estos años, se han puesto de manifiesto en la aplicación práctica de los Reglamentos derogados, introduciendo criterios interpretativos y modificaciones orientadas, por una parte, a facilitar el cumplimiento de la legalidad y, por otra, aclarar ciertos conceptos oscuros que ponían en entredicho las garantías propias del principio de seguridad jurídica.

El artículo 2 LOPD dispone que la protección establecida en esta ley será de aplicación a "*los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento*". La protección se extiende también "*a toda modalidad de uso posterior de esos datos por los sectores público y privado"* y se construye a través de dos conceptos básicos: el dato personal y su tratamiento.

El dato personal se define como *"cualquier información concerniente a personas físicas identificadas o identificables*", lo que abarca la "*información fotográfica, acústica*

[405] GOÑI SEIN, J.L.: «Los límites de las potestades empresariales *vs*. Derecho de la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral en las redes sociales», *op.cit.*

o de cualquier tipo", según aclara el art. 5.1f RDP. Por "*tratamiento*" se entiende: "*cualquier operación o procedimiento técnico sea o no automatizado, que permita la recogida, grabación o conservación, elaboración, modificación, cancelación, bloqueo, o supresión , así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias",* art. 5.1.t) RDP.

Las imágenes y sonidos que se obtienen de la instalación de cámaras, para el control de la actividad de los trabajadores, solo son considerados datos de carácter personal cuando permiten la identificación de las personas que aparecen en ellos, no aplicándose la LOPD en caso contrario. Los datos personales de los trabajadores una vez registrados, están sometidos a una obligación de secreto profesional, que vincula al responsable del fichero y a quienes intervengan en el tratamiento (art. 10 LOPD). Este mencionado deber permanece después de incluso de extinguido el contrato de trabajo, sin que se haya fijado un período máximo de vigencia para esta obligación.

Existen tres niveles de seguridad, básico, medio y alto, que se aplicarán a los datos obtenidos por ley, los datos sensibles, por lo general, se incluyen en el deber de protección más alto:

- Los ficheros de *nivel básico* son los que contengan datos de carácter personal, tales como nombre, dirección, teléfono, correo electrónico, DNI, etc.
- En el *nivel medio* se encuentran los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, tributarias y servicios financieros.
- Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud, vida sexual, así como los que contengan datos recabados para fines policiales tienen un *nivel de seguridad alto*.

Recoge el artículo 4.1 LOPD siguiendo la Directiva 95/46, que los datos de carácter personal, solo se podrán coger para su tratamiento, "*cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas y explícitas y legítimas para quien se haya obtenido*", es la consagración del principio de proporcionalidad, se vincula a la exigencia de que los datos aun siendo idóneos, no deben ser excesivos respecto al cumplimiento de su finalidad.

Por otro lado, el art. 4.2 LOPD prohíbe que los datos puedan ser usados para una "*finalidad incompatible*", lo que significa que:

- No pueden recogerse datos con fines indeterminados o inespecíficos. (Supone una variación con respecto a la LORTAD, que recogía la expresión clara "*finalidad distinta*" que no admitía muchas interpretaciones o matizaciones, mientras que ahora se nada en la ambigüedad lo que puede inducir a confusiones y malas interpretaciones[406]).
- La finalidad perseguida a la hora de recabar los datos, debe mantenerse tanto al informar sobre su obtención, como al autorizarse la misma, mediante el consentimiento del afectado durante toda la relación laboral.

Los arts. 4.3 y 4.4 LOPD consagran los principios de veracidad y actualización, los datos "*serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado*", y, por tanto, los que sean inexactos o incompletos deberán ser cancelados y debidamente sustituidos.

Los arts. 4.5 y 16 LOPD respecto a la cancelación y descontextualización, indican "*los datos serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad que justificó su recogida; sin que puedan ser conservados durante un período superior al necesario para los fines que justificaron su recogida".*

Los arts. 4.6 y 15 LOPD proclaman el principio de accesibilidad, "*los datos serán almacenados de forma que permitan el ejercicio del derecho de acceso*".

El artículo 4.7 LOPD consagra el principio de legalidad; se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Estos principios, que la propia ley incorpora bajo la rúbrica "*calidad de los datos",* son en realidad meras concreciones del principio de finalidad que se erige en el verdadero principio básico de la protección de datos[407].

En la legislación laboral no encontramos una regulación específica destinada a la protección de los datos de los trabajadores. La LOPD tampoco ha regulado de manera expresa la intervención de los representantes de los trabajadores en relación con la

[406] FREIXAS GUTIERREZ, G.: *La protección de datos de carácter personal en el derecho español*, ed. Bosch, 2001, pág. 153.

[407] THIBAULT ARANDA, J.: «La incidencia de la Ley Orgánica 15/1999, de 13 diciembre de protección de datos de carácter personal, en el ámbito de las relaciones laborales», *op. cit.*, pág. 171.

protección de datos, que son así "*los grandes ausentes*" de la misma[408]. La omisión resulta singularmente llamativa dadas las importantes competencias que éstos tienen en materia de información, consulta y control[409].

Las relaciones laborales no han quedado al margen de este proceso, aunque la protección, dejando aparte las posibles medidas recogidas en la negociación colectiva, deba aplicarse a partir de la LOPD y no de la legislación laboral.

I) La AEPD

En particular, con respecto a la videovigilancia, la Agencia Española de Protección de Datos ha adoptado una postura flexible cuando se trata de instalación de sistemas de vigilancia en el ámbito de la empresa, en estos casos admite que puede no ser necesario el consentimiento, teniendo en cuenta las excepciones art. 6 LOPD, párrafo 1, *"salvo que la ley disponga lo contrario* y párrafo 2º, inciso segundo "*o cuando en una relación laboral sean necesarios para su mantenimiento o cumplimiento*" y de conformidad con lo dispuesto en el art. 20.3 ET.

La AEPD presume que la autorización legal al empresario para adoptar medidas de control a sus trabajadores, así como el consentimiento prestado en el contrato de trabajo, llevan implícito el consentimiento de los trabajadores para su grabación, poniendo como condición para admitirla que la "*medida adoptada supere el juicio de proporcionalidad al que hace referencia el TC".*

El artículo 5 LOPD regula un derecho de información cuyo objeto recae básicamente sobre los ficheros de datos de carácter personal, la finalidad de su recogida, los destinatarios de la información, los datos del responsable del fichero y los derechos del interesado. La vinculación de dicho derecho de información de los interesados que desde otra perspectiva, es un deber para los responsables del tratamiento de datos con el consentimiento es notoria, si bien en este caso conviene distinguir:

---

[408] THIBAULT ARANDA, J.: «La incidencia de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en el ámbito de las relaciones laborales», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 2, 2000, pág. 183.

[409] CARDONA RUBERT, M. B.: *Informática y contrato de trabajo (aplicación de la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal)*, ed. Tirant lo Blanch, 1999, págs. 333 y ss.

- Supuestos en que los datos se recaban del propio interesado, por lo que la información debe ser necesariamente previa a dicho consentimiento (apartados 1- 3 del artículo 5).
- Otros supuestos en que los datos proceden de terceras fuentes, y por tanto la información es posterior a la obtención de dichos datos, por lo que, en algunos casos concretos, desaparece el derecho-deber de información.

Aunque las diferencias entre los supuestos referidos son acusadas, en ambos existe una clara vinculación entre el derecho de información y el mismo derecho fundamental de protección de datos personales derivado del artículo 18.4 CE, en la medida en que este derecho se manifiesta en una facultad de disposición sobre los propios datos personales, que requiere habitualmente el consentimiento para la obtención, tratamiento y cesión de dichos datos, sea anterior o posterior a la obtención de los propios datos, así como las facultades de acceso, rectificación, cancelación y oposición; y tanto dicho consentimiento como las facultades presuponen a su vez que el titular posee la información necesaria.

J) Derecho de información

El TC no ha concretado si dicha vinculación entre información y derecho de protección de datos permite considerar que aquél forma parte del contenido esencial de este derecho fundamental, limitándose a señalar que la información es "*complemento indispensable*" del derecho derivado del artículo 18.4 CE. Entendemos que sí puede defenderse que el derecho de información sea una manifestación de dicho contenido esencial, pues aludiendo a las vías que el TC señaló, el derecho no sería recognoscible como tal, ni los intereses que protege quedarían efectivamente protegidos, si no se prestase de algún modo consentimiento para el tratamiento de los datos personales, y dicho consentimiento deberá ser necesariamente informado.

Únicamente en el caso de que los datos no se hayan recabado del interesado, desaparece la necesidad de informar sobre aquellos aspectos que venían vinculados al proceso de obtención de datos cuando éstos proceden de su titular, pero en cambio se añade la necesidad de informar del contenido del tratamiento y de la procedencia de los datos.

K) Consentimiento del trabajador

El consentimiento como principio general, se encuentra regulado en el art. 6.1 LOPD, según el cual "*el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa*". La literalidad del precepto puede darnos a entender el carácter inexcusable del consentimiento, y, por otro, la posibilidad de que pueda haber excepciones a la regla general, de hecho, son bastantes los supuestos en los que la propia ley dispone otra cosa, de alguna manera perdiendo ese carácter de generalidad.

Las excepciones al consentimiento se hallan en el apartado siguiente, art. 6.2 LOPD, siendo de especial relevancia a los efectos que aquí importa, lo regulado en el inciso segundo, cuando se establece que no será necesario el consentimiento, "*cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".* Dicho consentimiento no será necesario, por ejemplo, para llevar a cabo la elaboración y pago de las nóminas, la gestión de seguros sociales, o la comunicación de los datos del empleado a la Hacienda Pública o a los Organismos de la Seguridad Social. La no exigencia del consentimiento del trabajador para el tratamiento de sus datos personales por el empresario se limita a aquellas finalidades que vengan impuestas por la Ley o que sean necesarias para el mantenimiento y cumplimiento de la relación laboral. El empresario no podrá utilizar los datos del trabajador sin su consentimiento para fines distintos de los indicados.

L) Consentimiento en videograbaciones

Recapitulando lo anterior, siendo el consentimiento un requisito ineludible para el tratamiento de los datos de carácter personal, queda excluido en el supuesto de que exista una relación laboral entre las partes, en consecuencia, dicho requisito no resulta exigible tampoco en los supuestos de captación de imágenes de los trabajadores que constituyan en sí mismas un tratamiento de datos en términos de la LOPD.

Lo que con carácter general sí se establece como requisito previo a la videovigilancia es del deber de información, un derecho que a raíz de la última

jurisprudencia constitucional; STC 39/2016, de 3 de marzo[410], es cada vez menos prolijo en cuanto a sus términos. La doctrina constitucional anterior que era la establecida en la STC 29/2013, de 11 de febrero[411], afirmaba que la habilitación legal para recabar los datos personales sin necesidad de consentimiento en el ámbito de las relaciones laborales no eximía del derecho de información del trabajador, dado que era complemento indispensable del derecho fundamental. Este derecho de información no podía ser suplido o subsanado por la existencia de anuncios sobre la instalación de las cámaras o por que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos. Se hacía necesaria una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que la captación podía ser dirigida, se debían concretar las características y el alcance del tratamiento de datos que iba a realizarse. Esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos. Y por último, se tenía que explicitar muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

La STC 39/2013, de 3 de marzo de 2016[412], modifica la anterior doctrina, y establece una nueva afirmando que el deber informativo previo a someter a videovigilancia al trabajador, se entiende cumplido con la colocación de los distintivos informativos previstos en la Instrucción 1/2006 de 8 de noviembre de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, en definitiva, un simple cartel expuesto al público informando de que la zona está sometida a videovigilancia para el TC cumple con el deber del art.18.4 CE

El problema es cómo llega el TC a esta conclusión, desde nuestro punto de vista y uniéndonos así a parte de la doctrina[413], tal razonamiento se fundamenta en una doctrina equivocada que alude al consentimiento del empleado cuando entendemos que se confunde y pretendía referirse al deber de información previo al trabajador, siendo poco menos que un auténtico disparate jurídico la argumentación efectuada. Las consecuencias que extraer son las siguientes:

---

[410] STC 39/2016, de 3 marzo (RTC 2016\39).
[411] STC 29/2013, de 11 febrero (RTC 2013\29).
[412] STC 39/2016, de 3 marzo (EDJ 2016/20055).
[413] RODRÍGUEZ ESCANCIANO, S.: «Posibilidades y límites en el uso de cámaras de videovigilancia dentro de la empresa. A propósito de la sentencia del Tribunal Constitucional de 3 de marzo de 2016», *Diario La Ley*, núm.8747, 2016.

1) El empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 ET.

Esta afirmación era por todos sabida, y no existía ningún conflicto o discusión en la doctrina, no se aporta nada nuevo, en este aspecto, es más la parte recurrente nada alega respecto a esta cuestión.

2) Para valorar si se ha vulnerado el derecho a la protección de datos *ex* art 18.4 CE por incumplimiento del deber de información, la dispensa del consentimiento al tratamiento de datos en determinados supuestos debe ser un elemento a tener en cuenta dada la estrecha vinculación entre el deber de información y el principio general de consentimiento. ¿ No parece contradecirse lo expresado con lo manifestado en el punto anterior?

En puridad, lo que debe valorarse es la información previa aportada al trabajador, pues por imperativo del art. 6.2 LOPD, no será necesario el consentimiento, "*cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral".*

3) El incumplimiento del deber de requerir el consentimiento del afectado para el tratamiento de datos o del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada[414]. Hasta aquí la doctrina del TC, nunca antes a nivel constitucional se había sustentado el deber de información previa art. 18.4 CE en el principio de proporcionalidad, sino en el derecho a la intimidad del art. 18.1 CE

La doctrina de la STC 29/2013 de 11 de febrero[415], no se basaba en dicho principio de proporcionalidad, pues consideraba la cuestión de delimitación previa; se constataba si se había llegado al alcance de información previa exigido, y en caso contrario, se declaraba que se lesionaba el 18.4 CE, pero no se sometía la medida al juicio de

[414] Recoge la sentencia: " *La relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y* bienes *constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE*" (FJ 4º).

[415] STC 29/2013 de 11 febrero (RTC 2013\29).

proporcionalidad, pues al fin y al cabo supone un juicio de valor que entiendo que no procede en el deber de información para cumplimiento del art. 18.1 CE.

La cuestión de la delimitación previa es más simple que el triple test del juicio de proporcionalidad: ¿se le ha dicho al trabajador que va a ser grabado, que la finalidad de la medida es para control de la actividad laboral y con fines disciplinarios que pueden acabar en un despido? En definitiva, el espíritu de la sentencia STC 39/2016, de 3 de marzo se encuentra en el voto particular del magistrado OLLERO TASSARA[416], a la STC 29/2013, de 11 de febrero, pero expresado de una manera aún más confusa.

M) Requisitos del consentimiento

Cuando el empresario maneje ficheros de los trabajadores con un nivel de seguridad alto, sí que será necesario el consentimiento previo del trabajador, como ejemplo, un control de acceso al trabajo a través de la prueba del ADN, o disponer en redes sociales de datos del trabajador o de su propia imagen para publicitar la empresa con fines comerciales. A tal fin, conviene que dicha información se incorpore a un documento que sea firmado por el trabajador a modo de *recibí* y que puede serle entregado en el mismo momento de la firma del contrato de trabajo[417].

El artículo 10 RPD establece las causas legitimadoras del tratamiento de los datos personales, partiendo de la regla general del consentimiento del interesado y delimitando posteriormente las causas legitimadoras, así que el art. 10.1. RPD, parte de la premisa esencial de que "*los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera mostrado su consentimiento para ello"*.

---

[416] El Magistrado OLLERO TASSARA con referencia expresa a la doctrina de la STC 186/2000, de 10 de julio, afirmaba que aquella, tras analizar la cuestión a enjuiciar realizaba la correspondiente ponderación, en base al principio de proporcionalidad, mientras que la sentencia de cuyo sentido disentía, no aplicaba el triple test de proporcionalidad, a su juicio, a todas luces necesario. Por otro lado, consideraba un error que se realizara la fundamentación, en base a la STC 292/2000, de 30 de noviembre, pues ésta se pronunciaba en abstracto sobre la constitucionalidad de una ley y no sobre un hecho concreto como el que se enjuiciaba, lo que hacía que el derecho a la protección de datos no se hubiera interpretado de manera restrictiva sino en abstracto, queriendo apuntar a una interpretación exorbitante del mismo, es decir, fuera de lo normal o razonable

[417] MUÑOZ CORRAL, E.: «La protección de los datos de los trabajadores en el nuevo reglamento de desarrollo de la LO 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal», *Revista de Jurisprudencia El Derecho*, núm. 3, 2008, págs.5-11 (EDB 2008/13499).

De esta manera, y como señala la STC 292/2000, de 30 de noviembre[418], el consentimiento se configura como piedra angular del sistema de protección de datos en el Derecho español, de modo que el tratamiento de datos deberá basarse en el poder de decisión del interesado[419]. Dispone el artículo 12.1 RPD, "*el responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos, de carácter personal salvo en aquellos supuestos en que no sea exigible, con arreglo a lo dispuesto en las leyes".*

La AEPD, siguiendo las recomendaciones del Consejo de Europa, ha venido a indicar en numerosos informes, que el consentimiento deberá ser:

A) Libre, sin vicios en los términos del Código Civil.
B) Específico, es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, como lo impone el art. 4.2 LOPD.
C) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de meros actos realizados por el afectado; consentimiento presunto.
D) Informado, que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades con las que se produce. Precisamente el art. 5. 1 LOPD, impone el deber de informar.

Estas cuatro características son el fundamento de las reglas generales del art. 12 RPD. De este modo, el RPD establece una vinculación entre los principios esenciales del derecho fundamental a la protección de datos: la finalidad y el consentimiento. Debemos recordar que nos encontramos ante la regulación de un derecho fundamental, que determina, según el TC, un poder de disposición del afectado sobre la información que le concierne.

Cuando una empresa ponga en conocimiento de sus trabajadores que el uso de los medios técnicos proporcionados por la misma deben destinarse exclusivamente a tareas profesionales, en tanto elemento de trabajo propiedad de esta, así como que tales

---

[418] STC 292/2000 de 30 de noviembre (RTC 2000\292).

[419] PUENTE ESCOBAR, A.: «Legitimación para el tratamiento» en AA. VV. MARTÍNEZ MARTÍNEZ, R. (Coord.): *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD*, ed. Tirant lo Blanch, 2009, págs. 23-26.

instrumentos no pueden dedicarse a fines particulares, excepto en casos puntuales justificados, no resultará necesario recabar el consentimiento de los empleados para su vigilancia o control, pero sí será necesario que se facilite al trabajador información clara y precisa al respecto. Esta afirmación encuentra fundamento en la excepción a la obligación de recabar la aquiescencia prevista en el art. 6.2 LOPD, que legitima todo tratamiento de datos personales que se ajuste al desarrollo, mantenimiento y cumplimiento del contrato de trabajo, entendiendo que no es necesaria la autorización expresa del interesado para tal fin.

Sin embargo, lo que el empresario ha de observar, en todo caso, es el derecho de información del trabajador sobre el tratamiento de los datos (art. 5 LOPD). Es más, la propia AEPD, en Informe núm. 247/2008[420], insiste en que el art. 20.3 ET habilita al empleador a controlar el uso de instrumentos informáticos, pero siempre que previamente haya alertado al trabajador de dicho extremo.

Los tribunales deben ser conscientes de que la LOPD implanta mecanismos cautelares con el fin de prevenir las posibles violaciones que del tratamiento de la información pudieran derivar para la intimidad del individuo-trabajador, poniendo en práctica los principios generales anteriormente aludidos de congruencia, pertinencia y racionalidad. Se reconocen conjunto de garantías y derechos destinados a reforzar su posición: seguridad de los datos, secreto profesional, control de cesión a terceros, derechos de información, acceso, rectificación y cancelación.

Es evidente que el derecho a la protección de datos personales presenta un perfil fuertemente imbricado con las nuevas tecnologías, a pesar de ello, la atención de los tribunales y la doctrina es proporcionalmente menor. De ahí la importancia que adquiere la labor de la AEPD, pues a través de sus dictámenes y criterios se llenan los vacíos existentes en la actualidad[421].

---

[420] El mencionado informe viene a concluir lo siguiente "podemos señalar que el artículo 20.3 del Estatuto de los Trabajadores habilita al Empresario a *controlar el correo electrónico que él otorga a los trabajadores para el desarrollo de sus funciones, pero siempre que previamente haya informado sobre dicho extremo y cumpla de ese modo el deber de informar previsto en el artículo 5.1 de la Ley Orgánica 15/1999*".

[421] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C. : *Las TIC's en el ámbito laboral*, *op.cit.*, pág. 25.

N) El debate doctrinal

Señala MERCADER UGUINA que esa penetración de las nuevas formas de control tiene una especial gravedad en las relaciones laborales, en la medida en que estamos ante vínculos que perduran en el tiempo, que tienen un indudable carácter personal, que afectan a ámbitos muy diversos de la persona humana y que se proyectan sobre un gran número de posibles afectados[422].

THIBAULT ARANDA argumenta que desde la perspectiva de las relaciones laborales, el trabajo llevado a cabo por el legislador merece un juicio moderadamente favorable. La LOPD incrementa la protección de los datos de carácter personal del trabajador al incluir en su ámbito de aplicación los ficheros convencionales y extender la obligación de información, al tiempo que amplía los derechos del trabajador y permite "*agilizar*" el uso de la informática en la gestión del personal al suprimir algunos requisitos excesivamente formalistas, entre otros, la no exigencia del consentimiento en el precontrato o la posibilidad de utilizar los datos del trabajador para finalidades compatibles[423].

En palabras de GOÑI SEIN, todo ello resulta muy discutible, porque aun cuando pueda presumirse el consentimiento de la habilitación legal, ello no prejuzga la legitimidad de cualquier sistema de grabación en la empresa, o dicho de otra manera, cabe deducir de la habilitación legal *"una especie de patente de corso para actuar discrecionalmente"*[424].

Para DESDENTADO BONETE y MUÑOZ RUIZ una exigencia fundamental para el tratamiento de datos y, por tanto, para la instalación de la videovigilancia, es el consentimiento del afectado. La existencia del consentimiento es, en ocasiones,

---

[422] MERCADER UGUINA, J.R. : *Derecho del trabajo, nuevas tecnologías y sociedad de la información*, ed. Lex Nova, 2002, pág 107.

[423] THIBAULT ARANDA, J.: «La incidencia de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en el ámbito de las relaciones laborales», *op. cit.*

[424] GOÑI SEIN, J.L.: *La Videovigilancia empresarial y la protección de datos personales*, *op. cit*., pág.101.

problemática, tratándose de unas técnicas de vigilancia cuya instalación se establece sin advertencia previa[425].

TASCÓN LÓPEZ afirma que el consentimiento queda prácticamente relegado a la categoría de mera condición de licitud, entre las muchas previstas por la norma, desvirtuando en buena medida, la regla de orden en virtud de la cual y como punto de vista el consentimiento parecía necesario[426].

Señala MUÑOZ CORRAL que sería recomendable que la información a los trabajadores sobre el tratamiento de sus datos personales se lleve a cabo por medios que permitan a la empresa conservar prueba de que se ha efectuado de modo idóneo, puesto que la carga de la prueba del cumplimiento del deber de informar corresponde al empleador.

O) Las etapas de la doctrina constitucional

a) Primera etapa

Durante bastante tiempo, el respeto a la dignidad del trabajador, impuesto por el art. 20.3 ET como límite al ejercicio del control sobre el uso de los medios electrónicos en la empresa, ha quedado confinado a la intimidad y, en algún caso, al secreto de las comunicaciones. La conformidad constitucional de los medios de control se ha examinado solo desde este prisma, relegando a un segundo plano, cuando no obviando, la amalgama de informaciones obtenidas del trabajador considerados como *"datos personales".* Por tanto, en esta fase, la protección de datos, se concibe como una función de garantía del derecho a la intimidad.

---

[425] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op.cit*, pág. 64.

[426] TASCÓN LÓPEZ, R.: «El tratamiento por la empresa de datos personales de los trabajadores. ¿Un problema resuelto o caído en el olvido?», *Revista Aranzadi Social* núm 5, 2005 (BIB 2005\2432).

b) Segunda etapa

En década de los años noventa del s. XX empieza a cambiar el planteamiento con la STC 254/1993 de 20 de julio[427], dictada en un recurso donde la protección de datos se concibe como "*un instituto de garantía de otros derechos*" [428], fundamentalmente, "*el honor y la intimidad*", pero también "*un instituto que es en sí mismo un derecho o libertad fundamental".*

El TC procede a estimar el recurso de amparo planteado por considerar que ha sido vulnerado el derecho del recurrente por la decisión judicial que se declaró ajustada a Derecho la denegación presunta del Gobernador Civil de Guipúzcoa y del Ministro del Interior de solicitud de información de los datos de carácter personal existentes en ficheros automatizados de la Administración del Estado. De la opinión mayoritaria, disiente un miembro del tribunal que considera que la pretensión del actor, de solicitando pongan determinados datos personales, no es amparable en virtud del Convenio del Consejo de Europa de 28 de enero de 1981, ratificado por España.

c) Tercera etapa

En el inicio del siglo XXI, el proceso de reconocimiento del derecho a la protección de datos como autónomo, marca un precedente importante, con las SSTC 290/2000 y 292/2000. Por un lado, la STC 290/2000, 30 de noviembre[429] se pronunció sobre la constitucionalidad de la ya entonces derogada Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal de 1992 (LORTAD). Aunque no aborda cuestiones sustantivas sobre el derecho, es muy interesante el voto particular del Magistrado Manuel Jiménez de Parga, en el que se expresan las razones por las cuales,

---

[427] STC 254/1993, de 20 de julio (RTC 1993\254).

[428] El Tribunal Constitucional, sigue la estela del *Bundesverfassungsgericht* alemán que en sentencia de fecha 15/12/1983 había establecido la existencia de un derecho de autodeterminación informativa, derivado del derecho general a la personalidad del artículo 2 de la Ley Fundamental , fue estableciendo en diversas sentencias de los años 90 del siglo XX la existencia de este derecho de "*libertad informática".*

[429] STC 290/2000, de 30 de noviembre (RTC 2000\290).

a su juicio, "*debió afirmarse de modo explícito, en la argumentación de ella, que nuestro Tribunal reconoce y protege ahora un derecho fundamental, el derecho de libertad informática, que no figura en la Tabla del texto de 1978".*

Por su parte la STC 292/2000, de 4 de enero[430], parte del reconocimiento de un derecho fundamental específico, derecho a la protección de datos o libertad informática, que coexiste con otros derechos. Para el Tribunal Constitucional "*la garantía de la vida privada y de la reputación tiene hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad*". Y que se traduce en un derecho de control sobre los datos relativos a la propia persona.

El TC declara la inconstitucionalidad de los incisos "*cuando la comunicación hubiere sido prevista por las disposiciones de creación de fichero o por disposición de superior rango que regule su uso"* del art. 21.1, *"impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas"* y "*o administrativas*" del art. 24.1, y todo el apartado 2 de la LO 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal.

Entiende la Sala que el límite establecido por el art. 21.1 LOPD, al permitir que una norma de rango inferior a la Ley autorice la cesión de datos entre Administraciones sin previo consentimiento del afectado, supone una restricción que sólo podría establecer una Ley, contrariando la reserva legal establecida por el art. 53.1 CE; que la posibilidad de que, con arreglo al art. 24.1 LOPD, la Administración pueda privar al interesado de información relativa al fichero y sus datos, invocando los perjuicios que semejante información pueda acarrear a la persecución de una infracción administrativa, supone una grave restricción de los derechos a la intimidad y a la protección de datos del art. 18.4 CE , y que además "*puede causar grave indefensión al interesado"* .

El constituyente quiso garantizar mediante el actual art. 18.4 CE, no solo un ámbito de protección específico sino también más idóneo que el que podrán ofrecer por sí mismos, los derechos fundamentales garantizados en el apartado 1 del precepto.

La peculiaridad de este derecho fundamental a la protección de datos respecto del derecho fundamental a la intimidad radica en su distinta función, lo que apareja por consiguiente que también "*su objeto y contenido difieran*". Insiste después con respecto a este extremo, subrayando que *"La función del derecho fundamental a la intimidad del*

[430] STC 292/2000, de 30 de noviembre (RTC 2000\292).

art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado… Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin" (FJ 5º).

d) Cuarta etapa

Viene marcada por la STC 29/2013, de 11 de febrero[431], constituyó un hito porque dos motivos fundamentales; el primero porque estableció un canon de control de constitucionalidad más rígido que el que la jurisprudencia constitucional venía aplicando respecto al otros derechos fundamentales como el derecho a la intimidad; como segundo motivo porque rechazó la existencia de norma legal en las relaciones laborales que autorizara restricciones del derecho a la información sobre el tratamiento de datos personales, no considerando hábil a tal fin el art. 20. 3 ET. Desde esta máxima, por tanto, negada la validez constitucional de restricciones al derecho fundamental de los trabajadores *ex* art.18.4 CE, quedaba en consecuencia impedida la ponderación de la medida empresarial.

e) Quinta etapa

Está determinada por la STC 39/2016, de 3 de marzo[432], que modifica muy sustancialmente la doctrina aplicable, sí puede haber sistemas sorpresivos o no informados de tratamiento, por lo que la protección del 18.4 CE en esta materia presenta perfiles difusos. Con esta sentencia se reformula la naturaleza de la autorización que recoge la LOPD, que pasa a ser indirecta, y no personal, pese a que estamos ante personas perfectamente individualizables con las que existe una relación contractual.

---

[431] STC 29/2013, de 11 de febrero (RTC 2013\29).

[432] STC 39/2016 de 3 marzo (RTC 2016\39).

Se produce, pues, un descenso en el grado de protección del derecho fundamental del art. 18.4 CE, que se añade al dato previo de que la ley ya ha establecido que no es preciso en estos casos el consentimiento, con lo que la información constituía la pieza clave del contenido esencial del mencionado derecho[433].

III. ACTUACIONES PREVENTIVAS U ORDENADORAS DEL CONFLICTO

Una de las características que presenta el uso de los medios tecnológicos de la empresa, es, sin duda, la insuficiencia del marco de regulación interprofesional.

Como el poder de dirección del empresario es imprescindible para la buena marcha de la organización productiva, el empresario tiene la facultad, y entre otras, de adoptar las medidas de vigilancia y control que estime más oportunas para verificar el cumplimiento por parte del trabajador de sus obligaciones laborales. Por tanto, no se duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador; tampoco la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión.

A fin de rebajar la expectativa de intimidad, de legitimar el control sobre la actividad de sus empleados, de evitar la vulneración de derechos fundamentales, de satisfacer las exigencias albergadas en las normas sobre protección de datos, o de posibilitar la ulterior utilización de las pruebas halladas, la empresa activa frecuentemente mecanismos que debemos analizar.

Existen dos tipos de control empresarial: uno, que simplemente tiene por objeto el conocimiento de la forma en la que se ejecuta la prestación del trabajo; y, otro, de finalidad disciplinaria, que se dirige a vigilar el uso indebido de las herramientas de trabajo.

---

[433] CABELLOS ESPIERREZ, M. A.: «El derecho a ser informado como elemento esencial del derecho a la protección de datos. Una visión crítica de la jurisprudencia del Tribunal Constitucional y de su cambio de doctrina en la STC 39/2016», *Revista Vasca de Administración Pública, Herri-Arduralaritzako Euskal Aldizkaria*, núm. 106, 2016, pág. 213.

1. Información previa al trabajador

A) Planteamiento

El correo electrónico e Internet y otros recursos tecnológicos que la empresa pone a disposición del trabajador (como son también el ordenador personal, *smartphone*, *tablets*, etc.) cabe caracterizarlos, por un lado, como herramientas de trabajo habituales y básicas de la mayoría de las empresas, que agilizan y mejoran los servicios a sus clientes; por otro lado, como instrumentos de comunicación, y como tales, susceptibles de un uso social.

A menudo, los medios tecnológicos son utilizados por los empleados para buscar o transmitir información con fines particulares, ajenos a los intereses de la empresa. En caso de ausencia de norma expresa, se parte del reconocimiento tácito por parte del empresario del derecho a un uso social de los medios informáticos a favor del trabajador, concibiéndose esta conducta como inocua.

B) Presunción de tolerancia

La STS 28 de junio de 2006[434] fue la primera sentencia del Alto Tribunal que abordó el problema del uso de las herramientas informáticas para fines particulares. Marcó un antes y un después, al hilo de una progresiva evolución del ámbito de la intimidad del trabajador en el marco de las nuevas tecnologías. La referida sentencia, asumió la posición de la Sala de lo Social del TSJ del País Vasco, que partía de un razonamiento según el cual *"la falta de prohibición específica*" por parte de la empresa respecto a un uso privado de las herramientas informáticas, equivalía a "*autorización*", y la carga de la prueba de la existencia de una prohibición la tenía el empresario.

Este derecho al uso social tolerable de la Red, no obstante, podría ser limitado o casi eliminado mediante una regulación unilateral o bilateral, en su caso. Por lo que mientras que no haya una orden o una regulación empresarial, o no se demuestre que exista, ni existe incumplimiento por el mero uso de las tecnologías, ni el empresario puede

[434] STS 28 de junio de 2006 (RJ 2006\8452).

acceder sin más a los datos del correo y los archivos temporales de Internet del trabajador, ya que estos quedan protegidos por el derecho a la intimidad, como consecuencia de la doctrina con origen en el TEDH analizada[435].

Es una circunstancia a tener en cuenta la existencia de la generalización de una cierta tolerancia con respecto al uso moderado de los medios de la empresa. El art. 3 del Código Civil afirma que las normas deben interpretarse desde la realidad social del tiempo en que son aplicadas[436]; en este sentido la doctrina viene admitiendo cierta tolerancia social sobre el uso de estas herramientas de trabajo, incluso de manera extralaboral[437].

Incluso, por las dificultades prácticas de establecer una prohibición absoluta, es recomendable no establecerla; piénsese, por ejemplo, en el acceso a Internet desde el teléfono particular del trabajador, lo que llevaría, al emplear la videovigilancia para verificar el cumplimiento de las órdenes, dada la imposibilidad de fiscalizar el móvil particular.

C) Orientaciones de la AEPD

La Guía 2009 de la AEPD sobre la Protección de Datos en las Relaciones Laborales[438] señala que debe cumplirse con el deber de información a los trabajadores. Este deber resulta particularmente relevante cuando se trate de controles sobre el uso de Internet y del correo electrónico[439]: "*En este caso es muy recomendable que la información a los trabajadores sea clara en lo que respecta a la política de la empresa en cuanto a utilización del correo*

---

[435] El Tribunal Europeo de Derechos Humanos, en los términos de las SSTDH de 25 de junio de 1997 -caso HALFORD- y de 3 de abril de 2007 -sentencia COPLAND- valora la existencia de una lesión del art. 8 del Convenio Europeo para la Protección de los Derechos Humanos.

[436] GARCÍA ORTIZ, S y SALAS DARROCHA, J.T.: «STC 170/2013 y nueva doctrina sobre el derecho a la intimidad del trabajador» *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 30, 2014. pág. 464.

[437] SEMPERE NAVARRO A.V. y MATEOS y de CABO, O.: «Uso y control de herramientas informáticas en el trabajo (Marco legal, pautas judiciales convencionales)» en AA. VV. SAN MARTIN MAZZUCONI, C. (Dir.): *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, 2014, pág. 165.

[438] *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales1.pdf* , pág. 26.

[439] En igual sentido, la Recomendación 1/2013 de la Autoridad Catalana de Protección de Datos, sobre el uso de correo electrónico en el ámbito laboral, que pretende dar pautas para que las empresas puedan regular y controlar el uso del correo electrónico en el ámbito laboral. Esta Recomendación incluye el contenido mínimo de una política de uso de correo electrónico, mecanismos de identificación, autenticación y confidencialidad de las comunicaciones, admisión si cabe de uso privativo del correo electrónico, uso del correo electrónico con finalidades sindicales, mecanismos de control por parte de la empresa y consecuencias que se derivan del dicho control *http://www.apd.cat/es/contingut.php?cat_id=146&cont_id=626*.

electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales. Así como que incluya la finalidad de la vigilancia, y cuando pueda repercutir sobre medios que el trabajador utiliza normalmente una información sobre las medidas de vigilancia adoptadas".

También es aconsejable la instalación de mecanismos preventivos, como la exclusión técnica de la posibilidad de establecer determinadas conexiones y como realizar advertencias informáticas al usuario sobre el uso inadecuado[440].

Por ello es determinante, en este sentido, que la política de la empresa sea clara en cuanto a lo que está permitido y lo que, por el contrario, está prohibido, realizando una descripción exhaustiva sobre el uso de los sistemas de comunicación de la empresa, con fines privados o personales. Así el trabajador tendrá clara su expectativa razonable de confidencialidad e intimidad en la utilización de dichos medios; cuestión que, de no quedar clara, puede dar lugar a situaciones conflictivas.

2. Códigos de conducta

A) Idea general

Las grandes multinacionales estadounidenses hace ya tiempo que recurren a este método, explicitando de forma escrita las pautas de conducta requeridas a sus empleados[441]. Asimismo, la doctrina ha dado un claro apoyo a la utilización de códigos o subcódigos de conducta, también llamados protocolos de control y uso o manuales internos, códigos de ética, "*códigos de comportamiento ético y profesional*", en definitiva, normas que integran el denominado "*soft law*".

En un principio las empresas eran reacias a la puesta a disposición de los protocolos a los empleados por el uso contraindicado que de los mismos pudieran hacer (sobre todo se desconfiaba de que fueran a parar a manos de los sindicatos y estos a su vez adoptaran determinadas medidas legales). Pero en la actualidad, este temor se ha superado y se ha abierto un margen de tolerancia remarcable en la medida en que se

[440] PEDRAJAS QUILES, A.: «Derechos fundamentales de la persona, del trabajador y autonomía privada» en AA. VV. SALA FRANCO, T. (Coor.) *Libro Homenaje a Abdón Pedrajas Moreno, op cit.* Pág. 422.

[441] *Ibídem,* pág. 161.

constata el retorno en eficacia y motivación de los trabajadores. Según el último sondeo del INE, el 37% de las empresas tiene definida una política de seguridad para el uso de las tecnologías de la información y de la comunicación, y esta proporción supera el 50% en las empresas con más de 50 empleados[442].

Realmente nos encontramos con una muestra más del poder de dirección del empresario, pero de lo que no cabe duda es de que se ha fomentado la presencia de los protocolos sobre el uso de los elementos en la realidad productiva de nuestro país; su frecuencia en la doctrina judicial sobre esta materia es buena prueba de ello[443].

B) Contenido

El contenido de estos códigos, sus límites, sus exigencias y las posibilidades abiertas o no al trabajador en el uso privado de tales medios se convierten en el elemento clave para determinar la legalidad, no ya sólo de este uso, sino también del posible control por parte del empresario.

En este sentido, en las empresas, se han desarrollado protocolos de control y uso, que son manuales internos compuestos por una serie de imposiciones y prohibiciones que regulan el uso, para fines privativos, que los trabajadores pueden hacer de los medios técnicos, telefonía y medios informáticos, principalmente, que se ponen a su disposición.

A través de un catálogo de exigencias éticas, que debe presidir el comportamiento de los empleados, se expanden los contornos del deber de diligencia y buena fe de los medios informáticos empresariales, mientras que los de la contraparte contractual permanecen inalterables: por lo que dichos manuales, sin la necesaria participación sindical, lo que hacen es terminar por reforzar los poderes de la empresa.

---

[442] INE (2016, 28 de junio) «Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas», *op.cit*

[443] Ejemplos de la aplicación por parte de la empresa de los protocolos de actuación son STSJ Madrid de 31 octubre 2016 (EDJ 2016/234673) , STSJ Baleares de 14 enero 2016 (EDJ 2016/13178), STSJ del País Vasco de 24 de febrero de 2015 (EDJ 2015/35809), STSJ de Cantabria de 18 de junio de 2014 (EDJ 2014/98256), STSJ de Asturias de 30 de julio de 2013 (JUR 2013\281620), STSJ de Asturias de 15 de julio de 2011 (EDJ 2011/199223), STSJ de Andalucía de 14 de abril de 2010, (JUR 2010\218261), y por último STSJ de Cataluña de 13 de mayo de 2009 (JUR 2010\255125).

Normalmente, los códigos de conducta poseen carácter unitario, van dirigidos a todos los empleados de la empresa; aunque también se observan casos, donde el personal directivo no queda sujeto a estas normas y lo están a otras más específicas. Asimismo en las grandes empresas suele ser norma común que el código de conducta sea el mismo para todos[444].

C) Naturaleza

Desde el punto de vista jurídico las normas que contienen los códigos de conducta son más que meras recomendaciones, pues nacen como reflejo de la intención impositiva de sus autores. Por ello se puede afirmar que la autorregulación es algo que se suele enmarcar en un ámbito más bien teórico, y de las buenas intenciones, ya que no suele implicar unas consecuencias jurídicas claras[445].

Junto con las instrucciones relativas al desarrollo de la actividad productiva, los códigos de conducta también prevén los medios de control destinados a detectar los incumplimientos de las normas sobre el uso de Internet.

La doctrina alerta del riesgo que corren los derechos de los trabajadores; ante la falta de negociación colectiva, la empresa acaba ocupando el espacio que el legislador ha dejado vacante, mediante los códigos de conducta que no son otra cosa que mecanismos de autorregulación. Las normas de uso del correo electrónico y de la navegación por Internet suelen ser muy restrictivas, dando origen a una "*libertad residual a merced del empresario*"[446]. A raíz de la última jurisprudencia constitucional se ha calificado la situación de *particular gravedad*, pues la empresa es el agente único de gobierno de la aplicación de los derechos fundamentales en el uso y control de las herramientas informáticas, sin que haya lugar a una intervención mínima de trabajador en la configuración de sus propios derechos individuales en la relación de trabajo[447].

---

[444] TOSCANI JIMÉNEZ, D. y CALVO MORALES, D. :«El uso de Internet y el correo electrónico en la empresa: límites y garantías». *Revista Española de Derecho del Trabajo*, núm. 165, 2014 (BIB 2014/1654).

[445] SEMPERE NAVARRO, A.V. y MATEOS y de CABO, O.: «Uso y control de herramientas informáticas en el trabajo (Marco legal, pautas judiciales y convencionales*)*», *op. cit,* pág. 93.

[446] GOÑI SEIN, J.L.: «Los Derechos Fundamentales Inespecíficos en la Relación Laboral Individual: ¿Necesidad de Reformulación?» *op.cit* Pág. 24

[447] GOÑI SEIN, J.L.: «Los límites de las potestades empresariales *vs*. Derecho a la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral de las redes sociales.)», *op. cit*

D) Consecuencias del incumplimiento

Si el trabajador infringiera lo preceptuado en los protocolos de uso y control fijados por la empresa, se neutralizaría su expectativa de intimidad. Doctrina seguida por la STS de 8 de marzo de 2011[448], que nos viene a decir que no constituye una prueba válida para proceder a un despido disciplinario disponer de los datos de navegación obtenidos de un ordenador de la empresa, sin que exista información sobre la prohibición de su uso personal.

Por lo cual el hecho de que la empresa pueda acceder al disco duro del ordenador de su empleado y seguir su navegación es lícito, siempre que se haya destruido previa y claramente cualquier expectativa de intimidad, lo que se puede lograr a través de protocolos de control, basándose, fundamentalmente en la STEDH de 3 de abril de 2007[449] (Caso *Copland)*, incluso, en este caso, la Agencia de Protección de Datos impuso a la empresa una multa de 60.000 euros por monitorizar la navegación del empleado por Internet sin aviso previo[450].

El incumplimiento de los códigos de conducta de la empresa, si son difundidos entre los trabajadores, puede enfocarse como desobediencia a órdenes empresariales y no sólo como transgresión de la buena fe contractual. Asimismo, y desde otra perspectiva, estas directrices patronales podrían suponer un límite a una eventual responsabilidad civil del empleador por actos del trabajador en la utilización inadecuada de los medios empresariales[451].

E) Implementación

A fin de que pueda efectuarse un control adecuado sobre el empleo que hacen los trabajadores de estos medios tecnológicos, ellos deben conocer con carácter previo las condiciones de uso de los medios que se ponen a su disposición. La regulación al efecto ha de ser expresa y clara y deberá ponerse en conocimiento de los trabajadores a través de una forma adecuada, que permita suficiente difusión, comunicando inmediatamente las posibles modificaciones. Únicamente, bajo estas condiciones, la infracción de la

---

[448] STS 8 de marzo de 2011 (RJ 2011\932).
[449] STEDH de 3 de abril de 2007 (TEDH 2007\23).
[450] Resolución R/02615/2010.
[451] SEMPERE NAVARRO, A.V y SAN MARTÍN MAZZUCCONI, C.: *Nuevas tecnologías y Relaciones Laborales*, *op. cit*, pág.42.

normativa establecida podrá autorizar el ejercicio del poder disciplinario por parte del empleador.

Cuando existan trabajadores contratados previamente a la elaboración e implantación de un código, la empresa deberá tratar de buscar, si es posible, el consentimiento de éstos o de sus representantes, como elemento para obtener el consenso y evitar futuras controversias; pero partiendo de la base de que es el poder de dirección de la empresa el que habilita a ésta para fijar unilateralmente dichos protocolos, la falta del consentimiento por los empleados no será un obstáculo para la aplicación y exigencia de las normas contenidas en éste[452].

F) Debate de contenidos

Cierto sector de la doctrina pone de relieve el peligro que supone que los códigos de conducta contengan prohibiciones absolutas de uso de los medios informáticos de la empresa para fines privados para obtener una licencia para fiscalizar su control, sin demasiadas dificultades, porque se convierten en una potente herramienta del empresario[453], incluso hay quienes consideran que los protocolos anulan directamente el ejercicio de los derechos fundamentales, dando así origen a una libertad residual a favor del empleador[454]. Por otro lado, respecto a las prohibiciones *"absolutas*" de uso, que han sido ratificadas por el Tribunal Supremo en varias ocasiones, algunas sentencias de tribunales menores las censuran por el hecho de que en la sociedad del conocimiento y de las comunicaciones no se puede impedir, desde el sentido común, un uso social de aquéllas.

Ciertos sectores doctrinales afirman en este sentido que no debe olvidarse que el correo electrónico no se trata sólo de un instrumento productivo, sino también, en nuestra realidad actual, de un mecanismo de comunicación entre las personas, incluso en el trabajo. Y por lo que respecta a Internet, es una importante fuente de información, cada

[452] MIRÓ MORROS, D.: «El uso del correo electrónico en la empresa: protocolos internos», *op.cit.*

[453] GUITIERREZ PÉREZ, M.: «Prohibición expresa del uso privado del ordenador de la empresa como fundamento para su control. STSJ Andalucía 14 noviembre 2013», *Revista Española de Derecho del Trabajo* núm. 165, 2014.

[454] GOÑI SEIN, J.L.: «Los Derechos Fundamentales Inespecíficos en la Relación Laboral Individual: ¿Necesidad de Reformulación?», *op. cit.*, pág. 24.

vez más asequible, por lo que resulta poco razonable en la actualidad que se exija a los trabajadores un uso estricta y rigurosamente laboral[455].

Por el contrario, consideramos acertada la existencia de estos protocolos, puesto que es más seguro jugar un partido con las reglas establecidas que sin determinar; supone seguridad jurídica, además, las arbitrariedades de las empresas están siempre sometidas al control de los tribunales y las medidas de fiscalización deben ser enjuiciadas, ora con arreglo al principio de proporcionalidad, ora con arreglo al principio de autodeterminación informativa.

G) Corolario

Por tanto, el control empresarial debe quedar sujeto a los siguientes límites para que resulte lícito:

- Que se hayan establecido previamente las reglas de uso de los medios informáticos puestos a disposición del trabajador, ya sean prohibiciones absolutas o parciales.
- Que igualmente se informe a los trabajadores de los medios de control que van a ser usados para fiscalizar el uso de los medios informáticos.

A modo de conclusión, debemos destacar la importancia de la existencia en la empresa de un código de conducta telemático, adaptado y actualizado a los nuevos medios informáticos; pues las repercusiones por la falta de regulación o por la inadecuada regulación interna son ciertamente relevantes.

[455] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C. «Sobre el control empresarial de los ordenadores», *op.cit.* (BIB 2012\984).

3. Negociación Colectiva

A) Funcionalidad

Teniendo presente la indefinición legal y la dispersión jurisprudencial existente, a los Convenios Colectivos les corresponde una importante labor de equilibrio y moderación de las facultades empresariales tras un análisis meditado y exhaustivo sobre los intereses en conflicto.

Allá por en el año 2007 el Acuerdo Interconferencial para la Negociación Colectiva [456] ya mostraba su preocupación por resaltar que uno de los aspectos que debía tomarse en cuenta era la incidencia de las nuevas tecnologías en el ámbito de la empresa y en consecuencia, instaba a los negociadores a que trataran este aspecto en sus acuerdos[457].

Por tanto, debiera ser la negociación colectiva la que entre a regular el ejercicio de este derecho de información telemática, que debe pautar entre otros los siguientes aspectos:

- Volumen de correo electrónico admitido: número, tamaño, formato.
- Posibilidad o no de contar con un espacio en la intranet de la empresa para los sindicatos.
- Titularidad del derecho; secciones sindicales, representantes unitarios, ambos[458].

B) Valoración

La gran mayoría de los convenios que han articulado un marco de regulación en este ámbito lo han hecho limitando el acceso de los trabajadores a los sistemas telemáticos de la empresa. La doctrina pone de relieve determinadas orientaciones generales en los convenios colectivos que regulan el uso de las nuevas tecnologías en la empresa, que pueden resumirse en los siguientes puntos:

---

[456] BOE 24/2/2007

[457] SEMPERE NAVARRO, A.V, y MATEOS y de CABO, O.: «Uso y control de herramientas informáticas en el trabajo. (Marco legal, pautas judiciales y convencionales.)» *op. cit*. ,pág. 81.

[458] NIETO ROJAS, P.: «El correo electrónico como medio de transmisión de información sindical y el papel de la negociación colectiva en la fijación de su alcance», *Nueva revista española de Derecho del Trabajo*, núm. 172, 2015.

- Establecimiento de prohibiciones totales o de limitaciones significativas de los usos personales de la informática de la empresa con previsión de sanciones específicas, en función de la gravedad. Lo cual hace referencia a sanciones leves y a sanciones muy graves, incluido el despido.
- Aparición de reglas más flexibles que permiten usos razonables o moderados del material informático de la empresa, o incluso de una cuenta personal del trabajador a utilizar fuera del horario del trabajo.
- Existencia de previsiones especiales para determinados "*usos de riesgo*"; correos masivos, cadenas de juegos de azar, pornografía, contenidos ofensivos, etc…
- Reconocimiento de la facultad del empleador de realizar comprobaciones de uso de auditorías informáticas con aplicación, en algunos casos, de causas de justificación (indicios racionales de usos abusivos) y de garantías de procedimiento (presencia del trabajador afectado, de un representante…).
- Previsión de reglas de uso compartido del ordenador por varios trabajadores o de prohibición de vías de acceso para despersonalizar la utilización del ordenador[459].

Asimismo, se advierte que cuando los Convenios abordan las regulación del uso de las nuevas tecnologías, en la mayor parte de los casos de forma impecable, existen algunos supuestos en los que se establece un control desorbitado por parte del empresario, mucho más allá de los límites legales y de la doctrina del TC sobre principio de proporcionalidad[460].

Con respecto al control empresarial para verificar el cumplimento por parte del trabajador de sus obligaciones y deberes laborales, en los convenios colectivos suele disponerse que se realizarán con la consideración debida a su dignidad, en este sentido, la inspección que realice la empresa sobre los archivos, material, emails y su uso de internet, debe garantizar la privacidad y dignidad de aquellos[461].

Como ya se ha manifestado, nos encontramos ante un número *in crescendo* de convenios colectivos, que regulan la limitación del acceso a las nuevas tecnologías, pero el número de convenios que regulan este aspecto es aún minoritario.

---

[459] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op. cit* pág. 149-150

[460]SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: «Derechos fundamentales inespecíficos y negociación colectiva», *op. cit,* pág 299.

[461] *Ibídem,* pág 127.

Los convenios a este respecto, se van aproximando de una manera "*muy tímida y limitada*[462]*",* ya que en ocasiones establecen la prohibición o limitación de uso, pero no concretan a lo largo de su articulado la posibilidad de que se efectúen controles por el empresario, y la información previa a éstos sobre dichas medidas o reglas que indiquen el uso que los trabajadores han de hacer del ordenador[463].

C) Tipología

Los convenios colectivos que regulan esta materia, tanto los de ámbito empresarial como supraempresarial, pertenecen a muy diversos sectores productivos o actividades no limitándose a entornos en los que el uso de las nuevas tecnologías pueda estar más presente, lo que manifiesta que esa incipiente voluntad reguladora de estas cuestiones se está produciendo con carácter general.

Por sectores, los que regulan de una manera minuciosa dedicando a menudo, un capítulo entero sobre utilización del correo electrónico e Internet son las grandes empresas de telecomunicaciones, de nutrición, editoriales y prensa, sobre todo; por las especiales cautelas que han de tener con la posible falta de buena fe de los trabajadores respecto a la divulgación de información. Podemos citar, varios ejemplos.

* Convenio colectivo estatal para el sector de ortopedias y ayudas técnicas de 3 de marzo de 2016[464], en su art. 54 apt. 9: "*La utilización de los medios informáticos propiedad de la empresa (correo electrónico, intranet, etc.) para fines distintos de los relacionados con el contenido de la prestación laboral. En el caso de que la utilización fuera abusiva o causase perjuicio a la empresa la falta se calificará como grave*".

*Convenio colectivo para el sector de Pompas Fúnebres de Galicia de 22 de mayo de 2015[465], en su art. 45: "respecto del uso de las nuevas tecnologías en el trabajo, la utilización del correo electrónico y de la navegación por internet sólo está permitida por motivos estrictamente laborales y el uso y control de los ordenadores y de los programas informáticos instalados y facilitados por las empresas quedará limitado exclusivamente

[462] SEMPERE NAVARRO y MATEOS y de CABO.: «Uso y control de herramientas informáticas en el trabajo. (Marco legal, pautas judiciales convencionales)», *op. cit*, pág. 80.

[463] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit.*

[464] RCL 2016\378

[465] LG 2015\141.

por razones de trabajo, siendo el trabajador el único responsable de la custodia de las claves de acceso utilizadas para su trabajo, las cuales son personales e intransferibles".

*Convenio Colectivo de Unidad Editorial General de 17 de marzo de 2015[466]: "Los empleados... podrán utilizar el correo electrónico facilitado por la Empresa para su uso personal y familiar en términos razonables y moderados. La utilización personal se procurará fuera de las horas de trabajo a fin de impedir cualquier perjuicio a las funciones laborales. El carácter razonable y moderado de los envíos personales se presumirá, salvo prueba en contrario, hasta el número de ochenta correos mensuales. Superado ese número, corresponderá al empleado justificar su procedencia». De manera que un empleado de la citada empresa puede enviar correos electrónicos de carácter privado con el límite cuantitativo que fija su uso moderado".

* III Convenio colectivo del Grupo 20 Minutos (antes Grupo Multiprensa) de 9 de abril de 2014 [467] "los trabajadores podrán utilizar una cuenta de carácter personal, de manera esporádica y cuando sea necesario, desde el sistema informático de la Compañía, siempre que dicha utilización se realice fuera del horario de trabajo. En este supuesto, los trabajadores no podrán utilizar el nombre y/o marca de la Compañía en los mensajes que remitan". Si bien los límites al uso del correo electrónico en la empresa, en general, son tratados en el siguiente epígrafe, es conveniente matizar aquí que en caso de que los trabajadores utilicen su propio correo personal en la red de comunicación de la empresa, dicho uso no puede ser realizado durante los tiempos dedicados al desempeño de la prestación. Respetándose tal condición, los eventuales registros que el empresario puede realizar en su correo no alcanzarían a estos e-mails".

* V Convenio colectivo de Telefónica Servicios Audiovisuales SAU, de 3 de febrero de 2016[468], recoge respecto al uso de las de las nuevas tecnologías la prohibición general de uso con fines particulares, reservándose el derecho, cuando existan indicios de la infracción, realizar las pertinentes comprobaciones:

> *"Todos los trabajadores de la empresa deben tener acceso a las nuevas tecnologías, proporcionando las herramientas adecuadas para el correcto desarrollo del trabajo asignado.(…)*
>
> *Dado que esta nueva situación puede producir efectos no deseados, por la posible utilización no adecuada de los mismos, ambas partes consideran conveniente fijar las reglas que deben regir la utilización de las herramientas y medios técnicos puestos a disposición de los trabajadores por la empresa.*
>
> *Esta regulación debe partir de dos premisas fundamentales: en primer lugar, el legítimo derecho de la empresa de controlar el uso adecuado de las herramientas y medios técnicos que pone a disposición del trabajador para realizar su actividad y, por otra parte, debe salvaguardarse el derecho a la intimidad del mismo.*

---

[466] Resol. de 17 de marzo de 2015, de la Dirección General de Trabajo de la Consejería de Empleo, Turismo y Cultura, sobre registro, depósito y publicación del acta de acuerdos de la comisión negociadora de 30 de septiembre de 2014, del convenio colectivo de la empresa "Unidad Editorial General, Sociedad Limitada"

[467] BOE 23 abril 2014, núm. 98.

[468] BOE 16 febrero 2016, núm. 40

A tal efecto, se acuerdan las siguientes facilidades y normas de funcionamiento que pretenden regular, por un lado, las actuaciones de la empresa y, por otro, establecer las reglas a las que el trabajador y sus representantes deben someterse cuando utilicen los medios técnicos puestos a su disposición para la realización de su prestación laboral y funciones de representación, respectivamente.

a) Dotación individual y colectiva para el acceso al correo electrónico y a internet.

Durante la vigencia del presente convenio colectivo, la empresa dotará de acceso a internet a todos los trabajadores que dispongan de un puesto de trabajo con pantalla de visualización de datos. A su vez, dichos trabajadores dispondrán, siempre que lo soliciten,de una dirección propia de correo corporativo.

(...)

b) Utilización del correo electrónico e internet por los empleados.

Los empleados podrán utilizar el correo electrónico, la dirección e-mail, e internet con libertad y en el sentido más amplio posible, para el desempeño de las actividades de su puesto de trabajo.

Siempre que precisen realizar un uso de estos medios que exceda el habitual, envíos masivos o de especial complejidad, utilizarán los cauces adecuados, de acuerdo con su jefe inmediato, para no causar daños en el desarrollo normal de las comunicaciones y en el funcionamiento de la red.

Con carácter general, los empleados de Telefónica Telecomunicaciones Públicas s.a. No podrán utilizar el correo electrónico ni internet para fines particulares.

En este sentido, bajo ningún concepto podrán los empleados utilizar estos medios para realizar envíos masivos de mensajes, enviar mensajes con anexos de gran tamaño (capacidad), ni realizar cualquier tipo de envío sin relación alguna con el desempeño profesional, que interfiera las comunicaciones del resto de empleados o perturbe el normal funcionamiento de la red de la empresa. Igualmente, no está permitido el envío de cadenas de mensajes electrónicos, la falsificación de mensajes de correo electrónico, el envío de mensajes o imágenes de material ofensivo, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, etc., aquellos que promuevan el acoso sexual, así como la utilización de la red para juegos de azar, sorteos, subastas, descarga de vídeo, audio u otros materiales no relacionados con la actividad profesional.

El incumplimiento de estas normas determinará la utilización por la empresa de las restricciones que considere oportuno en la utilización de estos medios y la aplicación del régimen disciplinario, en su caso.

Cuando existan indicios de uso ilícito o abusivo por parte de un empleado, la empresa realizará las comprobaciones oportunas y, si fuera preciso, realizará una auditoría en el ordenador del empleado o en los sistemas que ofrecen el servicio, que se efectuará en horario laboral y en presencia de algún representante de los trabajadores o de la organización sindical que proceda, en caso de afiliación, si el empleado lo desea, con respeto a la dignidad e intimidad del empleado."

D) Alcance de la STC 170/2013

A este particular cabe resaltar que la STC 170/2013, de 7 de octubre, ha marcado un punto de inflexión, una gran novedad con respecto a la doctrina anterior constitucional, fijando importantes directrices[469]. La principal novedad reside en que considera que el requerimiento previo a una posible intervención del correo corporativo por parte de la empresa que, es la promulgación de una política empresarial sobre el uso del correo electrónico, puede sustituirse por un artículo en el Convenio Colectivo que sanciona el

[469] MIRÓ MORROS, D.: «El uso del correo electrónico en la empresa: protocolos internos», *op.cit.*

uso desviado de tal medio. Incluso, en este caso concreto, que se tipificaba como leve[470] la conducta imputada, por incumplir el trabajador, se deriva la responsabilidad de manera implícita a lo establecido en el Convenio[471].

El hecho de la prohibición de uso de las tecnologías para un empleo particular, ya sea por medio de un protocolo al efecto, o bien como es el caso de la STC 170/2013, de 7 de octubre, a través de Convenio Colectivo, permite que la empresa fiscalice el contenido de los correos electrónicos enviados y recibidos por el trabajador, sin advertencia previa al trabajador. Asimismo enerva la expectativa razonable de confidencialidad, razón por la cual no se consideran vulnerados derechos constitucionales (ni el secreto de las comunicaciones, ni el de intimidad).

Cierto sector de la doctrina califica como inadmisible y un retroceso, el razonamiento de la STC 170/2013, de 7 de octubre, pues de ella se extraen dos conclusiones con las que se debe estar en total desacuerdo; a saber: 1) el hecho de que un Convenio Colectivo tipifique una conducta como sancionable equivale a prohibirla, aunque no lo anuncie expresamente; 2) un Convenio Colectivo podrá limitar decisivamente el ejercicio de derechos fundamentales[472].

Según el Alto Tribunal, el incumplimiento de lo previsto en el Convenio Colectivo no habilitaría interferencias en el proceso o en el contenido de la comunicación, sin perjuicio de que pueda acarrear algún tipo de sanción. Antes al contrario, hubiera sido necesario que se advirtiera expresamente al trabajador sobre la práctica de la supervisión laboral, y, como no se hizo, se incumple con ello el derecho a la protección de datos. Ante la ausencia de este requisito debería abogarse por la falta de idoneidad procesal de la prueba recabada, pues constituye una prueba ilegítimamente obtenida que debió declararse nula, aunque evidencie un incumplimiento grave y culpable del trabajador, capaz de justificar un despido, derivado de una vulneración de la buena fe contractual,

---

[470] Era de aplicación el XV Convenio Colectivo de la industria Química Española (Feique), y que en su art. 59.11, tipificaba como falta leve la utilización de los medios informáticos propiedad de la empresa para fines distintos de los propios del trabajo, con la salvedad de lo dispuesto en el art. 79.2, por su parte este artículo parte de un principio general de uso exclusivo para el trabajo y añade como excepción para los representantes de los trabajadores el uso del correo electrónico para comunicarse entre sí con la dirección de la empresa. Se requería el previo acuerdo con la empresa para cualquier uso ajeno (Resolución de la Dirección General de Trabajo de 9 de agosto de 2007, BOE 29 de agosto de 2007).

[471] CARRASCO DURÁN, M.: «El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa», *Revista Aranzadi Doctrinal* núm. 9, 2014.(BIB 2013\2695).

[472] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit.*

consecuencia de la revelación de secretos empresariales. Y ello porque las intromisiones empresariales, enderezadas a verificar o comprobar la existencia de las comunicaciones, incluso cuando *ex post* pueda quedar acreditada la transgresión por parte del trabajador, exigirían, en todo caso, el conocimiento previo de la práctica de control empresarial o la concurrencia de la pertinente autorización judicial que cita el propio art. 18.3 CE[473].

A raíz de esta doctrina constitucional y para dar cumplimiento a los derechos constitucionales de la intimidad y de las comunicaciones, se ha recomendado que las empresas cumplan con las exigencias de transparencia en el control de los correos electrónicos, de forma análoga a los avisos que se utilizan en caso de grabación de las conversaciones telefónicas mantenidas con los servicios de atención al cliente[474].

4. Intervención de los representantes de los trabajadores

A) Alcance del deber de emitir informe

El Estatuto de los Trabajadores establece en su artículo art. 64.5.f) que el comité de empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por éste, sobre la implantación y revisión de sistemas de organización y control del trabajo, estudios de tiempos, establecimiento de sistemas de primas e incentivos y valoración de puestos de trabajo[475].

Este artículo establece un requisito de carácter procedimental, que incide directamente en el art. 20.3 ET, el informe preceptivo por parte de los representantes, al fin y al cabo, se presenta como una garantía de control del ejercicio de la facultad empresarial, pues con carácter general, la participación de los trabajadores modula de

[473] RODRÍGUEZ ESCANCIANO, S.: «El control empresarial de la mensajería electrónica como prueba de la transgresión de la buena fe contractual. A propósito de la STC de 7 de octubre de 2013» *op.cit.*

[474] FERRANDO GARCÍA, F.: «Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías», *Estudios financieros. Revista de trabajo y seguridad social* ,núm. 399, 2016, págs. 58-59.

[475] En el artículo 64.6 ET se prescribe que en todo caso, la consulta deberá permitir que el criterio del comité pueda ser conocido por el empresario a la hora de adoptar o de ejecutar las decisiones. Los informes que deba emitir el comité de empresa deberán elaborarse en el plazo máximo de quince días desde que hayan sido solicitados y remitidas las informaciones correspondientes".

alguna manera los poderes del empresario. La función de control de las decisiones del empresario, por parte del comité de empresa, está muy atenuada aunque el informe es previo a su ejecución, se refiere a decisiones que ya han sido adoptadas.

La doctrina advierte del carácter no vinculante del informe del comité de empresa para el empleador lo cual significa que con independencia de la opinión o estimación en contra por parte de los representantes legales, el empresario podrá poner en funcionamiento tal medida de control[476].

B) Consecuencias de la infracción

En cualquier caso, pese a la escasa virtualidad que el ordenamiento jurídico atribuye a este informe, su solicitud es preceptiva. La ausencia de solicitud al comité de empresa vulnera los derechos de consulta que la legislación atribuye a los representantes de los trabajadores, como una infracción administrativa grave, tipificada en el artículo 7.7 LISOS[477].

Sin embargo, estas consecuencias no son de aplicación a los supuestos en que, habiendo solicitado dicho informe a los representantes de los trabajadores, estos no lo han emitido en el plazo de quince días; pues en este caso, se tiene por evacuado, lo que permite al empresario, ejecutar libre y válidamente su decisión. Esta pasividad del comité de empresa, supondría una dejación de las funciones, que sería censurable por parte del colectivo de representados[478].

La STC 186/2000, de 10 de julio[479] responde, ante el recurso de amparo planteado a la cuestión de falta de información previa, respecto a la instalación de la videovigilancia al comité de empresa, contestando que la cuestión carece de trascendencia desde el punto de vista constitucional, siendo de legalidad ordinaria.

---

[476] MONEREO PÉREZ, J.L: «Artículo 64» en AA. VV., MONEREO PÉREZ, J. L. y ALARCÓN CARACUEL, M. R. (Coors.): *Comentario al Estatuto de los Trabajadores*, ed. Comares, 1998, pág. 738.

[477] Son infracciones graves: La transgresión de los derechos de información, audiencia y consulta de los representantes de los trabajadores y de los delegados sindicales, en los términos en que legal o convencionalmente estuvieren establecido,

[478] 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» en AA. VV, VICENTE PACHÉS, F. (Coor.) *El control empresarial en el ámbito laboral*, ed. CISS PRAXIS, 2005, págs. 56-58.

[479] STC 186/2000, de 10 de julio (RTC 2000\186).

C) Limitaciones del eventual acuerdo

La doctrina alerta sobre la escasa o nula eficacia de la búsqueda de una solución convencional con los representantes de los trabajadores, porque estos no tienen capacidad para legitimar la adopción de dispositivos de control en el lugar del trabajo, si resultan ilícitos, ni pueden impedir el ejercicio de las acciones de protección del derecho fundamental. Si alguno de los trabajadores considerara vulnerado su derecho, podría instar la correspondiente acción, ya que los derechos individuales son irrenunciables y no pueden ser objeto de tráfico, cuando la adopción de la medida implica vulneración de algún deber jurídico[480].

En concreto, con respecto a la videovigilancia a los trabajadores, cabe puntualizar que la empresa deberá preavisar a los representantes legales de los trabajadores de la instalación de las cámaras[481], detallando su ubicación y los motivos del control a través de la misma[482].

5. Pactos individuales

A) Funcionalidad

En ausencia de códigos o protocolos y de previsiones colectivas, o como complemento a los mismos, algunas empresas incluyen en sus contratos de trabajo cláusulas que contienen medidas de control en la materia y advierten acerca de qué tipo de uso o mensajes pueden ser objeto de investigación empresarial.

Por ejemplo, para evitar la utilización irregular de las herramientas informáticas que proporciona la empresa, pueden incluirse cláusulas que limiten su uso a lo estrictamente laboral; o que fijen en qué medida se pueden utilizar para usos particulares, posibilitando que, en caso de transgresión, se tomen las medidas que mejor procedan.

---

[480] GOÑI SEIN, J.L.: *La Videovigilancia empresarial y la protección de datos personales, op. cit.*, pág.246.

[481] HOLGADO GÓNZÁLEZ, M.: «La protección constitucional de la intimidad de los trabajadores frente a el uso de las nuevas tecnologías de la comunicación» en AA. VV, GALÁN MUÑOZ, A. (Coord.): *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación, op.cit.*, pág.59.

[482] VIDAL LÓPEZ, P. :«La utilización de las cámaras de videovigilancia para fines disciplinarios y de control del trabajo», Actualidad Jurídica Aranzadi núm. 888, 2014 (BIB 2014\2177).

También existen cláusulas de confidencialidad, en virtud de las cuales el trabajador no puede desvelar ninguno de los conocimientos que tenga respecto a clientes, colaboradores, cifras u objetivos de la empresa, a través de ningún medio, incluidos los telemáticos.

B) Criterio del Grupo "artículo 29"

En líneas generales, la doctrina se muestra reacia a la admisión de las cláusulas contractuales que autorizan los controles empresariales; apuntando que suelen ser mecanismos de adhesión, susceptibles de encubrir auténticas renuncias al derecho del afectado[483].

Realmente, se ha comprobado como algunas empresas se valen de esta posibilidad para incluir en el contrato de trabajo disposiciones por las que el trabajador autoriza a la empresa a que acceda a su correo electrónico, apertura de ficheros, etc. Lo que no es de recibo, ya que no resulta asumible que el trabajador pueda renunciar a un derecho fundamental (art. 18 CE). A este respecto el Grupo de Trabajo de la UE "*Artículo 29*" ha opinado lo siguiente:

> *"Si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, actuará de forma engañosa si intenta legitimar este tratamiento a través del consentimiento. El recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.[484]"*

Por tanto, la dudosa validez jurídica de estos preceptos se debe principalmente a que generalmente, no aparecen como cláusulas libremente pactadas, sino impuestas por el empresario[485].

C) Criterio de la AEPD

A este respecto, y en sentido contrario, se ha pronunciado la Agencia Española de Protección de Datos, en el Informe 464/2013[486] sobre *Anexo al contrato de trabajo sobre deber de confidencialidad. Uso de internet y correo electrónico*, que resuelve la consulta

---

[483] Art.3.5 ET:" *Los trabajadores nos podrán disponer válidamente antes o después de su adquisición de los derechos que tengan reconocidos por disposiciones legales de derecho necesario*".

[484] Opinión del Grupo de Trabajo del art. 29 núm. 8/2001 sobre el tratamiento de datos de carácter personal en el contexto laboral. Aprobado 13 de septiembre de 2001.

[485] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op. cit.*

[486] *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2013-0464_Anexo-al-contrato-de-trabajo-sobre-deber-de-confidencialidad.-Uso-de-internet-y-correo-electr-oo-nico..pdf*

planteada por un trabajador de una empresa en la que cuestiona si es conforme a LOPD, y su normativa de desarrollo, la actuación de la empleadora consistente en la entrega a todos los trabajadores junto con la nómina de un determinado mes, de un Anexo al contrato relativo al deber de confidencialidad, así como respecto del uso de Internet y del correo electrónico para fines profesionales.

En el Informe se recoge la doctrina de la STS 26 de septiembre de 2007 [487], que afirma "*lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios*" y la STC núm. 170/2013 de 7 de octubre[488], que habla "*de la inexistencia expectativa razonable de privacidad*", pues existía una prohibición en el Convenio Colectivo del uso de los medios informáticos para fines particulares. Por lo que el Informe núm. 464/2013 de la AEPD viene a concluir que sí que es lícita la firma del Anexo al contrato de trabajo:

> *"Mediante la firma del Anexo al contrato de trabajo existiría una información al trabajador del uso que debe darse a este tipo de medios; la firma del Anexo es uno de los medios a través de los cuales el empresario puede probar dicha circunstancia; como podría por otro lado acreditarse mediante la aportación de otros indicios que coadyuvaran a entender cumplido este requisito, pero siendo la firma uno de ellos, totalmente lícita y admitida en Derecho[489]".*

D) Valoración

No obstante y pese a que la posición mayoritaria rechaza que las normas sobre el uso de las nuevas tecnologías queden determinadas en el contrato de trabajo, encontramos posturas minoritarias en sentido opuesto, que consideran esencial incluir en el contrato de trabajo las cláusulas contractuales que recojan el marco jurídico vigente en la empresa en relación al uso de la tecnología[490].

En todo caso, es sabido que si las partes del contrato pactan condiciones lesivas de los derechos fundamentales, en tal coyuntura entrarían en funcionamiento los mecanismos generales de depuración del ordenamiento jurídico, con la consiguiente declaración de ilicitud y de nulidad de los pactos correspondientes[491].

Con la finalidad de vigilar y limitar el tiempo de conexión a Internet, como elemento de control de la productividad, para garantizar la estabilidad del sistema en

---

[487] STS 26 de septiembre de 2007 (RJ 2007\7514).

[488] STC 170/2013, de 7 de octubre (RTC 2013\170).

[489] *Ibídem*, pág. 6

[490] MIRÓ MORROS, D.: «El uso del correo electrónico en la empresa: protocolos internos», *op.cit.*

[491] GARCÍA MURCIA, J.: «Presentación» en AA. VV. GARCÍA MURCIA, J. (Dir.): *Derechos del Trabajador y Libertad de Empresa*, ed. Aranzadi, 2013, pág. 45.

cuanto a consumo de recursos (banda ancha, número de conexiones, protocolos usados…) y por razones de seguridad y confidencialidad de datos sensibles, existen formas de prevención respecto al uso de los medios empresariales puestos a disposición de los trabajadores que pueden ser arbitrados por un técnico de sistemas responsable del control informático.

6. Mecanismos de prevención

A) La criptografía

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad las comunicaciones, la información y a las entidades que se comunican[492].

Con la finalidad de vigilar y limitar el tiempo de conexión a Internet, como elemento de control de la productividad, para garantizar la estabilidad del sistema en cuanto a consumo de recursos (banda ancha, número de conexiones, protocolos usados…) y por razones de seguridad y confidencialidad de datos sensibles, existen formas de prevención respecto al uso de los medios empresariales puestos a disposición de los trabajadores que pueden ser arbitrados por un técnico de sistemas responsable del control informático.

B) Uso de ventanas emergentes

A modo de recordatorio, se informa al empleado, a través de ventanas que "*saltan*" cuando accede a Internet y al correo electrónico recordando que existe una política corporativa de uso de estos medios y le advierten de las consecuencias de su incumplimiento.

[492] PASTOR FRANCO, J. y SARASA LÓPEZ, M.A.: *Criptografía digital: fundamentos y aplicaciones*. Universidad de Zaragoza, 1998, pág. 53.

C) Identificación del usuario

El problema es reside que en muchas ocasiones, los Tribunales se encuentran con contraseñas públicas, o al menos conocidas por varios trabajadores, o incluso, sin contraseña, ante lo cual suele concluirse que es imposible saber quién es el autor de la conducta irregular[493].

Lo recomendable es que a cada se trabajador se le proporcione un nombre de usuario y una clave privada para acceder a los medios informáticos, que ha de ser personal e intransferible y que el empleado ha de modificar la primera vez que acceda al sistema, lo que asegura la confidencialidad de los datos y la intimidad. Así se garantiza el empleo individual de las herramientas y se facilita, en caso de producirse, la depuración de responsabilidades[494].

Como así sucedió en la STSJ de Galicia de 15 de julio de 2014[495], en la que una empresa de telemarketing proporcionó a cada teleoperadora una clave de usuario para acceder al sistema; que identificaba a quién y desde qué terminal actuaba. De esta forma se demostró la autoría de una trabajadora responsable de ciertas irregularidades detectadas por la empresa, que fue despedida disciplinariamente y la extinción contractual fue validada por el Juzgado de Instancia. Posteriormente, la Sala de lo Social de Galicia confirmó la procedencia del despido, pues la trabajadora procedió con deslealtad, al actuar de manera fraudulenta en operaciones de venta de seguros de reparación a particulares, cargando en cuentas de clientes abiertas en entidades de crédito primas por seguros a los que los titulares no habían dado su conformidad; y fue descubierta por ser su identidad plenamente identificable como usuario.

D) Existencia de dos cuentas de correo electrónico

En caso de que la empresa permita el uso personal del email, los empleadores deben proporcionar a los trabajadores dos cuentas de correo electrónico:

---

[493] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*, *op.cit.*, pág. 24.

[494] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: *Derechos Fundamentales Inespecíficos y Negociación Colectiva*, *op. cit*. pág 166.

[495] STSJ Galicia de 15 julio de 2014 (AS 2014\2241).

- Una de *uso profesional exclusivo*, en la que se permitiría un control dentro de los límites constitucionales.
- Otra de *uso estrictamente privado*, que solo sería objeto de medidas de seguridad y que se controlaría para prevenir abusos en casos excepcionales.

Esta opción reduciría el riesgo de intromisión de los empresarios en la vida privada de sus trabajadores. Se favorecería también a los empleados, porque se les permitiría saber con seguridad el nivel de confidencialidad que pueden esperar[496].

F) Revisión periódica del cumplimiento

Si las empresas definen y comunican una política de uso de las herramientas de trabajo, pero no realizan control alguno de su cumplimiento se genera una situación de tolerancia empresarial que dificultará la implementación de medidas disciplinarias[497].

7. Mecanismos de protección integral

El incremento de la velocidad de los ordenadores y los nuevos algoritmos de ataque que surgen continuamente hace preciso el aumento constante de la seguridad de los sistemas criptográficos; porque lo que hoy en día es seguro puede que no lo sea al cabo de pocos años[498]. Un nivel de seguridad acorde con los riegos actuales se consigue implantando mecanismos criptográficos de protección integral como los sistemas *DLP*

[496]Recomendación del Grupo de Trabajo "Artículo 29" en Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, pág.23. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/B.2.52-cp--wp55---vigilancia-comunicaciones-electr-oo-nicas-trabajadores.pdf*

[497] AGUSTINA SANLLEGHÍ, J.R.: «¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa? Estudio interdisciplinar sobre políticas de uso de las TIC, prevención y gestión de "conflictos" en una muestra de empresas españolas», *IDP: revista de Internet, derecho y política*, núm. 16, 2013,pág. 15.

[498] FERRÁNDEZ AGULLÓ, F. Tesis doctoral: Sistemas criptográficos de curva elíptica basados en matrices. Universidad de Alicante, 2005, pág. 2. *http://rua.ua.es/dspace/handle/10045/11218*

(*Discrete Logarithm Problem*)[499] que abarcan todas las herramientas informáticas y los medios de seguridad que implementa una compañía con el fin de que sus sistemas informáticos no sean violados y los datos no se pierdan o sean robados[500]. En definitiva, son sistemas que están diseñados para detectar y prevenir el uso no autorizado y la transmisión de información confidencial.

DLP es un sistema que está diseñado para detectar posibles transmisiones irregulares de los datos y evitar, mediante el seguimiento, la detección y el bloqueo de los datos sensibles, mientras que están en uso (acciones de punto final), en movimiento (el tráfico de red), y en reposo (almacenamiento de datos).

Identificación de datos.- Los datos se clasifican como estructurados o no estructurados[501]. Los datos estructurados residen en campos fijos dentro de un archivo, como una hoja de cálculo, mientras que los datos no estructurados se refieren a las libres formas de texto, como en los documentos de texto o archivos PDF.

A) Control de la navegación por Internet

El acceso a Internet en horas de trabajo por parte del trabajador, además del descenso en la productividad que genera, puede también provocar daños y pérdidas ocasionados por los virus informáticos en los ordenadores de la empresa. También la instalación de *software* puede ser perjudicial, pues la descarga de archivos e instalación de programas saturan la capacidad de los equipos informáticos, ralentizan la velocidad de procesamiento y producen errores y bloqueos, generando costes para la empresa.

Es por ello que muchas empresas han optado por usar programas informáticos que registran todo lo que hace su empleado tenga o no interés laboral, de ahí que la doctrina hoy utilice el término "*trabajador transparente o trabajador de cristal"*[502] para

---

[499] Sistema software de prevención de datos comercializado con nombres como *Data Leakage Prevention* o *Data Loss Prevention*.

[500] SANLLEHÍ, J.R. «¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa?» *op.cit.*, pág. 16.

[501] Se estima que el 80% de todos los datos es no estructurado y el 20% estructurados.

[502] SEGOVIANO ASTABURUAGA, M. L: «El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores», *Revista jurídica de Castilla y León*, núm. 2004, págs. 149-156.

hacer referencia a los inminentes mecanismos informáticos de control empresarial que son utilizados por las empresas para controlar lo que está relacionado con el trabajo o lo que no lo está.

Los servidores *proxy*[503] son la herramienta más utilizada para bloquear y filtrar el contenido de la Web, ya sea de manera local en la propia red empresarial o a través del proveedor de Internet. Estos servidores pueden estar implementados en los mismos cortafuegos que utilice la empresa (son de los firewalls existentes los más modernos y punteros).

Se establecen mecanismos que impiden el acceso a determinados sitios web por su contenido claramente no profesional; como redes sociales, páginas de apuestas, pornográficas, redes *peer to peer (P2P)*[504] que provoquen la descarga de contenidos protegidos por derechos de autor y que pueden conducir a la vulneración de leyes de propiedad intelectual; todo ello no será accesible desde los puestos de trabajo.

Los *proxy* no solo chequean páginas webs, sino que también pueden analizar y limitar su uso dependiendo del tráfico utilizado en ese momento[505].

B) Evitación de "pérdidas" y "fugas" de información

Los términos " *pérdida "*y "*fuga de datos*" están estrechamente relacionados y se suelen usar indistintamente, aunque son algo diferentes. Los incidentes de pérdida de

---

[503] Solución *software* implementada para interceptar los mensajes de solicitud HTTP para responder a la demanda en representación de los usuarios de la red corporativa.

[504] Ciertas empresas en Internet ofrecen la posibilidad de subir archivos a sus servidores, por remuneración directa (incrementándose en ese caso el espacio de almacenaje o la velocidad de subida y bajada), o de forma gratuita (con menor espacio y velocidad, y obteniendo beneficios, en ese caso, exclusivamente a través de los ingresos la publicidad). Dichos archivos pueden, en principio, ser de cualquier tipo, pero suelen ser utilizados por los usuarios para almacenar copias de obras de terceros protegidas por el derecho de autor que luego, son puestos a disposición del que lo interese; bien mediante la difusión de los enlaces a tales archivos a través de dichas páginas webs o, en la mayoría de los casos, de otras webs (que no tienen los archivos, solo sus referencias). *Vid*. CASTAÑO MARTÍNEZ, M.S.: «La política cultural y los nuevos canales de acceso a la cultura», *Economía industrial*, núm. 389, 2013, pág.36.

[505] Por ejemplo, en un supuesto en *streaming*, la limitación del tráfico podría suponer que se pudiera ver una determinada página web, pero no reproducir los vídeos que encuentren en ella.

datos, se convierten en incidentes de fuga de datos, en los casos en los que en los medios de comunicación de la empresa que contienen información sensible se pierde esta información, y posteriormente, es adquirida por personas no autorizadas. Sin embargo, una fuga de datos es posible sin que los datos se pierdan en el origen.

Las tecnologías o medios empleados para tratar los incidentes de fuga de datos se pueden dividir en las siguientes: medidas estándar de seguridad, medidas de seguridad avanzadas o inteligentes, control de acceso y encriptación y los sistemas DLP. Las *medidas de seguridad avanzadas* emplean algoritmos de aprendizaje de máquina y razonamiento temporal para detectar el acceso anormal a los datos (por ejemplo, bases de datos o sistemas de recuperación de información) o cambio anormal de correo electrónico, para detectar personal autorizado con fines fraudulentos (*honeypots*[506]) y realizar verificaciones basadas en las actividades habituales para detectar el acceso a los datos anormales (por ejemplo el reconocimiento de las pulsaciones del teclado dinámica[507]). Consisten en monitorear de manera masiva toda la información que fluye: los adjuntos que se envían por correo electrónico, páginas web de almacenamiento en línea, discos duros virtuales, sistemas de mensajería instantánea, etc.

i. Los sistemas DLP

Los DLP son métodos exactos. Implican registro de contenido, cruce de datos exacto y la probabilidad de un falso positivo es casi nula. Todos los otros métodos son imprecisos y pueden incluir: palabras clave, léxicos, expresiones regulares[508], etiquetas

[506] Significa "*tarro de miel".* Cuando un atacante se conecta al servicio y trata de penetrar en él, el programa simula el agujero de seguridad pero realmente no permite ganar el control del sistema. Registrando la actividad del atacante, este sistema recoge información sobre el tipo de ataque utilizado, así como la dirección IP del intruso, entre otras cosas.

[507] Los ritmos de pulsaciones de teclas de un usuario se miden para desarrollar una plantilla biométrica única de los usuarios al escribir patrón para la autenticación futuro. Los datos de temporización de pulsaciones de teclas registrados se procesan luego a través de un algoritmo único, que determina un patrón primario para futuras comparaciones.

[508] Permiten reconocer una serie de cadenas de caracteres que obedecen a un patrón automatizando el proceso de búsqueda de modo que sea posible utilizarlo muchas veces para un propósito específico, a través de una secuencia de caracteres.

de metadatos[509], análisis bayesiano[510], análisis estadísticos, tales como la máquina de aprendizaje[511], etc.

Los sistemas DLP serían recomendables para todas las empresas para prevenir abusos y ataques. El problema es que su coste es elevado y no todas pueden acarrear unos gastos elevados, ni tienen una dimensión que los haga viables. Además hay que tener en cuenta que en España la mayor parte de las empresas son PYMES[512].Los sistemas DLP protegen de las amenazas que son creadas desde dentro de la empresa, y que pueden consistir en fugas o pérdidas de datos:

- A través de los correos electrónicos.
- Por mensajería instantánea.
- Mediante la navegación en páginas no seguras en la Web.

Existen diferentes tipos de sistemas *DLP*, básicamente reconducibles a dos variantes:

A) DLP Red[513]: Consisten en una solución de *software* o *hardware* que está instalado en la red puntos de salida, analiza el tráfico de red para detectar los datos

[509] Son un grupo de datos, llamado recurso. Información que no es relevante para el usuario final pero sí de suma importancia para el sistema informático que maneja los datos que son enviados al mismo junto a la información cuando se realiza alguna petición o actualización de la misma.

[510] En la teoría de la probabilidad el teorema de Bayes es un resultado enunciado en 1763 que expresa la probabilidad condicional de un evento aleatorio A dado B en términos de la distribución de probabilidad condicional del evento B dado A y la distribución de probabilidad marginal de sólo A. Es de enorme relevancia puesto que vincula la probabilidad de A dado B con la probabilidad de B dado A. Hoy en día uno de sus campos de aplicación es el reconocimiento de patrones por ordenador.

[511] Rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas que permitan a los ordenadores a aprender. De forma más concreta, se trata de crear programas capaces de generalizar comportamientos a partir de una información no estructurada suministrada en forma de ejemplos. Es, por lo tanto, un proceso de inducción del conocimiento.

[512] Durante 2016, la PYME española mantiene una particular importancia en su contribución a la generación de empleo empresarial, ocupando al 66, 9% del total de trabajadores. *Vid.* Retrato de las PYMES 2016. Dirección General de Industria y de la Pequeña y Mediana Empresa. Ed. Ministerio de Industria, Energía y Turismo, 2017, pág.3 *http://www.ipyme.org/publicaciones/retrato-pyme-dirce-1-enero-2016.pdf*

[513] Para datos *aka* en movimiento, sistema que procede al cifrado de la sesión de red entera iniciada. Los datos en movimiento son datos que están siendo transmitidos en una red. La mayor amenaza a este tipo de datos son las intercepciones y alteraciones que puedan sufrir. Los datos de su nombre de usuario y contraseña nunca deberían ser transmitidos en una red sin que estar protegidos, ya al igual que los datos de una cuenta bancaria. Si se cifra es la sesión entera de red iniciada, entonces no hay que preocuparse acerca de posibles ataques a los datos que se transmitan en ella.

sensibles que se está enviando en violación de las políticas de seguridad de la información.

B) Punto final DLP[514]: se caracterizan por ejecutarse en estaciones de trabajo de usuarios finales o servidores de la organización. Pueden ser utilizados para controlar el flujo de información entre los grupos o tipos de usuarios por ejemplo, "murallas chinas"[515]. También son capaces de controlar el correo electrónico y la mensajería instantánea de comunicación antes de que se almacenen en el archivo de la empresa, de tal manera que son comunicación bloqueada es decir, que no llega a ser enviada porque el sistema no lo permite.

ii. Legitimación judicial

Un ejemplo de uso de estos servidores, se recoge en la STSJ de Madrid de 27 de enero 2014[516], en la que se declara procedente el despido de un trabajador por haberse detectado que estaba realizando actividades ilícitas que contravienen el código de conducta existente en la empresa al respecto; y, además, suponía un riesgo de fuga de datos, como se recoge en el hecho probado cuarto:

> *"(…) datos de flujo a Internet que no coinciden con las aplicaciones que típicamente deben ser permitidas en el acceso a Internet, y que suponen potenciales puertas de fuga de información o de entrada de troyanos, spyware o zombies (…) se está produciendo la instalación y uso de aplicaciones personales (…) hay tráfico de aplicaciones que pueden ser utilizados para ocultar actividades (…) uso de aplicaciones que pueden conducir a la pérdida de datos (…) uso de aplicaciones utilizadas para comunicaciones personales*".

---

[514] Para datos *aka* en reposo, sistema que ayuda a asegurar y proteger los datos en reposo con el fin de cumplir con los compromisos de cumplimiento y seguridad, con esta característica, se cifran automáticamente los datos antes de continuar a su almacenamiento y los descifra después de la recuperación.

[515] Concepto fue popularizado en Estados Unidos después de la crisis de 1929 , cuando el gobierno promulgó la separación de información entre los bancos de inversión y la bolsa, con el fin de limitar el conflicto de intereses. En la actualidad es un término informático que define a la barrera de seguridad implementada dentro del sistema informático de una organización de la empresa para evitar el intercambio de información que podría causar perjuicios. Por ejemplo, se puede levantar una muralla China para aislar a quienes hacen inversiones de los que están al tanto de la información confidencial que podría influir en las decisiones de inversión.

[516] STSJ Madrid de 27 enero de 2014 (AS 2014\660).

iii. Extracción de datos vía USB

La exportación indebida de datos puede llevarse a cabo utilizando un lápiz de memoria al que se vierten a través de su inserción en el puerto[517].

La STSJ de Madrid de 25 de marzo de 2011[518] confirma el despido disciplinario de la trabajadora que fue descubierta, a través del DLP "*Symantec Data Loss Prevention*" copiando masivamente en un puerto USB, datos confidenciales. Se determina que existe una clara transgresión de la buena fe contractual (art. 54.2 d ET) que justifican el despido aunque no se haya causado un perjuicio económico a la empresa, ni conste obtención de un lucro personal, pero tal conducta constituye una desobediencia grave a las indicaciones de la empresa (art. 54.2.b ET) y se hace merecedora de la máxima sanción del ordenamiento jurídico.

No se disponían de tales medios en el caso que resuelve la STSJ de Madrid de 31 de enero de 2012[519], en la que el recurrente, de profesión ingeniero industrial[520], es despedido de manera disciplinaria. La Sala de lo Social confirma el despido que fue declarado en la instancia, al haberse demostrado que el trabajador ejecutó en diferentes días más de 1.000 accesos a archivos desde su ordenador con la consiguiente copia a un soporte externo USB, que contenía información con detalles referentes al secreto industrial de su empleadora[521]. Resulta sorprendente que una empresa grande y con capacidad económica no invierta en mecanismos informáticos al efecto que impidan fugas de datos.

---

[517] Para evitar almacenar información corporativa en soportes extraíbles o limitar el volumen de lo extraído previo consentimiento de un responsable.

[518] STSJ de Madrid de 25 de marzo de 2011 (EDJ 2011/61673).

[519] STSJ País Vasco de 31 enero de 2012 (AS 2012\2861).

[520] A título de curiosidad, con un sueldo mensual bruto de aproximadamente 13.500 euros.

[521] La empresa recurrida presentó una oferta técnica-económica para la ejecución de unos trabajos que le habían sido requeridos para un proyecto en Bangladesh y sospecharon del recurrente cuando una mercantil de la competencia presentó una propuesta casi igual a la suya, por lo que se auditó el ordenador portátil del trabajador y se comprobó que realizó un uso desviado del mismo.

iv. Capturas de pantalla

En los incidentes de fuga de datos, los datos sensibles se revelan a personas no autorizadas, ya sea por dolo o error involuntario. Tales datos sensibles pueden ser muy variados, dentro de la información privada de la empresa: relativos a la propiedad intelectual, al secreto industrial, a información financiera, datos de tarjetas de crédito, etc.

v. Sistemas de seguridad

Algunos sistemas de seguridad de red[522]relacionados con la prevención de fuga de datos son los siguientes: *information leak detection and prevention* (ILDP[523]), *information leak prevention* (ILP[524]), *content monitoring and filtering*(CMF[525]), information protection and control(IPC[526]), y *extrusion prevention system*el (EPS[527]), como oposición a *Intrusion prevention systems* (IPS[528]), también conocido como *intrusion detection and prevention systems* (IDPS[529]).

7. Vigilancia oculta

A) Idea general

En los casos en que la empresa tiene claras sospechas de que un trabajador transgrede la buena fe contractual, se obvia la información a los trabajadores, respecto al control que se va a realizar, pues no obedece al propósito genérico de vigilar y controlar a los trabajadores, sino que responde a unas circunstancias muy concretas la existencia de sospechas sobre graves irregularidades o actividades fraudulentas en la empresa, y en

[522]Disposiciones y políticas adoptadas por administrador de red para prevenir y controlar autorizado el acceso, uso indebido, modificación o rechazo de una red de ordenadores y recursos de la red accesible. Consiste en monitorizar la red y las actividades del sistema de actividad. Las funciones principales de los sistemas de prevención de intrusión son identificar la actividad fraudulenta, informar sobre esa actividad de registro, intentar bloquear / detenerlo y notificarlos.

[523] Información de detección de fugas y la prevención.

[524] Prevención de fuga de información.

[525] Monitorización y filtrado de contenido.

[526] Protección y control de la información.

[527] Sistema de prevención de extrusión.

[528] Sistema de prevención de intrusiones.

[529] Sistema de prevención y detección de intrusiones.

la necesidad de grabar o fiscalizar el ordenador del trabajador que ha transgredido la buena fe, o a través de la videovigilancia oculta como recoge la STC 39/2016, de 6 de marzo[530].

Como ha subrayado el Tribunal Constitucional, en este tipo de controles, la necesidad de secreto está implícita. Una doctrina avalada por el Tribunal Constitucional, como ya hemos visto en la en la STC 186/2000, de 10 julio[531], que considera ajustada a Derecho la instalación "*de modo completamente secreto"* del circuito de televisión que enfoca a cajas registradoras, y su fin es "*controlar un acusado descuadre en caja"* y que no fue puesto en conocimiento de los trabajadores ni del comité de empresa, "*por el razonable temor de la empresa de que el conocimiento de la existencia de la filmación frustraría la finalidad apetecida* ".

C) Criterios judiciales

Al amparo de esta doctrina constitucional, un número notable de decisiones ha considerado lícita la instalación por parte de la empresa de labores de seguimiento ocultas y observación de trabajadores sospechosos.

En muchas de las sentencias analizadas, el uso personal del ordenador no constituye el incumplimiento principal, sino que es, simplemente, el medio que se utiliza por la empresa para probar un incumplimiento más grave que es el que provoca el despido, normalmente porque el trabajador ha utilizado también el ordenador como medio para cometer la infracción.

D) Razones del control oculto

Por tanto, los controles ocultos son únicamente aceptables cuando se cumplen estos dos requisitos: 1º) Pretenda ponerse en evidencia la conducta ilícita de un concreto trabajador, sobre el que se tienen razonables y fundadas sospechas. 2º) Que "*no exista*

[530] STC 39/2016, de 3 marzo (RTC 2016\39).
[531] STC 186/2000, de 10 de julio (RTC 2000\186).

otro medio de descubrir al infractor"[532] . ¿Pero qué cabe entender por razones fundadas? No basta con la mera sospecha para inspeccionar los datos personales del trabajador, pues por encima de cualquier interés patrimonial se encuentra el respeto a la dignidad y al honor de la persona. La sospecha ha de venir fundada en un acto de deslealtad del trabajador, es decir, debe haber indicios razonables de sospechas que en su caso se puedan probar.

El problema reside en qué cabe entender por "deslealtad". Para un sector de la doctrina, la sospecha debe venir fundada en un acto punible, en una conducta delictiva, y motivada por pruebas e indicios serios, no por simples comentarios que pueden ser ciertos o no[533]. Mientras que, para otro sector, únicamente, consiste en desobedecer las órdenes empresariales produciéndose una transgresión de la buena fe empresarial y no es necesario nada más, no es preciso que la conducta pueda ser considerada delictiva.

Estos dos presupuestos de hecho aludidos se dan en la ya comentada STC 170/2013, de 7 de octubre[534], en la que se invadió el derecho a la intimidad del trabajador, fiscalizando el correo electrónico del mismo, ante indicios de transgresión de la buena fe contractual, que es el título legitimador. Se trataba de que a la empresa le habían proporcionado "*indicios razonables*" de que el trabajador traspasaba información confidencial de la empresa a personal de otra entidad mercantil, utilizando en dicha transmisión medios que eran propiedad de la empresa, en concreto, teléfono móvil y correo electrónico. Se demostró que desde el correo electrónico corporativo, el demandante había transmitido todos los datos relativos a la previsión de la cosecha de dos años una empresa de la competencia. La expresa prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales llevaba implícita la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales,

---

[532] *Vid.* FERNÁNDEZ VILLAZÓN, L. A.: «Las facultades empresariales de control de la actividad laboral». *op. cit*., pág. 49, señala que además circunscribe tales controles ocultos "*defensivos*" a la persecución de delitos y de las faltas laborales más graves.

[533] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op. cit.*

[534] STC 170/2013, de 7 de octubre (RTC 2013\170).

incluida la adecuación de su prestación a las exigencias de la buena fe en base a los arts. 5.a y 20.2 y 3 ET.

Doctrina especializada considera que el criterio general de la doctrina no se ve alterado por la STC 170/2013, de 7 de octubre[535], sino que convalida lo mantenido en las SSTS de 26 de septiembre 2007[536] y de 6 de octubre de 2011[537], en el sentido de que una vez establecidas las reglas de uso, su incumplimiento por parte del trabajador justifica una auditoría sin conocimiento del mismo y es ilícita la prueba obtenida tras una auditoría de los ordenadores, sin haber establecido esas reglas[538].

III. DECISIONES DISCIPLINARIAS: ACREDITACIÓN Y SANCIÓN DE INCUMPLIMIENTOS

De los controles ordenados a verificar el uso inadecuado de los instrumentos tecnológicos del empresario puede derivar el descubrimiento o la comprobación de que efectivamente el trabajador los usa para fines personales, cuando en el ámbito de la empresa en la que trabaja existe una prohibición expresa; o bien los utiliza de manera abusiva o indebida. De dicha verificación puede seguirse como efecto, la imposición de una sanción que cabrá, en función de las circunstancias concurrentes en cada caso, pudiendo alcanzar la máxima del despido disciplinario, si llegara a integrar plenamente el supuesto de transgresión de buena fe contractual previsto en art. 54.2 d) del ET.

[535] *Ibídem.*

[536] STS 26 de septiembre de 2007 (RJ 2007\7514).

[537] STS 6 de octubre de 2011 (RJ 2011\7699).

[538] FOLGUERA CRESPO, J.A.: «¿Puede el empresario controlar los ordenadores y correos electrónicos de sus empleados? (STC 170/2013, as.”ALCALIBER”)», *op. cit.*, pág.53.

1. La prueba de los incumplimientos

A) Nulidad de pruebas ilícitas

La regla de exclusión de la prueba obtenida con violación de derechos fundamentales no es una creación de nuestro Tribunal Constitucional. Esta importante prohibición tiene sus orígenes más remotos en el Derecho Romano, con la formulación del principio que proscribía el aprovechamiento de los resultados del propio comportamiento ilícito[539]; debe su formación a la labor realizada por los diferentes autores del S. XIX y estando presente en la mayor parte de los países civilizados.

El proceso no es una institución jurídica autónoma e independiente sino que se halla inmerso en la jerarquía de valores propia del Estado de Derecho y en esa jerarquía se encuentran, en primer lugar, los derechos fundamentales, como condensación de la dignidad y libertad de la persona; por lo que la verdad procesal, valor necesariamente secundario, solo puede alcanzarse a través de procesos compatibles con los derechos fundamentales, nunca con su vulneración.

Una cuestión de especial importancia es que la nulidad por vulneración de libertades públicas y derechos fundamentales del trabajador, puede producirse cuando la decisión se fundamente en pruebas obtenidas con transgresión de esos derechos y libertades.

B) Pruebas ilícitas e ilegales

Se deben diferenciar dos supuestos: El primero, que la empresa obtiene los elementos de convicción vulnerando derechos fundamentales o libertades públicas y esos elementos son los que llevan a aplicar una medida sancionadora por parte del empresario. En tal caso, la relevancia de los mismos en la decisión empresarial es obvia y está plenamente justificada la nulidad de la sanción. El segundo supuesto, cuando el empleador sanciona en base a medios lícitos, o que no suponen vulneración alguna, pero luego *a posteriori*, ante la reclamación del trabajador, realiza averiguaciones en las que

[539] «*Nemo ex suo delicto meliorem suam conditionem facere potest*», esto es, nadie puede mejorar su condición por su propio delito (Digesto, L: XVII, 134, 1).

sí se vulneran los derechos de su empleado. En este caso, la violación por parte del operario no parece que contamine la sanción llevada a cabo[540].

Lo que nos lleva a realizar una delimitación entre la prueba ilícita y la prueba ilegal. Una medida de control empresarial puede constituir una infracción, por vulnerar alguna regla de ejercicio sobre ese control, pero no constituirá una prueba ilícita aunque sí constituirá una prueba ilegal si no ha vulnerado un derecho fundamental del trabajador. La prueba simplemente ilegal es a la que se refiere el art. 283 LEC cuando establece que "*nunca se admitirá como prueba cualquier actividad prohibida por la ley"*. La prueba ilegal lleva a una decisión en el marco del proceso, no debe admitirse su práctica.

En el supuesto de la prueba ilícita, se va mas allá, ni debe ser admitida por el juez su práctica, ni deben ser aceptadas por el juez sus resultados fácticos, en el caso de haberse practicado fuera del proceso. Con lo que puede haber una decisión de inadmisión de prueba, como una decisión de exclusión de sus resultados a la hora de la valoración.

Por tanto, aunque la prueba ilícita haya acreditado el hecho, se tendrá esta por no aportada. La exclusión es amplia porque afecta a los efectos directos e indirectos de la violación, lo que establece "*una cadena de contaminación*", en el sentido de que se produce la anulación de los resultados de una prueba licita, si tiene su origen en una ilícita. El hecho, sin embargo, podrá, acreditarse por otras pruebas que no tengan conexión con la violación del derecho fundamental.

E) Jurisprudencia constitucional relevante

La doctrina especializada señala que un hito en su momento lo supuso la STC 114/1984, de 29 de noviembre[541], que tiene el mérito de haber marcado un cambio de rumbo en el tratamiento en nuestro país de la prueba obtenida con violación de derechos fundamentales, pues hasta la fecha los jueces estaban obligados a admitirla si era relevante para el caso en cuestión. Pero, a partir de esta importante sentencia, no han de

---

[540] ALFONSO MELLADO, C.L.: «Despido, prohibición de discriminación y derechos fundamentales» en AA. VV. SALA FRANCO (Coor.) *Libro Homenaje a Abdón Pedrajas Moreno ,op.cit.*, págs. 56-57.

[541] STC 114/1984, de 29 de noviembre (RTC 1984\114).

prestarle ningún valor[542]. Se trataba de un caso de grabación fonográfica de la conversación por el interlocutor y su admisión como prueba en un proceso laboral por despido y aunque el juez, finalmente denegó el amparo, estimando que no hubo lesión de derecho fundamental, en esta sentencia se estableció como principio la imposibilidad de valorar procesalmente la prueba obtenida con violación de derechos fundamentales, "*como una expresión de una garantía objetiva e implícita en el sistema de los derechos fundamentales*". Se encuadra el secreto de las telecomunicaciones dentro de una naturaleza dependiente y funcional, en la que el derecho a la libertad de las telecomunicaciones actúa como instrumento de garantía[543].

F) El artículo 11.1 LOPJ

Esta es también la tesis que luego fue acogida expresamente en el art. 11. 1, inciso segundo LOPJ, respecto a las reglas de exclusión de las pruebas obtenidas mediante la vulneración de derechos fundamentales. El tenor literal del precepto dice así:*" No surtirán efecto las pruebas obtenidas, directa o indirectamente violentando los derechos o libertades fundamentales".* De ello se deduce que hay prueba ilícita cuando existe lesión de un derecho fundamental, eso sí, la prohibición de valorar en acto de juicio pruebas obtenidas con violación de los derechos fundamentales no se encuentra de manera expresa en la Constitución Española, ni puede afirmarse que tampoco forme parte del contenido esencial de cada uno de los derechos constitucionales.

El Tribunal Constitucional viene considerando desde hace ya muchos años, con el respaldo de la inmensa mayoría de la doctrina, que dicha regla constituye una garantía que se deduce del conjunto de la regulación constitucional sobre derechos fundamentales. Esta regla se repetía en el art. 90.1 LPL y se recoge hoy en el art. 90.2 LRJS, en línea con lo que ya establecía el artículo 287 LEC.

---

[542] GALVEZ MUÑOZ, L.: «La ineficacia de la prueba obtenida con violación de derechos fundamentales. Normas y Jurisprudencia (TEDH,TC,TS,TSJ y AP) en los Ámbitos Penal, Civil , Contencioso- Administrativo y Social» *Cuadernos Aranzadi de Derecho Constitucional* núm. 10, 2003, pág. 49 (BIB 2002\2566).

[543] RODRÍGUEZ LAINZ, J.L: «Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013 de 7 de octubre)» *op.cit.*

Los destinatarios últimos de esta norma de exclusión son los jueces, que no pueden otorgar relevancia jurídica alguna al material probatorio obtenido con violación de derechos fundamentales y en consecuencia, no es posible hacer uso del mismo, como base o fundamento de ninguna actuación judicial. En caso contrario, estarían a su vez lesionando el derecho a un proceso con todas las garantías y el principio de igualdad de partes.

A *sensu contrario*, solo las pruebas obtenidas legítimamente, a saber con observancia de las garantías constitucionales y legales, pueden fundar una sentencia ajustada a derecho.

G) El debate sobre nulidad de la prueba y del acto inducido

Obsérvese que se discute sobre la validez o no de una prueba; en particular, ello significa que a la hora de realizar la calificación del despido, será la que proceda, según lo articulado por la prueba que al final se considere válida, y según lo dispuesto en el art. 108 LRJS. Para la mayor parte de la doctrina, la nulidad de la prueba no se extiende al despido, en cuya calificación han de ponderar las causas que han motivado la decisión empresarial, no la forma como ha intentado acreditarse su procedencia o investigarse la conducta del trabajador.

La doctrina más especialiada afirma que en los supuestos de que se trate de la única prueba de cargo, la simple declaración de invalidez de la prueba, si no va acompañada de privación de cualquier efecto extintivo, no restituye al trabajador en la integridad de su derecho vulnerado, por lo que se debe determinar el despido nulo[544].

[544] GOÑI SEIN, J.L.: *La Videovigilancia empresarial y la protección de datos personales*, *op. cit.*, pág. 248.

4. Transgresión de la buena fe contractual por uso irregular de las nuevas tecnologías

El deber de buena fe impone al trabajador obligaciones de hacer (colaboración en el trabajo, aviso de contratiempo, riesgos, etc.) y de no hacer (revelación de secretos, engaño, fraude, hurto, aceptación de sobornos, etc.). El deber de buena fe conecta otras obligaciones legales (no competencia desleal especialmente) o contractuales (no competencia después del contrato de trabajo, permanencia en la empresa).

A) La buena fe: delimitación conceptual

La buena fe es un principio general del Derecho recogido en el art. 7 CC, que se supone en el contratante y que hay que proteger. La buena fe se integra en el contrato por imposición del art. 1258 CC que dice lo siguiente: ”*Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no solo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley”.*

La integración consiste en extraer consecuencias complementarias concordes con el conjunto del ordenamiento, aun cuando no estuvieran expresamente previstas en el contrato. Puede suponer la agregación de derechos y obligaciones no contemplados por las partes, ni por las leyes dispositivas, la sustitución de estipulaciones pactadas o incluso la nulidad de alguna de las cláusulas. Se trata de algo más que la mera interpretación. Y en ámbito laboral, las obligaciones que derivan para el empresario y el trabajador se hallan sometidas a la buena fe, al ser parte del contenido contractual, su transgresión por parte del trabajador, es un incumplimiento del contrato de trabajo que puede dar lugar a la acción de extinción contractual por despido disciplinario (art. 54. 2 d ET).

El Estatuto de los Trabajadores establece el deber general del empresario de actuar de buena fe, lo que determina la interdicción a la arbitrariedad en su actuación; un comportamiento de control de la actividad del trabajador, que sea transgresor de la buena fe contractual por parte del empresario, puede dar lugar al recurso del trabajador al

mecanismo de la extinción contractual, *ex* art. 50 ET, en este sentido STSJ Cataluña de 11 junio 2003[545].

La buena fe marca la pauta de conducta a seguir en la relación de trabajo. Es consustancial al contrato de trabajo que por su naturaleza sinalagmática genera derechos y deberes para ambas partes, por lo que la transgresión de la buena fe constituye una actuación contraria a los especiales deberes de conducta que han de presidir el contrato de trabajo de acuerdo con los artículos 5 a) y 20.1 ET, la esencia del incumplimiento no está en el daño causado, sino en el quebranto de la confianza depositada y la lealtad debida, al configurarse la falta por ausencia de valores éticos, lo que no queda enervado por la ausencia de perjuicio a la empresa o lucro personal. No es necesario que la conducta tenga carácter doloso, también se engloban acciones culposas cuando la negligencia sea grave e inexcusable.

La buena fe implica, como hemos dicho, derechos y deberes recíprocos para las partes, que se concretan en el deber de mutua fidelidad entre el empresario y el trabajador, en una exigencia de comportamiento éticamente protegido y exigible en el ámbito contractual[546].

No cabe defender la existencia de un deber genérico de lealtad con un sentido omnicomprensivo de sujeción del trabajador al interés empresarial, pues ello no es acorde con el sistema constitucional de relaciones laborales (STC 120/1983, de 15 de diciembre[547]) de manera que, aunque un efecto típico de la relación laboral sea supeditar ciertas actividades a los poderes empresariales, no basta con la sola afirmación de interés empresarial para restringir los derechos fundamentales del trabajador, dada la posición su prevalente. De ahí que sea necesario atender a las circunstancias concretas del caso y realizar sobre ellas una ponderación adecuada (STC 151/2004, de 22 de octubre[548] y STSJ de 18 enero 2017[549]).

---

[545] STSJ Cataluña de 11 junio 2003 (EDJ 2003/71487).

[546] MONTOYA MELGAR, A. *La buena fe en el Derecho del Trabajo*, ed. Tecnos, 2001, pág. 35.

[547] STC 120/1983, de 15 de diciembre (EDJ 1983/120).

[548] STC 151/2004, de 22 de octubre (EDJ 2004/135035).

[549] STSJ Castilla y León de 18 enero 2017 (EDJ 2017/4794). El TSJ entiende que no consta que las presuntas irregularidades en la conducta de la actora haya supuesto un perjuicio notorio y grave para la empresa, no pudiendo calificarse la mismas como fraude, deslealtad o abuso de derecho al no existir comportamiento malicioso por parte de la misma; conducta a la que sólo cabría imputarle una cierta

B) La buena fe y el uso de TICs

El TS cuenta con una elaborada doctrina sobre el deber de buena fe; es consustancial al contrato de trabajo y se concreta en una exigencia de comportamiento ético jurídicamente protegido y exigible en el ámbito contractual, plasmándose en directivas que suponen valores como la lealtad, honorabilidad, probidad y confianza[550].

Configurado ya el deber de buena fe, su relación con los medios empresariales y los criterios de aplicación para detectar la conducta desviada del trabajador, se pueden sintetizar en:

- Infringe el deber de buena fe la utilización de un instrumento de trabajo facilitado por la empresa para actividades ajenas a esta, salvo autorización expresa.

- Como regla general, el permiso no puede presumirse, ya que no responde a la finalidad con la que la empresa adquiere el elemento en cuestión y la entrega al trabajador[551].

C) El abuso de confianza

El abuso de confianza es una modalidad cualificada de la transgresión de la buena fe contractual, consistente en el uso desviado de las facultades conferidas, con riesgo o lesión de los intereses de la empresa, el trabajador utiliza en beneficio propio la confianza que en él tenía depositada su empleador. En realidad, esta causa opera como un cajón de sastre para multitud de conductas vulneradoras de la buena fe que no alcanzan a encontrar una tipificación más detallada. Una manifestación especial de la buena fe es el respeto de la confianza que va implícita en ciertos encargos o ciertos puestos de trabajo, por la

---

negligencia, pero en ningún caso mala fe, por lo que la misma no se puede considerar fraudulenta o abusiva en el puesto de trabajo, y, por consiguiente, tal sanción por despido se ha de calificar como manifiestamente desproporcionada.

[550] SEMPERE NAVARRO, A.V. y MATEOS y de CABO, O. :«Uso y control de herramientas informáticas en el trabajo (Marco legal, pautas judiciales convencionales) La buena fe» en AA. VV. SAN MARTÍN MAZZUCCONI, C. (DIR): *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, pág. 151.

[551] AGUT GARCÍA, C.: «Las facultades empresariales de vigilancia y control sobre útiles y herramientas de trabajo y otros efectos de la empresa» en AA. VV. VICENTE PACHÉS, F. (Coor.): *El control empresarial en el ámbito laboral*, ed. CISSPRAXIS, 2005, págs 111-114.

singularidad de las tareas (dirección, mando) o porque exigen una especial responsabilidad (vigilancia, contabilidad).

El examen de las sentencias dictadas en la materia nos lleva a encuadrar en el abuso de confianza en el puesto de trabajo como analizaremos de manera detallada en la parte especial, las utilizaciones abusivas de Internet, o del correo electrónico con fines lúdicos, o excesos en la comunicación personal, que provocan una reducción del tiempo de trabajo. A estos casos les es de aplicación el art. 54.2 d ET.

Doctrina especializada explica que en la transgresión de la buena fe contractual la esencia del incumplimiento no está en la causación de un daño, sino en el quebranto de la lealtad, honorabilidad, probidad y confianza, por lo que la inexistencia de perjuicio alguno a la empresa o de lucro personal no enerva la transgresión. Señala, no obstante, que cualquier uso irregular de las nuevas tecnologías no es causa para despedir[552].

D) Doctrina gradualista

La teoría gradualista busca la necesaria proporción entre la infracción y la sanción, aplicando un criterio individualizador, que valora las peculiaridades de cada caso concreto; pues el despido, como máxima sanción que cabe en el marco de la relación laboral, debe reservarse para aquellos comportamientos graves y culpables de especial significación que encajen dentro de los supuestos que el Estatuto de los Trabajadores contempla, siendo necesario para calificar su procedencia conjugar todos los factores de relevancia, como son la existencia de dolo o culpa, la intensidad de la falta, las circunstancias concurrentes de toda índole.

Aplicado ello al uso indebido de las nuevas tecnologías, significa que se debe ponderar el perjuicio que causa, si el incumplimiento se hizo en la jornada de trabajo, si existe manera de medir la pérdida económica, etc. Asimismo, que se ha de valorar el modo en que la empresa controla este tipo de conductas, y reacciona ante ellas; no es lo mismo una clara prohibición por parte del empresario, que un ambiente generalizado de permisión al cumplimiento[553].

---

[552] THIBAULT ARANDA, J.: *Control Multimedia de la Actividad Laboral, op. cit.* ,pág.71.

[553] AGUT GARCÍA, C. :«Las facultades empresariales de vigilancia y control sobre útiles y herramientas de trabajo y otros efectos de la empresa» en AA. VV. VICENTE PACHÉS, F. (Coor). *El control empresarial en el ámbito laboral*, *op.cit*., págs. 111-114.

Algunos autores entienden incluso que menores connotaciones de gravedad a la hora de valorar la conducta tiene la visita a páginas deportivas durante tiempo de trabajo, que el mismo tiempo empleado en lugares de contenido erótico o pornográfico. Cuestionan este extremo pues que se considere incumplimiento una visita informática a una página de revista "*caliente"* y se admita sin problemas similar conducta a acceder a una web de un equipo futbolístico o de una asociación excursionista es un reproche moral que no debería trascender a lo jurídico[554]. Otros sectores consideran que el concreto contenido de las comunicaciones no puede pasar totalmente desapercibido como factor agravante de la conducta[555].

La teoría gradualista cuenta con mayores defensores que detractores, salvo que tal actividad del trabajador tenga un coste económico para la empresa o el tiempo dedicado sea muy elevado, en definitiva, conductas que supongan una clara transgresión de la buena fe contractual. Fuera de estos supuestos, el resto de conductas, suponen simples distracciones de las tareas del trabajador, cuya calificación jurídica ha de realizarse con arreglo a los estándares o patrones de conducta exigibles, lo que depende, por otro lado y en gran parte de la política empresarial establecida.

E) Doctrina judicial discordante

Respecto de si en materia de transgresión de buena fe y abuso de confianza es posible acoger la teoría gradualista de la infracción los Tribunales se pronuncian en ambos sentidos.

Tesis gradualista.-A favor de la teoría gradualista , y aunque aceptando la ilicitud de la conducta se considera improcedente el despido, respecto al uso de privado de correo electrónico o Internet. Salvo que se acredite que dicho uso ha sido anormal, ha implicado coste económico para la empresa o ha tenido una finalidad o modalidad ilícita. Si el uso no ha sido excesivo, se aplica la teoría gradualista en los siguientes supuestos: trabajador que envía dos correos electrónicos con contenido pornográfico (STSJ Madrid

[554] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C.: Nuevas tecnologías y Relaciones Laborales, *op. cit.*, pág.55.

[555] THIBAULT ARANDA, J.: Control Multimedia de la Actividad Laboral, *op.cit.* pág.77.

de 11 de mayo de 2004[556]); el envío de correos electrónicos que ocuparon un tiempo de 48 minutos en dos meses (STSJ de Valencia de 7 de octubre de 2008[557]).

También se ha aplicado a la visita de páginas web y el uso del ordenador con fines particulares.- Estas conductas, para ser sancionables, han de implicar, o bien un coste económico para la empresa, por ejemplo cuando la consulta exige una conexión tarifada por tiempo con la compañía telefónica o un proveedor de servicios ISP, o bien un abandono de las tareas laborales con disminución del rendimiento. En este último caso la disminución del rendimiento ha de ser valorada conforme a la teoría gradualista y a la tipificación contenida en los convenios colectivos, se aplica la teoría gradualista en los siguientes supuestos: el intento sin conseguirlo un único día de reiniciar el ordenador varias veces para usarlo para algún fin particular (STSJ de Las Palmas 23 de mayo de 2006[558]), la visita a páginas web por ser una conducta tolerada por la empresa (STSJ de Madrid de 9 de diciembre de 2004 [559]).

Gravedad intrínseca.- Por el contrario, no se puede aplicar la teoría gradualista , si nos hallamos ante un caso claro transgresión de la buena fe contractual caracterizada por la necesaria lealtad y confianza que ha de observarse en la relación laboral (STSJ de Madrid de 26 de enero de 2015 [560]) o cuando la conducta causa perjuicios por bloquearse la red empresarial debido al uso abusivo (STSJ de Cataluña de 22 de julio de 2004[561]).

[556] STSJ Madrid de 11 de mayo de 2004 (EDJ 2004/109501).
[557] STSJ de Valencia de 7 de octubre de 2008 (EDJ 2008/261120).
[558] STSJ de Las Palmas 23 de mayo de 2006 (EDJ 2006/18680).
[559] STSJ de Madrid de 9 de diciembre de 2004 (EDJ 2004/204807).
[560] STSJ de Madrid de 26 de enero de 2015 (EDJ 2015\16515).
[561] STSJ de Cataluña de 22 de julio de 2004 (EDJ 2004\93282).

5. Desobediencia en relación con el uso de las nuevas tecnologías

El poder de dirección empresarial no es un poder omnímodo o absoluto, pues los propios preceptos mencionados parten de que las órdenes empresariales hayan sido dictadas *"en el ejercicio regular de sus facultades directivas"*[562] .

Por desobediencia se entiende no sólo la actitud de rebeldía abierta y enfrentada contra las órdenes recibidas del empresario en el ejercicio regular de sus funciones directivas (STS de 24 de febrero de 1986[563]), sino también el acto de incumplimiento, consciente y querido, de las obligaciones que el contrato de trabajo entraña para el sujeto trabajador (STSJ de Galicia de 29 de marzo de 2011[564]) La desobediencia ha de darse frente a las órdenes del superior, que tenga competencia para ello, y han de ser claras y concretas, dentro del ámbito de la empresa y en el área de sus facultades, de manera que es necesario que se trate de un incumplimiento.

En nuestro sistema de relaciones laborales, el poder de dirección de la empresa viene atribuido al empresario *ex* art. 20 del ET, uno de los deberes laborales que se impone en el art. 5. c) ET al trabajador es el de "*cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas",* constituyendo su incumplimiento causa legítima para proceder a su despido disciplinario , como recoge el art. 54.2 b) ET.

El deber de obediencia es una manifestación del deber de buena fe contractual y se traduce en la necesidad de asumir o aquietarse a las órdenes e instrucciones recibidas por el empresario "*conformadoras del normal devenir de la actividad laboral*", en definitiva, el trabajador no puede "*erigirse en definidor de sus propias obligaciones contractuales"*[565].

---

[562] LLUCH CORELL, F. J.: «El poder de dirección del empresario y el *ius resistentiae* del trabajador. Respuesta de los tribunales», *Revista de Jurisprudencia El Derecho*, núm. 3, 2005 pág.5 (EDB 2005/171178).

[563] STS de 24 de febrero de 1986 (EDJ 1986\1208).

[564] STSJ de Galicia de 29 de marzo de 2011(EDJ 2011\78253).

[565] ASQUERINO LAMPARERO, Mª. J.: «El derecho de resistencia frente al poder de dirección», *Revista Doctrinal Aranzadi Social* núm. 8, 2012 (BIB 2012\3372).

Hemos de partir de la idea -presunción *iuris tantum*- de que la orden emitida por el empresario es legítima, no siendo el trabajador la persona llamada a "*evaluar con sus propios criterios la regularidad de la orden empresarial*" (STSJ de Castilla La Mancha de 6 de julio de 2006[566]); esto es, el trabajador no puede despojarse de su condición de prestador de servicios por cuenta ajena y asumir una posición de organización que tan sólo le compete al empresario.

IV. APUNTE DE DERECHO COMPARADO

Esta Parte Primera, sobre bases conceptuales y contexto del tema, bien podría concluir sin más puesto que solo pretendemos examinar el sistema español. Ahora bien, con la exclusiva finalidad de servir como piedra de toque, hemos optado por incorporar un breve apunte sobre dos sistemas extranjeros bien distintos: el portugués y el estadounidense.

Como es sabido, a diferencia de que ocurre en los países del *common law*, donde el legislador ha sido particularmente incisivo en la regulación del uso de las nuevas tecnologías en el trabajo, los ordenamientos del *civil law*, que por tradición estaban más llamados a hacerlo, parecen haber optado, en mayor o menor medida, por el abstencionismo legal, confiando al buen juicio de sus tribunales la solución de estos conflictos y también, por tanto, la regulación de estas cuestiones.

El Estatuto de los Trabajadores es mucho "*más evanescente*" que los ordenamientos de nuestro entorno al no entrar el legislador a valorar en concreto los posibles conflictos que puedan plantearse entre la utilización de medios mecánicos de vigilancia y control de la actividad laboral y el derecho a la protección del trabajador.

[566] STSJ de Castilla La Mancha de 6 de julio de 2006 (EDJ2006\299878)

1. Derecho Portugués

A) Regulación general

La Ley básica en el ámbito del Derecho Laboral es el "Código do Trabalho"[567], que ha sido objeto de una duodécima revisión muy reciente[568], introduciendo algunos cambios en la Ley 7/2009, de 12 de febrero. Existen también un conjunto de reglamentos que, junto con esta ley, rigen las actividades laborales.

Dentro del Código do Trabalho en los arts. 14 a 22 se recoge una subsección llamada *Direitos de personalidade*[569], de los que merece destacare el art. 20.1[570], que recoge la prohibición genérica del uso de las nuevas tecnologías con fines de controlar la actividad de los trabajadores[571], con las siguientes excepciones:

- Por motivos de protección y seguridad de las personas o por requisitos específicos inherentes a la naturaleza de la orden de la actividad empresarial (art. 20.2).
- Si el empleador informa al empleado acerca de la existencia y el propósito de los métodos de vigilancia utilizados y, en particular, consigna las siguientes palabras en lugares sujetos a videovigilancia , según el caso: "*Este sitio está bajo la supervisión de un circuito televisión cerrada*" o bien "*Este lugar está bajo la vigilancia de un circuito cerrado de televisión que procede a la grabación de imagen y sonido*", seguido de la identificación de símbolo (art. 20.3)[572].

---

[567] *http://www.cite.gov.pt/pt/legis/CodTrab_LR1_002.html#L002S3*

[568] Ley núm. 28/2016 de 23 de agosto, modifica el *Código do Trabalho*, aprobado por la Ley núm. 7/2009, de 12 de febrero.

[569] Derechos de la personalidad.

[570] Art. 20 *"Meios de vigilância a distância*

1 - O empregador não pode utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador".

"*El empleador no puede utilizar mecanismos a distancia para vigilancia en el lugar de trabajo, a través del uso de medios tecnológicos, con el fin de controlar el funcionamiento de trabajo de los empleados*".

[571] Se considera infracción administrativa muy grave la violación del párrafo 1.

[572] Constituye infracción administrativa de la violación del párrafo 3.

Si el control se ejerce sobre el uso de las nuevas tecnologías de la información y comunicación propiedad de la empresa, ha de tenerse en cuenta la limitación que deriva del art. 21 del Código do Trabalho que establece que para proceder al uso de medios de control a distancia el empresario ha de solicitar autorización de la Comisión Nacional de Protección de Datos (art. 21.1) [573]y sólo podrá concederse si es necesaria, adecuada y proporcionada a los objetivos perseguidos el uso de los medios de comunicación (art. 21.2).

Con respecto a los datos personales recogidos a través de estos medios de control a distancia se recoge que han de mantenerse durante el tiempo necesario para la continuación de la utilización de los fines para los que están destinados, y se deben destruir en el momento del traslado del trabajador a otro puesto de trabajo o la terminación del contrato de trabajo (art. 21.3).

El art. 22 del Código do Trabalho respecto a los mensajes de los trabajadores y el acceso a la información de los mismos, reconoce el derecho a la reserva y a la confidencialidad sobre el contenido de la naturaleza personal de los mensajes y acceso a la naturaleza no profesional de la información que envía, recibe o ve, en particular, por correo electrónico (art. 22.1). Y matiza en el párr. 2 que "*el párrafo anterior no restringe la facultad del empleador de establecer normas para el uso de los medios de comunicación en la empresa, incluyendo la dirección de correo*".

A) Videovigilancia

El Supremo Tribunal de Justiça en sentencia de 8 de febrero de 2006[574] declaró que la instalación de sistemas de video vigilancia en el lugar de trabajo implicaba la restricción del derecho de privacidad y sólo podían aparecer cuando se justificara como necesaria para la consecución de los intereses legítimos y dentro de los límites establecidos por el principio de proporcionalidad.

[573] La solicitud de autorización mencionada en el apartado 1 deberá ir acompañada de un dictamen previo del comité de empresa en caso de incumplimiento de este aspecto se produciría una infracción administrativa grave

[574] Supremo Tribunal de Justiça. Proc.: 05S3139. Pte.: FERNANDES CADILHA

El empleador puede utilizar medios de monitorización de la distancia cuando tiene como finalidad la protección y seguridad de las personas y de los bienes y debe entenderse, sin embargo, que esta posibilidad se limita a los lugares abiertos al público o de los espacios de acceso a personas ajenas la empresa, donde hay un riesgo razonable de los delitos contra las personas o contra la propiedad.

Por otro lado, ese uso debe dar lugar a una forma de vigilancia general, para detectar hechos, situaciones o eventos fortuitos, no una vigilancia dirigida directamente al puesto de trabajo o en el campo de acción de los trabajadores.

Los mismos principios se aplican incluso si la base de la autorización para la recogida de grabación de imágenes se compone de un riesgo potencial para la salud pública que puede venir desde el interior de las instalaciones de la entidad de desviación de drogas dedicadas a la actividad farmacéutica.

Por tanto, sentadas las premisas anteriores, es ilegal por ir contra la privacidad la captura de imágenes a través de las cámaras de vídeo instaladas en el lugar de trabajo y dirigidas a los trabajadores, de manera continua y permanente sin causa que lo justifique.

El visionado de las imágenes captadas por las cámaras de vigilancia de vídeo, autorizado por el organismo competente, sirvió para que el empleador confirme la conducta ilícita de un empleado que era perjudicial para el objetivo de protección de personas y bienes, y no para controlar su desempeño profesional, es legal para su tratamiento como prueba en los procedimientos disciplinarios y judiciales[575].

B) GPS

El Supremo Tribunal de Justiça en sentencia de 13 de noviembre de 2013[576] estableció que el GPS no podía ser calificado como un medio de vigilancia remota en el lugar de trabajo, tal como se define en el Código do Trabalho, ya que sólo se permite la ubicación del vehículo en tiempo real, haciendo referencia únicamente a una determinada zona geográfica. Instalar GPS en un vehículo afecta exclusivamente a las necesidades del servicio del empresario, como tal tecnología no permite la captura o grabación de imágenes o sonido, no se vulneran derechos de la personalidad del trabajador, incluyendo la intimidad de su vida privada y familia.

[575] TR Lisboa Fecha: 16-11-2011 Proc: 17 / 10. Pte.: SA FERNANDES, P.

[576] Supremo Tribunal de Justiça Proc.: 73 / 12 Pte.: BELO MORGADO, M.

Como la prueba del GPS no se anula, se considera que existe una causa justa para el despido del trabajador, controlador de transporte de vehículos de mercancías peligrosas ya que se probó que de forma deliberada durante 18 veces en un período de tres meses, se apartó de la ruta especificada para el transporte de mercancías, lo que dio como resultado no sólo en el aumento de las distancias recorridas, sino también el aumento de los riesgos derivados de la circulación de un vehículo peligroso que no conducía por la ruta recomendada.

En igual sentido se pronuncia el Supremo Tribunal de Justiça en sentencia de 22 de mayo de 2007[577] respecto a la solicitud de extinción un técnico de ventas contractual por haber procedido la empresa a instalarle un GPS instalado en su vehículo de trabajo. Se resuelve este sistema no capta las circunstancias, la duración y los resultados de las visitas a los clientes o identifica preferencias, por lo tanto, no incide en la esfera íntima del trabajador, por lo que hay que concluir que se carece de justa causa para proceder a la resolución del contrato de trabajo, argumentada en una supuesta infracción del artículo 20 del Código do Trabalho.

C) Correo electrónico

El contenido de los mensajes de carácter personal, enviados o recibidos por el trabajador, incluso ordenadores de la empresa, están cubiertos por el derecho de reserva y confidencialidad consagrado en el art. 21 del Código do Trabalho y no puede, por lo tanto, sin el consentimiento del trabajador, utilizarse para fines disciplinarios, ni es una prueba válida sino nula, incluida la prueba testifical sobre el contenido del correo[578].

La doctrina judicial consolidada nos viene a decir que el hecho de que las conversaciones de chats privados o e-mails se encuentren almacenados en el servidor central de la empresa, en ningún caso significa que su contenido no deje de ser personal y confidencial. En ausencia de cualquier reglamentación previa para uso personal y profesional de Internet, por parte de los trabajadores ,el acceso a los correos de los mismos es indebido e ilícito por la empresa[579].

---

[577] Supremo Tribunal de Justiça Proc.: 07S054 Pte.: PINTO HESPANHOL.
[578] TR Puerto Fecha: 08/02/2010 Proc: 452 / 08 Pte: PAULA CARVALHO LEAL, P.
[579] TR Lisboa Fecha: 07/03/2012. Proc.: 24163 / 09. Pte: ZAPATERO, J.E.

En el sentido anteriormente expuesto, se pronuncia el Supremo Tribunal de Justiça en sentencia de fecha 5 de julio de 2007[580] al declarar que merecen protección legal las comunicaciones electrónicas privadas de los trabajadores, pues no sólo son las comunicaciones relacionadas con la vida familiar, emocional, sexual, salud, convicciones políticas y religiosas de los trabajadores mencionados en el art. 16, párrafo 2 *Código do Trabalho* las que han de ampararse también las comunicaciones de carácter personal del art. 21 del mismo código.

Según los hechos probados de la sentencia, se fiscalizó por el empresario un mensaje de correo electrónico del trabajador desde el escritorio de su ordenador. El contenido de dicho mensaje informaba del contenido de una reunión a la que había asistido el trabajador junto varios directivos de la empresa y realizaba consideraciones y comentarios sobre la misma y sobre tales personas. El correo fue enviado a la dirección electrónica de un amigo y durante las horas de trabajo.

El Supremo Tribunal de Justiça declara la naturaleza personal del contenido del mencionado correo electrónico del trabajador así como su confidencialidad, declara la protección legal y constitucional de la confidencialidad del mensaje, lo que produce la anulación de la prueba obtenida, lo que evita que el mensaje con ese contenido pueda ser justa causa del procedimiento disciplinario y en consecuencia, el despido es improcedente.

[580] Supremo Tribunal de Justiça Proc.: 07S043 Pte: PEREIRA, M.

D) Redes sociales

Los criterios parecen ser los similares a los de nuestro país, como veremos el derecho en colisión es el de la libertad de expresión[581], siendo con respecto al derecho a la intimidad, y a las comunicaciones un conflicto inexistente; un trabajador no tiene derecho a invocar el carácter privado del grupo y de la naturaleza de "personal" de publicaciones, no se benefician de la protección de la confidencialidad prevista en el artículo 22 del Código del Trabajo[582].

En este sentido, el Tribunal de Lisboa en sentencia de 24 de septiembre de 2014[583] declara que no resulta creíble el trabajador estuviera amparado por una expectativa razonable de intimidad por las expresiones vertidas en la red social Facebook contra su empresa, por el hecho de tener solo el contenido de sus conversaciones disponible para "amigos". Lo que se ha demostrado, siendo evidente que la divulgación del contenido en cuestión, aunque a disposición de los "amigos"[584], se debe considerar público. Por otro lado los insultos no puede estar amparados por un pretendido derecho a la libertad de expresión.

---

[581] En este sentido, TR Évora Fecha: 30/01/2014 Proc.: 8 / 13 Pte: Feteira, J. Declara que constituye "*una grave violación de los derechos laborales de respeto, civismo e incluso la lealtad debida a la representante legal de su empleador, por lo que constituye justa causa de despido, la revelación hecha por el empleado, a través de la red social Facebook "mensajes", cuya contenido sabía que le dolía el honor y el buen nombre del representante legal de ese y otros miembros de la tabla de gestión de más cuando no salió nada muestra hacia la verdad de las imputaciones realizadas a través de estos mensajes. La gravedad de este tipo de comportamiento se vuelve aún más evidente por las circunstancias del trabajador serán tomadas de forma velada, usando el subterfugio de un nombre de usuario y una fotografía que revela nada de su identidad, con el fin de ser reconocido* como un trabajador o incluso como asociado, que también era el empleador".

[582] TR Puerto Fecha: 09/08/2014 Proc.: 101 / 13 Pte: Costa Pinto, J.M

[583] TR Lisboa Juicio Fecha: 24/09/2014 Proc.: 431 / 13.6. Pte.: Freitas, J.

[584] Matiza el Tribunal que el concepto de "amigos" en Facebook encaja no sólo los amigos más cercanos, así como otros amigos, conocidos o incluso las personas que no conocen personalmente, sino creando una afinidad de interés en la comunicación en la red social que sea aceptarlas como "amigos".

E) Conclusión

En Portugal, existe una prohibición general de uso de los sistemas de vigilancia con excepciones por razones "*particulares exigencias inherentes a la naturaleza de la actividad*" o de seguridad "protección y seguridad de las personas y bienes". En los casos comprendidos en dichas excepciones resulta más fácil la instalación de los sistemas de control afectados, al exigirse sólo que el empresario informe al trabajador afectado *"sobre la existencia y finalidad de los medios de vigilancia utilizados".*

2. Derecho estadounidense

A) Legislación

EEUU no posee una regulación clara respecto al uso de las nuevas tecnologías y las relaciones de trabajo. Las leyes estadounidenses en esta materia, varían en función de múltiples factores; dependiendo del estado federal ante el que nos encontremos, según el tipo de la reivindicación que se postule, en base al carácter público o privado de la empleadora, y por último, en virtud de si existe una política empresarial corporativa respecto al uso de las nuevas tecnologías, o por el contrario, no hay ninguna regulación integral que respecto a las comunicaciones electrónicas o en relación la protección de datos personales[585].

El hecho cierto es que la preocupación del legislador por el control de las comunicaciones electrónicas, efectuadas desde el puesto de trabajo fue temprana, con respecto a otros países; data de 1986 con la promulgación de la denominada *Electronic Communications Privacy Act*[586] (ECPA[587]) aunque que ha sido modificada varias veces,

---

[585] *LEVINSON, A. Social Media, Privacy, and the Employment. Relationship: «The American Experience»*, Spanish Labour Law and Employment Relations Journal *núm. 1-2, 2013, pág. 22.*

[586] VIZCAÍNO RAMOS, I.: « La jurisprudencia de la Corte Suprema de los EEUU sobre el control de ordenadores personales en el puesto de trabajo. Un estudio del Caso City of Ontario v. Quon (2010)», Comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social. AEDTSS, pág. 4 del original impreso. *http://www.aedtss.com/images/stories/documentos/XXIV_CONGRESO_NACIONAL/pdf/1.48.pdf*

[587] Ley de la Intimidad de las Comunicaciones Electrónicas, Electronic Communications Privacy Act (ECPA) promulgada por el Congreso de EEUU el 21 de octubre de 1986, para extender las restricciones gubernamentales de las llamadas telefónicas a las transmisiones de datos electrónicos por ordenador.

una de las últimas reformas importantes fue 2008, pero la normativa se considera en algunos aspectos desfasada[588].

De la ECPA merece ser destacado el Título II, que protege las comunicaciones existentes en los depósitos electrónicos, sobre todo los mensajes almacenados en los ordenadores prohibiendo el acceso intencional, no autorizado a las comunicaciones electrónicas almacenadas; en función de esta prohibición varios tribunales estadounidenses han sostenido que un empleado que proporciona una contraseña al correo electrónico personal o de otras cuentas en línea en respuesta a la presión de un empleador no ha dado su consentimiento de manera libre y voluntaria[589]. Pero el hecho cierto es que la ECPA contiene muchas excepciones para la interceptación y la recuperación de las comunicaciones electrónicas llevadas a cabo por el proveedor del sistema de comunicación electrónica en el curso ordinario de los negocios o hecho con el consentimiento de los empleados, que hacen que *de facto* las protecciones legales no sean aplicables a la mayoría de las reclamaciones de los tribunales[590].

B) Datos relevantes

Para delimitar la materia deberíamos en primer lugar diferenciar si estamos ante una empresa privada o pública; en el primer supuesto, en el lugar de trabajo existen pocas restricciones legales sobre el poder de control del empleador del sector privado ya que está ampliamente facultado para la supervisión y vigilancia electrónica de sus empleados[591]. La mayoría de los contratos de trabajo actuales no contienen disposiciones sobre cuestiones tales como la vigilancia electrónica, los sindicatos podrían negociar restricciones en el uso del empresario de la supervisión y vigilancia de la tecnología relacionada con los empleados, pero dada la baja tasa de sindicalización en los EEUU,

---

[588] *LEVINSON, A. Social Media, Privacy, and the Employment. Relationship: The American Experience»,* op. cit., *pág. 22.*

[589] Ibidem.

[590] *LIEBERWITZ., L. «New technologies and working relationships in the United States», en AA. VV. SAN MARTIN MAZZUCONI, C. (Dir):* Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico, *ed. Eolas Ediciones, 2014, pág. 505.*

[591] *LIEBERWITZ, L.: « New technologies and working relationships in the United States» en AA. VV. SAN MARTIN MAZZUCONI, C. (DIR). Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico, Ed. Eolas Ediciones, 2014, pág. 505*

los convenios colectivos proporcionan a este respecto protección a un 7% por ciento del sector privado.

En el segundo supuesto, los trabajadores del sector público con un 35% de tasa sindicación de los empleados del sector público es significativamente más alta que la sector privado que en los cerca de treinta estados con leyes de negociación colectiva del sector público los empleados pueden ser capaces de negociar para decidir sobre la política de control empresarial.

Además los empleados públicos están cubiertos por la Ley de Derechos y Decimocuarta Enmienda de la Constitución de Estados Unidos, lo que restringe la injerencia del poder público sobre ellos; lo más relevante aquí son los derechos de privacidad protegidos por la prohibición de la Cuarta Enmienda de registros y detenciones arbitrarias llevadas a cabo por el gobierno.

El interés de la Supreme Court de los Estados Unidos por el control de las comunicaciones electrónicas en el puesto de trabajo es escaso[592].

C) Teléfonos móviles

El potencial para la protección constitucional de los empleados públicos se vio v limitado con el caso City of Ontario *vs* Quon[593], que dio origen a sentencia de fecha de 17 de junio de 2010 de la Supreme Court [594], en ella se resuelve el recurso frente a la

592 VIZCAÍNO RAMOS, I.: «La jurisprudencia de la Corte Suprema de los EEUU sobre el control de ordenadores personales en el puesto de trabajo. Un estudio del Caso City of Ontario v. Quon (2010)», o*p.cit*., pág. 5 del original impreso.

593 La ciudad de Ontario, en cuanto administración local, poseía su propia política de control de ordenadores personales de sus empleados públicos, había adquirido un novedoso sistema de buscadores alfanuméricos para realizar las comunicaciones, funcionaban de manera similar a los corroes electrónicos, pero en la política de uso de las nuevas tecnologías no se reflejaban la posible fiscalización de tales buscadores. El gasto disparado de este nuevo sistema de comunicación motivó que se realizara una investigación para detectar posibles usos desviados. Este policía local demandó a la ciudad que lo empleaba ante una Corte federal de Distrito radicada en California resultando que se desestimó íntegramente su demanda. El demandante recurrió, por ello, ante la Corte federal del Circuito que cubre el territorio del Estado federado de California con un resultado diametralmente opuesto, pues esta otra Corte sostuvo que el sargento *"tenía una razonable expectativa de intimidad en sus mensajes de texto*" por lo que la investigación realizada por la ciudad no había sido correcta.

594 *https://www.supremecourt.gov/opinions/09pdf/08-1332.pdf*

Corte de la ciudad de Ontario frente a un sargento de policía había visto revocada su sanción disciplinaria por parte del tribunal de apelación. Los hechos son los siguientes: un policía llamado Jeff Quon junto con otros dos oficiales compañeros, estaba intercambiando mensajes de naturaleza privada e incluso algunos de contenido sexual. Estos mensajes posteriormente fueron interceptados tras haber sido sometidos a una auditoría los móviles de los policías, y el Alto Tribunal declaró tal conducta como constitucionalmente admisible, sobre la base de "*propósito relacionado con el trabajo legítimo*" del empleador público para la búsqueda de investigar si los empleados necesitan una asignación de mensajes de texto más grande "*por lo que se declara el alcance razonable de la auditoría ya que la cuestión de si un trabajador tiene una expectativa razonable de intimidad tiene que realizarse sobre una base caso por caso*".

El ponente de la sentencia, magistrado Kennedy, asume la práctica inexistencia de precedentes pues reconoció, que desde que se había fallado en 1987 la Supreme Court de los Estados Unidos no había tenido ocasión de volver a pronunciarse sobre la cuestión y manifiesta que si un trabajador tiene una expectativa legítima de intimidad, la intrusión del empresario en esa expectativa, por razones relacionadas con el trabajo y por posibles irregularidades, debería enjuiciarse según la norma de la razonabilidad cualesquiera que sean las circunstancias.

D) Redes sociales

Respecto a las redes sociales, los tribunales normalmente no encuentran ninguna expectativa razonable que proteger porque entienden que no existen opciones de privacidad que limiten el acceso a los contenidos a unas pocas personas. Cabe destacar el caso Karl Knauz Motors Karl[595], en el que el *National Labour Relations Board*, se pronunció sobre si una empresa, en concreto un concesionario de coches, despidió o no con justa causa a un trabajador suyo por publicar en Facebook fotografías y realizar comentarios comentarios sarcásticos sobre un accidente en el que estuvo involucrado un cliente del concesionario en el que venía prestando servicios.

[595] Karl Knauz Motors, Inc. v. Robert Becker, Case Nº. 13-CA-46452 (July 21, 2011).*vid*. *https://www.crowell.com/files/Knauz-BM-358-NLRB-164.pdf*

Se falló que el contenido de lo publicado en la red social por el trabajador del concesionario, no era un argumento suficiente para justificar su despido, a pesar de ser publicado por el empleado en su página de Facebook, se decidió aplicar el estándar de Jefferson[596], el cual se utiliza cuando un empleado ha manifestado frente a terceros comentarios despectivos de su patrono o de sus productos[597]. Al aplicar el estándar, se determinó que en este caso el comentario no fue desleal ni en menosprecio al empresario, y entendió que los comentarios eran en sí un reflejo de la frustración previamente planteada con sucesos anteriores a los enjuiciados.

Otro proceso en el que no se declaró la improcedencia del despido fue el Rural Metro Case [598]: versa sobre un empleado de un senador que escribió en el perfil de Facebook de su respectivo estado para expresarse en desacuerdo con el manejo de los servicios de emergencias a nivel estatal; entre ellos, el modo en que operaba su jefe, ya que entendía que éste no estaba contribuyendo a mejorar la situación. En su comentario, incluyó detalles de la operación de emergencia, como por ejemplo, habló sobre la cantidad tan limitada de camiones disponibles para desarrollar este tipo de servicios. El tribunal razona para confirmar su despido, que en ningún momento el trabajador manifestó previamente estas preocupaciones a su jefe o con sus compañeros de trabajo, concluyó que, su comentario en la red social, no podía considerarse como una actividad protegida y, además, admitió que no el trabajador esperaba una acción en específico por parte del senador para remediar tal situación, si no que su intención era dar publicidad a la situación, es decir, dañar por dañar [599].

---

[596] DIAZ NOTA, R.G.: «Uso de las redes sociales: ¿Justa causa para despido?» ,*U.P.R Business Law Journal*, núm. 3, 2012, pág. 286.

[597] El caso NLRB *v*. Electrical Workers Local Case Nº. 1229, 346 U.S. 464 (1963), sentó el criterio, bajo el cual el estándar de Jefferson, se enjuicia analizando el contexto de la situación existente; si un comentario guarda relación con alguna disputa laboral subyacente, y si no la guarda, se considera que se trata de un acto desleal, temerario o de un comentario maliciosamente falso que justificaría en su caso, un despido. *Vid*. FINKIN, M.W. «Disloyalty - Does Jefferson Standard Stalk Still» *Berkeley Journal of Employment and Labour Law* núm. 28,2007, pág.546.

[598] Rural Metro, Case No. 25-CA-31802 (2011). http://s3.documentcloud.org/documents/267967/responsive-documents.pdf

[599] DIAZ NOTA, R.G.: «Uso de las redes sociales: ¿Justa Causa despido?» ,*op. cit.*, pág. 285.

PARTE ESPECIAL: CONTROL DEL TRABAJADOR MEDIANTE NUEVAS TECNOLOGÍAS

CAPÍTULO I. ACCESO A INSTRUMENTOS TELEMÁTICOS DE USO PROFESIONAL

1. El ordenador del trabajador

A) Planteamiento

Un equipo informático de trabajo no es una taquilla en la que el empleado deposita sus objetos personales durante la jornada, y cuya posibilidad de registro se encuentra claramente limitada en el art. 18 ET, de modo que no queda protegido por las mismas garantías. Partiendo del hecho de que el ordenador es un medio de la empresa puesto a disposición del trabajador para la realización de sus labores, el control de su uso es una responsabilidad del empleador, en virtud del art. 20.3 ET.

En cuanto al uso realizado de Internet por el empleado, habrá que diferenciar los casos en los que dicha herramienta informática sea necesaria para desempeñar su trabajo, o por el contrario, cuando no lo sea, en cuyo caso se podrá restringir la navegación. Y también habrá que atender a la política de empresa respecto al uso del ordenador, pues, por ejemplo, constituye despido procedente el simple borrado de material informático del propio terminal informático cuando la política de la empresa prohíbe cualquier manipulación del mismo, aunque no se haya demostrado ninguna finalidad de tal conducta ni ningún perjuicio[600].

Por otra parte, no se puede olvidar tampoco que gran parte de las visitas que aparecen en el historial de búsqueda no responden a actuaciones voluntarias de los usuarios, sino que simplemente se trata de las llamadas “pop-ups” (páginas web

[600] STSJ Cataluña de 24 de noviembre de 2015 (EDJ 2015/233357). En concreto, la actora firmó las normas de identificación de usuarios y claves de acceso, en las que figura expresamente que "*queda prohibido comunicar a otra persona el identificador de usuario y clave de acceso*" así como "*destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos de la entidad o de terceros*".

mayoritariamente de contenido publicitario que se despliegan automáticamente al realizar búsquedas de otra índole) y que en ausencia de "bloqueador de elementos emergentes" aparecen con ritmo vertiginoso y contribuyen sin duda a aumentar de forma brutal el registro del número de entradas en el historial[601].

B) Pautas de buenas prácticas

La Recomendación CM/rec(2015)5, relativa al tratamiento de datos personales en el entorno laboral se refiere a la utilización de Internet y de las comunicaciones electrónicas en el lugar de trabajo. En su núm. 14[602] dice:

---

[601] SELMA PENALVA, A.: «Los límites de la tolerancia en la utilización del ordenador de la empresa para fines personales», *Revista Doctrinal Aranzadi Social* núm. 83, 2012 (BIB 2012\289), págs. 51-65.

[602] Num. 14. "*Use of Internet and electronic communications in the workplace*

14.1. *Employers should avoid unjustifiable and unreasonable interferences with employees' right to private life. This principle extends to all technical devices and ICTs used by an employee. The persons concerned should be properly and periodically informed in application of a clear privacy policy, in accordance with principle 10 of the present recommendation. The information provided should be kept up to date and should include the purpose of the processing, the preservation or back-up period of traffic data and the archiving of professional electronic communications*". (Uso de Internet y comunicaciones electrónicas en el lugar de trabajo. Los empleadores deben evitar las injerencias injustificadas e inmotivadas pues existe el derecho de los empleados a la vida privada. Este principio se extiende a todos los dispositivos técnicos y las TIC utilizadas por el trabajador. Las personas afectadas deben estar debidamente informadas de una manera periódica y a través de una política de privacidad clara, de conformidad con el principio 10 de la presente Recomendación. La información proporcionada debe mantenerse actualizada y debe incluir la finalidad del tratamiento, la conservación o el período de copia de seguridad de los datos de tráfico y el archivo de las comunicaciones electrónicas profesionales).

14.2. "*In particular, in the event of processing of personal data relating to Internet or Intranet pages accessed by the employee, preference should be given to the adoption of preventive measures, such as the use of filters which prevent particular operations, and to the grading of possible monitoring on personal data, giving preference for non-individual random checks on data which are anonymous or in some way aggregated*". (En particular, en el caso de tratamiento de datos personales relativos a las páginas de Internet o Intranet a las que se accede por el empleado, debe darse preferencia a la adopción de medidas preventivas, como el uso de filtros que impiden las operaciones particulares, y para la clasificación de las posibles el seguimiento de los datos personales, dando preferencia por controles no individuales en los datos que son anónimos o de alguna manera agregada).

14.3."*Access by employers to the professional electronic communications of their employees who have been informed in advance of the existence of that possibility can only occur, where necessary, for*

- Que deben prevalecer las medidas preventivas (por ejemplo, filtrar las páginas web) sobre las de control o monitorización.
- Las comunicaciones electrónicas privadas en el trabajo no deberían monitorizarse en ningún caso.
- No debería permitirse el uso de sistemas que tenga por principal finalidad la monitorización de la actividad y el comportamiento de los empleados. Cuando dicha monitorización responda a fines legítimos como puede ser el correcto funcionamiento de la empresa, deberán adoptarse garantías adicionales, incluida la consulta a los representantes de los trabajadores.
- El empleador ha de evitar "infringir ataques injustificados y no razonables al derecho al respeto de la vida privada de los empleados".
- En segundo término, que la forma cómo se controlan y cómo se obtienen tales datos ha de ser bien conocida por el trabajador. Los controles tienen que ser

---

security or other legitimate reasons. In case of absent employees, employers should take the necessary measures and foresee the appropriate procedures aimed at enabling access to professional electronic communications only when such access is of professional necessity. Access should be undertaken in the least intrusive way possible and only after having informed the employees concerned". (El acceso de los empleadores a las comunicaciones electrónicas profesionales de sus empleados que han sido informados previamente de la existencia de esa posibilidad sólo puede producirse, en caso necesario, para la seguridad u otras razones legítimas. En el caso de los empleados ausentes, los empleadores deben tomar las medidas necesarias y prever los procedimientos apropiados destinadas a permitir el acceso a las comunicaciones electrónicas profesionales sólo cuando dicho acceso es por necesidad profesional. El acceso debe llevarse a cabo de la manera menos intrusiva posible y sólo después de haber informado a los trabajadores afectados).

14.4." The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances". (El contenido, el envío y la recepción de las comunicaciones electrónicas privadas en el trabajo no debe ser monitoreado bajo cualquier circunstancia).

14.5. "On an employee's departure from an organisation, the employer should take the necessary organisational and technical measures to automatically deactivate the employee's electronic messaging account. If employers need to recover the contents of an employee's account for the efficient running of the organisation, they should do so before his or her departure and, when feasible, in his or her presence". (Al dejar un trabajador la empresa para no volver más, el empleador debería adoptar las medidas organizativas y técnicas necesarias para desactivar automáticamente la cuenta de mensajería electrónica del empleado. Si los empleadores necesita recuperar el contenido de la cuenta de un empleado para la buena marcha de la empresa, deben hacerlo antes de su salida y, cuando sea posible, en su presencia).

preferentemente de carácter "poco intrusivo" y con conocimiento de las personas afectadas.

C) Criterios jurisprudenciales

En relación con la verificación del cumplimiento de los deberes laborales por parte del empresario, cuando se inspecciona el ordenador de la empresa en el que realiza su actividad el trabajador, existen pronunciamientos constitucionales y del Tribunal Supremo importantes que se desarrollaron ya en la parte general, SSTC 241/2012, de 17 de diciembre[603] y 170/2013, de 7 de octubre[604] y SSTS de 26 de septiembre de 2007[605], y 8 de marzo de 2011[606], cuya doctrina puede sintetizarse del modo siguiente:

1. Los sistemas informáticos de la empresa son un instrumento de trabajo sujeto a las facultades de control del empresario (STC 241/2012, de 17 de diciembre).
2. El empresario ha de establecer un protocolo sobre el uso de los medios informáticos, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la vetar determinadas conexiones, uso de programas informáticos de protección integral, etc.
3. Si no hay política empresarial sobre posibles límites de utilización del ordenador, se entiende que existe una situación de tolerancia empresarial y una expectativa razonable de intimidad del trabajador así como de confidencialidad, derechos amparables a nivel constitucional (STS de 8 de marzo de 2011). Por tanto existe en la empresa, un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados a los trabajadores.
4. Cuando existe una prohibición absoluta de un uso personal del ordenador, es posible su control y establecer mecanismos para controlar el uso exclusivamente laboral. Las expectativas razonables de intimidad y de confidencialidad quedan enervadas por esta prohibición absoluta.
5. La misma idea rige cuando la prohibición del uso personal se contiene en el convenio colectivo de aplicación (STC 170/2013, de 7 de octubre).

---

[603] STC 241/2012, de 17 de diciembre (RTC 2012\241).

[604] STC 170/2013, de 7 de octubre (RTC 2013\170).

[605] STS 26 de septiembre de 2007 (RJ 2007\7514).

[606] STS 8 de marzo de 2011 (RJ 2011\932).

D) Derechos fundamentales en conflicto

Precisamente, en este punto, es donde se ha planteado una fuerte tensión dialéctica entre dos derechos que gozan de una dimensión constitucional diferente[607]. De un lado, la propiedad privada y la tutela del patrimonio empresarial (art. 38 CE), y de otro lado, los derechos fundamentales del Cap. II, sección 1ª. Esta cuestión ha suscitado multitud de debates, pero sin duda el más conflictivo es el de determinar el alcance de cada uno de los derechos, así como las modulaciones de los mismos que podrán imponerse al trabajador[608]. De acuerdo con la doctrina constitucional, es preciso que el empresario disponga de los pertinentes instrumentos jurídicos, ya sean pactados o unilaterales, que le permitan, primero, prohibir o autorizar expresa o tácitamente y, en su caso, controlar y sancionar los incumplimientos de los trabajadores en esta materia. De lo contrario, se consideraría que esta actividad fiscalizadora vulnera su expectativa razonable de intimidad. Cabe hablar de un uso moderado. Un uso abusivo, lógicamente, no puede generar esta expectativa.

Respecto al secreto de las comunicaciones, la navegación por Internet, en páginas web no relacionadas con el trabajo del mismo modo que la participación en chats, foros de debate, etc., no se encuentran protegidas por este[609].

E) Enervación de la expectativa de intimidad

En lo que se refiere a la prohibición expresa de uso privado del ordenador, como vimos, neutraliza cualquier expectativa y no hay lesión de derechos fundamentales (intimidad y secreto de las comunicaciones) que pueda alegarse, en base a la STC 170/2013, de 7 de octubre[610], que establece que la prohibición de uso equivale a la

---

[607] MONEREO LÓPEZ, J.L. y LÓPEZ INSUA, B.M.: «El control empresarial del correo electrónico tras la STC 170/2013» *op. cit.*, pág. 2 del original impreso.

[608] *Ibídem.*

[609] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op.cit*., pág.85.

[610] STC 170/2013, de 7 de octubre (RTC 2013\170).

información a los trabajadores de la posibilidad de control del uso que hacen de los equipos informáticos[611].

Una parte importante de la doctrina que discrepa de este criterio de la enervación de la expectativa de protección de los derechos fundamentales por la existencia de una prohibición respecto al uso del ordenador, piensa que así se vacía de contenido los derechos fundamentales en colisión que amparan al trabajador[612], lo que contraviene uno de los derechos básicos de cualquier Estado de Derecho[613].

Respecto al derecho a la protección de datos, registrar la navegación y el acceso a los sitios visitados por los empleados, para su almacenamiento y posterior procesamiento, cuando queden identificadas las personas físicas, supone un tratamiento de datos de carácter personal, en los términos de la LOPD, en cuyo caso los trabajadores deberán ser informados por la empresa de que sus datos de navegación son parte de un fichero de datos personales.

F) Problemas de gestión empresarial

El uso de medios informáticos está planteando numerosos problemas de gestión empresarial, que también se manifiestan en el ámbito disciplinario. De esta manera están surgiendo cuestiones diferentes.

a) Acreditación de la autoría

Constituye un problema de prueba, cuando el ordenador es utilizado por varias personas incluso existiendo clave, si es compartida, pues, la acreditación de la autoría puede resultar imposible. En ese caso, lo oportuno es actuar *a priori*, regularizando la política de uso de los ordenadores de empresa, prohibiendo que se compartan claves, o se

---

[611] En este sentido: STSJ Cataluña de 14 octubre de 2015 (EDJ 2015/215454), STSJ de Cataluña de 23 junio de 2015 (JUR 2015\230355) y por último, STSJ Comunidad Valenciana de 19 mayo de 2015 (JUR 2015\204821).

[612] DE LA QUADRA-SALCEDO JANINI, T. y SUÁREZ CORUJO, B.: «¿Trabajadores incomunicados?: La deriva de la doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones». Comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social de 2014, pág. 11 del original impreso.

[613] MARÍN ALONSO, I.: «El uso por los trabajadores de las comunicaciones electrónicas en la empresa. ¿Se encuentran protegidas por el secreto de las comunicaciones?» Comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social de 2014, pág. 16 del original impreso.

acceda a los terminales informáticos sin usuario o contraseña; en definitiva, prevenir para evitar posibles confusiones. Dificultad probatoria que sucede en la STSJ de Valencia de 7 de septiembre de 2016[614], en la que resuelve, sorprendentemente, en sentido desestimatorio, el recurso de suplicación una empleada de una farmacia al declarase probada la procedencia de su despido, pese a que se constata que "*las claves de acceso a los ordenadores están pegadas al marco de la pantalla del ordenador, por lo que cualquiera de las trabajadoras podía tener acceso a ellas*" y que la Sala reconoce que "*la falta de identificación cuando se utiliza el ordenador del empleado de la farmacia que efectúa los pedidos y de quien recepciona los mismos dificulta la atribución de la autoría de la conducta*" . Pese a ello, la Sala del TSJ valenciano, valida que el Juzgador de instancia se haya servido de la prueba de presunciones para imputar a la trabajadora despedida la autoría de los hechos.

b) Archivos temporales

Los archivos temporales no son comunicaciones, ni archivos personales, sino copias que se guardan automáticamente en el disco duro del ordenador de los lugares visitados a través de Internet. Se trata de rastros o huellas de la navegación en Internet y pueden contener información de carácter personal; pueden arrojar datos reveladores de muchas circunstancias de índole personal como aficiones, curiosidades e ideología, etc. Aspectos todos ellas protegidos en el artículo 8 del Convenio Europeo de Derechos Humanos. Por tanto, que hay entender que estos archivos temporales entran, en principio, dentro de la protección de la intimidad.

En consecuencia, se vulneraría el derecho a la intimidad cuando se realizara una auditoría en una empresa dirigida a averiguar la utilización por parte de todos los empleados de la empresa de los ordenadores de la misma, a través de una terminal conectada a un servidor y detectara irregularidades en algunos de ellos, lo despidiera de

[614] STSJ de Valencia de 7 de septiembre de 2016 (EDJ 2016/201237).

manera disciplinaria si se hiciera referencia en la carta de despido no genéricamente a los tiempos y páginas visitadas, sino también al dominio y contenido de las mismas[615].

c) Monitorización

El Reglamento General sobre Protección de Datos de la UE[616] resulta parcialmente aplicable a los supuestos de monitorización y acceso al correo electrónico laboral. En la normas comunitarias se reconoce la posibilidad de acceso siempre y cuando se concurran las siguientes garantías: 1º) la necesidad de un propósito específico, explícito y legítimo (elemento de causalidad); 2º) que la supervisión sea una respuesta proporcionada sobre un patrón de riesgo (elemento de indispensabilidad);3º) la mínima repercusión sobre los derechos a la intimidad del trabajador (elemento de proporcionalidad); 4º) la presencia del trabajador y de sus representantes en el momento de apertura del correo (elemento garantista).

En España, si existe una prohibición absoluta de uso el empleador puede acceder a los mensajes del trabajador de carácter privado, ya que si lo hiciera la prueba así obtenida tendría plena validez en juicio (STSJ de Madrid de 6 mayo 2016[617] y STSJ Canarias de 8 enero 2016[618]). De modo que resulta posible la monitorización del ordenador del trabajador en busca de mensajes de tipo personal si hay un mandato del empleador que prohíba su uso particular.

---

[615] Páginas de contenido multimedia; web de piratería informática; webs de anuncios clasificados para particulares; web de acceso a televisión por Internet; acceso a correo personal; web de consulta para temas relacionados con el sexo femenino; etc).

[616] Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos.

617 STSJ Madrid de 6 de mayo de 2016 (AS 2016\1330). Declara que la monitorización del ordenador al ordenador del trabajador es legítima cuando, esta, de conformidad con las exigencias de la buena fe la empresa, establece las reglas de uso de los medios e informa a los trabajadores que va a existir un control sobre los mismos.

[618] STSJ Canarias de 8 enero 2016 (EDJ 2016/10725). El TSJ canario sostiene que en supuestos en que se aprecia una expresa prohibición patronal de realizar cualquier utilización de medios informáticos, no puede entenderse que exista una situación de tolerancia empresarial al uso personal del ordenador , por lo que no hay una expectativa razonable de confidencialidad derivada de la utilización de esos usos prohibidos, impidiendo que las medidas de control sobre las actividades realizadas con los equipos informáticos de la empresa vulneren los derechos a la intimidad personal o al secreto de comunicaciones.

Lo esencial es que la medida de control se realice respetando los parámetros constitucionales del principio de proporcionalidad. Los controles empresariales serán lícitos si se constata que la medida cumple con los consabidos juicios de idoneidad, de necesidad y de proporcionalidad en sentido estricto. Y en el caso de existencia de una prohibición absoluta de usar el ordenador para fines ajenos a la actividad laboral, la instalación del sistema de control sin conocimiento de los trabajadores no conlleva que la prueba así obtenida para justificar el despido sea ilícita; según la doctrina de la STS 6 de octubre de 2011[619]. En efecto, si no hay derecho al uso del ordenador para asuntos personales por existir esa prohibición, tampoco surge el derecho a que se le respete su intimidad.

d) Instalación de software o hardware

Instalación no autorizada ni consentida de *software* ilegal.- Se produce una vulneración de los derechos de autor, pues la protección de estos derechos respecto al *software* se concede a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en el Texto Refundido de la Ley de Propiedad Intelectual[620] en su art. 10. 1: *son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas: i) los programas de ordenador*". La Ley 24/2015, de 24 de julio, de Patentes[621], en su art. 4 afirma que no se considerarán invenciones en el sentido de los apartados anteriores "*los programas de ordenadores*".

Tal actitud por parte de un trabajador aparte de poder justificar un despido , lógicamente, también es ilícita, teniendo en cuenta que, incluso puede implicar la responsabilidad empresarial.

Descarga de *software* o *hardware* legal.- La conducta no supone una violación de los derechos de autor, pero podrá ser sancionada como desobediencia -aplicando la teoría gradualista- cuando se vulneren las instrucciones empresariales al respecto, que pueden prohibir tales conductas, sirva a título de ejemplo la STSJ de Castilla La Mancha

[619] STS de 6 de octubre de 2011 (EDJ 2011/308825).

[620] BOE 97/1996 de 22 de abril de 1996, modificado por la Ley 21/2014, de 4 de noviembre, BOE 268/2014, de 5 de noviembre de 2014.

[621] BOE 177/2015, de 25 de julio de 2015. En vigor desde el 1 de abril de 2017.

Sala de lo Social de 30 noviembre 2016[622], que confirma el despido declarado en la instancia de un trabajador que realizó descargas de información e hizo uso de programas informáticos de limpieza de registros para eliminar la huella de haber accedido al equipo informático de la directora de RRHH desde su equipo informático y de haber procedido a copiar determinados archivos.

En ausencia de prohibición empresarial ha de comprobarse si la conducta venía siendo tolerada o si por el contrario no lo estaba, teniendo en cuenta si se ha producido algún daño para la seguridad de la empresa.

No toda descarga de Internet ha de ser necesariamente intencionada o voluntaria por parte del trabajador, sino que puede ser consecuencia de la navegación por determinadas páginas web, en cuyo caso, únicamente, puede derivarse una sanción al trabajador por negligencia o incluso por desobediencia, si la empresa ha restringido la navegación por Internet a sitios determinados y concretos, pero nunca sancionar con un despido.

e) Borrado de datos, archivos y discos duros

Cada vez es más común, que en caso de conflicto empresarial, se susciten dudas sobre si el trabajador ha procedido a borrar archivos de su ordenador y que pudieran ser valiosos para la empresa. Al mismo tiempo, la costumbre extendida entre muchos trabajadores de incorporar en sus discos duros o correos electrónicos archivos privados hace difícil diferenciar en ocasiones si el borrado afecta a archivos de los que es titular el empresario o el empleado.

En muchos supuestos, el principal problema de prueba de los hechos, pero cuando queda constatado que el empleado ha borrado archivos de titularidad empresarial estamos ante un supuesto de daño a bienes empresariales que puede ser sancionado en función de su gravedad, con arreglo a la teoría gradualista de la misma manera que cualquier otro daño infligido al patrimonio empresarial.

A mayor abundamiento, es posible que la empresa, además de sancionar al empleado, reclame del mismo una indemnización de daños y perjuicios, siempre que acredite su autoría, los daños producidos y su valoración (STSJ de Valladolid de 12 de mayo de 2009[623]).

---

[622] STSJ Castilla La Mancha de 30 noviembre de 2016 (EDJ 2016/239066).
[623] STSJ de Valladolid de 12 de mayo de 2009 **(**EDJ 2009/118441).

Sin embargo hay que tener en cuenta que los archivos borrados por el sistema de vaciado de la papelera del sistema operativo pueden ser muchas veces recuperados con facilidad o que pueden existir copias de seguridad que permitan recuperar los archivos borrados, minimizando los daños o haciéndolos inexistentes, lo que permite aplicar la teoría gradualista; en este sentido la STSJ de Cataluña de 16 de diciembre de 2016[624] ,con respecto a la calificación del despido no considera transcendente el manipulado y borrado de programas de gestión empresarial.

G) Situaciones de tolerancia

a) Acceso descontrolado al sistema

La STSJ de Madrid de 7 de mayo de 2014[625] confirma la declaración de improcedencia del despido declarado en la instancia de la actora que trabajaba para un grupo de empresas que fabrica y distribuye productos de lujo de diferentes sectores. La conducta sancionada consiste en haber accedido a la base de datos de la empresa para manipular órdenes de trabajo con la finalidad de que la empresa no se percatara de la sustracción de dinero por parte de la empleada. La operación en el ordenador que realizaba la trabajadora era reflejar a la hora del pago de los clientes, una tarea que se denominaba *"incidencias en metálico*" que reducía de manera fraudulenta el importe a pagar por el cliente que se reflejaba en la caja, importe que no se le reducía al cliente sino que se lo quedaba la empleada despedida.

El problema es que la propia empleadora en la prueba de interrogatorio de partes reconoce que todos los trabajadores del departamento conocían las claves personales de acceso de los demás y podían entrar en el ordenador de un compañero con sus propias claves o con las del compañero, por lo que al no existir autor seguro, no hay despido:

> *"No se puede determinar con la mínima seguridad que la demandante fuese quien realizase ese acceso y manipulación pues todos los trabajadores conocen las claves de acceso de los demás y las usan en sustituciones, incluso el superior de la demandante ha empleado el ordenador de esta en alguna ocasión. El uso del ordenador de otro compañero de trabajo se produce cuando éste no está, dándose la circunstancia que la actora no permanecía sentada en su mesa de trabajo, sino que diariamente se desplazaba al taller, a la recepción y al almacén, además de sustituir a Joaquina. No se puede descartar que otro compañero de la demandante pudiese acceder al sistema desde el ordenador de ésta, aprovechando su ausencia, máxime considerando el breve margen temporal en que se desarrollaron los cambios en la base de datos,*

[624] STSJ de Cataluña de 16 de diciembre de 2016 (EDJ 2016/265306).
[625] STSJ de Madrid de 7 de mayo de 2014 (EDJ 2014/88737).

por lo que no se puede considerar acreditado que la demandante fuese la que modificó los números de teléfono de los clientes cuyas facturas no constaban abonadas, que sustrajese los importes correspondientp2ps a dichas facturas, que destruyese las mismas o que suplantase la identidad digital de Joaquina, para inculparla de dichas actuaciones. Lo expuesto lleva a desestimar el motivo y el recurso"(FJ 2º).

Por lo que cabe deducir, que una adecuada política empresarial con respecto al uso de las nuevas tecnologías que prohibiera el uso común de claves hubiera producido un resultado distinto.

b) Código de conducta desplazado

En STSJ de Madrid de 20 de mayo de 2013[626] se alza la empresa en suplicación frente a la sentencia que declaró el despido del trabajador como improcedente y ve desestimada su pretensión, pues, se valora que previamente ha existido en la empresa una situación de tolerancia de uso respecto al uso de nuevas tecnologías a pesar de haber un código que lo prohibía, lo que convertía la norma en papel mojado.

Los hechos son los siguientes: un ingeniero industrial, cuando llevaba ya varios años trabajado para la empresa, fue advertido mediante una comunicación interna de la política respecto al uso de las nuevas tecnologías, prohibiendo de manera expresa el uso particular. Cinco años después, en el 2012, es despedido de manera disciplinaria, por infringir esta prohibición. Todo comenzó cuando el sistema informático de la empresa al monitorizar la actividad de todos los empleados, en un control rutinario, alertó de que el trabajador que luego se vería afectado por el despido, era un usuario con un número de accesos notablemente superior al del promedio de la empresa. Por esta causa solicitó la emisión de un informe más específico en relación con los accesos no autorizados a Internet. Del referido informe se desprende que el recurrente había accedido a todo tipo de páginas (sobre bolsa, medicina, viajes, contenido pornográfico, etc.) Pero en la instancia se declara probado que no se puede asegurar que todas las conexiones se realizaran desde la terminal del recurrido, y además eran muy cortas.

Aunque existía y había sido publicado el código de conducta, también es lo cierto que por la utilización de la red para los mencionados usos no constaba que se hubiese despedido o sancionado a nadie hasta cinco años después de la comunicación interna de la política respecto al uso de las nuevas tecnologías. En efecto, transcurrido ese tiempo, comienzan a efectuarse los primeros despidos con causa en incumplimiento del código

[626] STSJ de Madrid de 20 de mayo de 2012 (EDJ 2013/167191).

de uso de nuevas tecnologías, lo que lleva al juez de instancia a la convicción de una situación de tolerancia de la empleadora con los trabajadores todos estos años respecto al acceso a Internet, no cabe pues imponer la sanción más grave, sería ir contra los propios actos:

> *"Lo cierto es que en el supuesto de autos, no consta (por haber resultado infructuosa en este aspecto la modificación de la relación fáctica de la sentencia impugnada) la conexión masiva del actor entre el 3 de octubre y el 8 de noviembre a páginas de contenido adulto, blogs y a compras on line a que refiere el recurrente en su escrito de recurso, ni se ha acreditado tampoco la disminución de rendimiento laboral del actor, apreciando el juez de instancia en la fundamentación jurídica, como ya hemos expuesto, con indudable valor de hecho probado, que " de un total de 60 presuntas visitas a páginas para adultos no se ha acreditado la conexión directa de la terminal del ordenador del actor, ni la entrada directa de este en las mismas, durante su jornada de trabajo y se trata de conexiones de solo segundos ", lo que atenuaría la gravedad de la falta imputada y ausente cualquier referencia a derechos fundamentales, el supuesto ha de enjuiciarse con los criterios de cualquier despido disciplinario , con atención a las circunstancias concurrentes para la calificación de la conducta del actor y acreditado que las conexiones a Internet lo fueron de segundos, como ya se ha dejado dicho, la conducta no puede calificarse como desobediencia muy grave y transgresión de la buena fe contractual o abuso de confianza en el desempeño del trabajo, con arreglo, respectivamente, al art. 54.2.b) ET en relación con el art. 54.p) que remite al 53.e) ambos del convenio colectivo y al art. 54.2.e) del ET en relación con el 54.c) del texto convencional, pues en lo tocante a la desobediencia, la conducta del actor no implica una actitud reiterada, constante y masiva de incumplir la orden de utilizar el sistema informático de la empresa para usos privados, por lo que la indisciplina aunque existiendo por lo evidente del acceso a Internet aunque fuera por segundos, no puede calificarse de la mayor gravedad"(FJ 2º).*

El criterio definitivo, por tanto, es que si ha existido tolerancia en la empresa, y ha quedado acreditada la conexión a Internet pero es brevísima ("*por segundos*" se reitera en varias ocasiones), no se le puede aplicar al trabajador la mayor sanción del ordenamiento laboral.

A igual resultado llega la STSJ de Madrid de 20 de mayo de 2013[627], en la que se despide por los mismo hechos a otro trabajador de la misma empresa y también confirma la improcedencia del despido, por la situación de tolerancia de uso privado existente en la empresa.

[627] STSJ de Madrid de 20 de mayo de 2013 (JUR 2013\294263).

H) Prohibiciones absolutas

Como ya analizamos las SSTS 26 de septiembre de 2007 [628], 8 de marzo de 2011 [629], y 6 de octubre de 2011[630]; en ellas se admite la validez de la prohibición absoluta de los medios empresariales para usos privados y este es el criterio delimitador que actualmente se asume.

a) Detección de bajo rendimiento

La STSJ de Cataluña de 13 de junio de 2016[631] resuelve el recurso de suplicación de la empresa, revocando la sentencia de la instancia, al entender que el despido es procedente al ser la infracción claramente vulneradora de la buena fe que ha de presidir el contrato de trabajo. Los hechos transcurren del siguiente modo:

- La Escuela Superior de Hostelería de Barcelona procedió a despedir disciplinariamente a una jefa de departamento, por vulneración de la buena fe contractual y disminución continuada y voluntaria del rendimiento, a una trabajadora tras constatar en una auditoría informática que la trabajadora había desobedecido la instrucción empresarial y se había conectado a Internet para uso privado. El uso era elevado entendía la empresa: 30 horas en 4 meses, tiempo que dedicaba a consultar su correo particular, jugar al parchís, consultar su perfil en redes sociales o páginas de ventas de viajes, telefonía o muebles, etc.
- La trabajadora impugnó el despido y en la instancia se calificó este de improcedente considerando el esencial principio de proporcionalidad en el ámbito disciplinario y la doctrina gradualista. Entendía el juzgador que el tiempo no era excesivo, que no se había generado un daño empresarial, ni siquiera un riesgo especial, y que la empresa disponía de medios técnicos más eficaces para impedir el uso no deseado del ordenador de la empresa; no constando además otras sanciones al demandante o a otros trabajadores que permitieran presumir el especial interés y rigor empresarial en el control de la utilización de equipos informáticos.

La Sala de Lo Social de Cataluña, considera el despido procedente, y revoca la sentencia de la instancia, por los siguientes motivos:

- No existe regulación convencional que suavice las causas de despido disciplinario contempladas en el ET.

---

[628] STS 26 de septiembre de 2007 (RJ 2007\7514).

[629] STS 8 de marzo de 2011 (RJ 2011\932).
[630] STS de octubre de 2011 (RJ 2011\7699).
[631] STSJ de Cataluña de 13 de junio de 2016 (EDJ 2016/140449).

- La prohibición había sido comunicada correctamente y era absoluta y fácil de entender en sus términos.
- La trabajadora desoyó tal prohibición de forma reiterada, lo que la sitúa al margen de la buena fe contractual con el plus de probidad exigible a quien desempeñaba un puesto de mando.
- Aunque la empresa podría haber realizado un control o auditoría previa en cualquier momento, su ausencia no modula la gravedad del ilícito consumado, tampoco que no hubiera sanción previa del actor o sus compañeros acredita que hubiera tolerancia empresarial a tales incumplimientos.
-

b) Navegación extralaboral

La STSJ de Madrid de 26 de Enero de 2015[632] estima la suplicación planteada por la consultora INDRA frente a la estimación de la demanda en la instancia de la trabajadora. Se declara que si existía una prohibición respecto al uso de las nuevas tecnologías y no había tolerancia de *facto*, la sanción ha de ser la del despido, no otra menor; por lo cual se revoca el pronunciamiento de la instancia. Al inicio de la relación laboral, en una cláusula del anexo al contrato de trabajo, la trabajadora despedida, asumió el compromiso de cumplir la política de seguridad informática que garantiza la confidencialidad, integridad y disponibilidad de sus sistemas de información. Dicha política se encontraba publicada en la intranet corporativa a la que tenían acceso todos los trabajadores respecto a la navegación por la Web. En ella se establece textualmente lo siguiente: "*Conectividad a Internet. Internet es una herramienta de trabajo. Todas las actividades en internet deben estar en relación con tareas y actividades del trabajo desempeñado. No está permitido utilizar, en caso de conexiones externas a Internet desde la red de Indra, cualquier otro medio (p.e. módems) que no sea el ofrecido por Red Corporativa*". La empresa dispone de un sistema de contraseñas privadas, personales e intransferibles para el uso de los medios informáticos. Asimismo, en su política corporativa figura lo siguiente: "*Indra se reserva el derecho de controlar, monitorizar o limitar el conjunto de servicios Internet accesibles para los usuarios, por motivos de seguridad o rendimiento de la Red*".

La empresa monitoriza la actividad del ordenador de la trabajadora despedida durante dos meses, por haber detectado índices de bajo rendimiento, y comprueba que dedica a navegar por Internet 16 horas y 47 minutos durante el mes de octubre (21 días laborables) y 10 horas 43 minutos en el mes noviembre (16 días laborables), hechos por los que procede a despedirla. La sentencia de instancia declara probado que: "*La actora ha*

[632] STSJ de Madrid 26 de enero de 2015 (JUR\2015\73985).

navegado por internet para usos personales en el ordenador de la empresa, 2 horas y 41 minutos en octubre de 2013 y 1 hora y 18 minutos en noviembre de 2013" (HP 8º). Las páginas web visitadas son de variada índole (prendas de vestir, redes sociales, etc.)

Por la parte recurrente se interesa la revisión de los hechos declarados probados, motivo que es desestimado, y asimismo interesa la revisión del Derecho aplicado, con expresa alusión a la doctrina de la STS de 6 de octubre de 2011[633]. La Sala resuelve que procede estimar este motivo porque se puede concluir que dada la existencia en la empresa de una prohibición absoluta sobre el uso de medios de la empresa (ordenadores y acceso a Internet) para fines ajenos a la actividad de la empresa, sin que conste la posibilidad del uso personal, infringir tal prohibición constituye una transgresión de la buena fe contractual. La empleada ha utilizado un medio cuya propiedad no le pertenece y cuyo uso está sujeto a las instrucciones del empresario, incumpliendo por ello con las normas dictadas a tal fin por el empleador, transgrediendo la buena fe contractual, por lo que se valida el despido como procedente y se revoca la sentencia de instancia.

Con tales hechos probados, lo que resulta sorprendente es que a la parte actora no se le denegara la demanda en la instancia, pues con independencia de que las horas de navegación no coincidieran con las de la carta de despido, consta probado que ha navegado por Internet para uso personal, siendo éste el hecho imputable, no la duración de las conexiones. Quizás el Juzgador aplicó la teoría la gradualista, entendiendo el incumplimiento como menor. Por otro lado, también resulta llamativo que una empresa puntera en tecnología no sea capaz de acreditar el número de las horas que imputa como navegadas, pues de alegar 16 horas de navegación a quedar como probadas tan solo 2 horas en un mes, hay una diferencia importante. Este argumento (aunque entendemos que erróneo) sirvió para hacer prosperar la demanda en la instancia.

c) Incumplimiento arrastrado

La STSJ de Madrid de 27 de enero de 2014[634] confirma la procedencia de un despido disciplinario interesante. Consta que la actora tenía conocimiento antes de ser despedida de la prohibición dirigida al personal de la empresa del uso de Internet para fines particulares. La empleadora encargó a la consultora KPMG un informe con ocasión

[633] STS 6 de octubre de 2011 (RJ 2011\7699).
[634] STSJ de Madrid 27 de enero de 2014 (AS 2014\660).

del análisis de los accesos a Internet por la IP asignada a la trabajadora, en el que se demostró el acceso de la misma a páginas web con fines particulares (con el identificador de usuario "*Pecas*", que era el de la empleada, observan un total de nada menos que 102.881 conexiones a Internet). Pese a ello la sentencia de la instancia califica el despido como improcedente, quizás porque diversos empleados habían usado Internet para fines privados y la empresa les había impuesto una sanción menor.

La Sala de segundo grado, revisando la crónica judicial de instancia, recalca que en una reunión celebrada con el Comité de Empresa la Dirección de la empresa recordó que el uso de internet y del teléfono es para fines exclusivos de trabajo, no estando permitido hacer uso para fines personales. Ante la modificación de tales hechos, la Sala argumenta:

> *"La elusión continuada y no esporádica u ocasional, de la orden empresarial, además de implicar desobediencia a órdenes e instrucciones legítimas y razonables del empresario, que la actora debía de cumplir ex arts. 5, a) y 20.2 del ET , transgrede gravemente el principio de buena fe contractual. Y si bien es cierto que en el enjuiciamiento del despido disciplinario, procede actuar con sujeción a criterios lógicos de proporcionalidad en la sanción que se adopte (doctrina gradualista), según jurisprudencia notoria y constante, en el caso enjuiciado no hay causa para hacerlo así" (FJ 3º).*

Por tanto, ante una prohibición de uso que consta en el código de conducta de la empresa, y que ha sido reiterada y recordada *a posteriori*, un incumplimiento continuado y no esporádico supone una transgresión de la buena fe que ha de presidir la relación de las partes.

d) Tareas no encomendadas

La STSJ de Madrid de 21 de enero de 2013[635] confirma la procedencia de un despido al probarse que la empresa no permitía un uso libre e ilimitado de acceso a sus archivos o intranet, y la recurrente había incumplido esta prohibición. La recurrente, de profesión delineante, ha realizado, en horario de trabajo, los planos de su vivienda y otras tareas de realización e impresión en formato *dwg*[636], en los que ha empleado más de 24 horas, que no se corresponden con ninguno de los trabajos que tiene asignados y que carecen de referencia de producción de su empresa. Y también ha trasladado a su disco local de archivos propiedad de la empresa, otros procedentes de su red informática. Se

[635] STSJ de Madrid de 21 de enero de 2013 (JUR 2013\71711).

[636] Formato de archivo informático de dibujo computarizado, utilizado fundamentalmente por el programa AutoCAD; software reconocido a nivel internacional por sus amplias capacidades de edición, que hacen posible el dibujo digital de planos de edificios o la recreación de imágenes en 3D; es uno de los programas más usados por arquitectos, ingenieros, diseñadores industriales y otros.

descarta que haya habido vulneración del derecho a la intimidad y al secreto de las comunicaciones:

> *"(...) Entendemos que la sentencia recurrida no ha infringido la doctrina sentada, en tanto ni nos encontramos ante información obtenida a través de correo electrónico, ni obrante en archivos personales o en el rastro dejado por la visita a páginas web, sino que se trató en todo caso del disco duro de su ordenador, constatándose, como se ha declarado probado, que no sólo guardaba archivos sobre cuestiones no relacionadas con las tareas que ella llevaba a cabo, sino lo que nos parece más importante, que en horario laboral, se ocupaba de menesteres ajenos a su trabajo" (FJ 3º).*

El disco duro del trabajador, por tanto, no se encuentra amparado bajo la protección de ningún derecho constitucional si existe una prohibición expresa que enerva la protección que le da el texto constitucional.

I) Realización de actividades ilícitas

Son supuestos que suponen una apropiación de archivos de la empresa para uso propio o comunicación no autorizada de los mismos a terceros. Cuando esos archivos contengan datos personales la apropiación o la comunicación de los mismos es ilegal por vulnerar la legislación sobre protección de datos, implicando la responsabilidad de la empresa, por lo que normalmente podrá considerarse como falta laboral grave. Lo mismo ocurre cuando se trate de archivos protegidos con derechos de autor o sujetos a propiedad intelectual e igualmente cuando se trata de informaciones sobre las que el trabajador debe guardar reserva o secreto. En otro caso habría que comprobar si existe una instrucción empresarial incumplida que permita sancionar la desobediencia o, en caso contrario, si con dicha conducta se viene a perturbar el orden productivo normal de la empresa.

a) Sustracción de información

La STSJ de Canarias de 8 enero 2016[637] confirma la procedencia del despido acordado por uso desviado de información privilegiada a través del ordenador del trabajo. El recurrente, con categoría director administrativo, poseía información confidencial de la empresa que estaba guardada en su ordenador, y a través de diversos dispositivos y correos electrónicos durante varios meses, procede a desviar información de diversa índole de la empresa datos sobre ERES realizados sobre los clientes y proveedores,

[637] STSJ Canarias de 8 enero 2016 (EDJ 2016/10725).

reenvío de correos corporativos a otra empresa del sector, etc. Existía una prohibición absoluta de uso de los medios informáticos para usos particulares, a través de un protocolo que el propio trabajador había confeccionado para la empresa con pautas para la seguridad informática, la protección de datos personales y la custodia de la información relevante.

La sentencia descartar que las medidas de control implementadas por la empresa hayan vulnerado el derecho del actor a la intimidad personal o al secreto de las comunicaciones, porque existían en la empresa unas reglas sobre el uso de los ordenadores de la empresa para la ejecución de la actividad profesional en las que se establece una prohibición expresa y rotunda de utilización del equipo informático por parte de la empresa, y el acceso a Internet para fines ajenos al laboral. Lo relevante para la concurrencia del tipo infractor es la realización de actuaciones desleales que supongan un abuso de la confianza depositada por la empresa, habida cuenta que, se trata de un trabajador que ocupa un puesto de dirección y tiene personal a su cargo, no solo se han incumplido reiteradamente los protocolos de actuación que él mismo ha elaborado y es responsable de velar por que sean cumplidos por sus subordinados, sino que además, ello se ha realizado prevaliéndose de la posición que tiene en el organigrama organizativo, y adicionalmente se ha utilizado indebidamente información confidencial de clientes en beneficio propio y de terceros.

b) Acceso a ordenadores ajenos

La STSJ de Galicia de 26 de noviembre de 2015[638] declara la improcedencia del despido porque acceder a los ordenadores de otros compañeros por parte de la trabajadora constituye una mera transgresión de la buena fe contractual o un abuso de confianza pero no es un incumplimiento grave y culpable.

Los hechos transcurren del siguiente modo: un técnico informático detecta un acceso al ordenador de la responsable de recursos humanos, y se procede a localizar la IP desde la que se ha partido. Se comprueba que la misma corresponde a la trabajadora que luego fue despedida, por lo que se decide auditar el ordenador de la empleada, comprobándose el acceso además a otros tres ordenadores: dos de responsables de servicio, y el otro de una formadora. En su recurso la parte recurrente reconoce el acceso

[638] STSJ Galicia de 26 de noviembre de 2015 (EDJ 2015/236174).

desde el ordenador de trabajo a otros de la empresa, pero expone que se hizo a través de un programa instalado en todos los equipos de los trabajadores y al que se podía acceder sin ningún tipo de prohibición o restricción.

La sentencia considera que la conducta es sancionable, pero no con el despido sino con otra sanción menor, una suspensión de empleo y sueldo[639] porque no se cumplen los requisitos jurisprudencialmente exigidos para el control empresarial del ordenador como herramienta de trabajo ya que:

"*La conducta del actor consistió en conectarse a los ordenadores de cuatro compañeros, mediante un programa que estaba a su disposición y en su ordenador , al igual que a la de todos los otros compañeros, sin que conste que en ningún momento se le hubiera advertido que dicho programa no podía ser utilizado.(…)*

> *En ningún momento se ha considerado acreditado que hubiera accedido a información confidencial o sensible ni mucho menos que hubiera procedido a descargarse o sustraer tal información. Una cosa es entrar y salir de un ordenador ajeno, y otra cosa es acceder a la información y sustraer la misma.(…) Por poner un símil que nos ayude a explicarnos: una cosa es abrir la caja registradora de una empresa, a pesar de que no sea necesario para el trabajo, y después cerrarla, y otra cosa es coger el dinero que hay dentro; o una cosa es abrir la puerta del despacho de un superior cuando este no está, y después cerrarla, y otra muy distinta es entrar en el despacho y sustraer la información que hay allí; y en el caso de autos no se ha acreditado que el actor hubiera pasado de la mera conexión, reiteramos, no prohibida" (FJ 3º).*

Otros dos datos que la Sala tiene en cuenta para revocar la sentencia de instancia son los siguientes: primero, que no consta acreditado el uso del programa informático para fines particulares, por lo que presume su uso profesional. Y, segundo aspecto a destacar, la escasa duración de las conexiones en los terminales ajenos. Respecto a la colisión con derechos fundamentales, se niega la intromisión al derecho a la intimidad y la sentencia se basa en una aplicación incorrecta por parte del Juzgado de lo Social de la teoría gradual de la transgresión de la buena fe.

Como reflexión final: El programa que se usó para acceder al ordenador, no consta si era de uso profesional o no, la sentencia dice que presume su uso como de trabajo, porque no se ha acreditado, y debería de haberse insistido en este extremo. En el supuesto de uso profesional, se debería haber determinado si lo habitual era hacer uso común de los ordenadores o bien se trataba de un uso restringido y cada trabajador solo accedía a un terminal.

[639] La Sala argumenta que no todo incumplimiento contractual del trabajador puede ser sancionado con la máxima sanción del despido, y que en este caso el incumplimiento que se le imputa no es tan grave como para llevar aparejada la sanción que se le impone, por lo que la misma es desproporcionada (FJ 2º).

J) Recapitulación

La conocida STS de 29 de septiembre de 2007 sienta el criterio de que el control del uso del ordenador facilitado al trabajador por el empresario no se regula por el art. 18 ET sino por el art. 20.3 ET. En las empresas ha de existir una protocolización de uso del ordenador entregado al trabajador que determine si se tolera su utilización privada o no.

Si consta acreditado el conocimiento del trabajador de la prohibición de uso particular de los ordenadores, no se aplica la teoría gradualista, pues nos hallamos ante un caso claro transgresión de la buena fe contractual caracterizada por la necesaria lealtad y confianza que ha de observarse en la relación laboral.

La existencia de un hábito social generalizado de tolerancia, con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores, crea una expectativa también general de confidencialidad en esos usos; expectativa que ha de ser protegida a nivel constitucional. En estos supuestos procede aplicar la teoría gradualista.

2. El correo electrónico del trabajador

A) Planteamiento

El correo electrónico es, sin duda, el medio más utilizado en la comunicación actual. Las ventajas del mismo dentro del ámbito laboral son incalculables pero, como siempre, la tecnología y el uso social de ésta en el trabajo han evolucionado más rápido que la adaptación de las empresas en el modo de controlar la utilización de este poderoso instrumento de transmisión de datos e información por parte de sus empleados[640].

Recordemos que en más de la mitad de las empresas no existe una política de uso respecto al empleo del correo, ni referencia alguna en el convenio colectivo aplicable y es aquí donde reside el problema, en la existencia de una expectativa razonable de intimidad[641].

[640] MIRÓ MORROS, D. «El uso del correo electrónico en la empresa: protocolos internos», *op.cit.*

[641] INE (2016, 28 de Junio) «Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas», *op. cit.*

Ante las nuevas necesidades prácticas y empresariales, el correo electrónico se ha convertido en un instrumento de doble filo: se trata de una herramienta de trabajo, pero al mismo tiempo supone un medio de comunicación con extenso uso personal. Por ende, en numerosas empresas ha quedado establecida una política de cierta tolerancia a dicho uso personal, lo que es una fuente de conflictos.

B) Pautas de buenas prácticas

La **Recomendación europea** CM/rec(2015)5[642] respecto al tratamiento de datos personales en el entorno laboral, en el ámbito de las comunicaciones electrónicas, contempla la concreta situación del acceso a los correos electrónicos que tengan un carácter profesional, y de cuyo control hayan sido informados con anterioridad los trabajadores, disponiendo que tal control será posible solo "*cuando sea necesario por razones de seguridad o por otras razones legítimas*", enfatizando en que con respecto a las comunicaciones electrónicas privadas en el ámbito del trabajo "*en ningún caso el contenido, el envío y la recepción deben ser objeto de vigilancia*". Por otro lado, se contempla la posibilidad del cese de un trabajador en la empresa, se recoge que el empleador debería tomar las medidas necesarias para desactivar automáticamente la cuenta de correo electrónico del trabajador al término de la relación laboral. En caso de que sea necesario recuperar contenidos de dicha cuenta, esta recuperación debería hacerse previamente a la salida del trabajador y, si es posible, en su presencia.

La AEPD ha suplido la ausencia sobre la falta de previsión de la neutralización o no del derecho a la autodeterminación informativa, analizando esta problemática desde la misma óptica. Lo esencial es que el trabajador esté informado acerca del control, a través de la política de la empresa en cuanto al uso del correo electrónico[643], de modo que conozca las conductas permitidas[644] y los medios de control que se utilizarán. Si estos dos aspectos se regulan, tanto los trabajadores como sus representantes, deberán ser informados del tipo de tecnología utilizada por el empresario en relación con la vigilancia

[642] *https://wcd.coe.int/ViewDoc.jsp?id=2306625*

[643] SAN MARTIN MAZZUCCONI, C.: «El derecho a la protección de datos personales de los trabajadores. Criterios de la Agencia Española de protección de Datos» en AA. VV. SAN MARTIN MAZZUCCONI, C. (DIR). *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, *op. cit*, pág. 224.

[644] Guía de la Agencia de protección de datos sobre «La protección de datos en las relaciones laborales», pág. 28.

y seguimiento de su actividad laboral, debiendo abstenerse el empleador de recoger datos personales que resulten excesivos en razón de la propia naturaleza de la relación laboral.

A su vez, los representantes de los trabajadores obtendrán cumplida información sobre la introducción de cualquier nuevo sistema de registro de datos que afecte al conjunto de los trabajadores, teniendo estos últimos la posibilidad de acceder a los datos que se procesen sobre ellos y el derecho a rectificar los posibles errores que les afecten.

Salvo excepciones extremas, fundamentadas en una firme sospecha sobre la existencia de actividades delictivas o dolosas del trabajador, el derecho de información en la recogida de datos constituye un requisito indispensable para utilizar, en su caso, la información recabada en el lugar de trabajo contra el propio trabajador. En este supuesto, el empleado deberá tener la oportunidad de acceder a la información que le es adversa a fin de poder rebatirla[645].

La AEPD, al igual que el TS, concibe el correo electrónico como un medio de trabajo propiedad del empresario y, por ello, a través de la información correspondiente o en su caso a través de la existencia de una prohibición, entiende que hay razones más que suficientes para poder fiscalizarlo. Pero otra cuestión distinta es el control oculto, si hay sospechas de irregularidades, este es el título legitimador para proceder a su fiscalización, no es posible obviamente ejercer los derechos de la LOPD[646].

C) Variables jurídicas relevantes

La primera cuestión que se nos plantea es que hay que delimitar supuestos distintos. En primer lugar si la cuenta de correo es corporativa y si el empleado está advertido de que el mismo no puede usarse con fines particulares. En este caso no parece que se puedan poner obstáculos a dicho control, más que el principio de proporcionalidad respecto a la idoneidad de la medida en relación con el trabajo que desarrolla y la ponderación del control que se realiza. En segundo lugar, si la cuenta de correo del trabajador es privada, su fiscalización vulneraría el derecho a la intimidad del mismo.

---

[645] Informe Jurídico AEPD núm. 2007-0391: «Cribado de correo electrónico».

[646] MUÑOZ RUIZ, A.B.: «Convergencia y Divergencia entre los Tribunales del Orden Social y la Agencia Española de Protección de Datos en materia de control informático de la prestación de trabajo. (Comentario a las SSTS de 8 de marzo y 6 de octubre)», *Revista Española de Derecho del Trabajo*, núm. 156, 2012, pág. 13.

La cuestión de fondo es que el uso del correo para fines particulares puede suponer un perjuicio, en cuanto al tiempo perdido por el empleado en tareas ajenas[647], porque desde el punto de vista del desgaste de los equipos informáticos y el coste que se ocasiona, es prácticamente cero[648].

Por tanto, el perjuicio sufrido por la empresa por el uso del correo electrónico para fines particulares es más bien de productividad de los empleados que del coste de infraestructura y medios técnicos; a no ser, de que el volumen de los correos electrónicos sea muy grande y además contengan ficheros de gran tamaño, lo cual puede suponer una saturación de la línea de Internet.

De las posibilidades de uso desviado del correo electrónico las que más riesgos entrañan son, por un lado, el envío de ingentes cantidades de email desde el correo de la empresa, y, por otro lado, traspaso de ficheros con "*material sensible*" de la empresa, realizando una "*fuga de información*" a favor de terceros competitivos con la actividad de la organización productiva que se desarrolla, lo cual podría incurrir incluso en un ilícito penal[649].

La mayor parte de la doctrina aplica como criterio ponderador el principio de proporcionalidad para considerar procedente un despido, siempre que hubiera una necesidad justificada objetiva y razonable[650].

D) Derechos fundamentales en conflicto

A nivel constitucional el correo electrónico posee varias peculiaridades importantes. Por lo pronto, en su control pueden resultar lesionados tres derechos fundamentales: el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos[651]. El TEDH ha establecido que la Convención Europea de Derechos Humanos (art. 8) ampara a los correos electrónicos enviados desde

---

[647] El daño ocasionado a la empresa se puede calcular si se conoce cuánto tiempo el empleado pierde en relación con la jornada laboral.

[648] Con una tarifa plana de conexión mandar un correo electrónico donde no se adjunta fichero no supone coste alguno.

[649] RODRÍGUEZ ESCANCIANO, S. *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op.cit.*, pág. 80.

[650] *Ibídem.*

[651] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: Control informático, videovigilancia y protección de datos en el trabajo, *op. cit,* pág. 185.

el trabajo y su vulneración da lugar a la oportuna indemnización por daños morales, en este sentido la STEDH de 3 de abril de 2007 [652], asunto Copland, que recoge que el derecho a la intimidad se extiende no solo al contenido de los mensajes electrónicos sino también a la ingente información que se acumula por su titular en un ordenador personal -entre otros datos sobre su vida privada y profesional-. Información que forma parte del ámbito de la intimidad constitucionalmente protegido, siendo el ordenador un instrumento útil para la emisión o recepción de correos electrónicos, puede quedar afectado el derecho a la intimidad personal en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado.

En ese control puede estar implicado un tercero ajeno a la relación contractual con las partes, el cual no tiene vínculo con la empresa ni está sometido a su poder de dirección ni de control. El derecho al secreto de las comunicaciones, el derecho a la intimidad, y el derecho a la autodeterminación informativa no dependen de la ubicación y de la propiedad de los medios electrónicos utilizados, según se establece en la CE en los principios jurídicos fundamentales.

El empresario, pese a poseer la titularidad de las herramientas de trabajo, es un tercero ajeno frente al que se puede oponer el derecho al secreto de las telecomunicaciones y el derecho a la intimidad; de modo que no pueda fiscalizar las comunicaciones privadas o profesionales. El derecho de propiedad no puede imponerse de tal forma a los derechos fundamentales.

En principio, tanto el Tribunal Supremo como el Tribunal Constitucional, en relación al uso del correo electrónico, han llegado a un punto de encuentro en este aspecto, respecto al derecho a la intimidad y al secreto de las telecomunicaciones, como ya vimos en el apartado de la expectativa razonable de confidencialidad. La información previa a los afectados o en su caso la existencia de una prohibición absoluta neutraliza estos derechos, por lo que aquí se realiza una remisión a dicha teoría general.

E) Criterios jurisprudenciales

[652] STEDH 3 de abril de 2007 (TEDH 2007\23).

Pese a las buenas prácticas europeas y españolas recomendadas, los Tribunales (STS de 6 de octubre de 2011[653], y las SSTC 241/2012, de 17 de diciembre[654], 170/2013, de 7 de octubre[655]), optan por una postura más flexible como ya vimos en la parte general, la advertencia sobre el posible control del correo ya es suficiente, no hay necesidad de determinar cómo se llevará a cabo ese control.

De modo que si lo único que hay es una prohibición de uso de medios telemáticos, no parece factible el ejercicio de los derechos contenidos en la LOPD, de la misma manera que si existe cierta tolerancia, sí es posible ejercerlos.

Debe tenerse en cuenta que la STS de 21 de septiembre de 2015[656], en la que el TS declara nula la práctica empresarial consistente en exigir a los empleados que faciliten "*voluntariamente*" sus datos electrónicos de contacto, correo electrónico y número de móvil y su compromiso para comunicar la inmediata variación de tales datos para que la empresa efectúe cualquier comunicación relativa a su relación laboral. Se desestima el recurso de casación ordinario interpuesto, y en consecuencia, se confirma la SAN de 28 de enero de 2014[657], que declaraba que la cláusula era contraria a la LOPD, pues estos datos de carácter personal voluntariamente se pueden poner a disposición de la empresa, pero no puede constar como específica cláusula- tipo.

Con arreglo a este criterio, el derecho fundamental a la autodeterminación informativa protege su utilización indebida, su obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles y tiene que quedar bajo el control de su titular, es decir, el trabajador:

> "*Como oportunamente indica el razonado informe del Ministerio Fiscal, «nos encontramos ante unos datos de carácter personal, cuyo conocimiento, uso y destino tiene que quedar bajo el control de su titular»; y la incorporación al contrato de una cláusula como la cuestionada «supone una conducta abusiva y no puede entenderse que el trabajador haya prestado su consentimiento de una manera libre y voluntaria*"(FJ 3º).

Ello es así porque el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento en relación a una previsión negocial referida a un derecho fundamental, y que dados los tiempos actuales, bien puede entenderse que el consentimiento sobre tal extremo no es por completo libre y voluntario. Por tanto, el Alto Tribunal declara la nulidad de este tipo de

---

653 STS 6 de octubre de 2011 (RJ 2011\7699).
654 STC 241/2012, de 17 de diciembre (RTC 2012\241).

655 STC 170/2013, de 7 de octubre (RTC 2013\170).

656 STS de 21 septiembre de 2015 (RJ 2015\4353).
657 SAN de 28 de enero de 2014 (EDJ 2014/5469).

cláusulas genéricas, desestima el recurso de la empresa y confirma la sentencia de la Audiencia Nacional que se pronunciaba en el mismo sentido.

F) Uso indebido con fines personales

a) Premisas

La utilización personalizada de correo electrónico, se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa. El uso para fines privados del instrumento de comunicación ha de reputarse en principio lícito y la prohibición de dicho uso puede vulnerar el derecho a la libertad individual de expresión y comunicación de los trabajadores, en los mismos términos que lo haría si se prohibiese a los trabajadores hablar entre sí.

Por tanto, si la utilización es exclusivamente personal, como consecuencia del establecimiento de una cuenta a nombre del trabajador, rige el secreto a las comunicaciones[658]. Es claro que las comunicaciones que realiza el trabajador como medio propio quedan fuera del control empresarial, aunque se realicen durante el tiempo y el lugar del trabajo[659].

Cuestión distinta es que, como ocurre con la simple comunicación verbal del trabajador con otros trabajadores, con clientes o con terceros en general, el uso concreto de dicha comunicación pueda reputarse ilícito , bien por su contenido -ofensas verbales y actos no amparados por la libertad de expresión-, bien por cuanto suponga una distracción indebida, con la consiguiente pérdida de dedicación a la actividad productiva, en cuyo caso la valoración de la conducta del trabajador depende de la gravedad de dicha distracción.

---

[658] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *op.cit*., págs. 32-34.

[659] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op.cit.,* pág. 185.

b) La doctrina del TEDH (Barbulescû)

La STDH de 12 de enero de 2016, caso Barbulescu *vs.* Romania[660], avala el despido de un trabajador de profesión ingeniero, por realizar un uso particular del correo electrónico, basando su fundamentación en que se demostró que incumplió el código interno de conducta que estaba establecido en la empresa, respecto a la utilización de las tecnologías de la información y de la comunicación[661]. En consecuencia, se puede entender que el empresario puede controlar el correo electrónico profesional de sus empleados, sin vulnerar por ello su derecho a la intimidad, recogido en el art. 8 del CEDH.

El empleador informó al trabajador que había realizado un control de la actividad de su cuenta de correo y había comprobado que la había usado para fines particulares, prohibidos por el protocolo sobre uso de nuevas tecnologías establecido en la empresa, por lo cual procedió a su despido disciplinario. En el acto de juicio se aportó como prueba documental de los hechos una transcripción de las comunicaciones de dicha cuenta de correo electrónico, en la que constaban intercambios de mensajes entre el demandado y varios familiares (novia y hermanos). El demandante negó que *de facto* se cumpliera el protocolo de la empresa, pues, en la práctica había una situación de tolerancia respecto al uso personal de la cuenta profesional y alegó que con el registro de su correo se había violado su derecho al secreto de la correspondencia.

Los tribunales rumanos estimaron la procedencia del despido, por considerar que este se había realizado conforme a la legislación local aplicable, así como la inexistencia de vulneración del derecho a la intimidad del trabajador, por cuanto este había sido informado de la normativa interna de la empresa y el registro de su correo era el único medio de comprobar si se había respetado esa normativa.

El recurrente alegó ante el TEDH que la decisión del empleador se basaba en una violación del artículo 8 del Convenio, que establece que "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*." Al respecto, el Tribunal europeo consideró que no resultaba abusivo que un empleador quiera verificar que sus empleados cumplen con sus obligaciones durante el horario de trabajo,

---

[660] STDH de 12 de enero de 2016 (EDJ 2016/87).

[661] Este código establecía, entre otras cosas: "*Queda terminantemente prohibido alterar el orden y la disciplina dentro de las instalaciones de la empresa y en particular (...) usar las computadoras, fotocopiadoras, teléfonos, télex y fax para fines personales*".

así como que el demandado había accedido a la cuenta de correo del actor en la creencia de que solo contenía comunicaciones de éste con los clientes de la empresa. Asimismo se alega que el actor había podido invocar ante los tribunales locales la pretendida violación de su vida privada y de su correspondencia, y en esa instancia no se ha realizado mención alguna al contenido de dichas comunicaciones, las transcripciones que aportó la empresa se utilizaron a efectos de acreditar que el interesado había utilizado el ordenador de la sociedad para fines privados y durante el horario de trabajo.

En consecuencia, el TEDH concluye que los tribunales internos han mantenido un equilibrio apropiado entre el derecho del actor al respeto a su vida privada y a la de su correspondencia conforme al art. 8 del Convenio y los intereses de su empleador. Por tanto, no aprecia una vulneración de dicho precepto. En definitiva, esta sentencia no viene más que a corroborar la doctrina de nuestro país de las SSTS de 26 de septiembre de 2007[662], y 6 de octubre de 2011[663], respecto a la prohibición de uso y la inexistencia de una expectativa de intimidad[664].

La sentencia cuenta, sin embargo, con voto particular[665] que discrepa del parecer de la mayoría y señala que "*el caso presentaba una excelente oportunidad para que el Tribunal Europeo de Derechos Humanos estableciera jurisprudencia en el área de la protección de la privacidad de las comunicaciones a través de Internet de los trabajadores*". La tesis fundamental del voto particular, y de perfecta aplicación a las relaciones laborales en España, es que no existe un poder absoluto del empleador sobre control de las relaciones de trabajo por vía informática. Argumento que en modo alguno se expresa con la misma claridad en la argumentación de la mayoría del tribunal. El voto particular parte de la premisa de que el poder empresarial ejercido, en este caso, a través de control en la empresa, no es discrecional ni arbitrario, que ha de estar debidamente

[662] STS 26 de septiembre de 2007 (RJ 2007\7514).

[663] STS 6 de octubre de 2011 (RJ 2011\7699).

[664] El propio TEDH alude a su propia doctrina recogida en otras sentencias anteriores, para recordar que la actuación empresarial debe estar guiada por la debida protección de otros derechos que no son los del trabajador, es decir que son del empleador para garantizar el buen funcionamiento de la empresa y prevenir que la información facilitada al trabajador, o a la que este tenga acceso por razón de su actividad profesional, sea utilizada de forma adecuada. Pero hay que tener en cuenta, que en cualquier caso, la persecución por parte empresarial del máximo aprovechamiento de sus trabajadores y de su productividad no es por sí mismo un interés de los protegidos por los arts. 8 y 10 del CEDH, y que las restricciones a los derechos reconocidos en el CEDH en el marco de una relación contractual son posibles pero siempre que estén debidamente justificados.

[665] Magistrado luso, Pinto de Albuquerque. P

justificado y conocido por los trabajadores[666]. Concluye que el trabajador no tenía suficiente conocimiento de las limitaciones y restricciones en el empleo de los medios tecnológicos para usos no profesionales y concluye que falta un elemento esencial para que pueda valorarse la conformidad a Derecho de una decisión empresarial restrictiva de derechos como los recogidos en el art. 8 del CEDH. Por lo cual la decisión empresarial no sería correcta y el gobierno rumano no habría adoptado las medidas adecuadas para evitar la vulneración del mencionado artículo[667].

Un importante sector de la doctrina de nuestro país se ha posicionado en el lugar de este voto disidente; se afirma que el razonamiento está plagado de contradicciones internas, pues, por un lado se presume la legitimidad general del sometimiento a vigilancia solo por la existencia de la prohibición de uso personal, sin exigir indicio suficiente para sospechar del incumplimiento[668], por otro lado, también se sostiene que la facultad conferida al empresario validada por el TEDH, plantea serias dudas de compatibilidad con los derechos a la intimidad y al secreto de las comunicaciones de los terceros no vinculados al empresario, que reciben y envían correos o mensajes al trabajador a través del medio de comunicación corporativo[669].

---

[666] El voto particular dedica un amplio espacio al estudio y análisis de la normativa internacional sobre la materia, reproduciendo amplios párrafos de los textos normativos para poner de manifiesto la importancia de que previamente los trabajadores tuvieran un conocimiento adecuado de la política empresarial al respecto y además que la decisión empresarial sobre las restricciones que puedan sufrir en el ejercicio de sus derechos de privacidad mientras esté en vigor la relación contractual.

[667] En suma, compartimos la conclusión de este voto disidente; pues de los hechos probados de la sentencia se desprende que no ha existido una regulación clara y precisa que justifique la restricción de un derecho reconocido en el CEDH, por lo que la expectativa razonable de intimidad despliega sus efectos para proteger al trabajador. En definitiva, se advierte que ni los tribunales nacionales rumanos ni el propio TEDH han reparado la vulneración del derecho al respeto de la vida privada del trabajador.

[668] MOLINA NAVARRETE, C.: «Expectativa razonable de privacidad" y poder de vigilancia empresarial: ¿*Quo vadis* Justicia Laboral?», Estudios financieros, Revista de trabajo y seguridad social núm. 399, 2016, pág.176.

[669] FERRANDO GARCÍA, F.: «Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías», Estudios financieros, Revista de trabajo y seguridad social núm. 399, 2016, pág. 58.

c) Uso personal masivo

La STSJ de Cataluña de 9 de junio de 2015[670] considera procedente el despido de una técnico de personal de recursos humanos de una empresa cárnica por estar constantemente mandando correos electrónicos desatendiendo incluso las llamadas entrantes del departamento que las debían atender sus compañeros. En la empresa existía una política de uso de las herramientas informáticas, pues la empresa realizó una comunicación escrita a todos sus trabajadores de que el ordenador constituye herramienta de trabajo y no estaba permitido el uso de los medios informáticos para fines distintos, sean o no de carácter personal.

En relación a la dirección de correo electrónico se establecía que la misma se facilita para uso profesional si bien se admite uso puntual y no prolongado en cuanto a su duración para fines particulares. Del relato de hechos declarados probados quedó acreditado que la recurrente, junto a otros dos compañeros, formaban el equipo de RRHH de la empresa, tenía acceso a servidor electrónico y correo electrónico de uso propio e intransferible, como cada trabajador de la empresa, y realizó las siguientes conductas incompatibles con el documento que había suscrito: 1º) Accedió indebidamente a la dirección de correo electrónico de su compañera de RRHH y realizó copias de varios emails y se las mostró a su otro colega, criticando y menospreciando a la autora de los mismos por el contenido que había leído en ellos. 2º) Accedió indebidamente al ordenador de su compañero y para proceder a borrar un archivo Excel, porque este empleado, a instancias de la empresa, comenzó a anotar el tiempo que la recurrente empleaba en conexiones a Internet para el envío de correos electrónico para uso particular o uso de teléfono móvil. Este compañero pudo comprobar tras ausentarse momentáneamente de su puesto de trabajo que el archivo correspondiente al control de trabajo de la actora había desaparecido. 3º) El responsable de departamento de informática accede a correo de empresa a nombre de la actora y obtiene listado de correos enviados a dirección ajena a empresa y cliente.

En el recurso interpuesto por parte de la representación de la trabajadora se solicitó revisión del derecho aplicado por infracción del art. 55 ET por adolecer la carta de despido

[670] STSJ Cataluña de 9 de junio de 2015 (EDJ 2015/131561).

de vaguedad y vulneración del art. 54.2 ET por inaplicación de la teoría gradualista puesto que los hechos no revisten la gravedad y culpabilidad suficientes. La Sala contesta que al no modificarse los hechos el resultado ha de ser el mismo que el establecido en la sentencia de instancia y además la conducta imputada no es solamente ofender a sus compañeros sino usar el material de la empresa en concreto el correo propio para fines particulares pese a estar prohibido excediendo el uso de este el límite de lo razonablemente tolerable.

d) Uso personal de correo por embarazada

La STSJ de Cataluña de 10 febrero de 2014[671] resuelve el recurso contra la sentencia de la instancia y desestima íntegramente la demanda de despido disciplinario, imputándosele a la actora un uso abusivo del correo electrónico no relacionado con el trabajo, pese a tener conocimiento de la prohibición establecida al respecto, ya que firmó en el año 2007 un documento de confidencialidad con la empresa, conforme al cual tenía el deber de guardar secreto respecto los datos e información de la misma. En el año 2012 volvió a firmar un documento de confidencialidad, sobre normas de uso del correo electrónico, sistemas informáticos y sistemas portátiles, con el compromiso de seguir manteniendo el secreto profesional y las medidas a tomar para su control. Se postula la nulidad del despido por estar la trabajadora embarazada al tiempo de la extinción contractual, la Sala resuelve lo siguiente:

> *"(…)Pese al estado de embarazo al tiempo del despido, no hay indicios de discriminación por razón de sexo, cediendo en cualquier caso la protección reforzada de la situación de embarazo (art. 55.5 ET) ante la acreditación de una causa disciplinaria que justifica la sanción de despido impuesta. La antigüedad de la actora (más de 5 años) y la no constancia de sanciones anteriores no atenúan una realidad claramente constitutiva de deslealtad con la empresa y de quebrantamiento de la buena fe, pues ese uso abusivo se ha producido de manera continuada, a sabiendas de la prohibición de la empresa, persistiéndose en el uso indebido del acceso a Internet incluso después de la firma del segundo documento de confidencialidad, todo lo cual hace que la conducta incumplidora alcance cotas de gravedad y culpabilidad suficientes para merecer la máxima sanción disciplinaria, procediendo por ello mantener la calificación de la decisión extintiva empresarial, al estar asimismo calificada tal conducta como muy grave en el Convenio Colectivo aplicable"*(FJ 3º).

La regulación legal de la nulidad del despido de las trabajadoras embarazadas constituye una institución directamente vinculada con el derecho a la no discriminación

[671] STSJ de Cataluña de 10 de febrero de 2014 (JUR\2014\89308).

por razón de sexo. La eficacia protectora del art. 55.5 ET, que proporciona a las mujeres en estado de gestación una ventaja procesal muy poderosa para la defensa de su puesto de trabajo, que es la presunción legal del móvil discriminatorio, pero la empresa ha destruido tal presunción probando que en modo alguno guarda relación con el despido pues en los hechos probados se ha declarado probado la existencia de una prohibición de uso del correo electrónico para fines particulares y también se ha constatado la utilización indebida de este.

e) Problemas de autoría

La STSJ de Valencia de 24 de mayo de 2013[672] aborda despido por utilización de los medios informáticos puestos a disposición de la trabajadora para un supuesto uso particular. Con anterioridad, a la actora se le notificó un despido objetivo, que se dejó sin efecto al acceder a su ordenador y comprobar que determinados archivos se habían borrado, por lo que se procedió a fiscalizarlo. La Sala de Valencia razona que, ante la inexistencia de prohibición al respecto, y por el hecho de que además muchos de los correos emitidos o recibidos lo fueron en épocas en que la trabajadora estaba fuera de su puesto de trabajo por diversos procesos de incapacidad temporal, hecho este que demuestra que su ordenador también era usado por otras personas, se confirma la sentencia de instancia[673].

---

[672] STSJ de Valencia de 24 de mayo de 2013 (AS 2013\2459).

[673] *5.(…) el despido enjuiciado merece la calificación de improcedente pues de la utilización por la actora de los medios informáticos puestos a su disposición a otros fines, teniendo en cuenta la inexistencia de ninguna prohibición al respecto o protocolo de uso personal de los medios informáticos puestos por la empresa a disposición de la actora, ni que el tiempo que la actora dedicó a remitir o recibir correo electrónico ajeno a su actividad en la empresa implicara dejación de sus funciones u ocupara una parte significativa de su tiempo de trabajo, máxime cuando no pocos de los correos que se consideran emitidos o recibidos por la actora lo han sido en épocas en las que la demandante se encontraba ausente de su puesto de trabajo, por causa de sus procesos de Incapacidad Temporal y por maternidad y que Grupo Quesada Jara,S.L. donde prestaba servicios el marido de la actora conformaba grupo de empresas con la demandada, lo que explica en cierto modo lo declarado en los hechos probados duodécimo y decimotercero.*

6.En consecuencia este motivo se desestima, al no apreciar ninguna de las infracciones jurídicas denunciadas porque no consideramos que los hechos constitutivos de incumplimiento contractual en que la actora haya podido incurrir (cuando estaba presente en su puesto de trabajo), tengan la gravedad

En consecuencia, el criterio delimitador ante la ausencia de prohibición expresa de uso particular del correo electrónico, es que se entiende que hay tolerancia, siempre que no conste que tal uso implica dejación de funciones o una ocupación significativa del tiempo de trabajo.

G) Utilización con fines profesionales

El correo electrónico se concibe como una herramienta de trabajo[674], el control de este tipo de correo se realizará, únicamente cuando resulte absolutamente imprescindible para el desarrollo de la prestación laboral. En los demás casos la supervisión tendrá que limitarse a controles externos que pueden suponer un sacrificio aceptable desde el punto de vista del principio de proporcionalidad[675]; por otro lado, también son recomendables, los controles preventivos a través de "*filtros*".

Cabe argüir que en supuestos de que el trabajador no realice un uso profesional del correo electrónico y cause un perjuicio a la empresa, ésta podrá perfectamente despedirle de modo disciplinario por transgresión de la buena fe contractual, art. 54. 2 d) ET.

Por otro lado también, cabe preguntarse si la dirección de correo electrónico profesional, constituye un dato de carácter personal o no, la Agencia de Protección de Datos ha resuelto en Informe núm. 0437/2010[676] que no cabe duda de que la dirección de correo electrónico, e-mail profesional, de empresa o corporativo de los trabajadores es un dato de carácter personal.

---

necesaria en razón de todas las circunstancias subjetivas y objetivas indicadas para hacerla merecedora del despido enjuiciado (significativamente la tolerancia empresarial que se trasluce de lo indicado en el epígrafe I del apartado 4 de este fundamento jurídico, y que la razonada sentencia de instancia destaca al final de su fundamento jurídico cuarto) y que la buena fe como destacó la doctrina constitucional subrayada en el apartado 2 de este fundamento jurídico no significa que exista un deber genérico de lealtad con un significado omnicomprensivo de sujeción del trabajador al interés empresarial, pues no resultaría acorde con el sistema constitucional de relaciones laborales" (FJ 4º).

[674] En este sentido se pronuncia la STS 26 de septiembre de 2007 (RJ 2007\7514).

[675] FERNANDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, ed. Aranzadi. 2003, págs. 139-142.

[676] *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2010-0437_Dato-de-correo-electr-oo-nico-de-empresa-de-los-trabajadores.-Cesi-oo-n-a-sindicatos.pdf*

Por tanto, si la empresa trata los datos de los remitentes y los destinatarios de los correos, grabándolos, en ese caso la empresa está obligada como responsable a cumplir con las obligaciones contenidas en la norma; debe informar a los trabajadores de los tratamientos que lleva a cabo con los correos electrónicos.

H) Uso con fines sindicales

a) Normas genéricas

El derecho a la libertad sindical se reconoce en el art. 28.1 CE y comprende el derecho a fundar organizaciones sindicales, el derecho de afiliación y de no afiliación a las mismas y el derecho a desarrollar la actividad sindical. Este último, en el plano colectivo, implica la facultad de los sindicatos de "*desplegar los medios de acción necesarios para que puedan cumplir las funciones que constitucionalmente les corresponden*", entre los cuales se encuentran la negociación colectiva y el conflicto colectivo.

La LOLS recoge el derecho de los trabajadores a recibir la información que les remita el sindicato (art. 8.1.c) y prevé igualmente que "*con la finalidad de facilitar la difusión de aquellos avisos que puedan interesar a los afiliados al sindicato o a los trabajadores en general*", la empresa pondrá a su disposición "*un tablón de anuncios que deberá situarse en el centro de trabajo y en el lugar donde se garantice un adecuado acceso al mismo*" art. 8.2. a) LOLS. Como vemos, la LOLS de 1985 está al margen de las nuevas tecnologías.

2. Modalidades

Dentro de este ámbito, merecen distinguirse, dos conceptos similares pero distintos: 1º) *Ciberderechos sindicales:* derechos sindicales de trabajadores no conectados on line con la empresa, como son los teletrabajadores con equipos no conectados al ordenador de la empresa y/o no conectados entre sí los equipos de los

teletrabajadores[677]. 2º) *Derechos sindicales on line*, -de conformidad con el Código de Conducta de la OIT[678].-, abarca no sólo el derecho de los trabajadores y de los sindicatos al acceso libre a los sistemas de correo electrónico de las empresas para enviar y para recibir comunicaciones, sino también el derecho de los trabajadores al acceso libre a internet para entrar en la página web del sindicato, y la garantía de no vigilancia sobre el correo electrónico o el acceso a internet para entrar en la página web del sindicato[679].

3. El caso de cabecera (BBVA)

El uso sindical de los medios informáticos de la empresa es un tema conflictivo que ha dado lugar a pronunciamientos judiciales del máximo interés, pero el *leading case* en la materia es, sin duda, el caso BBVA, resuelto por la STS de 26 de noviembre de 2001[680] , posteriormente revocada en amparo por la STC 281/2005, de 7 de noviembre[681].

La Federación de Servicios Financieros y Administrativos de Comisiones Obreras enviaba a sus secciones sindicales, a sus afiliados y, en general, a los trabajadores del BBVA mensajes de correo electrónico para transmitir información sindical. Para ello usaba su propio servidor interno, mandaba los mensajes al servidor del BBVA, que los redistribuía a sus destinatarios en las direcciones de correo electrónico del BBVA. Esta situación no planteó problemas hasta que, a partir de una determinada fecha, empezaron a recibirse de este sindicato correos masivos de gran tamaño que colapsaban la red. Ante esta situación la empresa decidió filtrar la entrada desde aquella dirección, rehusando los mensajes y notificando al remitente el rechazo.

El sindicato afectado presentó demanda de conflicto colectivo en la que solicitaba que se declarase su derecho a transmitir noticias de interés sindical a sus afiliados y

---

[677] LOUSADA AROCHENA, J.F.: La sentencia 281/2005, de 7 de noviembre, del Tribunal Constitucional, o la carta de bautismo de los ciberderechos sindicales, *Revista de Jurisprudencia El Derecho*, núm.2, 2006 (EDB 2006/424).

[678] Declaración de la OIT relativa a los Principios y derechos fundamentales en el trabajo y su seguimiento - adoptada por la Conferencia Internacional del Trabajo en su octogésima sexta reunión, Ginebra, 18 de junio de 1998 (Anexo revisado, el 15 de junio de 2010).

[679] *Ibidem.*

[680] STS de 26 de noviembre de 2001 (RJ 2002\3270).

[681] STC 281/2005, de 7 de noviembre (RTC 2005\281).

trabajadores a través del correo electrónico de la empresa. El Tribunal Supremo rechazó la pretensión en una argumentación sencilla, basada en cuatro premisas[682]:

- El Banco puso a disposición de sus empleados, como herramienta de trabajo, el correo electrónico para el desarrollo de su trabajo.
- No hay pacto individual ni colectivo que otorgue al sindicato tal derecho:
- El sindicato ha usado el mencionado medio de comunicación durante un año.
- No ha habido una adquisición del derecho por uso pacífico, sino simplemente una situación tolerada, mientras no produjo problemas en las comunicaciones.

El Tribunal considera que la utilización del correo electrónico de la empresa "*podrá ser objeto de negociación colectiva o acuerdo de cualquier tipo, pero, mientras no se obtenga, la utilización deberá ser expresamente consentida por la empresa*", y aclara que "*el art. 8 LOLS consagra el derecho de los afiliados a recibir la información que les remita su sindicato, más no establece que sea la empresa la que deba facilitar los medios materiales para llevarla a cabo"* (FJ 4º).

La solución del Tribunal Supremo fue anulada por el Tribunal Constitucional en una sentencia compleja y muy debatida por la doctrina científica: la STC 281/2005, de 7 de noviembre[683]. En ella, el TC afronta la cuestión desde la perspectiva del derecho fundamental a la libertad sindical, y recuerda que éste no sólo posee una dimensión asociativa u organizativa, sino también funcional que alcanza al derecho de los sindicatos a "*desplegar los medios de acción necesarios para que puedan cumplir las funciones que constitucionalmente les corresponden*" (FJ 3º).

Ello incluye, según se señala en el fundamento jurídico cuarto, el envío de información sindical "*a través de los cauces previstos en la ley y también por medio de otros que libremente adopte siempre que respete la normalidad productiva*", correspondiendo al empresario "*asumir ciertas cargas tasadas en la ley y dirigidas a hacer efectivo el hecho sindical informativo*". El TC constata la ausencia de una obligación legal de facilitar la transmisión de información sindical a los trabajadores, afiliados o no, a través de un sistema de correo electrónico con cargo al empleador y puntualiza que las empresas "*no están obligadas a dotarse de esa infraestructura informática para uso sindical*" (FJ 5º). Ahora bien, esto no significa, a juicio del Tribunal que no exista este derecho allí donde sí existen medios informáticos. Atendido el hecho de que la difusión de información sindical forma parte del contenido esencial del derecho fundamental, el Tribunal fija distintos criterios aplicables al caso: *" (...)*

[682] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op.cit*, pág. 202.

[683] STC 281/2005, de 7 de noviembre (RTC 2005\281).

a) El flujo de la información sindical resultará objetivamente perjudicado si el empleo de los instrumentos prácticos o medios materiales que pueden favorecerla es obstruido.

b) La garantía del contenido esencial del derecho fundamental, consistente en evitar el establecimiento de dificultades a su ejercicio más allá de lo razonable, no es ajena al empresario, en la medida en que la actividad sindical se desarrolle en el seno de su organización productiva.

c) Tenga o no un deber de colaboración en la promoción del derecho fundamental que venimos considerando conforme a la ley, los pactos o sus posibles concesiones previas, el empresario tiene en todo caso una obligación de no obstaculizar injustificada o arbitrariamente el ejercicio de dicho derecho" (FJ 7º[684]).

Por tanto, los límites que, según el TC, deben respetar los sindicatos para el envío de comunicaciones electrónicas serían los siguientes: 1) No obstaculizar la actividad normal de la empresa. 2) Respetar las condiciones fijadas por el empresario para realizar los envíos, ya que el correo electrónico sigue siendo un medio de producción cuyo uso preferente es el empresarial. 3) No causar mayores costes o gravámenes al empresario.

A modo de recapitulación, podemos concluir que esta Sentencia consagra el reconocimiento a las secciones sindicales (comités de empresa y delegados de personal) del derecho a ejercer las libertades de expresión e información sindical a través del correo electrónico corporativo. La clave de la decisión de la sentencia es que el contenido esencial de la libertad sindical tiene una nueva dimensión, ya que el empresario o cualquier tercero está obligado a no dificultar el desarrollo de la libertad sindical. Con lo que el derecho a la libertad sindical sale de su territorio clásico como derecho de libertad y se convierte en un derecho de prestación[685].

El criterio sentado por el TC resulta de enorme trascendencia, y no parece que existan especiales dificultades para proyectarlo más allá del estricto caso examinado. Eso significa que lo que aquí se mantiene respecto del uso del correo por los sindicatos, podría extenderse, en principio, al uso por los representantes unitarios, de las herramientas de trabajo propiedad de la empresa que sirven para ejercitar la libertad sindical[686]. La crítica más coherente de esta sentencia está en el voto particular que la acompaña, que resumimos en tres puntos:

---

[684] Y concluye que: " (…) Sobre el empresario pesa el deber de mantener al sindicato en el goce pacífico de los instrumentos aptos para su acción sindical siempre que tales medios existan, su utilización no perjudique la finalidad para la que fueron creados por la empresa y se respeten los límites y reglas de uso que a continuación enunciaremos, cuyo cumplimiento deberá examinarse en cada caso. En tales condiciones no puede negarse la puesta a disposición, ni puede unilateralmente privarse a los sindicatos de su empleo, debiendo acudirse al auxilio judicial si con ocasión de su utilización el sindicato llega a incurrir en excesos u ocasionar perjuicios, a fin de que aquéllos sean atajados y éstos, en su caso, compensados".

[685] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op.cit*, pág. 203.

[686] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: «El uso sindical del correo electrónico a la luz de la STC 281/2005, de 7 noviembre», Revista Doctrinal Aranzadi Social, núm. 17, 2005.

- El uso sindical de una determinada herramienta tecnológica de comunicación de propiedad de la empresa en modo alguno puede insertarse en el contenido esencial de la libertad sindical, sino que en todo caso su única calificación posible será la de contenido adicional de esa libertad, que necesita para su existencia una determinada base normativa o convencional.
- "*Es un inaceptable recurso dialéctico el acudir al contenido esencial, como fuente del pretendido derecho, para soslayar la carencia radical de otra fuente infraconstitucional de aquél*".
- Solo sobre la base de la existencia previa de un derecho de uso sindical puede limitarse el derecho de propiedad de la empresa en su facultad de disposición.

4. Otros casos relevantes

* Se ha entendido que el derecho al uso de Internet y la posibilidad de acceder al correo electrónico no se regula en la normativa, pero se considera una derivación del derecho de información sindical integrado, con carácter más genérico, en el derecho fundamental a la libertad sindical que se lesiona al prohibir a un sindicato el acceso a internet o al correo electrónico corporativo en igualdad de condiciones con los demás sindicatos, como proclama la STS de 23 de julio de 2008[687].

* Se sostiene que no se vulneran los derechos de libertad sindical y del secreto de las comunicaciones si se exige la identificación de una persona, para el uso de la cuenta genérica de correo electrónico con fines sindicales, como administrador de la misma (STS de 16 de febrero de 2010[688]).

* Se considera justificada la negativa empresarial a que los representantes sindicales utilicen los medios informáticos de la empresa para comunicarse con sus afiliados y con el resto de los trabajadores cuando su uso resulta perturbador, perjudicial y costoso (SAN de 12 de julio de 2010[689]).

* La STS de 24 de marzo de 2015 [690], en relación a su uso del correo electrónico, ha establecido que el derecho de libertad sindical no constituye un derecho ilimitado y la empresa puede organizarlo de modo que no se bloquee por envíos masivos amoldándose

[687] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op.cit.*, pág. 203.

[688] STS de 16 de febrero de 2010 (EDJ 2010/14364).

[689] SAN de 12 de julio de 2010 (EDJ 2010/141670).

[690] STS de 24 de marzo de 2015 (EDJ 2015/80833).

a la capacidad de los equipos técnicos, sobre todo cuando ésta ha elaborado el documento "*política de uso de correo electrónico corporativo*".

* La doctrina del TS ha admitido que se vulnera la libertad sindical cuando la empresa se niega de manera injustificada el acceso a la cuenta de correo electrónico . Además, el derecho a distribuir información a través del correo electrónico de la empresa comprende el derecho a acceder a la lista de direcciones electrónicas de la plantilla por parte de los sindicatos (STS de 14 de julio de 2016[691]). Asimismo, el Alto Tribunal, considera contrario a la libertad sindical la imposición de un conocimiento previo a la distribución de información sindical (STS de 2 de noviembre de 2016[692]).

I) Perspectiva penal

Desde el punto de vista del Derecho Penal, el art. 197 del CP castiga con penas de hasta cuatro años la interceptación ilegítima de las comunicaciones personales. En este sentido, la Sala Segunda del TS baraja criterios más estrictos y rigurosos, que la Sala Cuarta, para justificar la injerencia en el correo electrónico de los imputados, ya que para invadir el secreto de las comunicaciones se necesita una autorización judicial; de lo contrario la prueba que de tal medio se derive es ilícita.

La STS de fecha 16 de junio de 2014[693], dictada por la Sala 2ª, establece una importante matización a la validez probatoria, en el ámbito penal, del registro del correo electrónico corporativo de un trabajador; debiendo subrayarse su manifiesto interés en que la misma contribuya a "fijar una clara doctrina en materia de tanta trascendencia"[694].

---

[691] STS de 14 de julio de 2016 (EDJ 2016/145506).

[692] STS de 2 de noviembre de 2016 (EDJ 2016/215609). El TS considera que la actuación de una empresa, bloqueando, censurando y negándose a publicar las circulares y comunicados de un sindicato, por correo electrónico supone una vulneración del derecho fundamental a la libertad sindical (FJ 4º).

[693] STS, Sala 2ª, 16 junio de 2014 (RJ 2014\3451).

[694] La sentencia comienza poniendo en cuestión los criterios fundamentales que habían sido afirmados por la Sala de lo Social del Tribunal Supremo y luego confirmados por el Tribunal Constitucional. Señala de este modo la Sala de lo Penal del Tribunal Supremo que: «*considera conveniente (…), salir al paso de ciertas afirmaciones rotundas, incluidas en la propia Resolución de instancia a pesar de aquellas iniciales constancias referentes a la irrelevancia de la prueba, tales como las de que "...el*

Entiende el Tribunal que el citado precepto "*no contempla, por tanto, ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado ("correo corporativo"), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia*" (FJ 1º).

Tampoco, entiende la Sala de lo Penal, una supuesta "*tácita renuncia*" al derecho puede convalidar la ausencia de intervención judicial. Y ello, por un doble orden de razones, por un lado, "*porque obviamente dicha "renuncia" a la confidencialidad, o secreto de la comunicación, no se produce ni es querida por el comunicante que, de conocer sus consecuencias, difícil es imaginar que lleve a cabo la comunicación objeto de intervención*"; y por otra parte, "*porque ni aun cuando se entienda que la "renuncia–autorización" se haya producido resultaría operativa ya que, a diferencia de lo que ocurre con la protección del derecho a la inviolabilidad domiciliaria (art. 18.2 CE), nuestra Carta Magna no prevé, por la lógica imposibilidad para ello, la autorización del propio interesado como argumento habilitante para la injerencia*"[695].

La Sala Segunda declara imprescindible la previa autorización e intervención judicial, todo ello a partir del importante Auto de 18 de Junio de 1992[696] (caso "Naseiro"[697]), cualquiera que fueren las circunstancias o personas, funcionarios

---

ordenador registrado era una herramienta propiedad de la empresa y facilitada por la empresa a don (sic) Rodolfo exclusivamente para desarrollar su trabajo, por lo que entendemos que incluso en aquel supuesto en que pudiera utilizar el ordenador para emitir algún tipo de mensaje de carácter personal, entendemos que al utilizar precisamente un ordenador ajeno, de la empresa, y destinado exclusivamente para el trabajo a la empresa, estaba asumiendo –cediendo– la falta de confidencialidad –secreto– de las comunicaciones que pudiera tener el señor utilizando tal terminal informático».

[695] La sentencia recuerda que el régimen de protección del derecho al secreto de las comunicaciones es, sin duda, "el más enérgico de los que dentro del genérico derecho a la intimidad se contemplan en el repetido art. 18 CE al excluir cualquier posible supuesto que no contemple la intervención del Juez como tutelador del derecho del investigado, y ello porque al margen de otras razones, lo que es aún más decisivo, "porque por mucho que el investigado, como en el caso presente, sea empleado de la dueña del instrumento, la incursión en sus comunicaciones produce automática e inmediatamente la injerencia en el correspondiente derecho al secreto de los terceros que con él comunican, ajenos a esa relación con el titular de la herramienta y de sus condiciones de uso".

[696] ATS Sala 2ª de 18 junio 1992 (EDJ 1992/21750).

[697] Fue un presunto caso de corrupción del Partido Popular, conocido poco después de llegar Aznar a la presidencia del partido en 1989. Un juez instructor de Valencia dictó auto de procesamiento contra varios miembros del Partido Popular entre los que se encontraban su tesorero, Rosendo Naseiro y anterior tesorero, Ángel Sanchis Perales, también diputado y Pedro Agramunt, también diputado. Por la condición

policiales, empresarios, etc., que tales injerencias lleven a cabo. Señala la Sentencia que la referida limitación operará tan sólo respecto a lo que estrictamente constituye ese "*secreto de las comunicaciones*", de lo que resulta que el criterio para determinar qué es lo que el art. 18.3 CE protege se centraría exclusivamente en el concepto de "*comunicación*": cualquier relación entre personas que encajara en el concepto de comunicación estaría comprendido en el ámbito de aplicación del precepto.

No se discute que el secreto de las comunicaciones protege el mensaje, prohibiendo a terceros que accedan a él, con la consiguiente ilicitud de los actos que contravengan esta prohibición y las consecuencias que de ello derivan en el ámbito probatorio. Sin embargo, no quedarían bajo el régimen de tutela cualificada a que se refiere la Sentencia de la Sala de lo Penal del Tribunal Supremo, los denominados "*datos de tráfico*" o incluso la posible utilización del equipo informático para acceder a otros servicios de la red como páginas web, etc., de los mensajes que, una vez recibidos y abiertos por su destinatario, no forman ya parte de la comunicación propiamente dicha, respecto de los que rigen normas diferentes, como las relativas a la protección y conservación de datos (art. 18.4 CE) o a la intimidad documental en sentido genérico y sin la exigencia absoluta de la intervención judicial (art. 18.1 CE).

En estos casos, el secreto sólo cedería ante la resolución judicial que autorice la intervención de la comunicación; bien entendido que no se trata sólo de cualquier autorización judicial, sino de la que corresponda a una intervención que esté prevista en la ley. Por ello, no estando prevista una intervención específica para los incumplimientos laborales con carácter general, sólo podrían ser autorizados por el juez penal las intervenciones que correspondieran a la investigación de incumplimientos laborales, que pudieran calificarse como delitos en el marco del proceso penal en virtud del art. 579 LECRIM a cuyo tenor: «*Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la*

---

de aforados de estos dos últimos, la causa se derivó al Tribunal Supremo. En el TS quedó archivado el proceso por irregularidades en la instrucción del sumario, ya que las escuchas telefónicas ordenadas se habían decretado para investigar únicamente un supuesto de narcotráfico y, por tanto, su utilización en el presunto delito de financiación ilegal no gozaba de supervisión judicial. El tribunal ordenó la posterior destrucción de las cintas inculpatorias con las conversaciones de los implicados.

comprobación de algún hecho o circunstancia importante de la causa»[698]. En este sentido, cabe aludir la doctrina de la sentencia de la AP de Asturias de 17 de septiembre de 2015, que castigó con pena de prisión de dos años, a un empresario que encontrándose un trabajador suyo en proceso de incapacidad temporal "*interceptó,* "*bloqueó*" o "*redireccionó"* el correo electrónico del denunciante a su ordenador sin conocimiento previo ni consentimiento del mismo y figurando que los mensajes interceptados fueron "*leídos*" en su ordenador[699].

Y, trasladando estas conclusiones al sector social, cierta parte de la doctrina afirma que la postura en el orden laboral debería ser la misma que la de la Sala Segunda del Tribunal Supremo, tras la reforma de la LRJS, pues así se desprende del tenor literal del art. 90.4 de la LRJS[700], por lo que sería necesario revisar los criterios de la jurisprudencia para que sea válido un correo como prueba en acto de juicio o bien haya conocimiento expreso del trabajador u orden judicial[701]. Las dudas son razonables pero el efecto expansivo del pronunciamiento de la Sala de lo Penal del Tribunal Supremo no debería alcanzar a las prácticas actualmente existentes en nuestras empresas, salvo cuando la actividad de control pretenda, superando el régimen disciplinario laboral, alcanzar un expreso reproche penal.

J) Utilización para competencia desleal

En el marco de las relaciones laborales se pueden originar conflictos entre el titular de la empresa y los trabajadores. Estas controversias alcanzan uno de sus puntos culminantes en aquellos casos en los que por el empresario se entiende que algún empleado que está trabajando en su empresa actúa de forma desleal al entrar en

---

[698] GARCÍA PERROTE- ESCARTÍN, I. y MERCADER UGUINA, J.R: «El registro del correo electrónico de un trabajador en el ámbito penal requiere autorización judicial: los matices de una inquietante doctrina», *Revista de Información Laboral*, núm. 8, 2014 (BIB 2014\3741).

[699] SAP Asturias de 17 septiembre de 2015 (JUR 2015\233581).

[700] Dispone el artículo 90.4 LRJS: «Cuando sea necesario a los fines del proceso el acceso a documentos o archivos, en cualquier tipo de soporte, que pueda afectar a la intimidad personal u otro derecho fundamental, el juez o tribunal, siempre que no existan medios de prueba alternativos, podrá autorizar dicha actuación, mediante auto, previa ponderación de los intereses afectados a través de juicio de proporcionalidad y con el mínimo sacrificio, determinando las condiciones de acceso, garantías de conservación y aportación al proceso, obtención y entrega de copias e intervención de las partes o de sus representantes y expertos, en su caso».

[701] TOSCANI JIMÉNEZ, D.: «La vulneración del derecho a la intimidad por delatores, detectives privados y medios tecnológicos», *Revista Española de Derecho Social*, núm.71, 2015, pág. 70.

competición directa con los intereses de la misma. Se entiende por competencia desleal la actividad del trabajador encaminada a realizar labores de la misma naturaleza o rama de producción de las que está ejecutando en virtud de contrato de trabajo, sin consentimiento del empresario y siempre que le cause un perjuicio real o potencial (STS 22 de marzo de 1991[702] y SSTJ de Madrid de 19 de diciembre de 2012[703]).

En este sentido, es necesario diferenciar los supuestos de competencia desleal durante la vigencia del contrato de trabajo o una vez extinguido el mismo. En el primer supuesto, que es el que nos ocupa, el deber de buena fe, respeto y fidelidad exigible al trabajador en base al propio contrato de trabajo incluye la obligación del trabajador de abstenerse de realizar actividades que resulten competitivas para su empresa, tanto por cuenta ajena como también por cuenta propia[704].

a) Corrección de la carta de despido

Es frecuente encontrar en la jurisprudencia supuestos en los que el trabajador sustrae información de la empresa a la competencia través del correo electrónico, pero existen deficiencias en las cartas de despido entregadas y el despido es declarado improcedente:

- Carta de despido en la que se alega competencia desleal y no se especifican de manera adecuada las fechas (en algunas ocasiones solamente el mes) en que tuvieron lugar los hechos y si se detallan las empresas de la competencia con quien se relacionaban trabajador despedido y los mecanismos a través de los cuales se cruzaban comunicaciones (STSJ de Extremadura de 30 de junio de 2004[705]) .

- Imputar al trabajador haber remitido software de la empresa a una dirección de correo electrónico , sin especificar de qué software se trata, ni aportar datos sobre los envíos (STSJ de Cataluña de 9 de julio de 2002[706]).

---

[702] STS 22 de marzo de 1991 (EDJ1991/3175).

[703] STSJ de Madrid de 19 de diciembre de 2012 (EDJ 2012/311589).

[704] CORTÉS, S. y PEDRAJAS QUILES, A.: «Pactos de no competencia desleal para después de extinguido el contrato de trabajo», *TOGAS*, núm. 25, 2003 (EDB2003/254767).

[705]STSJ Extremadura de 30 de junio de 2004 (EDJ 2004/68309).

[706]STSJ Cataluña de 9 de julio de 2002 (EDJ 2002/45071).

- Imputar la utilización indebida del correo electrónico por competencia desleal precedida de sanción por los mismos hechos (STSJ de Valencia de 27 de abril de 2001[707]).

b) Captación de clientes para empresa competidora

La STSJ País Vasco de 8 noviembre 2016[708] aborda el caso de un director de oficina bancaria (Kuxtabank) que desarrolla una actividad concurrente o en competencia desleal con las que realizaba habitualmente la entidad bancaria en la que trabaja a través del correo electrónico particular. Se establece como hecho probado el envío masivo de correos electrónicos desde el ordenador del trabajo, con la finalidad de captación de fondos de inversión extranjeros, con un interés particular, concurriendo los requisitos exigidos en la jurisprudencia para entender que existe competencia desleal, a saber: 1) Estar un mismo sector de actividad industrial o comercial, la actividad desarrollada era efectivamente concurrente; el trabajador despedido realizaba tareas laborales de la misma naturaleza o rama de producción de las que se estaban ejecutando en virtud del contrato de trabajo suscrito. 2) Ausencia de consentimiento del empresario. 3) Posibilidad de perjuicio real o potencial.

La Sala pone el acento para justificar el despido en que lo característico de esta falta que se le imputa e es el elemento intencional que revela una premeditada conducta desleal del trabajador respecto del banco que le paga y le facilita los medios para adquirir la experiencia y perfeccionamiento profesional que luego se pretende utilizar en beneficio propio y demérito de los intereses de la entidad bancaria. Se razona que al haber quedado acreditada que la finalidad de los correos electrónicos, y a pesar de reconocer la Sala que el conflicto de intereses no era directo[709] y que la conducta no tenía exacto encaje en el Código Deontológico de Kutxabank, se justifica la procedencia del despido, porque los correos se enviaban en tiempo y lugar de trabajo y con los medios de trabajo facilitados, y a mayor abundamiento se adjuntaba un link a los correos que vinculaba ese uso particular a la entidad bancaria, comprometiendo con ello, la imagen del banco.

[707]STSJ Valencia de 27 de abril de 2001 (EDJ 2001/41088).

[708] STSJ País Vasco de 8 de noviembre 2016 (EDJ 2016/247909).

[709] Se reconoce que dicha actividad (inmobiliaria) podía, en principio, no concurrir con los intereses de la demandada, pero al tener la entidad bancaria como objeto social la prestación de servicios de inversión la incompatibilidad quedaba patente.

Parece que la Sala realiza "*un encaje de bolillos*" para justificar la procedencia del despido, fundándolo más en uso particular del correo electrónico que en la competencia desleal aludida en la carta de despido pues un banco aunque vende fondos de inversión, no es una inmobiliaria y más cuando se reconoce que tal conducta no encaja con lo previsto en el código deontológico sobre competencia. Independientemente de que se argumente, en los fundamentos de derecho que el uso particular estaba prohibido la conducta que se ha sancionado no era esa. En definitiva, la duda, en todo caso, está sembrada.

c) Información confidencial a la competencia

*** La STSJ de Galicia de 30 de mayo de 2014**[710] confirma la procedencia del despido fundamentado en la transgresión de la buena fe contractual. El recurrente, de profesión comercial, fue despedido disciplinariamente. Los hechos comenzaron cuando inició proceso de incapacidad temporal y fue requerido por la empresa para proporcionar la clave de su ordenador, con el fin de que alguien siguiera desarrollando sus funciones y se negó alegando no recordarla por su estado de nerviosismo a raíz de la ansiedad que sufría, además afirmaba que su equipo informático no funcionaba bien, habiendo tenido muchos virus, y había tenido que formatearlo varias veces.

El referido ordenador fue desbloqueado por técnicos externos que fueron contratados al efecto, manifestando estos que no presentaba ningún problema, y que no tenía ningún virus pero la carpeta de clientes estaba totalmente vacía y que el ordenador había sido objeto de un borrado de información selectivo e intencionado de datos, emails, y carpetas, que fueron recuperadas por dichos técnicos, previa realización de un clon del disco duro del ordenador. Se constató el envío desde ese ordenador de documentación confidencial para empresa del sector[711].

Se acciona por despido y la demanda es desestimada en la Instancia. Se recurre en suplicación; por dos motivos, en primer lugar, interesando la nulidad de la prueba motivo que se rechaza, en segundo lugar, se interesa la revisión del Derecho aplicado porque el pronunciamiento, se fundaba en una prueba nula ya que había sido obtenida por la

[710] STSJ de Galicia de 30 de mayo de 2014 (EDJ 2014/128490).

[711] A través de un detective la empresa tuvo la constancia de que el trabajador estaba prestando servicios para una mercantil de la competencia a la que se supone que le ha proporcionado los datos confidenciales extraídos de su ordenador. Ante tales hechos fue despedido.

empresa demandada de forma ilegal. La Sala contesta la fiscalización del ordenador y del correo del trabajador al juicio de proporcionalidad, y lo supera en base a la regla del triple test[712]. Tampoco existe vulneración del derecho al secreto de las comunicaciones, como se pretende de contrario, porque no rige entre los propios comunicantes, y los correos electrónicos han sido aportados por sus receptores.

* **La STSJ de Valencia de 12 de febrero de 2013**[713] desestima el recurso de suplicación de la trabajadora que a través del correo electrónico, reveló información confidencial a la competencia. La recurrente, comercial de una empresa de metales, ha venido revelando información sensible y confidencial a un intermediario ("*dealer*") de la competencia, de la más variada índole (datos de otros clientes y competidores extraída del sistema de información y contabilidad de la empresa, tales como datos contables, números de pedidos y volúmenes de ventas, importe de crédito comercial, porcentajes de descuento o formas de pago acuerdos de distribución con otros proveedores, estrategias de compra y distribución de la empresa, etc.) prevaliéndose del correo electrónico de la empresa. Existía una prohibición de uso personal de las herramientas de trabajo.

En el recurso de suplicación la trabajadora, invoca vulneración del secreto de las telecomunicaciones, a este respecto la Sala contesta, remarcando la inexistencia de una expectativa razonable de confidencialidad, porque si no hay derecho a utilizar el ordenador con fines privados por haber una prohibición para usos personales, no hay derecho constitucional que proteger y utiliza un símil para justificar su razonamiento:

> *"Una de las formas de bajar las barreras es la utilización de un soporte que está sometido a cierta publicidad o a la inspección de otra persona: quien manda una postal, en lugar de una carta cerrada, sabe que el secreto no afectará a lo que está a la vista; quien entra en el ordenador sometido al control de otro, que ha prohibido los usos personales y que tiene ex lege facultades de control, sabe que no tiene una garantía de confidencialidad"(*FJ 2º).

---

[712] "*Aún cuando los e-mails de los que estamos hablando hayan salido de la cuenta de correo, DIRECCION002, la empresa tiene conocimiento de los mismos, no por intromisión en la esfera privada del demandante, sino por aportación documental de su texto, por los receptores de los mensajes de correo, obtención de información que no puede considerarse ilícita, y que supera el examen de proporcionalidad, y necesidad*" (FJ 1º).

[713] STSJ Valencia de 12 de febrero de 2013 (JUR 2013\192329).

d) Filtraciones a terceros

La STSJ de Castilla y León de 18 de noviembre de 2013[714] también confirma la procedencia del despido por filtrar a terceros ajenos a la empresa información confidencial de la misma utilizando como medio el correo electrónico corporativo. El trabajador tenía como profesión la de director de planificación , tres años antes de que ocurrieran los hechos, la empresa le informó y le hizo firmar un documento con la política interna de seguridad y determinadas cláusulas de confidencialidad, pese a ello, se constata, el envío de información confidencial desde el correo corporativo. Por parte del trabajador, se alegan, entre otros motivos, vulneración del derecho a la intimidad por el acceso al correo electrónico corporativo en el ordenador proporcionado por la empresa.

La Sala resolvió que no existía tal violación, pues con amparo en el art. 20.3 ET, puede la empresa tomar, como medida oportuna, el examen de los correos remitidos desde el correo electrónico corporativo. Medida ésta que no compromete la dignidad del trabajador en cuanto no afecta a su ámbito personal o íntimo, sino que además es proporcionada y necesaria para comprobar el cumplimiento de confidencialidad y el deber de buena fe [715] .

Discrepamos en parte de la argumentación de la Sala, pues entendemos, que el motivo no se justifica de manera suficiente, ya que no se detalla como así se recoge en

---

[714] STSJ de Castilla y León de 18 de noviembre de 2013 (AS 2013\3234).

[715] *(...); ocurre que el ordenador al que se accedió a presencia notarial (hecho probado 19) no era precisamente el personal del actor, que no le fue proporcionado por la empresa, sino el que la empresa tenía en el despacho del centro de trabajo con correo electrónico corporativo, era un ordenador de la propia empresa al que podía el actor acceder desde una Blackberry que sí le había proporcionado la empresa, teniendo en la terminal sita en su despacho una dirección profesional diferente de las direcciones de correo electrónico a nivel particular como se describe en los hechos probados 4 y 4.1, que no son los que fueron revisados el 6 de julo de 2012 (hecho probado 19); parece claro que la empresa, con amparo en el artículo 20.3 del Estatuto de los Trabajadores sí puede tomar, como medida oportuna para verificar si un trabajador cumple con sus deberes, el examen de los correos remitidos desde el correo electrónico corporativo o de empresa, es decir el que la empresa pone a disposición del trabajador desde el ordenador que también la empresa pone a disposición del trabajador en su despacho, medida que estimamos no compromete la dignidad del trabajador en cuanto no afecta a su ámbito personal o íntimo, es proporcionada o necesaria para comprobar si el actor había faltado no solo a su compromiso de confidencialidad sino al más elemental deber de buena fe "* (FJ 4º)

los hechos probados, que existían sospechas de la actitud irregular del trabajador, no se explicita que conocía y había si había firmado que el uso del correo para fines ajenos al trabajo estaban prohibidos, en definitiva, faltan datos para considerar superado el juicio de proporcionalidad.

e) Fiscalización libre

La STSJ de Madrid de 16 de diciembre de 2013[716] confirma validez de la prueba esencial en que se funda el despido. El actor, con categoría de jefe de servicio técnico, se le proporcionó por parte la empresa un ordenador portátil para su trabajo. Existía un protocolo de uso del mismo, que recogía, entre otros el deber de respeto y confidencialidad de los datos, y la prohibición añadida de utilizar el correo electrónico para cualquier propósito ajeno a las actividades laborales autorizadas por la empresa; a pesar de ello, el trabajador realizó a través del correo corporativo operaciones comerciales en una empresa de la competencia. La sentencia de instancia examinó la objeción planteada por el demandante en el acto del juicio sobre la ilicitud de la prueba documental obtenida por la empresa de los archivos privados del correo electrónico y concluye, con cita de la STS de 26 de septiembre de 2007[717] , en que al existir en el presente caso una prohibición absoluta del empresario de utilizar el ordenador que se puso a disposición del actor para fines propios, no se infringe el derecho aducido como fundamento de la denuncia de conducta anticonstitucional de la demandada.

Argumenta la Sala que comparte el criterio de la instancia, siendo necesario recordar la STC 170/2013, de 7 de octubre[718], de la que pasa a reproducir en parte los fundamentos jurídicos, para luego concluir sobre la licitud de la prueba basada en una prohibición inicial existente, que el trabajador obvió[719]. Por tanto, la sentencia está

---

[716] STSJ de Madrid de 12 de diciembre de 2013 (JUR 2014\19902).

[717] STS 26 de septiembre de 2007 (RJ 2007\7514).

[718] STC 170/2013 de 7 de octubre (RTC 2013\170).

[719] *"En el presente caso, aun se puede calibrar con mayor claridad la ausencia de la vulneración de los derechos constitucionales invocados, desde el momento en que la empresa demandada tiene establecido un detallado, preciso, riguroso y bien perfilado protocolo de actuación en el uso del ordenador, del que el trabajador que lo usa tiene cabal y perfecto conocimiento, hecho que le impide invocar los derechos cuestionados cuando la empresa descubre las graves irregularidades acreditadas*" (FJ 3º).

motivada y basada en la doctrina constitucional al respecto, si hay prohibición expresa no existe expectativa razonable de intimidad y por tanto, ningún derecho constitucional se vulnera.

f) Contacto con empresas competidoras

La STSJ de Asturias de 30 de julio de 2013[720] acepta la nulidad de actuaciones instada por la empresa recurrente, por no haberse valorado la prueba documental aportada consistente en correos electrónicos. La sentencia de instancia consideró improcedente el despido de la actora al no existir prueba de los hechos imputados en la comunicación de despido disciplinario por competencia desleal efectuado por la empresa, por rechazar por ilícita y no valorarse la prueba documental aportada por la empresa -el contenido de diversos correos electrónicos de contacto entre la actora y varias empresas, alguna de la competencia-. Prevaleció la consideración de haberse obtenido la prueba de manera ilícita, con vulneración del derecho a la intimidad de la trabajadora y del derecho al secreto de las comunicaciones. Por encontrarse de vacaciones la trabajadora despedida, una compañera suya, entró a buscar un documento de su interés en el correo eletrónico de la ausente, y de manera casual encontró varios correos comprometedores, entre la trabajadora despedida y una empresa con la que la empleadora había rescindido el servicio. Tal hallazgo suscitó extrañeza en la trabajadora y dio parte a su superior el cual que fiscalizó todo el correo de la trabajadora despedida.

La empresa recurre, discrepando al entender que no cabe hablar de intromisión ilegítima en el correo, desde el momento mismo en que la trabajadoras eran compañeras de trabajo que se sustituían entre sí en tiempo de ausencia por vacaciones y tenían autorizado mutuamente el acceso a sus respectivos correos electrónicos para atender el despacho de todos los asuntos. Extremo que la Sala considera un argumento válido para revocar la sentencia, al no entender nula la prueba por no vulnerarse el derecho fundamental al secreto de las comunicaciones en su obtención[721].

---

[720] STSJ de Asturias de 30 de julio de 2013 (JUR 2013\281620).

[721] "*En este caso no es ya, como señala la juzgadora a quo que estemos ante un descubrimiento casual, sino que el hecho de hallarse autorizadas mutuamente Esther y Flora a entrar en sus respectivos correos en caso de ausencia de una de ellas, con el fin de seguir despachando los asuntos que los clientes de la empresa pudieran plantear, ha de ser interpretado como un elocuente reconocimiento de que en el*

K) Acceso al correo de otros compañeros

* **La STSJ de Rioja de 11 noviembre 2015**[722] confirma el despido disciplinario de una trabajadora, coordinadora de Cáritas Diocesana, que procedió de *motu proprio* a monitorizar los ordenadores de su centro de trabajo, sin existir una prohibición del uso del correo para fines privados, por vulnerar el secreto de las comunicaciones y de la intimidad personal de sus compañeros; puesto que con tal intrusión había tenido acceso a todos sus datos de trabajo y personales. La recurrente tenía entre sus funciones propias, controlar a los trabajadores, pero sus tareas no poseían autonomía; sino que debía ir respaldado por la dirección. La Sala entiende que ha habido una transgresión de la buena fe contractual cuando se descubrió por casualidad que había monitorizado al menos cuatro ordenadores de sus compañeros.

Los hechos acontecen del siguiente modo: en una reunión que se mantuvo en junio del año 2012, se acordó que dada la enorme cantidad de datos que manejaban, para que los ordenadores funcionaran durante más tiempo, la información que tenían los mismos, a partir de ese momento, o se borraba de los mismos, o se almacenaba en memorias externas (nunca en el disco duro). Posteriormente el informático de la empresa revisó todos para efectuar los cambios propuestos e instalar a instancias de la trabajadora despedida un programa espía. Para que los trabajadores no adviertan de la presencia del programa espía cambió el fondo de pantalla a color azul, y cuando fue preguntado por algunos por la razón del cambio de fondo de pantalla, mintió (porque así fue instado por la recurrente) y dijo que era para que el ordenador funcionara mejor.

ámbito de la relación laboral el contenido de los correos electrónicos que pudieran haberse cruzado entre sí o con terceros a través de sus respectivo ordenadores no constituía para ellas -o había dejado de constituir- un secreto perteneciente a la órbita de su intimidad, esto es, un secreto que tuvieran interés en poner a cubierto respecto de las intromisiones de su compañera de trabajo quien, a fin de cuentas, debía de seguir utilizando el ordenador que albergaba tales datos para su finalidad específica, esto es, como un instrumento de producción para solventar las necesidades de la empresa. Y si con su conducta Esther había dejado patente que el referido material no constituía un secreto, no es posible considerar que el acceso al mismo por parte de su compañera pueda constituir una intromisión en su intimidad cuando fue ella misma quien voluntariamente dejo aquel correo electrónico a su disposición "para el despacho de todos los asuntos" (FJ 2º).

[722] STSJ La Rioja de 11 de noviembre de 2015 (EDJ 2015/231472).

Más de un año después de los mencionados hechos, una trabajadora tuvo problemas con el programa de cobro de las cuotas a los socios y llamó al informático que para que le arreglara la disfunción, y mientras el ordenador arrancaba le preguntó en qué consistía uno de los programas que se estaba iniciando pensando que era un antivirus y este le respondió que era un programa espía que monitorizaba toda su actividad, que él lo instaló bajo las órdenes de la trabajadora que luego sería despedida, hacía más de un año. Ante el conocimiento de tales hechos, da cuenta a la dirección, que ordena desinstalar el programa de todos los ordenadores, encontrando cuatro que habían sido monitorizados.

La parte recurrente solicita mediante su recurso la anulación de la Sentencia dictada por el Juzgado de lo Social, y que dejándose sin efecto, se declare improcedente el despido. Articulando el recurso en tres motivos, el primero, al amparo de lo dispuesto art. 193 LRJS, para que se repongan los autos al estado en que se encontraban en el momento de cometerse la infracción del art. 24 CE por incongruencia omisiva en la sentencia recurrida de la que deriva indefensión, al no haberse dado respuesta a la alegación de que el despido no se tramitó según los cauces que determinaban los estatutos de la demandada pues se requería el dictamen del director de Cáritas Diocesana, cuestión nueva no planteada en demanda sino en acto de juicio que por extemporánea se rechaza; el segundo al amparo de lo dispuesto en el art. 193 b) LRJS, dirigido a la revisión fáctica de la sentencia que se deniega por el mismo motivo que el anterior, por extemporaniedad; el tercero, y el cuarto al amparo de lo dispuesto en la letra c del art. 193 LRJS, en aplicación de la Jurisprudencia recogida en la STS de 6 de octubre de 2011[723], la recurrente sostiene que su actuación estaba dentro de la legalidad y de la buena fe, ya que en un primer momento en junio de 2012 se comunicó la orden de utilización de los ordenadores solo para temas de trabajo y orden expresa de no utilización para temas personales, y posteriormente se instaló el programa en enero, por lo que no se ha dado ninguna vulneración de derechos; a lo que añade que nunca se realizó de espaldas a la dirección. Tales hechos no constan como probados y la Sala responde que la cuestión fundamental es haber obrado por su cuenta con ocultación al resto de trabajadores y con total desconocimiento de su superior jerárquico. Por tanto, este "*uso desviado*" transgrede la buena fe contractual, concluye la Sala.

[723] STS 6 de octubre de 2011 (RJ 2011\7699).

* **La STSJ de Asturias de 11 de julio de 2014**[724] resuelve el recurso de suplicación planteado en sentido desestimatorio. Previamente al despido, la recurrente se vio afectada por una suspensión temporal de su contrato por un ERE, asimismo su cónyuge que trabajaba en la misma empresa, fue despedido por causas objetivas, también tenían ambos un proceso penal abierto por presuntas apropiaciones indebidas por parte del marido y de las que ella se suponía era cómplice.

Se le hace entrega de la carta de despido por violar el secreto de correspondencia o documentos reservados de la empresa, realizar sin el oportuno permiso trabajos particulares durante la jornada, así como el empleo, para usos propios, de herramientas de la empresa. La demanda en la instancia, no prosperó, y recurre en suplicación, interesando la revisión de los hechos declarados probados, a lo que por parte de la Sala, no se accede, alega vulneración del derecho a la indemnidad motivo que se desestima y en el último motivo de recurso acusa a la sentencia de instancia de infringir la doctrina gradualista elaborada por el Tribunal Supremo[725].

---

[724] STSJ de Asturias de 11 de julio de 2014 (EDJ2014/143352).

[725] "*Resulta plenamente acreditado que el día 4 de noviembre de 2013 a la trabajadora demandante,(...) se le encomendó como tarea casar la cuenta de suplidos de HC Distribución revisando para ello archivos de papel A-Z. No precisaba usar el ordenador pero lo hizo para acceder a la cuenta de correo electrónico usada por el accionista mayoritario de la empresa y, desde esta, reenviar a su cuenta particular ocho correos consistentes en conversaciones entre aquel y su hijo y con diversos asesores de la empresa en materia laboral y fiscal, en relación con temas y procedimientos legales que enfrentaban a la accionante y su marido con la empresa.*

También lo está que la trabajadora pudo acceder a esos correos privados y confidenciales ,que contenían documentos adjuntos que la empresa pensaba utilizar como medios de prueba en aquellos, porque no se había anulado la delegación que tenía reconocida para gestionar la cuenta corporativa de la empresa pese a que desde hacía varios meses, se le había restringido el acceso tanto a ella como a su marido por sospechas de falsedad, estafa y apropiación indebida que motivaron la presentación de una querella admitida a trámite y tramitada en el Juzgado de Instrucción de Siero.

(...), por lo que la valoración de la gravedad objetiva de su conducta exige partir de las circunstancias que obran en la resolución recurrida y se impone como conclusión jurídica precisamente aquella a la que llegó la Magistrada de instancia, esto es, la de que la trabajadora incurrió en un grave quebrantamiento de la exigible buena fe contractual y que el despido había de calificarse como procedente, conforme a los Art. 54 del Estatuto de los Trabajadores.

Quien accede ilegítimamente al correo electrónico de otro atenta, independientemente de otra consideración ¿qué duda cabe que podría ser un ilícito penal? al derecho reconocido en el artículo 18.3 de la Constitución. La presencia de un elemento ajeno, en este caso la trabajadora, reenvía correos electrónicos de otro, es indispensable para configurar el ilícito constitucional aquí comentado. El remitente y su destinatario son las partes entre las que media el proceso de comunicación, la presencia virtual "*intrusa*" de la recurrente es la que motiva la sanción disciplinaria, por hechos culpables frente a los que no cabe aplicar la teoría gradualista al ir revestidos de manifiesta gravedad.

L) Recapitulación

En los casos en que en el que el uso desviado del correo electrónico es sancionable, no siempre procede la sanción de despido , sino que han de aplicarse tanto las previsiones del convenio colectivo, como la doctrina gradualista.

En todo caso, es conveniente que toda empresa en la que existan puestos con acceso a Internet adopte una política concreta de seguridad informática y uso de los medios tecnológicos, trasladando las correspondientes órdenes a los trabajadores. De esta forma la sanción se puede anudar al incumplimiento de tales directivas empresariales, porque si la empresa prohíbe el uso de estos medios para fines particulares, la prohibición determina que ya no exista una situación de tolerancia con el uso personal del ordenador y que tampoco exista lógicamente una expectativa razonable de confidencialidad. En estas condiciones el trabajador afectado sabe que su acción de utilizar para fines personales el ordenador no es correcta y sabe también que está utilizando un medio que, al estar lícitamente sometido a la vigilancia de otro, ya no constituye un ámbito protegido para su intimidad.; no pudiéndose aplicar la teoría gradualista, pues ésta no se aplica si nos hallamos ante un caso claro trasgresión de la buena fe contractual caracterizada por la necesaria lealtad y confianza que ha de observarse en la relación laboral.

No estamos ante un acto de tolerancia empresarial y los hechos acreditados y sancionados, infringen de forma tan manifiesta y concluyente el principio de la buena fe que ha de presidir el contrato de trabajo vulnerando la propia naturaleza y esencia de la relación laboral, que ninguna circunstancia permite degradar la gravedad y la culpabilidad de la infracción contractual" (FJ 2º).

En cuanto a la utilización de correo electrónico con fines sindicales, a través del servidor de la empresa, pesa sobre el empresario el deber de mantener al sindicato en el uso pacífico de los instrumentos adecuados para su acción sindical siempre que tales medios existan, su utilización no perjudique la finalidad para la que fueron creados por la empresa y se respeten los límites y las reglas de uso. El derecho al uso de Internet y la posibilidad de acceder al correo electrónico se considera una derivación del derecho de información sindical integrado, con carácter más genérico, en el derecho fundamental a la libertad sindical. La doctrina del TS ha admitido que se vulnera la libertad sindical cuando la empresa se niega de manera injustificada el acceso a la cuenta de correo electrónico.

3. El teléfono móvil del trabajador

A) Planteamiento

El impacto de las tecnologías de la información y la comunicación, como Internet y el teléfono móvil es tan espectacular que es lícito preguntarse si, en algunos casos, pueden provocar adicción, al igual que otras conductas socialmente aceptadas como comprar, jugar, trabajar y tener relaciones sexuales[726].

El teléfono móvil es un instrumento propenso al uso desviado, lo que debe llevar a las empresas a marcar claramente su prohibición y tras esto, controlar de manera aleatoria y pausada en el tiempo, si se cumple o no el mandato para no convertir en tolerancia ciertas prácticas o malos hábitos que pudieran existir si se prohíbe pero no se controla, que crearía un clima de permisividad. Con la generalización de la banda ancha entre 2010 y 2015, los servicios y dinámicas de acceso a Internet, la tecnología 4G y los proyectos globales de acceso a la Red, se han transformado totalmente con respecto al uso de dispositivos, consolidándose el acceso a través de teléfonos inteligentes o tabletas[727].

---

[726] CASTELLANA, CARBONELL, y OBERST.: «Sobre la adicción a Internet y al teléfono móvil», *RES: Revista de Educación Social*, núm.11, 2010.

[727] ROVIRA COLLADO, J.: «Redes sociales en la universidad: profesionales, académicas y de lectura», *Álabe, Revista de Investigación sobre Lectura y Escritura* núm. 13, 2016, pág. 3

B) Relevancia en la prestación laboral

Hasta tal punto se ha generalizado la implantación de teléfonos móviles que existen casos en los que los trabajadores pretenden que se realicen notificaciones por parte de la empresa a través de los mismos. Sirva de ejemplo la STSJ de Cataluña 31 de marzo de 2016[728] que ha declarado que no es correcto notificar al trabajador su despido a través de comunicación a su teléfono móvil, mientras que es adecuado notificar un despido al trabajador por burofax en el domicilio que la empresa tenía. No consta ningún indicio de cambio de dirección, por lo que la empresa demandada ha actuado de buena fe *a sensu* contrario de lo que alega la parte recurrente que pretendía que se le notificara la carta de despido por el teléfono móvil, sin ninguna garantía de seguridad y privacidad. En sentido, la STS 21 de septiembre de 2015[729], considera abusivo que se obligue a facilitar el teléfono móvil al trabajador firmar un contrato de trabajo.

En algunos casos el uso del teléfono móvil es indispensable para desarrollar la actividad propia así ocurre en el supuesto que resuelve la STSJ de Asturias de 6 de mayo de 2011[730] que declara que constituye una irregular readmisión la realizada por una empresa que readmite a un viajante sin restituirle su teléfono móvil. El TSJ estima parcialmente el recurso de suplicación interpuesto por el trabajador accionante frente al auto dictado en ejecución de sentencia de despido y declara irregular la readmisión realizada por la empresa de marmolería demandada y extinguida la relación laboral. Explica la Sala que el actor era viajante, a pesar de lo cual la empresa le reincorpora privándole de medios básicos de vehículo de motor y teléfono móvil con que contaba antes del despido para realizar esa actividad, restricción que le impide el ejercicio real de las tareas propias de su categoría.

[728] STSJ de Cataluña de 31 marzo de 2016 (JUR 2016\121577).
[729] STS de 21 septiembre 2015 (RJ 2015\4353).
[730] STSJ Asturias de 6 de mayo de 2011 (JUR 2011\195770).

C) Utilización del terminal propio (BYOD)

Con el acrónimo BYOD[731] se describe una nueva tendencia tecnológica en la que la política empresarial permite a los trabajadores utilizar sus propios dispositivos personales para usos profesionales. Asimismo, cuando el empleado además utiliza y comparte aplicaciones y tratamientos poniéndolos a "trabajar" en las funciones de su actividad en la empresa el término se amplia y se habla de BYOT[732] que abarca programas, aplicaciones, plataformas propias o compartidas en el concepto de utilización en común, etc[733].

En España, muchas empresas por política de ahorro eliminan los móviles corporativos y los sustituyen por subvenciones a los empleados por el uso de su móvil personal para fines profesionales (uso de voz y datos), tendencia que va en aumento, y que se trata de una práctica generalizada en el mundo anglosajón. El importe que la empresa pudiera satisfacer a sus empleados por la adquisición de su propio teléfono móvil se constituye en un rendimiento dinerario del trabajo[734].Estadísticamente está constatado que más de un 60% de los trabajadores de todos los ámbitos están demandando la posibilidad de poder usar sus propios terminales y esta demanda crece en las nuevas generaciones (un 90%) porque los trabajadores jóvenes lo ven como algo natural[735].

Las argumentos a favor de una tolerancia empresarial respecto al BYOD son varios: aumento de la productividad[736], mayor capacidad de respuesta frente a

---

[731] Siglas del inglés "*Bring your own dispositive*" que se traduce trae tu propio dispositivo. El fenómeno BYOD comenzó en el año 2009, en las entrañas de la empresa Intel al aceptar esta el creciente número de empleados que llevaban sus propios artefactos móviles al trabajo y los conectaba a la red telemática de la corporación.

[732] Siglas del inglés "*Bring your own technology"* que significa trae tu propia tecnología.

[733] DÁVARA RODRÍGUEZ, M. Á.: *Manual de Derecho Informático*, *op.cit*., pág. 577.

[734] DGT, Consulta Vinculante núm. V932/2014 de 2 abril 2014 (EDD 2014/73350). El rendimiento del trabajo que supone la adquisición del móvil por parte de la empresa, no se encuentra amparado por ninguno de los supuestos de exención establecidos legalmente. Por lo que se refiere a la compensación por el gasto producido por la utilización del servicio de telefonía, si tal compensación se limita a reembolsar a los empleados por los gastos ocasionados por esa utilización en el desarrollo de su trabajo, cabe afirmar que no comporta para ellos un supuesto de obtención de renta, es decir, no se entiende producido el hecho imponible del impuesto

[735] LAITA, C., MARÍN SANUI. D., ÑUNEZ, S, BECKER, C.: «Bring Your Own Device (BYOD)», *Bit: Boletín Informativo de Telecomunicación*, núm. 23, 2013, pág. 20.

[736] Al ser los trabajadores dueños de los equipos de comunicación, se les puede localizar/controlar de forma más estrecha.

incidentes[737] y disminución importante del número de equipos que realmente están descontrolados[738]. Los problemas surgen por pretender utilizar una única herramienta para todas las comunicaciones y para planificar todas las actividades, sin distinguir si son profesionales o de la vida privada, lo que implica riesgos en un doble sentido. Por un lado, existen problemas de seguridad, el riesgo de intrusiones es alto[739]; se genera una importante concentración de información, lo que hace muy atractivos los equipos como objetivos de ataque[740]. La solución sería no mezclar tres ámbitos que necesariamente no tienen nada que ver entre sí (trabajo, vida privada y ocio) como medida profiláctica que puede llevar a cotas de seguridad informática hoy no alcanzadas[741]. Por otro lado, el BYOD, entraña también implicaciones para la propia privacidad de los empleados. El uso de aplicaciones empresariales personalizadas permite a la empresa ejercer un monitoreo y control casi absoluto de la actividad del empleado. Las aplicaciones pueden recoger datos profesionales y personales del trabajador: la empresa puede ejercer un control de inicio y tiempo de ejecución mediante el comportamiento de sus aplicaciones personalizadas en su dispositivo móvil; por otra parte, la empresa puede acceder a los datos confidenciales del empleado almacenados en el dispositivo, desde mensajes SMS -incluyendo textos privados, imágenes, e incluso mensajes sonoros contenidos en el mensaje-, hasta todo lo incorporado en la tarjeta SD (memoria externa) como archivos personales fotos, música y documentos[742].

[737] Al tener accesibles los trabajadores más tiempo.

[738] Al gestionar todos los intentos de conexión de equipos.

[739] BYOD es un ejemplo de lo que se conoce como el "end *node problem"* o "problema *de seguridad en el punto final",*en un sentido muy simple, el nodo final es a menudo el eslabón más débil de que los expertos en seguridad y tecnología miran dentro de la red.

[740] Así, basta con explotar las inmadureces y debilidades de los jóvenes sistemas operativos que corren en ellos, la prolija variedad de modos de comunicación que atienden (voz, datos, mensajería, posición, trayectos, navegación, correo, etc.) y las innumerables aplicaciones de todo tipo que se instalan en ellos.

[741] DÁVILA MURO, J.: «Confines BYOD: Hic sunt Dracones», *Revista SIC ciberseguridad, seguridad de la información y privacidad*, núm. 104, 2013, pág.75

[742] GOÑI SEIN, J.L.: «Los límites de las potestades empresariales vs. Derecho a la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral de las redes sociales», *op.cit.*

D) Peculiaridades como medio probatorio

Los nuevos sistemas de grabación de imagen y sonido (teléfonos móviles, mp3 o mp4) hábilmente utilizados pueden constituirse en aliados de la víctima de acoso laboral o sexual para acreditar unas situaciones que normalmente suelen ofrecer una gran dificultad probatoria[743], en este sentido la STS (Sala Primera) de 20 de noviembre de 2014[744] resuelve sobre una reclamación ante la jurisdicción civil por importe de 3.000 euros solicitados en concepto de indemnización por daños a la intimidad de un empresario causados una antigua empleada que sostenía que era víctima de acoso laboral. Los hechos transcurrieron del siguiente modo: una trabajadora había grabado con su teléfono móvil una conversación en la que participaba junto con su jefe. En dicho diálogo el representante de la empresa le entregaba una carta por la que se le amonestaba formalmente y se le imponía una sanción de suspensión de trabajo y sueldo. La conversación fue utilizada posteriormente en un procedimiento laboral. Al parecer, la trabajadora había venido sufriendo varios episodios de acoso laboral con el propósito de que abandonara su puesto de trabajo. El fin de la grabación era protegerse frente a ofensas, dejando constancia de las mismas para una posterior reclamación judicial[745].

El TS desestima el recurso de casación interpuesto por el demandante considerando que la conversación grabada no afecta a su intimidad. Aunque reconoce el TS que el derecho a la intimidad no se desarrolla sólo en un ámbito doméstico o privado, sino que también existe en otros ámbitos como el profesional, en el que se generan relaciones interpersonales que también pueden dar lugar a espacios reservados propios de la vida privada, este espacio reservado no resulta afectado en la conversación que se da entre demandante y demandado.

Se trata de una actuación del demandante en calidad de representante de la empresa, en ejercicio de sus funciones, y no de carácter privado. Por otro lado, y desde el punto de vista del juicio de proporcionalidad o razonabilidad, el TS tiene en cuenta la previa situación de conflicto que enfrentaba a las partes, es sabido que pueden utilizarse

---

[743] SÁNCHEZ PÉREZ, J.: «El acoso sexual y su proyección en las relaciones laborales», *Revista de Información Laboral* núm. 8, 2015 (BIB 2015\4323).

[744] STS de 20 noviembre de 2014 (RJ 2014\6116).

[745] ÁLVAREZ OLALLA, P. «La grabación de imágenes y de sonido en el proceso civil y los derechos a la intimidad, propia imagen y secreto de las comunicaciones», *Nuevas resoluciones jurisprudenciales. Revista Doctrinal Aranzadi Civil-Mercantil*, núm. 10, 2015 (BIB 2015\106).

como prueba grabaciones de conversaciones telefónicas, o mensajes de móvil, en los que participe como interlocutor o destinatario la persona que aporta dicha prueba.

En efecto, no existe intromisión ilegítima en el caso de grabación de una conversación por parte de uno de los interlocutores. Salvo resolución judicial no puede oponerse, sin quebrar su sentido constitucional, frente a quien tomó parte en la comunicación misma así protegida. Quien entrega a otro la carta recibida o quien emplea durante su conversación telefónica un aparato amplificador de la voz que permite captar aquella conversación a otras personas presentes no está violando el secreto de las comunicaciones, sin perjuicio de que estas mismas conductas, en el caso de que lo así transmitido a otros entrase en la esfera "*íntima"* del interlocutor, pudiesen constituir atentados al derecho garantizado en el art. 18 CE .Tampoco existe vulneración del derecho a la intimidad o al secreto de las comunicaciones cuando uno de los interlocutores, en lugar de grabar personalmente la conversación, autoriza a un tercero a hacerlo[746].

Por lo que *a priori* no se puede declarar legítima o ilegítima la captación de la imagen, la grabación de una conversación entre el que la graba y un tercero, o el acceso a las comunicaciones o documentos ajenos, propiciados por la cercanía que permiten las relaciones familiares o laborales, para su utilización como prueba en un pleito. En todo caso, habrá que atender, para la valoración o no de la ilicitud, a la triple regla de la idoneidad de la medida para lograr el fin pretendido (probar una alegación en juicio), necesidad (inexistencia de otro medio menos lesivo de los derechos del investigado para conseguir tal fin) y proporcionalidad entre la intensidad de la invasión de los derechos del investigado y la utilidad de la misma. Asímismo ha te tenerse en cuenta, especialmente en el caso de los trabajadores, las razonables expectativas de privacidad respecto a sus actuaciones, en atención a las circunstancias concurrentes[747].

E) Supuestos de uso abusivo o indebido

El teléfono móvil es un instrumento propenso al uso desviado, lo que debe llevar a las empresas que no quieran dar lugar a este tipo de abusos a marcar claramente su

[746] *Ibídem.*
[747] *Ibídem.*

prohibición y a controlar con rapidez si se incumple o no, pero el hecho cierto es que respecto a esta cuestión han de ponderarse las circunstancias del caso concreto:

A) Ante un presunto uso desviado, la inexistencia de política al respecto y la ausencia de requerimiento de justificación de llamadas particulares, no se puede instar un despido disciplinario. A mayor abundamiento, por un lado, la empresa disponía mensualmente de la factura que registraba el número de llamadas del empleado y, sin motivo alguno, esperó varios meses hasta que procedió a incoar un expediente disciplinario; por otro lado, no atendió a la disponibilidad del trabajador de asumir el coste de las llamadas efectuadas (STSJ de Castilla y León de 26 de octubre de 2005)[748].

B) El uso abusivo del teléfono móvil de empresa, resulta especialmente grave, por el número de llamadas diarias, que excedía de treinta de forma habitual y por el coste de las mismas, que superaba en ocasiones su propio salario mensual además tal uso resultaba notorio entre los compañeros, lo que justifica el despido disciplinario (STSJ de Madrid de 28 de mayo de 2007)[749].

C) La utilización del teléfono móvil por parte de un conductor de autobús de escolares, durante la conducción, constituye tanto una desobediencia, como una negligencia grave que pone en evidente riesgo la seguridad del servicio y de los niños transportados, y también una transgresión de la buena fe contractual y un abuso de confianza (STSJ de Cantabria de 29 de septiembre de 2015[750]). En igual sentido el despido disciplinario considerado como justificado de un conductor de camión sancionado por saltarse un semáforo por ir hablando por el teléfono móvil, implicando riesgo de accidente (STSJ de Andalucía de 24 septiembre de 2015 [751]).

D) La utilización indebida del teléfono móvil proporcionado por el Club de Fútbol Deportivo Alavés durante situación de IT por parte del deportista y la negativa a su devolución tras dos requerimientos por parte del mencionado equipo, justifica su despido disciplinario (STSJ del País Vasco de 24 de febrero de 2009[752]). Mientras que la utilización del teléfono móvil de la empresa durante situación de IT, no siendo su uso no

[748] STSJ Castilla y León de 26 de octubre de 2005 (EDJ 2005/205394).
[749] STSJ Madrid de 28 de mayo de 2007 (EDJ 2007/116611).

[750] STSJ Cantabria de 29 de septiembre de 2015 (EDJ 2015/196965).
[751] STSJ de Andalucía de 24 septiembre de 2015 (JUR 2015\261008).
[752] STSJ del País Vasco 24 febrero de 2009 (AS 2009\1747).

restringido y el consumo realizado casi insignificante, no justifica el despido disciplinario (STSJ de Castilla y León de 26 de octubre de 2005[753]).

F) Sustracción de un móvil ajeno

El hurto del teléfono móvil se considera una transgresión de la buena fe contractual y un abuso de confianza en el desempeño del puesto de trabajo, si dicho hurto se produce dentro del centro de trabajo, en este sentido:

A) Sustraer el teléfono móvil a una compañera se considera "*incumplimiento contractual, definido como "la transgresión de la buena fe contractual, así como el abuso de confianza en el desempeño del trabajo", en el artículo 54.2 d) del ET, y cabe considerarla, como grave y culpable, tal como se exige en el apartado 1 de dicho precepto, para que el contrato de trabajo pueda extinguirse, por decisión del empresario, mediante despido*" (STSJ de Galicia de 21 de julio de 2003) [754].

B) Respecto a la acusación de sustraer un teléfono móvil a una cliente "*resulta evidente la intrascendencia que a los efectos de resolver este pleito tiene el hecho de que la denuncia por hurto la realizara la clienta y no la empresa*" (FJ 3º), también es irrelevante que "*cuando la clienta acude a la tienda, le entrega el móvil sin ofrecer resistencia alguna*" ,"*el valor de lo sustraído*" o "*la intachable conducta previa de la actora que cuenta con una antigüedad de casi tres años*" porque ocultar que el teléfono móvil de la cliente se hallaba en la tienda "*pone de manifiesto una clara transgresión de la buena fe contractual que coloca en entredicho la fiabilidad de la empresa cara a sus clientes y que resulta intolerante para la continuidad de la relación laboral, por lo que procede, tras la desestimación del recurso, confirmar la sentencia impugnada*"(FJ 5º) (STSJ Islas Canarias de 29 enero de 2010) [755]. En igual sentido se resuelve en el supuesto de hecho de hecho del auxiliar de vuelo que se apropia de un teléfono móvil con su correspondiente cargador de un pasajero (STSJ Islas Canarias de 20 noviembre de 2010) [756].

---

[753] STJ de Castilla y León de 26 octubre de 2005 (AS 2005\3180).
[754] STSJ Galicia de 21 julio de 2003 (JUR 2004\178279).
[755] STSJ Islas Canarias de 29 enero de 2010 (JUR 2010\158450).
[756] STSJ Islas Canarias de 20 de noviembre de 2009 (JUR 2010\428).

F) Uso instrumental para realizar actividades ilícitas

A) Constituye un abuso de derecho realizar grabaciones indiscriminadas a compañeros de trabajo con el teléfono móvil pues supone un quebranto de la buena fe contractual, deslealtad y abuso de confianza en el trabajo, falta de respeto y consideración a superiores y compañeros de trabajo (STSJ de Galicia de 17 de marzo de 2016)[757].

B) Emitir una canción de claro contenido xenófobo desde un teléfono móvil amplificando su sonido[758] mediante un megáfono para que la oyera un compañero de trabajo extranjero constituye transgresión de la buena fe contractual (STSJ de Navarra de 19 noviembre de 2012) [759].

C) Realizar fotografías con el móvil por debajo de la falda de las compañeras y poner el móvil entre los muslos de una de ellas, es una conducta libidinosa que implica ofensa a la libertad sexual, intimidad y dignidad de aquellas, genera un clima intimidatorio y hostil, constitutivo de la falta muy grave del art. 54.1 ET, en cuanto ofensas verbales o físicas a compañeros, determinante o causa de despido disciplinario (STSJ de Andalucía de 11 de febrero de 2008)[760].

G) Recapitulación

En relación con el control empresarial de la actividad laboral y el uso del móvil podemos destacar que la existencia de un hábito social de tolerancia con los usos personales del teléfono facilitado por la empresa crea una expectativa general de confidencialidad en los trabajadores. Por el contrario, si hay prohibición absoluta de los usos personales por las reglas establecidas por la empresa o por convenio, queda eliminada toda expectativa de intimidad o confidencialidad.

---

[757] STSJ Galicia de 17 marzo de 2016 (JUR 2016\92693).

[758] En un contexto de huelga, un trabajador recrimina la postura de dos compañeros de trabajo que sólo pretendían facilitar el acceso a las instalaciones de la empresa a los trabajadores que no participaban en la huelga y ofende gravemente a uno de ellos, de nacionalidad rumana, no se ampara el derecho al insulto, ofensas verbales por las que se produce una transgresión de la buena fe contractual.

[759] STSJ de Navarra de 19 noviembre de 2012 (AS 2013\1166).

[760] STSJ Andalucía de 11 febrero de 2008 (AS 2009\1210).

Del análisis de las diversas resoluciones judiciales, observamos que lo que impera es el casuismo, habiendo de atender el juzgador a las circunstancias de caso concreto.

CAPÍTULO II. CONTROL LABORAL DEL TRABAJADOR

1. Videovigilancia

A) Delimitación

El trabajo no es un acto íntimo sino un acto social que puede ser supervisado mediante videovigilancia, siempre que esa supervisión se mantenga dentro de los límites estrictamente laborales[761]. Tiene como finalidad la prevención de conductas ilícitas, o bien, la prevención de riesgos laborales.

Las numerosas sentencias que se han enfrentado con problemas relacionados con la captación y transmisión de las imágenes de las personas por un sistema de videovigilancia comienzan por destacar que la imagen es un dato de carácter personal protegido por la legislación en materia de protección de datos pues aunque tales imágenes no se graben o conserven constituyen un tratamiento de datos[762].

B) Pautas de buenas prácticas

* En el ámbito internacional, el Repertorio de Recomendaciones Prácticas de la **OIT** en materia de protección de los datos personales de los trabajadores[763], establece lo siguiente: "El secreto en materia de vigilancia sólo debería permitirse cuando:- a) se realice de conformidad con la legislación nacional. -b) existan sospechas suficientes de actividad delictiva u otras infracciones graves".

* En el ámbito europeo, la **Recomendación CM/rec(2015)5**, relativa al tratamiento de datos personales en el entorno laboral, en el apto. 15, hace alusión a los sistemas y tecnologías de la información para el control de los empleados, "en especial la videovigilancia". Se abordan los siguientes aspectos: 1º) Utilización prohibida en

---

[761] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit*., pág. 20.

[762] CÓRDOBA CASTROVERDE, D.: «Las cámaras de videovigilancia en la jurisprudencia. Respuesta de los tribunales», *Revista de Derecho Inmobiliario*, núm. 2, 2015 (EDB 2015/98693).

[763] Recomendación de la OIT de 1 de septiembre de 1997 sobre Protección de los datos personales de los trabajadores. Repertorio de recomendaciones prácticas, pág. 8 del original impreso. *http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf*

cualquier caso para el control de lugares (ej.: vestuarios, lavabos) que guarden relación con la vida íntima de las personas afectadas[764]. 2º) Se plantea con carácter general que la introducción y utilización de sistemas tecnológicos que tenga por finalidad directa y principal "*el control y el comportamiento de la actividad de los empleados*" no debería estar permitida, y que en el supuesto de ser necesarios, será licita, por los motivos listados de "protección de la producción, de la salud, de la seguridad o la gestión eficaz de una organización"[765], medidas de control que deberán ser consultadas y puestas en conocimiento de la representación de los trabajadores. 3º) La información deberá ser facilitada de forma accesible, es decir a través de los canales de información habitualmente utilizados por el empleado, y actualizada. Todo este tratamiento de datos personales ha de partir de dos principios generales recogidos en el apartado 14, que se refiere a Internet y las comunicaciones electrónicas pero que es perfectamente extrapolable a todos los demás: en primer lugar que el empleador ha de evitar "*infringir ataques injustificados y no razonables al derecho al respeto de la vida privada de los empleados*"; y en segundo término, que la forma cómo se controlan y cómo se obtienen tales datos ha de ser bien conocida por el trabajador. Los controles deben ser preferentemente de carácter "poco intrusivo" y con conocimiento de las personas afectadas. 4º) Respecto al tratamiento de los datos sensibles, establece con múltiples cautelas en punto a permitir su utilización y con el establecimiento de garantía jurídicas apropiadas para evitar el riesgo de discriminación. Esos datos sensibles son los contemplados en el art. 6 de la Convención de 1981: "*Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas, la misma norma regirá en el caso de datos de carácter personal referentes a condenas penales*", y su tratamiento sólo está permitido cuando sea indispensable por razón de las características del reclutamiento o para la ejecución de obligaciones legales que deriven del contrato de trabajo.

---

[764] Núm. 15. 2. "*The use of video surveillance for monitoring locations that are part of the most personal area of life of employees is not permitted in any situation*".

[765] Núm. 15. 1. "(…)*To protect production, health and safety*".

* La Instrucción núm. 1/2006, de 8 de noviembre, de la **AEPD** sobre tratamiento de datos personales con fines de vigilancia a través de cámaras o videocámaras[766], en su Exposición de Motivos expresa la necesidad de que el uso y empleo de estos mecanismos de grabación sea proporcionado a la finalidad que se persigue, y que deje al margen dos clases de grabaciones: las de contenido estrictamente doméstico y las que tienen relación con las grabaciones realizadas por las Fuerzas y Cuerpos de Seguridad del Estado.

C) Variables jurídicas relevantes

En este punto se hace necesario delimitar la implantación y utilización de medios televisivos para el control de la producción en el trabajo y el empleo de esos medios para controlar la actividad y el comportamiento de los trabajadores.

Con respecto a la implantación y utilización de medios televisivos, hay que decir que los aparatos que normalmente utilizan las empresas de control suelen ser medios audiovisuales, a saber, cámaras para grabar la imagen y el sonido (ya sea circuito abierto o cerrado). En algunas ocasiones su utilización está justificada para controlar la integridad física del trabajador, o la seguridad de la empresa (como puede ser el caso de la realización de actividades peligrosas o en las entidades de crédito, grandes superficies, joyerías, etc. De la jurisprudencia existente se desprende que la colocación de estos aparatos por razones objetivas derivadas de la actividad de la empresa es posible, de acuerdo con nuestro ordenamiento jurídico, teniendo en cuenta el poder de dirección que se otorga al empresario; por lo tanto, en principio, se admite la instalación de cámaras de vídeo para el control del trabajo y actividad de los empleados, sin que se considere atentatorio a los derechos fundamentales de intimidad personal y propia imagen[767].

Con respecto al uso de imágenes para fiscalizar la actividad del trabajador sigue plenamente vigente lo previsto en las SSTC 98/2000 de 10 de abril[768], 186/2000 de 10

---

[766] BOE núm. 296/2006 de 12 de diciembre *https://www.agpd.es/portalwebAGPD/canalresponsable/videovigilancia/common/Instruccion_1_2006_videovigilancia.pdf*

[767] MARTÍN JIMÉNEZ, R.: «El derecho a la intimidad del trabajador y las cámaras de vigilancia», *Diario de las Audiencias y TSJ*, núm. 291, 2002, pág. 1 del original impreso (EDB 2002/114290).

[768] STC 98/2000, de 10 de abril (RTC 2000\98).

de julio[769] y 39/2016, de 3 de marzo[770], cuya doctrina se aplicará conforme a las circunstancias concretas de cada caso. En la actualidad, cuando hablamos de videovigilancia no nos referimos tan solo a cámaras sino a cualquier sistema o dispositivo técnico que permita grabar y tomar imágenes (a saber, dispositivos *webcam*, circuitos cerrados de televisión, etc.) excluyendo las que se circunscriban al ámbito privado o familiar, en los casos en los que estas imágenes pertenecen a personas identificadas o identificables[771].

Y por terminar de precisar conceptualmente cuándo se utiliza una videocámara, no para prevenir, sino para investigar *a posteriori* y obtener pruebas relacionadas con delitos o recabar información sobre cuestiones específicas de carácter laboral, no cabe hablar en sentido estricto de videovigilancia, sino simplemente de tomas videográficas[772].

D) Normas relevantes

Como ya pusimos de manifiesto, no existe una normativa específica que regule la instalación y utilización de los mecanismos de control y vigilancia consistentes en la captación de imágenes dentro de los centros de trabajo, por lo que van a ser los órganos jurisdiccionales los encargados de ponderar, en caso de conflicto, cuándo un empresario puede usarlos al amparo de su poder de dirección, respetando siempre los derechos fundamentales del trabajador, en este supuesto de forma especial la intimidad y el derecho a la autoprotección informativa, teniendo, por un lado, presente el principio de proporcionalidad y, por otro, la existencia de una información previa sobre el uso de la videovigilancia.

* Sobre esta materia incide la **LO 4/1997, de 4 de agosto**[773], sobre la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. Hay que precisar que en lugares públicos sólo está permitida la instalación de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado, nunca por particulares, pues la seguridad

---

[769] STC 186/2000, de 10 de julio (RTC 2000\186).

[770] STC 39/2016, de 3 marzo (RTC 2016\39).

[771] *Vid*. Guía para la videovigilancia. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf*

[772] MARTÍN MORALES, R.: «El derecho a la intimidad: Grabaciones con Videocámaras y microfonía oculta», *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, núm. 6079, 2004.

[773] Desarrollada reglamentariamente por R.D 596/1999, de 16 de abril.

pública compete a la Policía (no obstante, se permite la videovigilancia como por derivación a los inmuebles y locales comerciales existentes dentro del edificio, a urbanizaciones privadas y comunidades de vecinos).

* Por su lado, la **Ley 5/2014, de 4 de abril, de Seguridad Privada**[774]. En su Artículo 5.f) establece que constituyen actividades de seguridad privada *la instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia*. Y en su art. 42 procede a regular los servicios de videovigilancia:

> "*1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.*
>
> *Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.*
>
> *No tendrán la consideración de servicio de videovigilancia la utilización de cámaras o videocámaras cuyo objeto principal sea la comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. Estas funciones podrán realizarse por personal distinto del de seguridad privada.*
>
> *2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular.*
>
> *3. Las cámaras de videovigilancia que formen parte de medidas de seguridad obligatorias o de sistemas de recepción, verificación y, en su caso, respuesta y transmisión de alarmas, no requerirán autorización administrativa para su instalación, empleo o utilización.*
>
> *4. Las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Cuando las mismas se encuentren relacionadas con hechos delictivos o que afecten a la seguridad ciudadana, se aportarán, de propia iniciativa o a su requerimiento, a las Fuerzas y Cuerpos de Seguridad competentes, respetando los criterios de conservación y custodia de las mismas para su válida aportación como evidencia o prueba en investigaciones policiales o judiciales.*
>
> *5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima*".

* **La LO 1/1982, de Protección Civil de Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen**, en su art. 7 considera intromisiones a la intimidad, entre otras, "*el emplazamiento en cualquier lugar de aparatos de escucha, de filmación de dispositivos ópticos o de cualquier medio apto para grabar o reproducir la vida íntima de las personas*".

* **La LOPD**, por su parte, no recoge en su articulado de forma detallada que la captación de imágenes de una persona está dentro del ámbito de la legislación en materia

[774] BOE 5 abril 2014, núm. 83. En vigor desde el 8-6-14.

de protección de datos, quizás porque no exista una identificación personal de las personas que son grabadas. Pero no existe duda alguna de que las imágenes conservadas en un soporte físico son un dato de carácter personal[775].

D) Criterios de la AEPD

* En la Instrucción núm. 1/2006 de la AEPD[776], como ya hemos apuntado, por su especial característica, el tratamiento de las imágenes obtenidas por video vigilancia se ha desarrollado de manera separada. En ella se regula el tratamiento de datos personales con fines de vigilancia a través de sistemas con cámaras o videocámaras y viene a clarificar este aspecto, incluyendo dentro del ámbito de la protección de datos la obtención de imágenes de personas físicas identificables.

* Resolución de la AEPD de 16 de abril de 2015[777].- Archiva la denuncia de dos trabajadores que fueron despedidos en base a lo desprendido en una grabación que utilizó su empresa a través de cámara oculta. En un primer momento, la AEDP requirió el soporte videográfico a todos los implicados, los empleados manifestaron que el único conocimiento que tienen del mismo por lo manifestado en la carta de despido, y la empresa negó haber hecho uso de la videovigilancia, la AEPD entiende que la empleadora está obstruyendo la labor instructora y procede a abrir proceso sancionador. Posteriormente, se aportó por la empresa la sentencia del Juzgado de lo Social que resuelve la impugnación del despido de los denunciantes, declarándolo procedente y teniendo por probado que quien compró e instaló la prueba videográfica fue un compañero de los denunciantes por lo que no se procede sancionar a la empresa por infracción del art. 18. 4 CE.

---

[775] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op.cit*., pág.58.

[776] BOE núm. 296/2006 de 12 de diciembre *https://www.agpd.es/portalwebAGPD/canalresponsable/videovigilancia/common/Instruccion_1_2006_videovigilancia.pdf*

[777] Proc. núm. PS/00665/2015 de la AEPD. *http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2015/common/pdfs/PS-00007-2015_Resolucion-de-fecha-16-04-2015_Art-ii-culo-40-LOPD.pdf*

* Resolución de la AEPD de 4 de noviembre de 2014[778].- La denunciante, empleada de una empresa de seguridad, manifestó haber sido sancionada por falta laboral grave. La empresa había utilizado y aportado en juicio las imágenes captadas por el sistema de videovigilancia del hospital en el que prestaba sus servicios sin que hubiera sido informada de que se utilizaban para el control laboral. De las actuaciones practicadas se constató que la implantación del sistema de videovigilancia, cuyo responsable era el hospital, tenía por finalidad la seguridad de las instalaciones y no el control laboral.

La aportación de las imágenes por la empresa en el juicio como prueba de la conducta laboral de la denunciante y del riesgo de seguridad provocado con la misma está legitimada por el criterio jurisprudencial, según el cual «*una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales, es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD). Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones*». En consecuencia, se archivaron las actuaciones.

H) Derechos fundamentales en conflicto

No existe en nuestra CE un precepto que se refiera de manera expresa a estas captaciones audiovisuales, pero los derechos fundamentales inespecíficos garantizan los derechos del trabajador, fundamentalmente, los derechos con los que se puede entrar en colisión son los del art. 18.1 CE referidos al honor, intimidad y a la propia imagen, así como el derecho a la autodeterminación informativa (art.18.4 CE).

La propia Exposición de Motivos de la Ley de Seguridad Privada[779] expone que *resulta especialmente relevante la regulación de los servicios de videovigilancia y de investigación privada, ya que se trata de servicios que potencialmente pueden incidir de forma directa en la esfera de la intimidad de los ciudadanos.* El derecho a la intimidad podría resultar lesionado si el control a través de la videovigilancia se practicara con una intensidad o exhaustividad superior a lo razonablemente esperable y consentido por el

[778] Resolución de archivo de actuaciones dictada en el Proc. núm. E/03357/2014 de la AEPD. *http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2014/common/pdfs/E-03357-2014_Resolucion-de-fecha-04-11-2014_Art-ii-culo-6.1-LOPD.pdf*

[779] BOE 5 abril 2014, núm. 83. En vigor desde el 8-6-14.

trabajador, extendiéndose sobre parcelas de lo íntimo o de lo privado, ajenas al funcionamiento de la empresa, o que anulan completamente todo margen para un mínimo desenvolvimiento de su personalidad[780].

Aunque la captación audiovisual propiamente dicha no provoque una lesión inicial del derecho al honor, esta puede producirse después, cuando se divulgue o difunda lo anteriormente grabado. Dependerá además de que el contenido de la grabación incorpore elementos capaces de producir deshonra, independientemente de que esta captación, por sí misma, suponga una lesión del derecho a la intimidad[781].

Con respecto al derecho a la propia imagen, si grabamos a un trabajador, esa imagen faculta al empleado a impedir su captación, grabación y reproducción lo que enlaza con el supuesto de hecho del art. 5 de LO 1/82, que considera una intromisión ilegítima "*la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, la imagen de una persona en cualquier momento de su vida privada o fuera de ellos*". Esta última referencia es la que dota de autonomía al derecho a la propia imagen y suscita su problemática laboral[782].

La configuración gráfica del derecho a la propia imagen en el ámbito del trabajo se aborda en la STC 99/1994, de 11 de abril, ya comentada. Su captación y difusión puede ser considerada legítima cuando ha consentido el trabajador o cuando la naturaleza del contrato de trabajo lleve implícita la cesión de este derecho a favor del público como sucede en las actividades en contacto con el público o accesibles a él[783].

En relación al derecho a la autodeterminación informativa, es posible su lesión. El art. 2 LOPD proyecta el ámbito de aplicación de la ley a "*todos los datos de carácter personal, registrados en soporte físico, que los haga susceptibles de tratamiento*" y,

---

[780] ÁLVAREZ ALONSO, D.: «Medios audiovisuales de vigilancia empresarial y derechos fundamentales del trabajador», Comunicación a la ponencia temática: El Derecho del Trabajo y las Relaciones Laborales ante los cambios económicos y sociales del X Congreso de Derecho del Trabajo y de la Seguridad Social AEDTSS 2011, ,pág. 4 *del original impreso*. *http://www.aedtss.com/images/stories/documentos/congresoeuropeocomunicaciones/1/123alvarez_alonso.pdf*

[781] MARTÍN MORALES, R.: «El derecho a la intimidad: Grabaciones con Videocámaras y microfonía oculta», *op.cit.*

[782] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op.cit*, pág. 61.

[783] LLANO SÁNCHEZ, M.: «Derecho a la propia imagen y apariencia externa del trabajador: sentencia TC 170/1987, de 30 de octubre» en AA. VV. GARCÍA MURCIA, J. (DIR) *Derechos del Trabajador y Libertad de Empresa*, *op.cit*, pág. 435.

según el RPD en su art. 5.1 f) comprende "*la información fotográfica, acústica o de cualquier tipo".* Ello ha sido consagrado por la STC 29/2013, de 11 de febrero[784], que entra de lleno en la materia para concluir que la falta de comunicación a los afectados por las grabaciones supone una vulneración del derecho a la protección de datos personales. Esta sentencia expresamente niega que quepa justificar la falta de información en el interés empresarial de controlar la actividad a través de "*sistemas sorpresivos o no informados de tratamiento datos que aseguren la máxima eficacia en el propósito de vigilancia*" [785]. El problema es que la STC 39/2016, de 3 de marzo[786], modifica de nuevo la doctrina aplicable, considerando lo contrario que si puede haber sistemas sorpresivos o no informados de tratamiento datos, como más adelante se analizará, por lo que la protección del art.18.4 CE en esta materia presenta perfiles difusos. Incluso se ha llegado a afirmar que cuando una medida de control del empresario afecte a este derecho, habrá de juzgarse la constitucionalidad de la misma siempre con arreglo al principio de proporcionalidad.

I) Requisitos para la instalación de videocámaras

Los informes y dictámenes elaborados en el seno de la Unión Europea respecto a la videovigilancia laboral apuntan una línea interpretativa bastante restrictiva sobre el uso de cámaras, en virtud de la cual se rechazarían los sistemas que tienen por finalidad directa controlar la calidad y la cantidad de las actividades laborales, solamente se podrían aceptar esos mecanismos si vienen requeridos por exigencias organizativas y productivas[787]. Por otro lado, siguiendo la línea marcada por la STC 98/2000, de 10 de abril[788], la colocación de micrófonos es, por el contrario, más difícil de justificar salvo excepciones por la naturaleza intrínseca del trabajo a desempeñar (telemarketing)[789], o por razones de seguridad de la empresa y de la integridad física del trabajador (entidades de crédito, joyerías, en el caso de aeronaves, "*cajas negras*", etc.) La grabación de la

[784] STC 29/2013, de 11 febrero (RTC 2013\29).

[785] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*. *op.cit*. , pág. 40.

[786] STC 39/2016 de 3 marzo (RTC 2016\39).

[787] *Ibídem.*

[788] STC 98/2000, de 10 de abril (RTC 2000\98).

[789] En el *telemarketing*, como se verá más adelante, si las conversacion1es no pudieran ser grabadas la prestación de trabajo, tampoco podría ser dirigida y vigilada por el empresario.

conversación suele ser más sensible para la intimidad que la grabación de una imagen, pues, la palabra puede revelar pensamientos y sentimientos internos que la imagen no proporciona, o si lo hace, es de manera muy limitada[790].

a) Consideración general

Con carácter general podemos afirmar que un empresario no puede instalar sistema de videovigilancia alguno, sin que dicha medida sea conocida por sus trabajadores y los representantes de los mismos emitan un informe preceptivo aunque no vinculante, a tenor del art. 64 ET. Se ha de informar a los empleados de la ubicación, de las características de los dispositivos utilizados, de la finalidad del control, de la existencia de un fichero con sus datos personales y de los derechos de acceso[791], rectificación y cancelación. Es suficiente con el previo conocimiento; no es necesario el consentimiento: salvo que se trate de despachos privados, en cuyo caso sí se debe recoger el consentimiento expreso.

El cumplimiento de la normativa de Protección de Datos no convalida una posible prueba ilícita por otro motivo; no contrarresta la nulidad de las pruebas obtenidas, aunque se cumplan los requisitos que analizamos a continuación.

b) Acreditación de la necesidad de instalar cámaras

El art. 4 de la Instrucción núm. 1/2006 establece que "las imágenes solo serán tratadas, es decir, tomadas y grabadas, cuando sean adecuadas, pertinentes y no excesivas, en relación con el ámbito y las finalidades determinadas, legítimas y explícitas que hayan justificado la instalación de las cámaras o videocámaras". Por tanto, no existe una prohibición del uso de las cámaras en el trabajo, pero deberá justificarse la necesidad de su implantación, es decir, tendrá que ser una medida imprescindible.

---

[790] MERCADER UGUINA, J.R.: *Derecho del Trabajo. Nuevas Tecnologías y Sociedad de la Información*, ed. Lex Nova, 2002, págs. 104-105.

[791] El afectado deberá remitir al responsable del tratamiento solicitud en la que hará constar su identidad junto con una imagen actualizada. Por ello, el art. 5 de la Instrucción 1/2006 contempla que el responsable podrá facilitar el derecho de acceso mediante escrito certificado en el que, con la mayor precisión posible y sin afectar a derechos de terceros, se especifiquen los datos que han sido objeto de tratamiento y, para el caso de que se le deniegue el derecho, podría acudirse mediante denuncia ante el Director de la Agencia Española de Protección de Datos.

La jurisprudencia del Tribunal Constitucional exige, además que la medida sea proporcional. Por lo tanto, es necesario que la instalación de cámaras sea equilibrada con las necesidades de la empresa. Se ha de constatar que se cumple con los tres requisitos conforme a la regla del triple test:

-Que la medida sea susceptible de alcanzar el objetivo propuesto.

-Que sea necesaria, pues no existe otra capaz de dotar la misma eficacia.

-Que sea ponderada o equilibrada. Pues de ella se derivan más beneficios o ventajas para el interés general.

Por ejemplo, si dos cámaras son suficientes para conseguir la finalidad pretendida, no deberán instalarse seis; y si con la grabación visual es suficiente, no será necesario grabar el sonido[792].

c) La publicidad

Conforme a la Instrucción 1/2006 de la AEPD se debe colocar en las zonas videovigiladas al menos un distintivo informativo, ubicado en un lugar suficientemente visible[793], tanto en espacios abiertos como cerrados, asimismo se ha de tener a disposición de los interesados impresos en los que se detalle la información prevista en el art. 5.1 LOPD.

Según declaró la STC 29/2013, de 11 de febrero[794], era necesaria una "información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que la captación podía ser dirigida" , información que debe "concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo".

Pero desde la STC 39/2016, de 3 de marzo[795] para entender satisfecha la obligación empresarial, parece ser que basta con el distintivo informativo general de "*zona videovigilada*", sin necesidad de comunicar a los trabajadores los ámbitos

[792] VIDAL LÓPEZ, P.: «La utilización de las cámaras de videovigilancia para fines disciplinarios y de control del trabajo», *Actualidad Jurídica Aranzadi* núm. 888, 2014 (BIB 2014\2177).

[793] La STC 39/2016 basa buena parte de su argumentación en el texto de la Instrucción, en lo referente al conocimiento de la instalación de las cámaras de videovigilancia por medio de un distintivo visible.

[794] STC 29/2013, de 11 febrero (RTC 2013\29).

[795] STC 39/2016, de 3 marzo (RTC 2016\39).

concretos de control de la prestación laboral a que pueden destinarse las grabaciones de las cámaras. Además, incluso si no llegara a ofrecerse esa información general, se deriva que, en tal caso, la instalación de videovigilancia por parte de la empresa no determinaría automáticamente la vulneración del art. 18.4 CE, sino que, por el contrario, la legitimidad constitucional de la medida empresarial vendría determinada por la superación o no del principio de proporcionalidad[796].

De este modo, por tanto, la nueva doctrina del TC proporciona ahora cobertura expresa al criterio de los pronunciamientos judiciales que, pese a lo indicado en la STC 29/2013, de 11 de febrero[797], no descartaban la validez de las medidas de videovigilancia sorpresiva o no informada ante la preexistencia de sospechas fundadas sobre la comisión de irregularidades en el trabajo, cuya constatación, obviamente, podría quedar frustrada si se hubiera exigido la previa comunicación a los trabajadores.

d) Imágenes en espacios públicos[798]

El art. 4.3 de la Instrucción núm. 1/2006 pretende no facilitar un salvoconducto a la autorización para instalar videocámaras con la prohibición de filmar en espacios públicos. Ello tiene su sentido en tanto en cuanto estaría invadiendo la esfera de competencias de las Fuerzas y Cuerpos de Seguridad del Estado que son quienes tienen como misión la seguridad pública[799]. Otra cosa es que el sistema de instalación de grabación pueda tomar imágenes de forma parcial de la calle, ya sea para vigilar quién o quiénes están intentando acceder a la empresa, forzando la puerta de entrada o la verja de acceso al recinto en los casos en que estas existan[800]. Por ello, el art. 4.3 de la Instrucción núm. 1/2006 señala que "*Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida*".

---

[796] GARCÍA RUBIO, M.A.: «Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales», *Revista de Jurisprudencia El Derecho*, núm. 2, 2016 (EDB 2016/53076).

[797] STC 29/2013, de 11 febrero (RTC 2013\29).

[798] Art.42.1 de la Ley de Seguridad Privada.

[799] MAGRO SERVET, V.: «Panorama legal sobre la videovigilancia. Viabilidad legal de su utilización en la seguridad pública y privada», *Revista de Jurisprudencia El Derecho*, núm. 4, 2008 (EDB 2008/133278).

[800] *Ibídem.*

Por tanto, la instalación de cámaras en zonas privadas no se extiende a la vigilancia de espacios públicos y solo la permite, cuando sea imprescindible, para la vigilancia previamente autorizada como es la impuesta para los bancos y entidades de crédito[801].

e) Cesión de imágenes a terceros

El art. 9 LOPD establece, con algunos matices, una obligación de resultado consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros, en consecuencia, no se pueden ceder la imágenes a personas ajenas, salvo que sea imprescindible para el desarrollo del trabajo o se encuentre previsto en la Ley, como ocurre en el caso de la comisión de delitos, por la debida colaboración con las Fuerzas y Cuerpos de Seguridad del Estado.

f) Acceso restringido a personal autorizado

Tanto desde el punto de vista técnico como físico, debe limitarse el acceso a las imágenes al personal autorizado. Asimismo debe garantizarse que el personal guardará el deber de secreto respecto a las imágenes, por lo que se recomienda disponer de una cláusula contractual firmada por dicho personal[802].

g) Ámbito físico imprescindible

Solo es lícito realizar grabaciones en el ámbito físico estrictamente imprescindible. Asimismo, está terminantemente prohibida la grabación en aquellos espacios del lugar de trabajo donde pudiera vulnerarse la dignidad del sujeto grabado, como pudieran ser vestuarios, baños, duchas[803]. Ni es lícita la grabación en dependencias que puedan considerarse como privadas, máquinas de *vending*, áreas de descanso, etc[804].

---

[801] MAGRO SERVET, V.: «Instalación y uso de cámaras de videovigilancia en espacios privados y públicos. Respuesta de los tribunales», *op.cit.*

[802] *Ibídem.*

[803] STC 98/2000, de 10 de abril (RTC 2000\98).

[804] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*, *op.cit.*, pág. 13.

h) Notificación a la AEPD

Existe la obligación de notificar el fichero a la AEPD, salvo que no se lleve a cabo la grabación de las imágenes sino tan solo la filmación.

i) Información de la finalidad disciplinaria

Conforme a la STC 29/2013, de 11 de febrero[805], la información había de ser previa, precisa e inequívoca, los sistemas de videovigilancia podían utilizarse para satisfacer la finalidad que justificó su adopción. Se exigía un deber de información que tendrá que concretar las características y el alcance del tratamiento de datos que va a realizarse. Es decir se debía advertir, en qué casos las grabaciones podrán ser examinadas, con qué propósitos y durante cuánto tiempo, aclarando específicamente si las mismas podrán utilizarse como sistema de control del trabajo y poder imponer sanciones disciplinarias en base a las mismas[806].

Por tanto se podía proclamar validez de las filmaciones si al momento de instalación de las cámaras se avisó de su finalidad disciplinaria y de control de la actividad laboral; y al mismo tiempo, la imposibilidad de ejercer el poder disciplinario para sancionar incumplimientos que no estuvieran relacionados con la finalidad anunciada al momento de la introducción de este sistema de control[807].

No obstante lo anterior, la STC 39/2016, de 3 de marzo[808] vino a romper con este requisito haciéndolo prescindible. Por lo que en la actualidad, no es necesario respetar la exigencia de información previa de la finalidad disciplinaria de la videovigilancia , tal omisión ya no es causa de nulidad de la prueba entendiéndose como suficiente la notoriedad de la presencia de la cámara, o, simplemente, la existencia de carteles conforme a la Instrucción núm. 1/2006 de la Agencia Española de Protección de Datos.

---

[805] STC 29/2013, de 11 febrero (RTC 2013\29).

[806] VIDAL LÓPEZ, P.: «La utilización de las cámaras de videovigilancia para fines disciplinarios y de control del trabajo», *Actualidad Jurídica Aranzadi* núm. 888, 2014.

[807] *Ibídem.*

[808] STC 39/2016, de 3 marzo (RTC 2016\39).

j) Principio de compatibilidad

La prohibición de usos incompatibles, que emana del art. 4.2 LOPD y del art. 42.2 de la Ley de Seguridad Privada, excluye el tratamiento de datos personales del trabajador para una finalidad distinta de la originaria con la que fueron recabados[809].

k) Conservación de las grabaciones

Según la referida Instrucción núm. 1/2006 de la AEPD sobre la conservación de imágenes con fines de videovigilancia, el plazo para la conservación de las mismas es de un mes. Se establece que la recuperación de las imágenes debe hacerse durante un tiempo máximo de 30 días, por lo cual los datos serán cancelados en este período máximo desde su captación.

Lo adecuado sería establecer en el dispositivo un sistema automático de borrado de imágenes, como máximo, cada treinta días, de manera que nunca haya imágenes más antiguas a este período[810].

[809] GOÑI SEIN, J.L.: «Los Derechos Fundamentales Inespecíficos en la Relación Laboral Individual: ¿Necesidad de Reformulación?», *op.cit* , pág. 77

[810] ADSUAR PRIETO, Y.: «Incremento del uso y el abuso en la videovigilancia», *Actualidad Jurídica Aranzadi*, núm. 851, 2012.

J) El caso Casino de la Toja (STC 98/2000, de 10 de abril[811])

a) Relevancia

Esta sentencia representa un *leading case* particularmente sobresaliente[812] en materia de derechos fundamentales y contrato de trabajo, porque refleja tanto la tensión

[811] STC 98/2000, de 10 de abril (RTC 2000\98).

[812] La repercusión de la STC 98 /2000, de 10 de abril, es amplia; hasta la fecha, ha sido citada, entre otras, por las siguientes sentencias de diferentes órdenes jurisdiccionales, que se detallan a continuación:

STSJ Castilla de 23 marzo de 2015 (JUR 2015\95400), STSJ Cataluña de 11 octubre de 2013 (AS 2013\3149), STC 170/2013 de 7 octubre de 2013, (RTC 2013\170), STS Sala de lo Penal, núm. 493/2010 de 25 abril de 2010, (RJ 2010\4922), STS, de 19 abril de 2011, (RJ 2011\2309), STS Sala de lo Civil, núm. 799/2010 de 10 diciembre de 2010 (RJ 2011\139), STSJ Islas Canarias (Las Palmas) núm. 118/2008 de 31 enero de 2008, (AS 2008\1185), STC (Sala Primera), núm. 206/2007 de 24 septiembre de 2007, (RTC 2007\206), STSJ Andalucía (Granada) núm. 2014/2007 de 18 julio de 2007, (AS 2008\174), STSJ C. Valenciana Sala núm. 2490/2007 de 4 julio de 2007, (AS 2007\2879), STSJ Cataluña núm. 4813/2007 de 28 junio de 2007, (AS 2007\2877), STSJ Galicia 26 marzo de 2007, (AS 2007\2822), STSJ Castilla y León (Valladolid) núm. 1479/2006 de 18 septiembre de 2006, (AS 2006\2995), STSJ Madrid núm. 412/2006 de 14 junio de 2006, (AS 2006\3406), STSJ Navarra núm. 92/2006 de 18 abril de 2006, (AS 2006\1190), STSJ Cataluña núm. 729/2006 de 26 enero de 2006, (AS 2006\801), STSJ Navarra núm. 320/2005 de 13 octubre de 2005, (AS 2005\3436), STSJ Cantabria, núm. 852/2005 de 15 julio de 2005, (AS 2005\1918), STSJ Andalucía (Granada) núm. 531/2005 de 23 febrero de 2005, (AS 2007\2191), STC (Sala Primera), núm. 196/2004 de 15 noviembre de 2004, (RTC 2004\196), STSJ Cataluña, núm. 6390/2004 de 21 septiembre de 2004, (AS 2004\2880), STSJ C. Valenciana núm. 2616/2004 de 15 septiembre de 2004, (AS 2004\3314), STSJ Madrid núm. 696/2004 de 6 julio de 2004, (AS 2004\2325), STSJ Murcia núm. 278/2004 de 29 abril de 2004, (RJCA 2004\749), STSJ Andalucía (Málaga) núm. 2002/2003 de 13 noviembre de 2003, (AS 2004\15), STSJ Cantabria, Sala de lo Contencioso-administrativo, de 21 febrero de 2003, (JUR 2003\122751), STSJ Murcia núm. 156/2003 de 3 febrero de 2003, (AS 2003\468), STSJ Andalucía (Málaga) núm. 39/2003 de 9 enero de 2003, (AS 2003\1373), STC (Sala Primera), núm. 70/2002 de 3 abril de 2002, (RTC 2002\70), STSJ País Vasco de 25 septiembre de 2001, (AS 2001\3373), STSJ Andalucía (Sevilla) núm. 1050/2001 de 9 marzo de 2001, (AS 2001\2788), STSJ La Rioja núm. 382/2000 de 5 diciembre de 2000, (JUR 2001\64756), STSJ Madrid núm. 511/2000 de 14 septiembre de 2000, (AS 2000\4136).

conflictiva subyacente entre derechos fundamentales y poderes empresariales, como la dificultad que comporta la articulación recíproca entre unos y otros[813].

La importancia y relevancia de esta sentencia, es una cuestión unánime en la doctrina. Se ha dicho que "tiene la virtualidad de configurar un ámbito protector del derecho a la intimidad en la empresa más amplio que el que parecía dominante en la jurisprudencia menor"[814]. O que "cubre un concreto aspecto de laguna normativa, la protección en el lugar de trabajo de las conversaciones del trabajador como manifestación del derecho a la intimidad, y configura toda una doctrina, fundamentada en torno al principio de indispensabilidad, que sirve para dar protección específica a la esfera privada y a los derechos fundamentales de la persona del trabajador, en relación con cualquier sistema o dispositivo de vigilancia y control empresarial"[815].

b) El supuesto

Este hito jurisprudencial resuelve el recurso de amparo interpuesto contra la sentencia de la Sala de lo Social del TSJ de Galicia, que revocaba otra anterior de instancia y declaraba que la decisión de una empresa sobre la instalación de micrófonos en un casino en La Toja, con la finalidad de controlar las conversaciones entre los empleados y los clientes, concretamente en la zona de ruleta y de la caja, que se realizaron con información previa a los trabajadores en determinadas dependencias del centro de trabajo, no vulneraba derecho fundamental alguno de aquellos. Disconforme con este fallo, se pidió el amparo ante el Tribunal Constitucional el cual lo otorgó al entender que se había producido una intromisión ilegítima en el derecho a la intimidad.

La Sentencia comienza rechazando la premisa de la que partía la anterior sentencia recurrida, de acuerdo con la cual el centro de trabajo no es un lugar por definición en el que se ejerza el derecho a la intimidad por parte de los trabajadores. Como novedad, respecto a la anterior doctrina constitucional, el TC rechaza su idea originaria de que el alcance del derecho a la intimidad de los trabajadores quede limitado "*a las zonas del centro de trabajo donde no se desempeñen los cometidos propios de la*

[813] ÁLVAREZ ALONSO, D. «Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: sentencia TC 98/2000 de 10 de abril» en AA. VV. GARCÍA MURCIA, J. (Coor.) *Derechos del Trabajador y Libertad de Empresa, op. cit,* pág. 339.

[814] THIBAULT ARANDA, J. *Control Multimedia de la Actividad Laboral*, *op. cit*, pág. 22

[815] GOÑI SEIN, J.L.: *La Videovigilancia empresarial y la protección de datos personales, op. cit.* págs. 40-41.

actividad profesional" y acepta que "*pueda producirse lesión del referido derecho fundamental en el ámbito del desempeño de las tareas profesionales*".

c) Lo esencial

Por otro lado, el concepto de derecho a la intimidad en el trabajo se refuerza, adoptando una nueva dimensión el conflicto que obliga a contemplar las medidas de control del empresario desde la prevalente posición de los derechos fundamentales. La facultad de instalar medios de control al trabajador no se considera un poder absoluto por parte del empresario, sino condicionado por los derechos fundamentales, y en concreto, el respeto a la intimidad del trabajador. A estos efectos "*habrá que atender no solo al lugar de trabajo donde se instalan los sistemas audiovisuales de control, sino también a otros elementos de juicio, entre los que señala el carácter no indiscriminado y masivo de la instalación, su visibilidad o carácter subrepticio y la finalidad perseguida*". Este es el primer paso del razonamiento, en el lugar de trabajo puede resultar afectada la intimidad del trabajador. Esta premisa desmonta el punto de partida de la doctrina social tradicional.

d) Intervención mínima

El segundo paso del raciocinio queda menos precisado, consiste en afirmar que la grabación de las conversaciones de los trabajadores entre sí y de estos con los clientes, lesiona el derecho a la intimidad, porque "*permite captar comentarios privados*", que "*son ajenos por completo al interés empresarial, y por tanto, irrelevantes desde la perspectiva de control de las relaciones laborales*". Se entiende que esto puede tener consecuencias negativas para los trabajadores, aunque no se especifica cuáles son estas. Eso sí, parece querer afirmar que *"los trabajadores se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa"*[816].

[816] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op. cit*, pág. 21

e) Interés empresarial

El tercer paso del razonamiento consiste en reconocer que también concurre un interés de la empresa en las escuchas pues estas servían para resolver posibles reclamaciones de los clientes respecto a determinadas zonas, que era donde se habían instalado los micrófonos, concretamente, en el juego de la ruleta y en los cambios de caja. A partir de este razonamiento, aparece el conflicto entre el interés empresarial y el derecho a la intimidad de los trabajadores del casino de la Toja.

El Tribunal Constitucional señala que se ha de proceder a realizar una ponderación adecuada, lo cual supone que "*las limitaciones o modulaciones tienen que ser indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés menos agresivas y afectantes del derecho en cuestión, habrá que emplear estas últimas y no aquellas otras más agresivas y afectantes"* (FJ 7º).

f) Conclusión

Entiende el TC que estamos ante una "*intromisión ilegítima en el derecho a la intimidad",* pues la empresa con el sistema de audición y grabación permite captar comentarios privados de los clientes y de los trabajadores, que son ajenos al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales. La actividad que se pretendía controlar por parte de la empresa, declara el TC, se encuentra en lo que ha denominado la "*propia esfera de desenvolvimiento del individuo*" por lo cual se rebasan las funciones de control en la prestación laboral, que legalmente le concede el art. 20.3 ET al empresario.

g) Valoración

Algún sector discrepa del juicio que establece la sentencia, al considerarlo "*peligroso*". Como todo razonamiento de ponderación, aseveran, que si las restricciones de la intimidad se hubieran fundado en la aplicación de medidas de control indispensables y estrictamente necesarias, el resultado podría haber sido otro. La ponderación, señalan, es un mandato de optimización que tiende a reducir el enjuiciamiento, y el margen de discrecionalidad resulta tan amplio, que la decisión es impredecible: por lo cual siempre existe el riesgo de la aplicación del equilibrio de la balanza en función de apreciaciones

subjetivas. Consideran estos autores que la recepción entusiasta del método de ponderación por parte de jueces y tribunales del orden social, ha llevado a juicios ponderativos demasiado inmediatos y discrecionales[817]. Esta cuestión se analizará de manera detallada en un apartado específico destinado al principio de proporcionalidad.

[817] *Ibídem*, págs. 22-23.

K) El caso Economato de Ensidesa (STC 186/2000, de 10 de julio[818])

Esta importante Sentencia del Tribunal Constitucional[819] desestima el recurso interpuesto por el recurrente, al considerar que la medida acordada por la empresa demandada estaba justificada por la necesidad al haberse producido irregularidades en la actuación profesional del trabajador, cajero de un economato. Se demostró así que la conducta del empleado era constitutiva de transgresión de la buena fe contractual; la filmación no constituía ninguna vulneración del derecho a la intimidad resultando una

[818] STC 186/2000 de 10 de julio (RTC 2000\186).

[819] Citada por importantes sentencias de diversos órdenes jurisdiccionales, que se enumeran de manera cronológica a continuación: STS núm. 630/2016 de 7 julio, (RJ 2016\4434) STC núm. 39/2016 de 3 marzo (RTC 2016\39) STC núm. 187/2014 de 17 noviembre (RTC 2014\18), STC núm. 170/2013 de 7 octubre. (RTC 2013\170) SSTJ Andalucía núm. 649/2012 de 8 marzo (AS 2012\2424), STSJ Madrid núm. 652/2011 de 8 julio de 2011, (AS 2011\2517),STSJ Castilla la Mancha núm. 1543/2010 de 9 noviembre de 2010, (AS 2010\3124), STSJ Islas Canarias núm. 631/2009 de 30 abril de 2009, (AS 2009\1763), STSJ Madrid Snúm. 290/2009 de 17 abril de 2009, (AS 2009\1656), STSJ núm. 118/2008 de 31 enero de 2008, (AS 2008\1185), STSJ Andalucía (Sevilla) núm. 3883/2008 de 25 noviembre de 2008, (AS 2009\255), STSJ Madrid núm. 412/2006 de 14 junio de 2006, (AS 2006\3406), STSJ País Vasco de 25 septiembre 2001, (AS 2001\3373), STSJ La Rioja núm. 379/2000 de 5 diciembre de 2000, (AS 2001\135), STSJ C. Valenciana núm. 2490/2007 de 4 julio de 2007, (AS 2007\2879), STSJ Cataluña núm. 4813/2007 de 28 junio de 2007, (AS 2007\2877), STSJ Madrid núm. 397/2007 de 4 junio de 2007, (AS 2007\2246), STSJ Galicia Sala de lo Social, Sentencia de 26 marzo 2007, (AS 2007\2822), STSJ Castilla La Mancha Sala de lo Social, Sentencia núm. 159/2007 de 1 febrero de 2007, (AS 2007\1596), STSJ Madrid núm. 61/2007 de 23 enero de 2007, (AS 2007\1963), STSJ Cantabria Sala de lo Social, Sentencia núm. 48/2007 de 18 enero de 2007, (AS 2007\1030), STSJ Castilla y León (Valladolid), Sentencia núm. 1479/2006 de 18 septiembre de 2006, (AS 2006\2995), STSJ Galicia Sala de lo Social, Sentencia de 5 junio 2006, (AS 2007\1762), STSJ Navarra núm. 92/2006 de 18 abril de 2006, (AS 2006\1190), STSJ Cataluña núm. 729/2006 de 26 enero de 2006, (AS 2006\801), STSJ Navarra núm. 320/2005 de 13 octubre de 2005, (AS 2005\3436), STSJ Andalucía (Granada) núm. 531/2005 de 23 febrero (AS 2007\2191), STSJ La Rioja núm. 91/2005 de 18 febrero de 2005, (RJCA 2005\101), STSJ Castilla y León (Valladolid) núm. 2006/2004 de 8 noviembre de 2004, (AS 2004\3073), STSJ Cataluña núm. 6390/2004 de 21 septiembre de 2004, (AS 2004\2880), STSJ País Vasco de 25 septiembre 2001 (AS 2001\3373), STSJ Galicia de 20 marzo 2002 (AS 2002\3385), STSJ La Rioja núm. 379/2000 de 5 diciembre (AS 2001\135).

medida proporcionada para la finalidad perseguida por la empresa, que no es otra sino la comprobación de las sospechas de la comisión por parte de la demandante de graves irregularidades en su puesto de trabajo.

a) El problema

El pronunciamiento, que resuelve sobre la instalación de un circuito cerrado de televisión de manera clandestina, enfocado a dos puestos de trabajo, en concreto, a la caja registradora y al mostrador de paso de un economato, ante las sospechas de la empresa de un comportamiento irregular, se reafirma, una vez más, en el principio de proporcionalidad como criterio base para determinar la legitimidad de cualquier medida restrictiva de derechos fundamentales.

Se trata de un cajero que, como "*consecuencia de un descuadre llamativo en los rendimientos de su sección*" es sometido a vigilancia a través de un circuito cerrado de televisión que enfocaba desde el techo únicamente a las cajas registradoras en las que se habían detectado anomalías y al mostrador de paso de las mercancías. Las cintas de vídeo grabadas revelaron que el actor había sustraído de forma reiterada mediante maniobras en el cobro de artículos a los clientes, diferentes cantidades de la caja.

La prueba videográfica que acreditaba estos hechos fue impugnada por vulnerar los derechos a la intimidad personal y a la propia imagen. La sentencia partía de la definición del derecho a la intimidad como garantía de "*un ámbito propio y reservado frente a la acción y conocimiento de los demás*", si bien recordaba que no estábamos ante un derecho absoluto y que "*las relaciones sociales y profesionales en que se desarrolla la actividad laboral no forma parte de la intimidad*". De ahí se pasaba al reconocimiento de la limitación del derecho fundamental del trabajador por las facultades de control del empresario, y a la aplicación del principio de proporcionalidad, realizando una ponderación de la medida restrictiva.

b) Doctrina básica

Es en esta sentencia, en comparación con la anterior STC 98/2000, de 10 de abril[820] , donde el Tribunal Constitucional efectúa una sistematización más compleja del

[820] STC 98/2000, de 10 de abril (RTC 2000\98).

principio de proporcionalidad, describiéndolo como un juicio que ha de ponderarse y constatarse si se cumplen tres requisitos:

> "*En efecto, de conformidad con la doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la propia observancia del principio de proporcionalidad". Afirma que "para comprobar si una medida restrictiva de una derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto superar el (juicio de idoineidad); si, además es necesaria, en el sentido de que no exista otra medida mas moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad) y finalmente si la misma es ponderada o equilibrada, por derivarse de ella mas beneficios o ventajas para el interés general que perjuicios o valores en conflicto (juicio de proporcionalidad en sentido estricto)"* (FJº 6).

De conformidad con la lógica aludida, se llega a la conclusión de que la medida de instalación de un circuito cerrado de televisión era una medida ajustada al principio de proporcionalidad, porque la filmación era: 1º) Una actuación justificada, ya que existían razonables sospechas. 2º) Idónea para la finalidad pretendida por la empresa que necesitaba saber si el trabajador cometía las irregularidades sospechadas. 3º) Necesaria, ya que la grabación constituye la prueba de tales irregularidades. 4º) Equilibrada, pues la grabación de imágenes se limitó a la zona de cajas y tenía una duración limitada, temporal.

c) Valoración

La conclusión es que la intimidad del trabajador no resulta agredida, no hay intromisión ilegítima y a diferencia de la STC 98/2000, de 10 de abril, en la que la medida no era de vigilancia ni control, aquí sí tenía esa finalidad, pues la había provocado la actitud irregular del trabajador.

La doctrina de los tribunales ha interpretado que la STC 186/2000, de 10 de julio[821] viene a matizar la doctrina fijada en la STC 98/2000, de 10 de abril[822]; en concreto en lo que respecta a la prohibición de la utilización indiscriminada de los dispositivos de control en los puestos de trabajo, aunque atendiendo a una cierta disponibilidad de uso de los dispositivos de control empresarial, cuando, por ejemplo, concurren razones de seguridad.

Cierta doctrina considera que la técnica casuística de la ponderación ha dejado en el aire dos cuestiones fundamentales. La primera, si el resultado hubiera sido el mismo si no hubieran existido sospechas sobre trabajador y la función de la video vigilancia hubiera

[821] STC 186/2000, de 10 de julio (RTC 2000\186).
[822] STC 98/2000, de 10 de abril (RTC 2000\98).

sido simplemente para controlar la prestación del servicio. Y la segunda, sobre el hecho de que no hubiese dado información previa ni a los afectados ni al comité de empresa. Respecto a esta última cuestión nos dice que el art 64.1.3 ET carece de relevancia constitucional; pero esta respuesta no elimina el problema de si para el trabajador es relevante que se le haya informado previamente de que iba a ser filmado. Argumenta que esta información es exigible en materia de protección de datos y de videovigilancia pública. Pero la sentencia se limita a realizar una reflexión en términos de eficacia que "*esquiva el problema*".

L) Los casos de La Toja y Ensidesa como doctrina constitucional de referencia

Ambas sentencias definen toda una pauta de resolución de conflictos en el ámbito laboral, habiéndose convertido en el canon prevalentemente utilizado en la práctica constitucional y judicial para valorar la legitimidad de cualquier medida restrictiva de derechos fundamentales pues hasta ese momento existían distintos pronunciamientos de los tribunales laborales, que no siempre eran coincidentes. Suponen un cambio de método o de enfoque a la hora de enjuiciar el problema, puesto que parten de que la instalación de los medios es *a priori* una medida restrictiva de los derechos del trabajador y por tanto, se ha de considerar también de modo restrictivo la posibilidad de recurrir a tal medida.

Generalmente se califica estos dos pronunciamientos como trascendentales, porque más allá de ofrecer soluciones y respuestas en torno a las posibles cuestiones que se susciten con respecto a las nuevas tecnologías, configuran una doctrina general acerca de los derechos fundamentales del trabajador y el alcance de la vigilancia y control en el marco de la relación laboral[823].

No en vano las SSTC 98/2000 y 186/2000 pueden considerarse como las primeras del más alto interprete de la Constitución que han abordado directamente el trasfondo constitucional de la adopción de medidas de control y vigilancia por parte del empresario. Aunque advierte no son las primeras en abordar el principio de proporcionalidad y no introducen una regla nueva, su novedad radica en su aplicación al ámbito de las relaciones

[823] THIBAULT ARANDA, J.: *Control Multimedia de la Actividad Laboral*, *op. cit.*, pág. 21.

privadas y más en concreto, al ámbito de las relaciones laborales desde su originario ámbito público[824].

Desde otras perspectiva, se entiende que estas dos sentencias se encuentran en buena sintonía con la jurisprudencia internacional y comunitaria pues existe plena coincidencia, al menos en dos puntos. Por una parte, en el rechazo hacia una concepción restrictiva de la vida privada del trabajador; y por otra, la aceptación de que la protección a la intimidad o privacidad puede proyectarse sobre posibles manifestaciones de lo personal en el ámbito del trabajo[825].

El análisis de las sentencias sociales posteriores muestra que la influencia de la doctrina constitucional ha sido relevante, produciéndose un cambio de orientación que ha llevado a variar frente el criterio "*locativo*" anterior que estaba centrado en la consideración del tiempo y del lugar del trabajo como un ámbito en principio ajeno a la intimidad, se ha llegado a otra postura en la que existe la premisa de que todo control audiovisual afecta a la intimidad, lo cual determina que ha de aplicar la ponderación; los principios han de ser sopesados en función de las circunstancias del caso concreto, en el sentido de que en determinadas condiciones un principio debe preceder a otro - con lo cual variarían las circunstancias del caso- si la relación de preferencia puede alterarse.

La doctrina actual afirma que el control empresarial no puede ejercerse sin límites objetivos ni de forma incondicionada ya que ello podría vulnerar la mencionada expectativa a la intimidad que debe protegerse adecuadamente. De ahí que dicho control deba someterse a una doble limitación: 1ª) Mediante el establecimiento por parte de la empresa de unas condiciones de uso que deben ser conocidas por los trabajadores. 2ª) Con la existencia de los mecanismos arbitrados para verificar la corrección de dicho uso.

---

[824] FERNANDEZ VILLAZÓN, L.A.*: Las facultades empresariales de control de la actividad laboral*, *op. cit*., pág .43.

[825] ÁLVAREZ ALONSO, D.: «Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: STC 98/2000, de 10 de abril» en AA. VV. GARCÍA MURCIA, J. (Dir.): Derechos del Trabajador y Libertad de Empresa, *op. cit*., pág 360.

M) El caso Universidad de Sevilla (STC 29/ 2013, de 11 de febrero[826])

a) Relevancia

Supuso un hito en tanto en cuanto fue la primera vez que en la jurisprudencia constitucional se aplicaban los principios de protección de datos a las técnicas de control empleadas por el empresario. En ella se consideró lesionado el derecho a la protección de datos del trabajador que recurrió en amparo, siendo el criterio dirimente no el principio de proporcionalidad sino el de ausencia de información previa al mismo. Esta solución, pues, supuso la admisión de los principios de protección de datos como canon de enjuiciamiento constitucional[827]; hasta entonces, llevar a cabo un control videográfico sin conocimiento de los trabajadores había sido declarado por el TC que era una cuestión de legalidad ordinaria que no le competía[828].

La sentencia generó un precedente importante para otras posteriores, por apartarse del que desde la STC 186/2000,de 10 de julio[829] venía siendo el paradigma generalizado en la jurisprudencia constitucional y ordinaria, resolviendo la cuestión simplemente aplicando la normativa de protección de datos, centrándose en particular en un ingrediente concreto[830] -novedoso o al menos no analizado en profundidad hasta ese momento-: el derecho a ser informados previamente a la recogida de datos personales[831].

b) El supuesto

El Tribunal Constitucional anuló las sanciones impuestas a un subdirector sancionado por una institución universitaria tras ser controlado con cámaras de

---

[826] STC 29/2013, de 11 de febrero (RTC 2013\29).

[827] GOÑI SEIN, J.L.: «Los Derechos Fundamentales Inespecíficos en la Relación Laboral Individual: ¿Necesidad de Reformulación?», *op. cit.*, pág. 42.

[828] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*, *op.cit.*, pág. 40.

[829] STC 186/2000 de 10 de julio (RTC 2000\186).

[830] SÁNCHEZ MIGALLÓN, R.D.: «La vigilancia de la actividad del trabajador mediante videocámaras y circuitos cerrados de televisión», *Revista Iuslabor*, núm. 3, 2014, pág. 6.

[831]ÁLVAREZ ALONSO, D.: «Medios audiovisuales de vigilancia empresarial y derechos fundamentales del trabajador», *op. cit.* , pág. 13.

videovigilancia para conocer si cumplía con su jornada laboral. La Sala consideró lesionado su derecho a la protección de datos. Afirmó que la actuación de la Universidad no podía justificarse por el hecho de que hubiera distintivos para advertir de la instalación de cámaras sino que era necesario que se informase a los trabajadores de forma previa, precisa y clara de las grabaciones y de su objetivo. En la base de su fundamentación aparece el siguiente relato:

> *"En el caso enjuiciado, las cámaras de video-vigilancia instaladas en el recinto universitario reprodujeron la imagen del recurrente y permitieron el control de su jornada de trabajo; captaron, por tanto, su imagen, que constituye un dato de carácter personal, y se emplearon para el seguimiento del cumplimiento de su contrato. De los hechos probados se desprende que la persona jurídica titular del establecimiento donde se encuentran instaladas las videocámaras es la Universidad de Sevilla y que ella fue quien utilizó al fin descrito las grabaciones, siendo la responsable del tratamiento de los datos sin haber informado al trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen. Vulneró, de esa manera, el art. 18.4 CE*" (FJ 8º).

Se establece además que la información a los trabajadores, había de ser previa y expresa sobre la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida[832].

c) Visibilidad de las cámaras

Por otra parte, el hecho de que las cámaras pudieran ser vistas por los trabajadores porque no se ocultaba su existencia y eran apreciables a simple vista, o la existencia de carteles informativos, tampoco se consideraba relevante por la doctrina del Tribunal Constitucional expuesta, para enervar la ilicitud de la prueba.

No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser

[832] Tampoco el interés privado del empresario podrá justificar que el tratamiento de datos sea empleado en contra del trabajador sin una información previa sobre el control laboral puesto en práctica. No hay en el ámbito laboral, por expresarlo en otros términos, una razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del art. 18.4 CE. Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa" (FJ 7º).

examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

d) Habeas data

Principalmente, uno de los efectos de esta Sentencia más destacados fue el hecho de que, con ella, el derecho a la protección de datos *ex* art.18.4 CE quedaba sujeto a un canon de control de constitucionalidad distinto al que previamente se había aplicado a otros derechos fundamentales cuando, como en este caso, entraban en conflicto con medidas empresariales de fiscalización de la prestación laboral[833].

Como ya se ha explicado, en la colisión con el derecho a la intimidad de las medidas de audio y videovigilancia enjuiciadas en las STC 98/2000 y 186/2000, el TC partió de la existencia de un conflicto entre un derecho fundamental del trabajador y la concreta medida adoptada por el empresario en ejercicio de su poder de dirección y vigilancia reconocido en el art. 20.3 ET y puesto en relación con los arts. 33 y 38 CE , de tal manera que, apreciada esa controversia entre bienes e intereses constitucionales, la solución debía alcanzarse mediante la aplicación del principio de proporcionalidad[834].

Por el contrario, la STC 29/2013, de 11 de febrero[835], aproximó el asunto debatido desde parámetros de enjuiciamiento distintos, al rechazar la existencia de norma legal en las relaciones laborales que autorizara restricciones del derecho a la información sobre el tratamiento de datos personales, no considerando hábil a tal fin el art. 20.3 ET. Desde esta máxima, por tanto, negada la validez constitucional de restricciones al derecho fundamental de los trabajadores *ex* art. 18.4 CE, quedaba en consecuencia impedida la ponderación de la medida empresarial y la consiguiente aplicación del principio de proporcionalidad[836].

De este modo, se establecía un canon de control de constitucionalidad más rígido que el que la jurisprudencia constitucional venía aplicando respecto al otros derechos fundamentales como el derecho a la intimidad, por esta razón a cuyo servicio se sitúa la

---

[833] GARCÍA RUBIO, M.A.: «Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales», *Revista de Jurisprudencia El Derecho*, núm. 2, 2016. (EDB 2016/53076).

[834] *Ibídem.*

[835] STC 29/2013, de 11 de febrero (RTC 2013\29).

[836] *Ibídem.*

garantía prevista en el art.18.4 CE cierto sector de la doctrina afirma que con la STC 29/2013, se otorgaba una protección cuasi absoluta al derecho fundamental del art. 18.4 CE[837].

e) Discrepancia

El voto particular del magistrado OLLERO TASARA, aludiendo a la doctrina de la STC 186/2000, afirma que esta sentencia tras analizar la cuestión a enjuiciar realizaba la correspondiente ponderación, en base al principio de proporcionalidad, mientras que la sentencia de cuyo sentido disiente, no aplica el triple test de proporcionalidad, a su juicio, a todas luces necesario. Por otro lado, considera un error que se realice la fundamentación, en base a la STC 292/2000, pues ésta se pronunciaba en abstracto sobre la constitucionalidad de una ley y no sobre un hecho concreto como el que se enjuicia, lo que hace que el derecho a la protección de datos no se haya interpretado de manera restrictiva sino en abstracto[838]. Estos postulados en buena medida se verán recogidos en la argumentación principal de la STC 39/2016, de 3 de marzo[839].

Algún autor comparte la opinión del Magistrado disidente, sostiene que dada la clara postura que hasta la fecha había mantenido el Tribunal Constitucional la STC 29/2013 plantea interrogantes que ya parecían estar cerrados[840], no realiza una interpretación flexible y equitativa del principio constitucional del art. 18.4 CE[841]. Opina que el fundamento de la sentencia es que no existe habilitación legal expresa para la omisión del derecho a la información sobre el tratamiento de los datos personales o al

---

[837] SANTANA BELTRÁN, S.: «A vueltas sobre el impacto en las relaciones laborales de la última doctrina constitucional acerca del derecho a la protección de datos ex. Art. 18. 4 CE STSJ País Vasco 18 junio 2013», *Nueva Revista Española de Derecho del Trabajo* núm. 171, 2014 (BIB 2014\4528).

[838]Argumenta además en el voto particular, que vía jurisdiccional, se había considerado probado que "*entre las diecinueve autorizaciones con que contaba la Universidad para hacer uso de los soportes informáticos o ficheros grabados por sus videocámaras*", figuraba una dirigida "*al control de acceso de las personas de la comunidad universitaria*". Igualmente que "*las zonas video-vigiladas con cámaras de vigilancia contenían distintivos informativos*", por lo que afirmando debía haberse denegado el amparo por no haberse vulnerado protección de datos del trabajador.

[839] STC 39/2016 de 3 marzo (RTC 2016\39).

[840] Se pregunta:*" ¿Dónde queda el carácter relativo y no absoluto de los derechos fundamentales? ¿Dónde queda la ponderación en relación con otros intereses de relevancia constitucional?".*

[841] RODRÍGUEZ COPÉ, Mª, L.: «Facultades de control empresarial y circuito cerrado de televisión STC 29/2013 de 11 de febrero», Temas Laborales: *Revista andaluza de trabajo y bienestar social*, núm. 121, 2013, págs. 189-200.

referido empleado universitario. Esa lógica fundada en la conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial, pues se confundiría la legitimidad del fin con la constitucionalidad del acto, cuando lo cierto es que cabe proclamar la legitimidad de tal propósito, pero del mismo modo, declarar que lesiona el art. 18. 4 CE, la utilización para llevarlo a cabo con medios encubiertos que niegan al trabajador la información exigible.

N) El caso Bershka (STC 39/2016, de 3 de marzo[842])

a) Relevancia

El TC con esta sentencia afirma que con ella se ha perfilado su doctrina, pero tal aseveración no es del todo acertada. En puridad, cabe sostener con rotundidad que el Pleno del TC ha cambiado de manera radical, la doctrina de la STC 29/2013, de 11 de febrero[843]. Sin embargo, resulta sorprendente que no se haya mencionado este trascedente cambio en el cuerpo de la sentencia[844].

El recurso de amparo fue admitido a trámite por la Sala Primera del TC, y esta hizo uso de la posibilidad ofrecida por el art. 10.1 n) de LOTC y propuso que el litigio fuera conocido por el Pleno del TC. Así ocurrió efectivamente: el motivo esgrimido para reunir al Pleno fue clarificar la doctrina existente sobre videovigilancia[845], aunque

---

[842] STC 39/2016, de 3 marzo (RTC 2016\39).

[843] STC 29/2013, de 11 febrero (RTC 2013\29).

[844] GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016», *Revista Aranzadi Doctrinal* núm. 5, 2016 (BIB 2016\21165).

[845] La razón que parece justificar la decisión de que el litigio fuera conocido por el Pleno del TC, se encuentra recogida en el último párrafo del FJ 1º:"*Debe añadirse, de otro lado, que el presente recurso de amparo tiene especial trascendencia constitucional [art. 50.1 b) de la Ley Orgánica del Tribunal Constitucional], pues las especificidades propias del caso permiten a este Tribunal perfilar o aclarar su doctrina en relación con el uso de cámaras de videovigilancia en la empresa [STC 155/2009, FJ 2 b)]. Se pretende, así, aclarar el alcance de la información a facilitar a los trabajadores sobre la finalidad del uso de la videovigilancia en la empresa: si es suficiente la información general o, por el contrario, debe existir una información específica (tal como se había pronunciado la STC 29/2013, de 11 de febrero*)".

realmente se produce un giro brusco en la doctrina o *overrruling*[846] que no fue presentado como tal.

La sentencia del TC desestima el recurso de amparo interpuesto por una trabajadora despedida por sustracción de dinero de la caja en la que prestaba su actividad, contra el auto que resolvía la desestimación de un incidente de nulidad de actuaciones planteado ante un TSJ.

b) El caso

La empleada interpuso incidente de nulidad de actuaciones ante la Sala de lo Social del Tribunal Superior de Justicia de Castilla y León que fue desestimado mediante auto. El TSJ respondió denegando el incidente de nulidad porque la sentencia cuya nulidad se instaba (STSJ de Castilla y León de 23 de julio de 2013[847]) era susceptible de recurso de casación para unificación de doctrina y porque la misma ya abordó la cuestión que se suscitaba en el recurso de suplicación.

Se desestimó la suplicación interpuesta contra la sentencia de la instancia, en la que se pretendía la declaración de nulidad del despido efectuado por vulneración de derechos fundamentales por obtención de las pruebas que posibilitaron el despido disciplinario de forma ilícita.

Para la sentencia de instancia, en la instalación de las cámaras y en la posterior grabación se cumplió de manera escrupulosa la normativa aplicable, ya que de acuerdo con la STC 186/2000, 10 de julio[848], concurría la situación precisa para el control oculto; esto es, sin notificar expresamente la colocación de la cámara a los trabajadores, porque era, en principio, el único medio posible dicho control para satisfacer el interés

---

[846] El art. 13 de la LOTC, recoge que: "*Cuando una Sala considere necesario apartarse en cualquier punto de la doctrina constitucional precedente sentada por el Tribunal, la cuestión se someterá a la decisión del Pleno"*. El precepto, que viene a acoger la técnica del overruling, contempla el hecho de que una Sala, cuya competencia básica es el conocimiento y resolución de los recursos de amparo, considere necesario apartarse en cualquier aspecto de la jurisprudencia o doctrina constitucional fijada, así ha de presuponerse, bien por la otra Sala, bien por el propio Tribunal en Pleno. Este último, por el contrario, no queda vinculado por su propia jurisprudencia, que puede cambiar en cualquier momento, si así lo entiende oportuno el propio Pleno. *Vid*. FERNÁNDEZ SEGADO, F. : «Los overruling de la jurisprudencia constitucional», *Foro Nueva Época*, núm. 3, 2006, pág. 28.

[847] STSJ Castilla y León de 24 julio de 2013 (JUR 2013\276661).

[848] STC186/2000, de 10 de julio (RTC 2000\186).

empresarial de saber fehacientemente quién estaba realizando los actos defraudatorios de los que indiciariamente ya se tenían conocimiento.

La demanda de amparo se fundamenta en la infracción de los siguientes arts:14, 15, 18.1, 18.4 y 24 CE por haberse admitido como prueba de cargo en el proceso por despido las grabaciones de vídeo presentadas por la empresa, prueba que la recurrente estima nula de pleno derecho al haberse obtenido vulnerando derechos fundamentales de la trabajadora. La decisión empresarial violaba su derecho al honor, intimidad y dignidad, y manifestaba que el centro de trabajo no existía comunicación al público ni carteles comunicativos de la existencia de cámaras de videograbación, ni tampoco comunicación a la AEPD, ni autorización por la Sección de Seguridad Privada de la Comisaría de Policía de León, ni tampoco comunicación o informe previo del comité de empresa de la instalación de la videograbación.

Los hechos transcurren del siguiente modo:

-Una empresa del grupo INDITEX (Bershka) despidió a una trabajadora por transgresión de la buena fe contractual porque sostenía que se había venido apropiando de efectivo de la caja de la tienda, en diferentes fechas y de forma habitual.

- Los hechos que dieron lugar al despido fueron conocidos a consecuencia de la instalación de videovigilancia oculta.

- Para proceder a tal instalación de cámaras ocultas, la empresa argumentó que a raíz de la instalación de un nuevo sistema de control informático de caja, había detectado que en la tienda y, en concreto, en la caja donde prestaba sus servicios la trabajadora existían múltiples irregularidades, por lo que entendía que había indicios para poder presumir una posible apropiación dineraria por parte de alguno de los trabajadores que operaban en dicha caja.

- Por tal motivo encargaron a una empresa de seguridad que instalara una cámara de videovigilancia en la tienda donde prestaba sus servicios la demandante y que controlara la mencionada caja en cuestión.

-La cámara se instaló no habiendo comunicando a los trabajadores dicha instalación, si bien en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo.

En las actuaciones seguidas en el Tribunal Constitucional el Ministerio Fiscal interesó la desestimación del amparo, planteando su inadmisión por defectos formales, y en el supuesto de que la Sala entrara a conocer del fondo consideraba que la decisión

empresarial cumplió con los criterios fijados por la Constitución y el propio Tribunal Constitucional para entenderla ajustada a derecho, entendiendo que la doctrina constitucional de referencia debía ser la de la STC 186/2000, de 10 de julio[849] y no la STC 29/2013, de 11 de febrero[850]. En un sentido parecido al del Ministerio Fiscal, se muestra la oposición al recurso planteada por la empresa.

c) Cuestiones procesales

El Tribunal Constitucional comenzó rechazando dos obstáculos procesales alegados, respectivamente por la empresa y por el Ministerio Fiscal:

-El primero, relativo a la vulneración de la subsidiariedad del recurso de amparo al no interponer recurso de casación de unificación de doctrina ante el TS, recordando el TC que "*por lo demás, no es suficiente alegar la abstracta procedencia de tal recurso, sino que, dada su naturaleza extraordinaria, corresponde acreditar la posibilidad de utilizar esa extraordinaria vía a la parte que pretende hacer valer la no interposición del recurso como motivo de inadmisibilidad de la demanda de amparo*" (FJ 2º).

-El segundo sobre la extemporaneidad del recurso de amparo al haber prolongado artificialmente el plazo para su interposición al haberse suscitado un recurso manifiestamente improcedente como era el incidente de nulidad de actuaciones, lo que se rechazó recordado la doctrina relativa a la necesidad para apreciar este obstáculo de que la "*improcedencia del recurso sea evidente, esto es, comprobable prima facie sin intervención de dudas interpretativas que sea necesario despejar por medio de criterios no absolutamente indiscutibles, ya que el respeto debido al derecho de la parte a utilizar cuantos recursos considere útiles para la defensa de sus intereses impide exigirle que se abstenga de emplear aquellos cuya improcedencia sea razonablemente dudosa y, en consecuencia, que asuma el riesgo de incurrir en una falta de agotamiento de la vía judicial previa*" (FJ 2º) concluyendo que " *la formulación del incidente de nulidad de actuaciones no puede considerarse como un recurso manifiestamente improcedente cuya interposición conlleve un alargamiento indebido de la vía judicial previa al recurso de amparo, puesto que el propio órgano judicial ante el que se promovió el incidente, lo admitió a trámite, dio traslado de la pretensión anulatoria a las demás partes, lo analizó y lo resolvió con un pronunciamiento desestimatorio*" (FJ 2º).

[849] STC 186/2000 de 10 de julio (RTC 2000\186)
[850] STC 29/2013, de 11 febrero (RTC 2013\29).

d) Consentimiento del trabajador

Por lo que se refiere, en primer lugar, a la violación del derecho a la autodeterminación informativa, el TC precisa que "*la imagen se considera un dato de carácter personal, en virtud de lo establecido en la LO 15/1999 art. 3, de protección de datos de carácter personal*" (FJ 3º).

El empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art 20.4 ET.

Para fundamentar tal aseveración se hace mención expresa de la doctrina contenida en la STC 292/2000, de 4 de enero [851] : "*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos*" (FJ 3º).

De este modo, se resalta que son "*elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele*" (FJ 3º).

[851] STC 292/2000, de 30 de noviembre (RTC 2000\292).

Por tanto, para el TC el consentimiento del afectado es, el elemento definidor del sistema de protección de datos de carácter personal. De lo que colige que en el ámbito laboral el consentimiento del trabajador pasa como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes. Por ello un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato.

Quizás el TC parece confundir los términos consentimiento y conocimiento previo del trabajador, porque ni tan siquiera existía debate con anterioridad a esta sentencia sobre la necesidad de consentimiento del trabajador en videovigilancia, por constituir una excepción del art. 6 LOPD. Una cosa es eximir del consentimiento, como hacen la LOPD y su reglamento de desarrollo y otra abogar por el consentimiento implícito. O hay consentimiento o no lo hay. La ley y su reglamento se decantan por la primera vía: no hay consentimiento y no hace falta que lo haya. En otros pasajes de la sentencia el TC abandona la citada tesis del consentimiento implícito para pasar a la de la improcedencia/inexistencia del consentimiento, de modo que en este punto ha faltado un mayor cuidado en la construcción de la argumentación de la sentencia[852].

e) Conocimiento del trabajador

Para entender satisfecha la obligación empresarial de conocimiento del trabajador basta con la mera información genérica. Sorprendentemente la fuerza prevalente del derecho del art. 18.4 CE, en esta sentencia se diluye con la sola constatación de una

[852] CABELLOS ESPIÉRREZ, M.A.: «El derecho a ser informado como elemento esencial del derecho a la protección de datos. Una visión crítica de la jurisprudencia del Tribunal Constitucional y de su cambio de doctrina en la STC 39/2016», Revista vasca de Administración Pública, núm. 106, 2016, págs. 201-202.

pegatina informativa[853] exigida por la Instrucción núm. 1/2006 de la Agencia Española de Protección de Datos[854].

Para el TC ya no hay que acudir a la información detallada de la STC 29/2013, de 11 de febrero[855], basta ahora con el distintivo informativo general de "*zona videovigilada*"; no hay necesidad de comunicar a los trabajadores los ámbitos concretos de control de la prestación laboral a que pueden destinarse las grabaciones de las cámaras; por tanto, los trabajadores se considerarán suficientemente informados con los carteles estándares indicativos de "*zona vídeo-vigilada*" [856].

f) Juicio de proporcionalidad

Por primera vez y en contra de la doctrina de la STC 29/2013, de 11 de febrero[857], se somete al juicio de proporcionalidad el derecho del art. 18.4 CE, afirmándose que "*la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad"*, premisa del todo errónea pues para determinar si existe o no infracción del art. 18. 4 CE, no existe un conflicto constitucional en este punto sino una cuestión de delimitación previa; previamente había información suficiente o no la había.

Este el punto más incoherente de toda la fundamentación jurídica de la sentencia; constituye un salto al vacío, un olvido del contenido esencial del derecho y su relegación a una situación de igualdad de trato con el principio de proporcionalidad[858], un "*verdadero despropósito jurídico-constitucional"* en palabras del Voto Particular.

---

[853] VALDÉS DAL-RÉ afirma en su voto particular de manera algo sarcástica que "*difícil que el derecho a recibir información pueda concretarse en una mera pegatina con el correspondiente distintivo visible en un cristal, una vez cumplido, eso sí, en contenido y diseño – como recuerda la Ponencia aprobada – el sin duda trascedente Anexo de la Instrucción citada*".

[854] MOLINA NAVARRETE, C.: «Expectativa razonable de privacidad y poder de vigilancia empresarial. ¿*Quo vadis* Justicia Laboral?», *CEFLegal revista práctica de derecho, Comentarios y casos prácticos*, núm. 399, 2016, pág.177.

[855] STC 29/2013, de 11 febrero (RTC 2013\29).

[856] PERE VIDAL, «Zona videovigilada: STC de 3 de marzo de 2016, sobre las cámaras de vigilancia en el trabajo», *Actualidad Jurídica Aranzadi* núm. 918, 2016 (BIB 2016\2495).

[857] STC 29/2013, de 11 febrero (RTC 2013\29).

[858] ROJO TORECILLA, E. (2016, 12 de marzo) Después de las Jornadas Catalanas de Derecho Social. ¿Constitucionalización del poder de dirección empresarial en la relación de trabajo? Nota crítica a

Argumenta el TC que en cuanto toda medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad, debe examinarse además el razonamiento de las sentencias impugnadas. De ellas se desprende que "*en el caso que nos ocupa, la medida de instalación de cámaras de seguridad que controlaban la zona de caja donde la demandante de amparo desempeñaba su actividad laboral era una medida justificada (ya que existían razonables sospechas de que alguno de los trabajadores que prestaban servicios en dicha caja se estaba apropiando de dinero); idónea para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en la CE art.18.1*".

En ningún momento la Sala se plantea de forma autónoma si se ha vulnerado el deber de información previa, cuyas excepciones sólo pueden fijarse vía legal, sino que ha centrado su argumentación en el papel complementario de la información con respecto al consentimiento (o no necesidad del mismo) por el afectado[859].

---

la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (sobre instalación de cámaras de *http://www.eduardorojotorrecilla.es/2016/03/despues-de-las-jornadas-catalanas-de_21.html*

videovigilancia) (I). El blog de Eduardo Rojo. Recuperado de *http://www.eduardorojotorrecilla.es/2016/03/despues-de-las-jornadas-catalanas-de_21.html*

[859] ROJO TORECCILLA, E. (2016, 21 de marzo) Después de las Jornadas Catalanas de Derecho Social. ¿Constitucionalización del poder de dirección empresarial en la relación de trabajo? Nota crítica a la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (sobre instalación de cámaras de videovigilancia) (II) *http://www.eduardorojotorrecilla.es/2016/03/despues-de-las-jornadas-catalanas-de.html*

g) Primer Voto Particular

En relación al primero de los votos que formula el magistrado VALDÉS DAL-RÉ[860], llama la atención sobre la *mutación constitucional que sufre el contenido esencial del derecho del art. 18.4 CE* y la ausencia de motivación sobre las razones del cambio en la jurisprudencia constitucional[861].

El voto particular centra su atención en el juicio de ponderación y proporcionalidad que la sentencia considera que debe realizarse en el caso enjuiciado, despreocupándose de cuál sea el contenido esencial del derecho en cuestión, puede igualmente efectuarse "incluso si los poderes empresariales se ejercitan con manifiesta irregularidad o exceso; esto es, fuera del marco de la ley", recordando que tal hipótesis está expresamente contemplada, de tal manera que pudiera llegar a darse el caso de prevalencia del ejercicio del poder de dirección empresarial, aún ejercido de manera no conforme a derecho sobre el derecho constitucional del art. 18.4 CE y la doctrina del TC en SSTC 292/2000 de 30 de noviembre y 29/2013 de 11 de febrero, siempre y cuando

[860] Previamente debemos recordar que fue el magistrado ponente de la STC 29/2013,de 11 de febrero con una construcción doctrinal mucho más sólida que la sentencia sobre la que formula el voto disidente.

[861] Recoge: «recta aplicación de un derecho fundamental como el garantizado en el art.18.4 CE hubiera comportado, como en el pasado fue argumentado con solvencia jurídica y mesura interpretativa, declarar que no hay una habilitación legal expresa para la omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales; y que tampoco es dable situar su fundamento en el mero interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. La lógica por la que ha optado la Sentencia de la mayoría, fundada en la más primaria utilidad o conveniencia empresarial, quebranta la efectividad del derecho fundamental de la CE art.18.4, en su núcleo esencial; confunde la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, LET art.20.3 en relación con el LOPD art.6.2) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, LOPD art.5). Y lo cierto es, sin embargo, que cabe proclamar la legitimidad de aquel objetivo (incluso sin consentimiento del trabajador, LOPD art.6.2, como señala la Sentencia aprobada) y, al mismo tiempo, hacer constar que lesiona la Const art.18.4 la utilización, para ejecutar el acto, de medios encubiertos que niegan al trabajador la información exigible».

ello resultara tras la utilización de aquellos juicios, planteando el voto particular en forma de duda, pero con un innegable contenido muy crítico[862].

h) Segundo Voto Particular

El segundo de los votos particulares es formulado por XIOL RÍOS y comparte sustancialmente, el voto anterior, si bien introduce algunas matizaciones porque a su juicio la sentencia básicamente, que sostiene que la información de la LOPD art.5 se cumple mediante un anuncio hecho al público sobre la existencia de cámaras de seguridad en el establecimiento y no, como entiende que debiera ser, con una información suministrada a los "trabajadores especificando el fin de control de cumplimiento de la relación laboral", en tanto dicho precepto "ordena específicamente que la información se dirija a los interesados, configurando con ello el contenido esencial del derecho, que en el ámbito laboral debe entenderse referido a los trabajadores". Señalando, además, que aunque se hubiera anulado la videovigilancia , no debieran ser anuladas las sentencias pues existían otros elementos probatorios de la procedencia del despido.

O) Doctrina de la Sala Cuarta del Tribunal Supremo

a) Supermercado Champion (STS de 13 de mayo de 2014[863])

El supuesto.- Recoge el conflicto entre derechos fundamentales, en el seno de un despido disciplinario basado en las grabaciones de imágenes, recoge el testigo de lo manifestado un año antes por la STC 29/2013 de 11 de febrero. El TS desestima el recurso de casación para la unificación de doctrina interpuesto por una conocida marca de supermercados (CHAMPION) y confirma la nulidad del despido disciplinario de la trabajadora, declarado por la STSJ del País Vasco de 9 de abril de 2013[864], al existir

[862] ROJO TORECCILLA, E. (2016, 21 de marzo) Después de las Jornadas Catalanas de Derecho Social. ¿Constitucionalización del poder de dirección empresarial en la relación de trabajo? Nota crítica a la sentencia del Tribunal Constitucional de 3 de marzo de 2016 (sobre instalación de cámaras de videovigilancia) (III). *http://www.eduardorojotorrecilla.es/2016/03/despues-de-las-jornadas-catalanas-de_80.html.*

[863] STS 13 de mayo de 2014 (EDJ 2014/102959).

[864] STSJ de 9 de abril de 2013 (EDJ 2013/308235).

vulneración empresarial de los derechos fundamentales del art. 18.4 CE, por la indebida utilización de las grabaciones de imagen en el lugar de trabajo a través de cámaras de videovigilancia.

Los hechos.- La cajera despedida generaba dos tickets, y posteriormente anulaba la compra de dos productos escaneados. Al día hábil siguiente se procedía a exhibirle el contenido de la grabación en la que se recogían tales hechos a la encargada. Transcurridos unos días, se despide a la trabajadora acusándola de beneficiar a su novio, no habiéndole vendido una botella de vodka, varias bebidas energéticas y otros artículos al haber sido anulada su venta, aunque no consta que tal ticket fuera vendido a su pareja. La cámara que se utilizó visualizaba las puertas de acceso y los lineales.

El procedimiento.- La Sala de lo Social del País Vasco dictó sentencia en un primer recurso interpuesto, declarando la nulidad de la sentencia, del Juzgado de lo Social, obligando a practicar una vista sobre la pertinencia de la prueba videográfica de la recurrente. El Juzgado de lo Social cumplió con tal exigencia y se celebró una vista en la que declararon dos testigos que coinciden en sus manifestaciones; uno de ellos es el representante de los trabajadores que afirma que cuando se instalaron las cámaras se interesó por la finalidad del uso de las mismas y se le contestó que eran para evitar robos de terceros, el otro era el responsable de seguridad nacional de la empresa y afirmó que el sistema de videovigilancia instalado era para disuadir de robos del público en general y fue, incluso más allá, precisando que si se sospecha de irregularidades de un cajero en concreto, se ha de instalar un sistema especial *ad hoc* consistente en una cámara que filme el puesto de trabajo del trabajador del que se sospecha y un dispositivo que asegure la sincronicidad entre la captación de imágenes y la generación de los tickets de caja. Posteriormente, se procedió a dictar nueva sentencia, en la que se volvió a declarar la nulidad del despido.

La sentencia de la instancia fue objeto de un nuevo recurso de suplicación que desestima las pretensiones de la empresa, a través de una nueva sentencia del TSJ del País Vasco, que es a su vez es sometida a recurso de casación para unificación de doctrina ante el TS.

El recurso de casación.- En su recurso la empresa señaló como sentencia de contraste la de la Sala de lo Social del TSJ de Canarias, de 3 de noviembre de 2011[865],

[865] STSJ de 3 de noviembre de 2011 (EDJ 2011/344134).

alegando vulneración del art. 20 ET, en relación con el 18.3 CE, así como de manera subsidiaria solicitó la declaración de la improcedencia del despido y no la de la nulidad, pretensión esta última que se rechazó de pleno al tratarse de una cuestión nueva, no planteada en la segunda instancia. Al analizar el primer motivo del recurso la sentencia incide en la clara delimitación entre el derecho reconocido en el art. 18.1 CE y el del art. 18.4 CE, pues a pesar de que tengan conexiones, son autónomos. (FJ 4.1º).

Tipo de problema.- Seguidamente en el FJ 4º.2, se pasa a afirmar que nos encontramos ante un supuesto distinto al analizado en la STC 186/2000, ya que en este caso se instalaban cámaras *ad hoc*, para fiscalizar la labor de una cajera de la que existían sospechas. Se obvia cualquier contenido o referencia a la sentencia de contraste de la Sala de lo Social de Canarias, de manera directa, adoleciendo la resolución en este punto de falta de motivación suficiente. Si acudimos a la lectura de la referida sentencia de contraste, observamos que sí que basa su argumentación en la STC 186/2000, pero el TS no menciona ni explica el sentido y contenido de la misma sentencia de contraste[866], quizás por no ahondar en el punto débil de ésta, que considero que es la ausencia de contradicción, que debería haber dado lugar a la inadmisión del recurso de casación de unificación doctrina, pues nos encontramos ante dos supuestos claramente distintos[867].

Referencia al caso Universidad de Sevilla.- Por el contrario, se sostiene que sí es subsumible en el mismo tipo el supuesto enjuiciado y el de la reciente doctrina constitucional sobre protección de datos*: "mayor conexión con el supuesto ahora analizado existe en el resuelto en la STC 29/2013, de 11 de febrero*" (FJ 4.3º). Por lo que de conformidad con la más reciente doctrina constitucional, es necesaria la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que la captación de imágenes está dirigida, sin que la ilegalidad

[866] Se trata de la confirmación del despido disciplinario de una trabajadora de MERCADONA, S.A., de la que existían sospechas de irregularidades por descuadre de su caja, se procede a instalar un sistema que graba su puesto de trabajo, y se constata su conducta trasgresora de la buena fe contractual, al grabarse cómo en tres días distintos arruga un billete y se lo esconde en la mano; un día de 50 euros, al día siguiente de 20 euros, y dos días después de 50 euros.

[867] En la sentencia de contraste se procede a avalar el uso de la videovigilancia oculta siendo inaplicable el art. 18.4 CE, por la razón que misma la sentencia razona en su FJ 4º: "*Debe dejarse apartada toda referencia a la protección del tratamiento informatizado de datos personales (L.O. 15/99) toda vez que la grabación no tiene la finalidad de ser archivada ni tratada informáticamente, sino exclusivamente la finalidad probatoria antes apuntada*". En la sentencia recurrida ante el TS, la grabación videográfica, era un hecho visible y por tanto, notorio y el control que se hacía era genérico, sin información previa a los trabajadores.

de la conducta empresarial desaparezca por el hecho de que la existencia de las cámaras sea apreciable a simple vista.

Discrepancia.- En esta sentencia, no hubo unanimidad, formula voto particular el Magistrado López García de la Serrana, quien estima que sí debía haberse casado y anulado la sentencia recurrida, pues argumenta que se ha violado por la mayoría el principio de tutela judicial efectiva que establece el artículo 24 de la Constitución porque se niega la revisión fáctica pretendida porque entiende que las fotos extraídas del video y la grabación videográfica son medios probatorios que no tienen valor de prueba documental y no son aptos, por ende, para la revisión fáctica interesada en el recurso de suplicación, cuando sí lo son. Vulneración de la doctrina del Tribunal Constitucional sobre la videovigilancia como prueba ilícita por violación del derecho a la intimidad al entender que no hay infracción alguna y que la doctrina es conforme a la emanada en la STC 186/2000 e inexistencia del derecho a la protección de datos pues ni tan siquiera fue alegado por la representación de la trabajadora.

Valoración.- Cierto sector de la doctrina al analizar esta sentencia critica que se haya dado un mayor peso que siguiendo la doctrina marcada por la STC 29/2013 de 11 de febrero, se haya otorgado mayor protección al derecho a la autodeterminación informativa que al derecho a la intimidad, pues una interpretación extensiva de este derecho, nos podría llevar a dejar vacío de contenido el art. 20.3 ET, posicionándose con la postura del voto particular de la STC 29/2013 de 11 de febrero del magistrado Ollero Terasa, que manifiesta que no ha de dejar a un lado el principio de proporcionalidad en relación con el art.18.1 CE[868] , posiciones que dieron posteriormente lugar a la doctrina constitucional actual contenida en la STC 39/2016, de 3 de marzo[869].

b) Tarjeta de fidelización en gasolinera (STS de 4 de mayo de 2015[870])

El caso.- El TS estima el recurso de casación para la unificación de doctrina interpuesto por la empresa, dictada por el TSJ de Castilla y León, que declara nula

[868] SANTANA BELTRÁN, S.: «A vueltas sobre el impacto en las relaciones laborales de la última doctrina constitucional acerca del derecho a la protección de datos ex. Art. 18.4 CE STSJ País Vasco 18 de Junio 2013», *op. cit.*, pág. 343.

[869] STC 39/2016, de 3 marzo (RTC 2016\39).

[870] STS de 4 mayo 2015 (JUR 2015\146308).

parcialmente por incongruencia omisiva y devuelve las actuaciones a la Sala de lo Social de origen para que resuelva, en los términos expuestos, el recurso de suplicación interpuesto.

Los hechos.- 1º) Fruto de un control rutinario en la empresa se observó un excesivo uso de dos tarjetas de fidelización expedidas a favor de un ayuntamiento de un pueblo, que no iban asignados a una matrícula concreta sino que eran para uso de toda la flota del citado consistorio municipal. Ello hizo surgir sospechas de una posible indebida aplicación de descuentos por parte de alguno de los trabajadores de la gasolinera, por lo que la empresa decide colocar tres cámaras ocultas. **2º)** Del visionado de las grabaciones se reveló que un trabajador de la gasolinera en connivencia con un empleado del ayuntamiento estaba aplicando para sí mismo y para otros clientes la tarjeta de fidelización del referido ayuntamiento en un total de 14 veces en cuatro meses. Por tales hechos, se despide disciplinariamente al empleado de la gasolinera. **3º)** El trabajador despedido procedió a impugnar su despido y en la instancia se declaró la nulidad de la prueba de la cámara oculta, y lo mismo sucedió en la segunda instancia.

El procedimiento.- La Sala de lo Social del Supremo, por el contrario, casó la sentencia de la Sala de lo Social de Valladolid que confirmaba la nulidad de la prueba videográfica oculta en la que se fundaba el despido efectuado a un empleado de una gasolinera por no haber informado previamente de la colocación de cámaras al trabajador. Como vemos, se produce una confusión al aplicar la doctrina sobre cámaras fijas que deriva de la STC 29/2013, en lugar de la cámaras *ad hoc* (doctrina de la STC 186/2000).

El recurso de casación.- La empresa, en su recurso de casación de unificación de doctrina, con todos los argumentos a su favor, en la segunda instancia discutió sobre inexistencia de nulidad de la prueba, pues se había aplicado una doctrina errónea, extremo que no fue contestado por la Sala de Valladolid, por lo que se casa para que dicte una nueva y se pronuncie sobre la cuestión que se planteó vía recurso de suplicación.

La nueva sentencia de suplicación.- Como consecuencia se dicta la STSJ de Castilla y León de 1 de octubre de 2015[871], que finalmente estimó el recurso de suplicación planteado por la empresa considerando que no resulta de aplicación al caso de autos la doctrina constitucional manejada por el juzgador, construida en la STC

[871] STSJ Castilla y León de 1 octubre 2015 (JUR 2015\240978).

29/2013 de 11 de febrero, sino frente a otro bien distinto en el que el mecanismo captador de imagen fue posicionado con la única finalidad de constatar la realidad de los hechos infractores que se presumía que cometía el actor:

"En conclusión, bajo el abrigo de la doctrina constitucional expuesta, entendemos que, habiendo detectado la compañía la presencia de irregularidades en el uso de la tarjeta profesional "Cepsa Star" titularidad del Ayuntamiento de Boecillo; empleó aquélla un sistema idóneo para la constatación de los hechos así como de su autoría; sin que con ello se menoscabara derecho fundamental alguno del trabajador; no cabiendo admitir que hubo previamente de comunicar al mismo el posicionamiento de dichos sistemas de filmación, pues es notorio que con ello se hubiera frustrado la efectividad de los aquéllos" (FJ 1º).

Por tanto, el recurso se estima declarando la procedencia del despido operado, pues el trabajador quebrantó el deber de buena fe mediante su obrar engañoso y doloso, pues consciente de la irregularidad de su proceder atribuyó puntos de fidelización a usuarios dispares a los legítimos acreedores de los mismos, con el consiguiente perjuicio para estos en la obtención de las oportunas ventajas derivadas del suministro en los puestos de servicios de gasolineras, siendo irrelevante a efectos de calificación de la actuación, la envergadura económica de dicho obrar.

c) Supermercado DIA (STS de 7 de julio de 2016[872])

El caso.- En ella el TS estima el recurso de casación para la unificación de doctrina de la empresa y declara válida la prueba videográfica que en segunda instancia se declaró nula y devuelve las actuaciones al TSJ de origen para que dicte sentencia sobre el fondo, teniendo en cuenta la prueba.

Los hechos.- Al haberse constatado en dicho centro un alto nivel de pérdidas desconocidas, más de 32.000 euros en el año 2012, la empresa había instalado varias cámaras de vídeo-vigilancia en las zonas de trabajo. La zona se hallaba provista de cámaras que también se hallan instaladas en otras zonas a excepción de aseos, vestuarios y oficina. Dicha instalación era conocida por el personal. Había carteles que advertían de la existencia de tal sistema de videovigilancia.

Una trabajadora que prestaba servicios como auxiliar de caja para los supermercados DIA, S.A. a jornada parcial, fue despedida por acceder un día a la zona

872 STS de 7 julio de 2016 (RJ 2016\4434).

denominada "reserva" que estaba destinada a almacenar. En base a dicha prueba se comprueba que consumió mercancía del supermercado (en concreto dos paquetes de lomo loncheado) y por ello es despedida. Se comprobó así mismo que otra empleada con la categoría de cajera se apropió de productos para su autoconsumo y fue también despedida.

El procedimiento.- La trabajadora interpuso demanda de despido que fue considerado procedente en la instancia considerando la prueba de videovigilancia aportada por la empresa. La empleada disconforme, recurrió ante el TSJ de Extremadura. En suplicación se declara la nulidad del despido, valorando la nulidad de la mencionada prueba que se entendía vulneradora del derecho a la intimidad de la trabajadora con base fundamentalmente en pronunciamientos del TC, sobre todo la STC 29/2013, de 11 de febrero[873] y del TS, la STS de 13 de mayo de 2014.

Se consideró, por un lado, que para la validez de este tipo de prueba no es suficiente que existieran distintivos anunciando la instalación de cámaras en un recinto universitario, ni que se hubiera notificado la creación del fichero a la AEPD, pues era necesario además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Por otro lado, se declaró la ilicitud de la prueba de videovigilancia pues la empresa reconoce que las cámaras se instalan sólo para evitar robos de terceros y por parte de los trabajadores no se conocía cuales cámaras estaban en funcionamiento. Aplicando esa doctrina al caso concreto, se consideró ilícita la prueba obtenida por las cámaras que habían sido instaladas en la zona de almacén.

Recurso de casación.- La empresa interpuso recurso de casación para unificación de doctrina admitiéndose la contradicción con la sentencia de contraste la STSJ de Cataluña de 1 de julio de 2013[874]. Esta sentencia rechazaba la aplicación de la doctrina constitucional mencionada alegando que no se trataba de cámaras instaladas de modo genérico, sino que por el lugar de ubicación de la cámara se mostraba claramente el objetivo empresarial y se conocía plenamente su existencia por los trabajadores afectados.

---

[873] STC 29/2013, de 11 febrero (RTC 2013\29).

[874] STSJ Cataluña de 1 julio de 2013 (AS 2013\2885). En la sentencia de comparación la trabajadora es despedida por retener el dinero cobrado a los clientes en la barra del aeropuerto dos días sin registrar los productos en el TPV ni entregar ticket, simulando utilizar el TPV. Sobre la caja operaba una cámara específicamente situada con el propósito de vigilar la actividad en la caja registradora o TPV, hecho perfectamente conocido por los empleados.

Criterio del TS.- El Tribunal Supremo considera la prueba videográfica lícita, casa y anula la sentencia de suplicación, con devolución del proceso a la Sala del TSJ de Extremadura para esta que resuelva sobre el fondo.

Invocación del caso Bershka.- La sentencia trae a colación la doctrina constitucional de la STC núm. 39/2016, de 3 de marzo[875] para aplicarla al supuesto que se está enjuiciando y se afirma que *de conformidad con la doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad"* (FJ 2º)[876]. Aquí se cumplían los tres requisitos, para considerar superado el canon de proporcionalidad de la videovigilancia:

- Si tal medida era susceptible de conseguir el objetivo propuesto (juicio de idoneidad). A lo que se respondió afirmativamente: "*En la empresa con motivo de unas pérdidas anormales en comparación con otros ejercicios, se había creado una situación de desconfianza generalizada, de manera que la colocación de las cámaras en las zonas conflictivas del lugar de trabajo se trata de una reacción empresarial a sospechas de posibles irregularidades"* (FJ 2º).
- Si, además, era necesaria, en el sentido de que no existiera otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad). También se consideró concurrente, pues: *"no se ha mostrado otra medida más idónea para averiguar el origen de las pérdidas"* (FJ 2º).
- Finalmente, si la misma era ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto), razonó la Sala que se ha encontrado ninguna medida " *más moderada en la consecución de tal propósito al contrario de lo que sucedería con otras medidas tales como llevar a cabo controles aleatorios que acarrearían molestias innecesarias a trabajadores sin responsabilidad alguna en los hechos que dieron lugar a la adopción de la medida"* (FJ 2º).

Información previa.- Respecto a la información previa a los trabajadores constaba en los hechos probados que los trabajadores conocían sobre la existencia de las cámaras y a partir de ahí sigue con el razonamiento de conjetura[877] en conjetura[878],

---

[875] STC 39/2016, de 3 marzo (RTC 2016\39).

[876] Aspecto del que discrepamos totalmente como ya se ha comentado *ut supra.*

[877] "*No solamente lo sabe por ser de común conocimiento para los empleados sino también por existir carteles indicadores".*

[878] "*La presencia de las cámaras en la mayor parte del centro de trabajo sugiere una finalidad protectora del patrimonio empresarial y la grabación de conductas que atenten contra esa finalidad como lo prueba que su instalación tuvo un detonante, las múltiples pérdidas últimamente sufridas lo que convierte a todas las personas que se encuentren en el recinto en sujetos de sospecha y es esa la razón de ser de las cámaras. Así, en un momento dado, permiten localizar la conducta irregular de dos trabajadoras, la demandante y la cajera principal, al menos según lo noticiado en estos autos".*

llegando a encontrarse afirmaciones tales como: *(…) Es conocedora de que en lugar en que se encuentra, zona de almacén dedicada a la compactación, no es un área de privacidad como lo son vestuarios y aseos. Semejante entorno específico excluye el factor sorpresa y muestra claramente la situación de riesgo asumido por la demandante y por cualquier otro responsable de conductas análogas"* (FJ 2º). ¿Se vuelve al criterio centrado en la consideración del tiempo y del lugar del trabajo como un ámbito en principio ajeno a la intimidad? Al menos lo parece, con este argumento el TS, impresiona estar retomando el criterio locativo de la jurisprudencia constitucional de los años 80 y 90 del siglo pasado.

Conclusión.- En definitiva, el TS considera que se está ante un supuesto de uso apropiado de la videovigilancia implantada y que la consecución de su objetivo se ha ajustado a las exigencias razonables de respeto a la intimidad de la persona al tiempo que no le crean una situación de indefensión. Los actos por lo que se sanciona a la trabajadora, tienen lugar en un marco de *riesgo asumido que excluye el factor sorpresa*, está en una zona de trabajo, no se encuentra los aseos o los vestuarios y la existencia de la videovigilancia y su finalidad, es conocida por los trabajadores; combatir las actividades generadoras de pérdidas, por lo que todo es ajustado al principio de proporcionalidad.

Valoración.- En definitiva, un razonamiento equivocado, con el que estamos en total desacuerdo, que supone un retroceso y recorte para los derechos fundamentales, una posición que va más allá, incluso que de la doctrina de la STC 39/2016, de 3 de marzo[879], en cuanto parece optar por un criterio locativo. Si al menos se hubiera fundado la sentencia en la doctrina de la videovigilancia oculta de la STC 186/2000, de 10 de julio[880], hubiera alcanzado una argumentación más coherente.

d) Doctrina del Pleno (I: STS de 31 de enero de 2017[881])

El caso.- Ahora el TS resuelve en Pleno sobre la validez de la prueba de la videovigilancia empleada para estimar el amparo de una empresa y justificar el despido de un trabajador como procedente, casando y revocando la sentencia dictada en su día por la Sala de Cataluña del TSJ y haciendo suya la doctrina analizada en la STC 39/2016, de 3 de marzo[882] , considerando válida la obtención la prueba videográfica, que rebaja

[879] STC 39/2016, de 3 marzo (RTC 2016\39).
[880] STC 186/2000, de 10 de julio (RTC 2000\186).
[881] STS de 31 enero de 2017 (EDJ 2017/11131).
[882] STC 39/2016 de 3 marzo (RTC 2016\39).

las exigencias informativas que debe facilitar la empresa al trabajador cuando instala un sistema de videovigilancia, respecto a la doctrina constitucional anterior .

Los hechos.- La empresa contaba con un sistema de videovigilancia por razones de seguridad, no tratándose de una instalación oculta, ya que era conocida por los trabajadores, aunque no se les hubiese informado expresamente de la finalidad de control de la actividad laboral.

Un trabajador con la categoría de dependiente y con una antigüedad considerable en la empresa, desde 1994, es despedido por transgresión de la buena fe contractual, fraude, deslealtad y abuso de confianza, mediante la manipulación de tickets y hurto de diferentes cantidades, en cuatro días distintos. De tales hechos tuvo conocimiento la empresa a través un sistema de videovigilancia del que era conocedor el trabajador, pero sin que se le hubiera informado del uso con finalidad disciplinaria de tales imágenes. Precisamente por esta falta de conocimiento de la finalidad sancionadora de la videovigilancia tanto la primera como la segunda instancia, declaran el despido improcedente, por no tener en cuenta esa prueba por su nulidad.

Test de proporcionalidad.- El TS recuerda que las facultades organizativas empresariales se encuentran limitadas por los derechos fundamentales del trabajador, quedando obligado el empleador a respetarlos y que la constitucionalidad de cualquier medida restrictiva de los mismos queda determinada por la estricta observancia del principio de proporcionalidad. Para comprobar que así sucede necesario enjuiciar la medida con arreglo al principio de proporcionalidad, y se considera que :

- Supera el juicio de idoneidad, por que la medida sea apropiada para conseguir el objetivo propuesto.
- Es acorde al juicio de necesidad, o sea, que no exista otra medida más moderada para la consecución del objetivo con igual eficacia.
- Supera, asimismo, el juicio de proporcionalidad, es decir, que se deriven de ella más beneficios para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Conclusión.- El uso de la videocámara reviste, en estos casos, carácter razonable y proporcionado a su objeto sin que por el lugar de su instalación exista riesgo para la vulneración del derecho al honor, a la intimidad personal y familiar ni por las circunstancias de tiempo y oportunidad lo haya tampoco para el pleno ejercicio de sus derechos al haber actuado el trabajador como lo ha hecho, siendo conocedor de que su conducta estaba siendo grabada.

Por otra parte, se excluye la indefensión que pudiera derivar de la afectación sorpresiva del trabajador, dado que existía constancia de las conductas irregulares y público conocimiento de la colocación de las cámaras.

e) Doctrina del Pleno (II: STS de 1 de febrero de 2017[883]).

Se trata del despido de otro trabajadores de la empresa del supuesto anterior, por idénticos motivos, y con aportación de la prueba obtenida mediante la grabación por las cámaras de videovigilancia de las irregularidades cometidas por el trabajador, constando en los hechos probados de ambas sentencias que el centro de trabajo contaba con un sistema de videovigilancia "*por razones de seguridad*" y que los actores era conocedores de la existencia del sistema pero "*sin que haya sido informado del destino que puede darse a las imágenes o que pudieran ser utilizadas en su contra*". Por lo que por no reiterar, no remitimos a lo manifestado *ut supra*.

f) Acceso al gimnasio (STS de 2 de febrero de 2017[884])

El caso.- El TS resuelve el recurso de casación unificación doctrina de una empresa, titular de una cadena de gimnasios en Cataluña, en sentido estimatorio, casando y revocando la sentencia dictada en su día por la Sala de Cataluña del TSJ.

Los hechos.- La instalación de las cámaras era conocida por todos los trabajadores, estaban instaladas en la entrada y en los espacios públicos del gimnasio, disponían de autorización de la Agencia de Protección de Datos. La autorización no contemplaba el uso con fines de control de horario laboral ni la utilización disciplinaria con los trabajadores, los cuales no habían sido advertidos explícitamente de esta posibilidad. Los hechos transcurren del siguiente modo: se despide disciplinariamente al director técnico que, mediante la manipulación del torno de entrada con su pulsera de acceso, facilitaba la entrada gratuita y sin registro a miembros de otros clubs deportivos,

[883] STS de 1 de febrero de 2017 (Id Cendoj ECLI: ES:TS:2017:811).

[884] STS de 2 de febrero de 2017 (EDJ 2017/11297).

tal imputación se comprobó a través de la prueba de la videovigilancia permanente que existía en el centro en el que venía prestando sus servicios.

Esa misma conducta ya había sido objeto de sanción años atrás a otro director técnico, de lo que había sido testigo el trabajador despedido en un juicio contra la empresa[885]. Existían quejas previas del trabajador despedido por parte de compañeros de trabajo acerca de otras conductas o irregularidades de las que tenía constancia la empresa.

Para el TS es relevante que: 1) Que el trabajador despedido no fuera "*un empleado de base"* sino "*Director técnico*". 2) Los trabajadores sabían que existían cámaras que les grababan. 3) Hubo con anterioridad otro proceso de despido por los mismos hechos y con semejante prueba videográfica; juicio al que el trabajador acudió en calidad de testigo de la empresa. Lo que lleva a la Sala a concluir que estas causas "*excluyen la afectación sorpresiva del trabajador, la indefensión que de ella pudiera derivar, posibles razones que hayan llevado a establecer en la sentencia el rechazo de la prueba videográfica, en el uso de la informática*".

Test de proporcionalidad.- Se somete la medida al juicio del triple test principios de necesidad, proporcionalidad e idoneidad de la medida, que se entiende que han respetado, por lo que la prueba videográfica no tenida en cuenta ni en la instancia, ni en la Sala del TSJ es válida. Asimismo: 1) No concurrían los presupuestos para un control mediante vigilancia oculta pues tal medida, afectaría a quienes nunca había participado en las conductas bajo sospecha. 2) La existencia de las cámaras era un hecho público y notorio, el público conocimiento de la colocación de cámaras aleja la idea de adopción sorpresiva de la conducta y del mantenimiento de una actitud tolerante de la empresa. 3) En cuanto al caso concreto del demandante, las quejas emitidas por sus compañeros le hacían acreedor a una mayor atención respecto del conjunto de sus deberes como trabajador de suerte que en lo que a su actitud personal concierne la proyección disciplinaria del medio empleado para la averiguación de sus infracciones no puede considerarse un exceso de las facultades que a su empleador confiere el artículo 5 c) del Estatuto de los Trabajadores.

---

[885] "Había asistido como testigo en 2012 a la entrega de la carta de despido a otro trabajador por una conducta análoga a la suya en relación al uso indebido del torniquete de entrada, lo que unido a la visible colocación de una de las cámaras sobre el torniquete de acceso crea una situación parangonable con la de los trabajadores en la sentencia de contraste".

M) Incidencia de la doctrina constitucional en la doctrina judicial

La SSTC 39/2016 y 29/2013 han tenido una importante repercusión en los diversos TSJ, por lo que cabe marcar un antes y un después de ellas. Antes de la STC 29/2013 el TC hasta entonces había establecido los principios en esta materia sobre la base de la colisión de las facultades de control con el derecho a la intimidad de los trabajadores, sin ninguna referencia al derecho de autodeterminación informativa que consagra el art.18.4 CE, por lo que no hay reflejo de tal doctrina en los diferentes tribunales de justicia. Tras la STC 29/2013, de 11 de febrero, sí que se atiende específicamente a las exigencias derivadas del respeto al contenido esencial del derecho en materia de protección de los datos de carácter personal. No obstante, la doctrina establecida en el TC 29/2013 obtuvo una recepción matizada:

- Así, ciertamente, en aplicación de esta Sentencia, los órganos judiciales vinieron declarando el carácter lesivo del derecho a la protección de datos cuando se trata de grabaciones del lugar de trabajo que se utilizan como medida de control de la prestación laboral sin haber informado previamente a los trabajadores de este fin.
- Ahora bien, también algunos pronunciamientos diferenciaron los supuestos en que la videovigilancia se instala, no como medida permanente y preventiva, sino con carácter puntual ante la existencia de previas y fundadas sospechas de irregularidades en el trabajo, no apreciándose que en tal caso la ausencia de comunicación previa al trabajador comportara necesariamente vulneración del art. 18.4 CE y aplicando, por el contrario, el juicio de proporcionalidad como criterio de solución en base a la doctrina de la STC 186/2000 por el marcado carácter oculto de la videovigilancia[886]

Desde nuestro punto de vista, habría que diferenciar, como razona el MF en la oposición al amparo del recurso que dio origen a la STC 39/2016, dos supuestos que parecían estar delimitados antes de la irrupción de esta sentencia:

- *Cámaras ocultas*. Como sabemos, es el supuesto que resuelve la STC 186/2000, de 10 de julio[887]. Se trata de la instalación ocasional y temporal de una cámara de grabación en el puesto de trabajo tras acreditadas sospechas razonables de incumplimientos contractuales que fueron probados de esta manera, es una grabación episódica y breve de una cámara que no es permanente. El canon de enjuiciamiento para medir el

[886] GARCÍA RUBIO, M.A.: «Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales», *Revista de Jurisprudencia El Derecho*, núm. 2, 2016 (EDB 2016/53076).
[887] STC 186/2000, de 10 de julio (RTC 2000\186).

mecanismo de control es el principio de proporcionalidad, basándose en la técnica del triple test (justificación, idoneidad y necesidad). El derecho que se encuentra en posible colisión con el contenido en el 18. 1 CE. Algunas sentencias siguen este criterio y recogen la doctrina de la STC 186/2000, sirva a título de ejemplo: STSJ de Valencia de 21 de abril de 2015[888], STSJ de Andalucía de 15 de abril de 2015[889] y STSJ de Cataluña de 3 de febrero de 2015[890].

- *Cámaras fijas*. Es el caso de la STC 29/2013, que es sustancialmente distinto al anterior, lo que se enjuicia es la licitud como prueba a efectos sancionadores laborales de las imágenes obtenidas por un sistema permanente de cámaras ubicadas no en puestos de trabajo sino en lugares comunes y de paso con publicidad y comunicación a la AEPD, pero sin advertencia alguna de su posible utilización para vigilar incumplimientos laborales. La sentencia constitucional es exigente en cuanto al cumplimiento del deber de información previa para que la captación de imágenes que constituye un tratamiento de datos personales resulte respetuosa con el derecho fundamental del art. 18.4 CE; el canon de enjuiciamiento es si ha habido información suficiente o no [891].

Por tanto, en los casos de instalaciones móviles y temporales de videovigilancia no entraría en juego el debatido art. 18.4 CE, sino exclusivamente la tutela de la intimidad del primer apartado del mismo precepto. Tras la STC 39/2016, de 3 de marzo parece que ya no hay distinción conceptual entre cámaras fijas y móviles, se establece una doctrina común para la videovigilancia, la información previa con un distintivo conforme a la Instrucción 1/2006 de la Agencia Española de Protección de Datos es suficiente.

O) Tipología judicial

a) Cocinera que hurta (STSJ de Andalucía de 13 de junio de 2016[892])

Resuelve el recurso de suplicación de una trabajadora que fue despedida y en la instancia el despido fue calificado como procedente, recurre en suplicación y ve

[888] STSJ de Valencia de 21 abril de 2015 (JUR 2015\203358).
[889] STSJ de Andalucía de 15 abril de 2015 (JUR 2015\142928).
[890] STSJ de Cataluña de 3 de febrero de 2015 (AS 2015\1247).
[891] Algunos críticos afirman que resulta sorprendente que en el análisis del art. 18.4 CE y su posible vulneración se haya dejado de lado el debido juicio de proporcionalidad, *vid*. SANTANA BELTRÁN, S.: «A vueltas sobre el impacto en las relaciones laborales de la última doctrina constitucional acerca del derecho a la protección de datos *ex.* Art. 18.4 CE STSJ País Vasco 18 de Junio 2013», *Nueva Revista Española de Derecho del Trabajo* núm. 171, 2014, pág. 343.
[892] STSJ Andalucía de 13 junio de 2016 (JUR 2016\208169) .

desestimadas sus pretensiones. Los hechos son los siguientes, una trabajadora ayudante de cocina en una residencia de estudiantes es despedida por un incumplimiento de su contrato de trabajo, imputándosele apropiarse indebidamente de alimentos procedentes de suministros efectuados para la alimentación de alumnos y empleados en los horarios de comidas. La prueba en la que los hechos se basan se consigue a través de videovigilancia oculta instalada por un detective privado.

Hechos.- La empresa tras haber puesto en marcha un control de acceso al servicio de comedor detectó irregularidades en la información de gestión que hasta este momento se le estaba facilitando: había una diferencia muy grande entre el gasto de comida y el número de comensales. Se procede a instalar tres cámaras ocultas, dos en el almacén y una en un pasillo junto a la cocina y se comprueba que una empleada, sin contar con autorización está sustrayendo comida por lo que es despedida disciplinariamente.

La trabajadora impugna el despido que es desestimado en la instancia y recurre en suplicación. Los motivos de recurso son tres dos revisiones de hechos probados de la sentencia que son desestimados y dos motivos de recurso por vulneración del Derecho aplicado, el motivo objeto de análisis, por su interés con la materia que nos ocupa, es el de violación del art. 18.4 CE de la Sala parece que parte de un error conceptual respecto al derecho a la autodeterminación informativa, pues lo primero que se afirma es que se duda de su carácter autónomo[893]. Por otro lado, somete el art. 18. 4 CE al juicio de proporcionalidad, siguiendo la estela de la STC 39/2016, de 3 de marzo[894]:

[893] "El art.18.4 CE dice sólo que la ley limitará el "uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", por lo que el mero incumplimiento de la legislación sobre protección de datos no debe justificar un reproche de infracción de un derecho fundamental. En las relaciones entre particulares, al menos, es necesario que, a través del incumplimiento de las normas sobre protección de datos se hubiera afectado a la intimidad personal o familiar o al ejercicio de algún otro derecho fundamental del particular por la conducta del otro particular para negar validez en nuestro caso a la grabación videográfica como prueba del incumplimiento contractual del trabajador. Aun en el supuesto que se considerase que el art. 18.4 CE configura un derecho a la protección de datos autónomo, entendemos que la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. La constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad"(FJ 3º).

[894] STC 39/2016, de 3 marzo (RTC 2016\39).

Idoneidad.- El primer subprincipio de idoneidad no supera la adecuación desde nuestro punto de vista, aunque la Sala de Andalucía opina de manera contraria; la medida es arbitraria, de los hechos declarados probados se recoge que había sospechas de irregularidades de algún empleado porque había una diferencia muy grande entre el gasto de comida y el número de comensales, pero no hay ningún dato que sostenga tales afirmaciones, por lo que la intervención en los derechos fundamentales no es adecuada a contribuir a la obtención de un fin constitucionalmente legítimo. La Sala considera lo contrario y razona: *"En el caso concreto de autos existían indicios, que ya no solo sospechas, de que alguno de los trabajadores se estaba apropiando de víveres, por lo que la medida de instalar unas cámaras enfocando a las dos salidas y entrada trasera del edificio y en la despensa, como en el pasillo de acceso a las dependencias del despacho del Jefe de Cocina y en el pasillo del vestuario - sin alcanzar a la puerta de acceso- y en el exterior del recinto de la cocina resulta justificada pues se pretendía verificar quien cometía tales irregularidades, si era algún trabajador, y adoptar medidas disciplinarias en ese caso, por lo que la medida es idónea para dicha finalidad".* (FJ 3º).

No hay ningún dato objetivo que pruebe la desproporción entre el número de comensales y la cantidad de comida sustraída, a menos que la trabajadora despedida se dedicara al *estraperlo* de lo detraído, en caso contrario, imputar tales irregularidades tan solo a ella no resulta coherente. Pese a ello la Sala repite en su argumentación la siguiente afirmación: *"La empresa adoptó la medida cuestionada no sobre sospechas sino sobre indicios que había en curso un fraude"* (FJ 3º). Se afirma pero no se explica en qué consisten esos "indicios", que se insiste que varias veces en que no son sospechas. Si acudimos a la definición de la RAE, por *indicio* se entiende "fenómeno que permite conocer o inferir la existencia de otro no percibido" y *sospecha* significa "acción y efecto de sospechar" y este verbo a su vez "imaginar algo por conjeturas fundadas en apariencias o indicios". Por tanto, la expresión es del todo desafortunada, los indicios llevan a sospechar, no al revés.

Necesidad.- El segundo subprincipio de necesidad, implica la comparación entre la medida adoptada por la empresa y otros medios alternativos que se pudieran haber escogido. La Sala simplemente afirma que "la grabación servía de prueba de tales irregularidades, por lo que la medida resulta necesaria" (FJ 3º), sin mayores razonamientos.

Proporcionalidad.- Conforme al tercer y último subprincipio de proporcionalidad en sentido estricto, (la Sala insiste en este punto en el carácter oculto de la prueba videográfica para comparar el supuesto con el de la STC 186/2000, de 10 de

julio[895]) parece equilibrada ya que con arreglo a la referida sentencia, concurría la situación precisa para el control oculto, esto es sin notificar expresamente la colocación de la cámara a los trabajadores, porque era, en principio, el único medio posible dicho control para satisfacer el interés empresarial de saber fehacientemente quién estaba realizando los actos defraudatorios de los que indiciariamente ya se tenían conocimientos. La empresa adoptó la medida cuestionada no sobre sospechas sino sobre indicios que había en curso un fraude.

Razonamiento adicional.- A igual conclusión afirma la Sala se habría llegado en el supuesto de aplicar la doctrina de la STC 39/2016, de 3 de marzo[896]. Ahí se nos dice que una de las excepciones contempladas en la ley a la necesidad del consentimiento en el tratamiento de datos de carácter personal son los datos que se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento (art. 6 LOPD). Por ello, un tratamiento de datos cuya finalidad es el control de la relación laboral debe entenderse amparado por esta excepción, pues está dirigido al cumplimiento de la misma. El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato.

Consentimiento.- Recordemos, como hemos tenido ocasión de comentar, el consentimiento del trabajador no era necesario pues la existencia del contrato de trabajo excluía el principio general de necesidad de consentimiento, por lo que era una excepción a la regla general. En el análisis de la STC 39/2016, de 3 de marzo[897] ya se argumentó que a nuestro juicio de esta parte parecía que la sentencia confundía el término información previa con el concepto de consentimiento otro tanto de lo mismo ocurre aquí pues se reitera el argumento de la mencionada sentencia constitucional, a todas luces, erróneo.

[895] STC 186/2000, de 10 de julio (RTC 2000\186).
[896] STC 39/2016, de 3 marzo (RTC 2016\39).
[897] STC 39/2016, de 3 marzo (RTC 2016\39).

b) Acosador laboral (STSJ de País Vasco de 3 de mayo de 2016[898])

El caso.- El TSJ vasco declara que la instalación de cámaras de vídeo-vigilancia dirigidas a la mesa del trabajador denunciante de acoso, sin haber comunicado su instalación ni estar señalizadas, constituye una prueba válida. La videovigilancia oculta tenía el objetivo de descubrir la veracidad de los hechos denunciados y asimismo encontrar a la persona que acosaba al trabajador, por lo que dicha medida cumple los requisitos del juicio de proporcionalidad de ser justificada, idónea para la finalidad pretendida, necesaria y equilibrada.

Los hechos.- Como consecuencia de diversos hechos de los que tuvo conocimiento la empresa, que podían constituir acoso en el trabajo y que acaecieron en un concreto puesto de trabajo que ocupaba un determinado empleado supuesta víctima de hostigamiento, se procedió a la colocación de dos cámaras para tratar de detectar posibles hechos anómalos. Estas dos cámaras se instalaron única y exclusivamente hacia el puesto de trabajo del trabajador acosado.

El visionado de la cámara oculta desprende que de madrugada entre la una y las cuatro de la madrugada, otro trabajador de la empresa accede al puesto de trabajo del empleado hostigado, leyendo documentos del puesto de trabajo ajeno e incluso sustrayendo diversa documentación. El trabajador que accede al puesto del otro empleado no tiene ningún cometido en su trabajo relacionado con ese puesto. Ante tal actitud, se sanciona al trabajador que cometió la falta con una suspensión de empleo y sueldo de un mes.

El procedimiento.- El trabajador en la instancia, pretendía que se declarara la nulidad de la prueba pero vio desestimada su demanda, y se confirmó la suspensión. En vía de suplicación el trabajador interpone dos motivos instando la modificación de los hechos declarados probados, que son desestimados y por ultimo interesa la revisión del Derecho aplicado instando la nulidad de la prueba por vulneración del art. 18.4 CE y en consecuencia la improcedencia de la sanción.

Doctrina.- En primer lugar el TSJ alude al difícil equilibrio entre los límites del derecho a la intimidad de los trabajadores y el poder de dirección empresarial, sobre todo

[898] STSJ País Vasco de 3 mayo de 2016 (AS 2016\1328).

en el ámbito de las nuevas tecnologías, y en concreto en las pruebas de video-vigilancia para control de los trabajadores exigen que la lectura del art. 20.3 de ET. Se considera que la instalación de cámaras no obedeció al propósito de vigilar y controlar genéricamente el cumplimiento por los trabajadores de sus obligaciones (a diferencia del caso resuelto en STC 98/2000), sino que, como previamente se habían advertido irregularidades en el comportamiento de los cajeros en determinada sección del economato y un acusado descuadre contable, se adoptó la medida de vigilancia de modo que las cámaras únicamente grabaran el ámbito físico estrictamente imprescindible (las cajas registradoras y la zona del mostrador de paso de las mercancías más próxima a los cajeros), respetándose, en definitiva, el principio de proporcionalidad.

Y trayendo a colación la doctrina de la STC 39/2016, afirma "*es esta postrerísima decisión constitucional la que tiene que compaginar esta Sala (…) Es por ello que en el supuesto de autos las grabaciones efectuadas por la empresarial en el espacio físico y temporal que se reseña por la instancia (cámaras que apuntan a determinadas mesas de trabajo del hostigado y del responsable), devienen per se adecuadas para comprobar la realidad de unas conductas sospechosas respecto de unos indicios, exigencia de control de un situación de acoso respecto de un trabajador que se trata de corregir y disciplinar en advertencias y comportamientos no negados, sobreentendidos en función de las informaciones facilitadas por la empresarial al conjunto de la plantilla, ante la comprobación de las irregularidades y con el objetivo de determinar una aplicación severa en el ámbito disciplinario, respecto de esas situaciones irregulares (conductas referidas al hostigamiento ya narradas), que hacen que entendamos que los motivos razonables y el panorama indiciario se basen en comportamientos detectados que quedan acreditados por la sospecha y concuerdan con la exigencia de un control empresarial de la forma particular y acotada en la grabación de tiempo y espacio presentadas*" (FJ 4º) .

Conclusión.- Con lo que concluye, que considera que resulta patente que la medida de videovigilancia no supone una ideación de control generalizado, global e indiscriminado, sino que se justifica en la previa sospecha y en su realidad confirmada y constatada con posterioridad, que no es premisa pero si conclusión del argumento, que por ello verifica la justificación de la medida, la idoneidad de su finalidad, la de necesidad de su exigencia y el equilibrio físico y temporal, que descartan cualquier lesión de derechos fundamentales propios del art. 18 CE.

En definitiva, se trata de una buena construcción argumental de la Sala del TSJ del País Vasco, basándose realmente más en la fundamentación de la STC 186/2000 que en los de la STC 39/2016, aunque, obviamente, no se recoge de esta manera expresa.

c) Encargado sustractor (STSJ Asturias de 22 de enero de 2016[899])

El caso.- La sentencia resuelve el recurso de la empresa, la parte recurrida era un trabajador encargado de una tienda de perfumes, bajo cuyo mando prestaban servicios varias trabajadoras, que comunicaron a la empresa recurrente la comisión por parte de aquél de irregularidades en el desempeño de sus funciones.

Los hechos.- Para investigarlo, la empresa entre otras medidas decidió instalar cámaras de videovigilancia. El centro de trabajo tenía una distribución espacial interna que separaba la parte destinada a la exposición y venta al público de la zona reservada al personal, denominada por la empresa "*backoffice*", formada por un pasillo y al final un reducido espacio destinado a oficina donde está instalada la caja fuerte que solo manejaba el trabajador despedido.

La empresa colocó un sistema cerrado de televisión y grabación para la vigilancia del "*backoffice*", cuya instalación comunicó previamente al comité de empresa poniéndole de manifiesto que tenía por finalidad investigar la actuación del presunto culpable. La demandada también instaló cámaras de vídeo en el espacio de exposición y venta al público, informando al comité de empresa antes de su instalación, en comunicación independiente de la relativa al "*backoffice*", que era una medida incardinada "*dentro de un proceso general que se está aplicando en la compañía y por el cual se está procediendo a instalar este tipo de sistemas de control y seguimiento del trabajo*".

El demandante fue el único trabajador de la tienda ignorante de la colocación de ambos sistemas de videovigilancia, los cuales junto con la colaboración de un detective privado fueron utilizados para observar y dejar constancia de las actuaciones imputadas en la carta de despido. En concreto, "*la grabación de la zona de tienda permitió a la empresa atribuir al trabajador la ficción de dos devoluciones de producto*s", al captar actos integrantes de una operación ejecutada por el demandante para vender productos no destinados a la venta y mediante devoluciones simuladas quedarse con el dinero obtenido; y la grabación conseguida con sistema de videovigilancia de la zona reservada se utilizó

[899] STSJ de Asturias de 22 enero de 2016 (JUR 2016\35391).

por la empresa como medio para probar la apropiación por aquél de la cantidad de 216 euros. Esta imputación, sin embargo, la Juzgadora de Instancia no consideró acreditada por fundarse en una prueba videográfica declarada nula por los motivos que a continuación pasamos a exponer.

Sentencia del Juzgado.- En el análisis de los sistemas de videovigilancia dispuestos por la demandada, la sentencia del Juzgado aprecia "*que solo las cámaras instaladas en el backoffice se sustraía (sic) formal y singularmente al conocimiento del demandante, porque tenía por objeto la vigilancia estricta de su modo de actuar*". Las restantes cámaras respondían a una medida general e indiscriminada para el control y seguimiento del trabajo que afectaba a toda la plantilla, ante lo cual no estaba justificado que el trabajador despedido ignorara su existencia y función a diferencia del personal restante. Sin embargo, la instalación y utilización del circuito cerrado de televisión en el *backoffice* sin conocimiento del demandante constituyó una medida justificada, idónea, necesaria y equilibrada, desde la perspectiva de los derechos fundamentales afectados por la decisión empresarial (arts. 18.1 y 4 de la Constitución).

Por el contrario, "el demandante no debió quedar fuera de la información del hecho de la instalación de cámaras de grabación en el interior de la zona del centro de trabajo destinada a tienda, y como quiera que se le privó de esa información a tiempo, la empresa vulneró el derecho constitucional del art. 18.1 CE, lo que supuso la nulidad del despido (...)". Se procedió a estimar la demanda que impugnaba el despido, declarándolo improcedente.

Suplicación.- La empresa procedió a recurrir en suplicación, y sostuvo que tanto la vigilancia oculta como la permanente, recogían las condiciones para que la medida fuera constitucional. Al mismo tiempo que pone en duda el desconocimiento por el demandante de la implantación del sistema de videovigilancia y de su finalidad, entendió que con la comunicación realizada a la representación de los trabajadores la empresa cumplió con los deberes informativos que cupiera exigírsele.

El debate se centra, por consiguiente, en el sistema de videovigilancia instalado en el espacio del comercio destinado a la venta, donde trabajadores y clientes realizan públicamente las transacciones comerciales propias de la actividad empresarial. Al tratarse de una zona no reservada resulta difícil considerar que la esfera privada del trabajador comprendida en su derecho a la intimidad en sentido estricto haya resultado afectada por la acción empresarial. Aunque sin atender a las circunstancias concretas de

los actos no cabe una exclusión rotunda, lo cierto es que los datos consignados en la sentencia de instancia no son reveladores de una posible afectación de ese derecho.

Doctrina.- A ello contestó la Sala de lo Social de Asturias que: "*La captación, registro y tratamiento con fines disciplinarios de imágenes por medios informáticos si incide en el derecho fundamental a la propia imagen art. 18.1 CE y arts 1, 2.1 y 3 a) LOPD y sobre todo, en el derecho fundamental a la protección de datos de carácter personal recogido en el art. 18.4. Como señala la STC 29/2013 , con cita de su sentencia 292/2000, de 30 de noviembre , este derecho fundamental "amplía la garantía constitucional a todos aquellos datos que identifiquen o permitan la identificación de la persona y que puedan servir para la confección de su perfil (ideológico, racial, sexual, económico o de cualquier otra índole) o para cualquier otra utilidad que, en determinadas circunstancias, constituya una amenaza para el individuo (...), lo cual, como es evidente, incluye también aquellos que facilitan la identidad de una persona física por medios que, a través de imágenes, permitan su representación física e identificación visual u ofrezcan una información gráfica o fotográfica sobre su identidad*" (FJ 2º).

Los hechos declarados como probados revelan que la empresa dio un tratamiento diferente a los dos sistemas de videovigilancia que colocó en el centro de trabajo. Esta diferencia se puso de manifiesto en las comunicaciones dirigidas por la empresa a la representante legal de los trabajadores. La colocación del circuito cerrado de televisión y grabación en la zona de *backoffice* fue una consecuencia de la denuncia efectuada contra el demandante y respondió exclusivamente a la finalidad de "*identificar al autor de las supuestas irregularidades con relevancia disciplinaria*". Por el contrario, el sistema instalado en el espacio compartido por trabajadores y clientes forma parte, según la demandada, "*de un proceso general que se está aplicando en la compañía y por el cual se está procediendo a instalar este tipo de sistemas de control y seguimiento del trabajo*". A tenor de esta última comunicación escrita ninguna razón hay para mantenerlo oculto y tan es así que según expresa esa "*medida general (...) ha sido comunicada a la plantilla mediante la BCP remitida a todas las tiendas en fecha 29 de octubre de 2014*".

El distinto régimen aplicado en la sentencia de instancia a uno y otro sistema de videovigilancia, criticado en el recurso, no es más que el correcto reflejo del distinto tratamiento y finalidad que les dio la empresa. Una vez hecha la diferencia y aplicada, la demandada no puede, después de ver y utilizar las imágenes grabadas para el despido disciplinario del trabajador, transformar la vigilancia de la zona común en una medida semejante al control establecido para el espacio reservado.

Decisión.- El incumplimiento por la empresa del deber informativo supuso una violación de los derechos fundamentales del demandante (art. 18.4 CE) afectados por la medida intrusiva. Y aunque la parte recurrente quisiera limitar la consecuencia de su

infracción a la validez del medio de prueba obtenido con la grabación de imágenes, la Sala considera que la nulidad del despido constituía el efecto necesario y adecuado de la actuación empresarial.

d) Cajera sustractora (STSJ de Madrid de 11 de mayo de 2015[900])

La Sala desestimó el recurso de suplicación de la empresa que estimó en la instancia la nulidad de la prueba videográfica empleada para despedir al trabajador, basándose en una infracción del art. 18. 4 CE. La Sala de lo Social de Madrid afirmó que los antecedentes de hecho son casi idénticos a los de la STS de 13 de mayo de 2014, por lo que, en consecuencia, la respuesta es también la misma:

"El caso ahora enjuiciado guarda notables similitudes con el resuelto por la transcrita sentencia del TS de 13-5-14 puesto que también se trata de grabaciones efectuadas por una cámara que permite tomar imágenes del supermercado en la zona de las cajas y en nuestro supuesto no consta en modo alguno que existiese información de la empresa a los trabajadores o a sus representantes legales de la finalidad de dichas cámaras en relación con los posibles incumplimientos laborales que se pudiesen cometer, que debía comprender, en términos de la STC 29/13 , la información previa y expresa, precisa, clara e inequívoca de la finalidad de control de la actividad laboral"(FJ 2º).

Al no haber cumplido la empresa tales exigencias se declara la nulidad de las grabaciones efectuadas y al no haber prueba del despido, se declara improcedente.

e) Dependiente de Hipermercado (STSJ de Murcia de 23 de marzo de 2015[901])

El caso.- Un trabajador con una antigüedad de más de 25 años en una conocida multinacional (CARREFOUR) es despedido disciplinariamente por unos hechos que se comprueban por existir video vigilancia en la zona en la que trabajaba, sin haber notificado la empresa la existencia de la misma a sus empleados. Se solicita la revisión del Derecho aplicado por vulneración del derecho a la autodeterminación informativa, *ex* art. 18.4 CE y la Sala de lo Social de Murcia no se pronuncia sobre tal extremo aludiendo que en la instancia, la demanda debería haberse dirigido frente al Ministerio Fiscal si se entendía vulnerado un derecho fundamental, y como no se dirigió acción frente a este, no podía haber en la segunda instancia posicionamiento sobre la pretendida vulneración.

[900] STSJ de Madrid de 11 mayo de 2015 (JUR 2015\150826).
[901] STSJ de Murcia de 23 de marzo de 2015 (QSJ 2015/48541).

Valoración.- Parece que la Sala de Murcia, confunde la posibilidad de que la prueba sea nula por vulnerar el art. 18.4 CE con una posible nulidad del despido por violación de derechos fundamentales; y al no pronunciarse la Sala de Murcia sobre un extremo del recurso planteado de manera motivada, se está produciendo una infracción del principio judicial de tutela efectiva del art. 24 CE.

f) Dependiente de textil STSJ de Madrid de 9 de febrero de 2015[902]

El caso.- La Sala de lo Social de Madrid confirma la sentencia de la instancia en la que se declaró procedente el despido del trabajador. Los antecedentes del caso son los siguientes: una empresa realiza inventario en su tienda, desprendiéndose del mismo que en una de sus secciones faltaban muchos más productos que en otras (más de 100 sobre unos 4 de los otros departamentos), por lo que se exhorta al personal de esa sección a que informe si las piezas que faltaban se encontraban en alguno de sus departamentos. No se devuelve ninguna por lo que se deciden instalar cámaras ocultas durante un mes en esa sección en la que se detectaron las anomalías, en concreto sobre unos armarios. De las grabaciones se desprende que un trabajador en dos días distintos sacó del armario un total de seis prendas (en concreto, dos chaquetas, una bandolera, un maletín y un bolso) las introdujo en bolsa de la marca y las sacó de la tienda. Se le despide por estos hechos.

El recurrente alega infracción del art. 18.4 CE y de la doctrina de la STC 29/2013, sosteniendo que el registro en la persona del trabajador sería más moderada y menos invasiva, concluyendo por aducir que no consta comunicación a la AEPD ni se ha facilitado información al demandante sobre la videovigilancia.

Doctrina.- La Sala contesta que lo correcto es aplicar la doctrina de la STC 186/2000 y que en base a esta resulta proporcionada la medida de control por lo que la prueba es válida y el despido procedente, se declara aplicable el art. 18.1 CE y se somete al principio de proporcionalidad:

"*La actuación de la empresa en este caso en cuanto medida restrictiva de un derecho fundamental, el del art. 18.4 de la Constitución, supera el juicio de proporcionalidad, pues cumple los tres requisitos o condiciones siguientes (STC 186/2000). (…) La idoneidad no es cuestionable pues la grabación demostró en el juicio la conducta del trabajador que se le atribuía en la carta de despido e hizo posible la*

[902] STSJ de Madrid de 9 febrero de 2015 (AS 2015\649).

extinción del contrato de trabajo mediante despido disciplinario procedente por haber incurrido en un comportamiento muy grave. La necesidad es negada por el recurrente aduciendo que podría haberse utilizado un registro, pero no explica por qué un registro en la persona del trabajador es menos invasivo que una grabación de imágenes, aparte de que esta medida de control es menos idónea, ya que si resulta fallido un primer registro es claro que el trabajador culpable ya queda alertado"(FJ 4º).

Como la vigilancia oculta lleva implícita por su característica esencial la ausencia de conocimiento de la misma por parte del trabajador, esta sentencia argumenta, que se ha de considerar admisible la sustitución de la información a los trabajadores por la efectuada al presidente del Comité de empresa (no al Comité pues el recurrente era miembro del mismo), razonamiento erróneo e innecesario pues es esta una cuestión de legalidad ordinaria sobre la misma que no pende la licitud de la prueba:

> *"Y en cuanto a la proporcionalidad en sentido estricto, el interés general de evitar la impunidad de conductas como la sancionada resulta superior al leve menoscabo relativo al tratamiento de datos, sobre todo teniendo en cuenta que las imágenes ni siquiera fueron tomadas por la demandada sino por una empresa del sector de vigilancia, se informó previamente al presidente del comité de empresa y no consta que hayan sido utilizadas para otra finalidad que su presentación en juicio" (FJ 4º).*

g) Consumos tolerados (STSJ de Galicia de 23 de diciembre de 2014[903])

El caso.- La Sala estima el recurso de la trabajadora que vio denegada su petición en la instancia. La conducta imputada que se dio por probada, fue consumir ocasionalmente productos destinados a la venta, pero el hecho cierto es que había una situación real de tolerancia empresarial, así como una falta de advertencia previa. Los antecedentes de hecho de esta sentencia son: se despide a una trabajadora por consumir ocasionalmente productos destinados a la venta en base a una cámara oculta que se instaló en su puesto de trabajo que era un kiosko. Se sospechaba que podía quedarse con dinero pues a la empleadora en las cuentas de los últimos meses arrastraba pérdidas y en base a este motivo es por el que se instala una cámara *ad hoc*.

La doctrina.- La trabajadora, vencida en la instancia, pretende que se declare la nulidad de la prueba videográfica en base a la doctrina de la STC 29/2013, la Sala responde que es de aplicación lo previsto en la STC 186/2000, por lo que hay que someter la medida de vigilancia oculta al principio de proporcionalidad y por tanto a la técnica del triple test :

"*verificar si esa vigilancia supera el juicio de proporcionalidad subdividido en los tres subjuicios de idoneidad, necesidad y proporcionalidad en sentido estricto. Y, a juicio de la Sala, en el caso de autos*

[903] STSJ Galicia de 23 diciembre de 2015 (AS 2014\3272).

falta la justificación de esas sospechas previas, lo cual repercute después en la no superación del triple juicio de proporcionalidad de la vigilancia videográfica" (FJ 4º).

Con toda la lógica la Sala entiende que la existencia de pérdidas en una empresa no justifica en modo alguno acudir a la prueba videográfica oculta, por lo que declara la prueba nula. Y aquí podría haber concluido la sentencia, pero va más allá y afirma: "*cobran verosimilitud las alegaciones de la recurrente de que existía una tolerancia empresarial acerca del consumo moderado de ciertos productos del kiosco de la cual aquella se pretende aprovechar para librarse de algunos trabajadores*"(FJ 5º).

Valoración.- Si la prueba que se ha anulado revelaba el consumo de productos del quiosco por la trabajadora, no se comprende que se vuelva a pronunciar sobre los citados hechos si no constan y han sido anulados, quizás la Sala en un exceso de interés por apoyar la tesis de la recurrente, enfatiza y se sumerge en un terreno innecesario.

h) Empleada de cafetería (STSJ de Madrid de 3 de junio de 2014[904])

El caso.- En ella se aplica al empleo de videovigilancia oculta la doctrina de la STC 29/2013, de 11 de febrero, de manera errónea, pues para estos supuestos hubiera correspondido aplicar la doctrina de la STC 186/2000.

Los hechos.- Una cocinera de una cafetería de un gimnasio en el que existía videovigilancia en zona de bar y en el pasillo hacia la cocina con carteles de advertencia, es sometida a un control oculto a raíz de unas supuestas sospechas por un problema en un pedido en una factura a un proveedor cuyo desfase en el precio fue asumido por este y no por su empleador. Se instalan en la cocina dos detectores de humo que no son tales sino cámaras de videovigilancia. De la grabación oculta se desprende que en diferentes días se introdujo productos de la cafetería en el bolso sin abonar el importe de los mismos por lo que es despedida de manera disciplinaria, procede a impugnar su despido que es desestimado en la instancia.

Doctrina.- La trabajadora recurre alegando nulidad de la prueba por vulneración del art. 18.1 CE, la Sala contesta afirmativamente pero entendiendo infringido el mismo artículo pero en su apartado 4, con expresa referencia a la STC 29/2013, dice: *" no consta en el relato fáctico que exista " .. información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida.*

[904] STSJ de Madrid de 3 junio de 2014 (JUR 2014\226766).

Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo" (FJ 5º).

Se confunden los requisitos exigidos para la videovigilancia genérica con los de la oculta, en los que no hay necesidad de información previa pues la finalidad de este tipo de vigilancia se desvirtuaría, pero la Sala considera lo contrario: *"Concluimos que no hay una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales, y que tampoco podría situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia"* (FJ 5º).

Valoración.- Se insiste en otros extremos que en este caso consideramos que carecen de relevancia jurídica en este supuesto, como el hecho de que no constara que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos.

Al mismo resultado se podría haber llegado, pero realizando una correcta maniobra jurídica aplicando la doctrina de la STC 98/2000 y acudiendo al principio de proporcionalidad, a la técnica del triple test, preguntándonos si la actuación de la empresa era justificada, y se respondería que no porque un problema en un pedido de un día puntual que no produjo perjuicio económico no es motivo suficiente para considerarlo una razonable sospecha, la injerencia en la esfera de la trabajadora es desmedida, se debió buscar otro mecanismo no tan intrusivo como una cámara *ad hoc* en su puesto de trabajo dados los antecedentes, por lo que la prueba videovigilancia es no proporcional y por tanto es nula, pero no por infracción del art. 18.4 CE sino del art. 18.1 CE.

i) Suplantación de personalidad (STSJ Asturias de 23 de mayo de 2014[905])

El caso.- En ella se resuelve el recurso de suplicación de la empresa CARREFOUR, contra la sentencia que en la instancia declaró la nulidad del despido disciplinario del actor, por violación del art. 18.4 CE, haciéndose eco en sus FJ 1º, 2,º y 4º de la doctrina dimanante de la STC 29/2013, como también lo hizo el Juzgado de lo Social.

[905] STSJ de Asturias de 23 de mayo de 2014 (JUR\2014\183640).

Los hechos.- Los hechos sucedieron del siguiente modo: se sanciona a un trabajador por suplantar la personalidad de otro al registrar con la tarjeta de una compañera[906] la finalización de la jornada laboral hasta en cuatro ocasiones distintas, lo que según las normas de régimen interno estaba prohibido, pues el uso se prescribía como personal e intransferible. La información vertida en la carta de despido se obtuvo de la visualización conjunta de tres cámaras de videovigilancia situadas en diferentes ubicaciones: zona de acceso a vestuarios, zona próxima a la máquina de fichaje y zona de salida y entrada de público en general. Se ha de precisar que al trabajador sancionado, no se le observa en ningún momento fichar.

El recurso y la doctrina.- Los motivos que se formulan en el recurso son tres: el primero de ellos, defiende la nulidad de la sentencia de instancia al haber considerado ilegal la prueba de grabación videográfica aportada por la empresa; tal argumento, es desestimado por la aplicación indebida de la doctrina de la STC 186/2000; ni tan siquiera el derecho fundamental en colisión es el mismo que en el supuesto que se trata en la sentencia que se usa de contraste, que es el derecho a la intimidad.

En el segundo motivo, se solicita la revisión de los hechos probados, a lo que se accede parcialmente, pues ni el relato fáctico, ni la fundamentación jurídica de la sentencia contiene, prevención alguna frente al contenido de las normas básicas de régimen interno, que informan que el control que se realiza por parte de la empresa está destinado a los clientes y a los trabajadores.

En el tercer motivo, se critica por desacertada la declaración de nulidad del despido y se argumenta a favor de la procedencia de la decisión extintiva por motivos disciplinarios, lo que se desestima. La pretensión se rechaza porque no hubo información proporcionada al trabajador que fuera específica respecto a en qué casos las grabaciones pueden ser examinadas para la imposición de sanciones disciplinarias por incumplimiento del contrato de trabajo. La información era genérica y ni tan siquiera en ella se hace referencia al sistema de videovigilancia, lo que incumple el art. 18.4 CE, pues la exigencia de información ha de ser previa, precisa e inequívoca.

[906] La compañera también es despedida, su demanda es turnada en igual Juzgado de lo Social, con el mismo resultado, y la empresa recurre en suplicación y es desestimada la pretensión por idénticos motivos. *Vid*. STSJ de Asturias de 23 de mayo de 2014 (EDJ 2014/101903).

Se procede, en consecuencia, a confirmar la resolución recurrida por la desatención de la empresa del deber informativo que le incumbía cumplir para utilizar los datos personales del recurrido.

j) Cocinero bebedor (STSJ de Valencia de 17 de diciembre de 2013[907])

El caso.- En ella desestima el recurso de suplicación interpuesto por el trabajador demandante con más de 20 años de antigüedad en la empresa, contra la sentencia que declaró la procedencia de su despido. Se instalaron por parte de una conocida cadena hotelera, NH en uno de sus establecimientos, dos cámaras ocultas durante tres meses ante las sospechas de una supuesta ingesta de alcohol del jefe de cocina, en horas de trabajo, por un descuadre de las consumiciones alcohólicas en la zona de cafetería (al realizar el inventario de botellas faltaban varias, en base a las consumiciones registradas).

La prueba.- Se corroboran los hechos a través de la prueba videográfica, en la que se comprueba que el recurrente en 16 ocasiones aparece fumando o bebiendo. La prueba que es impugnada por ilícita, esta se fundamenta en base a la doctrina constitucional: *"Por lo que se refiere a la utilización por parte de la empresa de las cámaras de grabación la sentencia es impecable haciendo relación a la doctrina tanto constitucional como la ordinaria, que viene exigiendo que la utilización de estos medios visuales cumpla los tres requisitos de idoneidad proporcionalidad y necesidad para proteger el derecho constitucional a la intimidad de los trabajadores, que en el caso se justifican para detectar la anomalía que se estaba produciendo"* (FJ 2º).

El criterio.- Se realiza, por tanto, el enjuiciamiento, en base al principio de proporcionalidad, superando la medida de control el triple test de la STC 186/2000, la prueba era idónea pues existían sospechas razonables y fundadas basadas en un descuadre en el inventario, se somete a control un tiempo determinado, el necesario para corroborar las sospechas, que fueron la base del despido disciplinario.

k) Dependiente de SABECO (STSJ del País Vasco 18 de Junio de 2013[908])

El caso.- Recurre en suplicación el trabajador la sentencia de instancia que desestimó su demanda contra Supermercados Sabeco, S.A. En ella se declarada

[907] STSJ de Valencia de 17 diciembre de 2013 (JUR 2014\83014).

[908] STSJ de País Vasco de 18 de junio de 2013 (EDJ 2013/307538).

procedente el despido del que fue objeto al resultar acreditados los hechos imputados en la carta de despido a través de prueba videográfica que descubría irregularidades (consistentes en la anulación de productos una vez escaneados) cometidas en el cobro de productos a sus clientes, apropiándose indebidamente de diversas cantidades de dinero. Las cajas del supermercado en las que trabajaba el actor estaban conectadas a un ordenador central que controlaba la actividad de los mismos. Esta terminal reportó un incidente detectando anomalías en el puesto del trabajador recurrido, pues recogía un número excesivo de devoluciones superior a la media, se visiona la cinta de la cámara que estaba instalada en su puesto comprobándose cómo anulaba gran cantidad de productos y se apropiaba el dinero.

La prueba.- Por la Sala se procede a anular la prueba videográfica por falta de información previa al trabajador, señalándose doctrina constitucional al respecto y concluyendo lo siguiente:

> *"No consta así que se diera información previa alguna al trabajador de tal grabación, ni tampoco de la instalación y finalidad de aquellas cámaras.*
>
> *Y es que de que, con independencia de que la finalidad de la instalación de las cámaras pueda ser en esencia la que defiende la empresa - la prevención de hurtos y similares- lo cierto es que en este concreto caso se usó con la indicada y distinta finalidad de controlar la actividad de la demandante y luego para sancionar a la misma con el despido.*
>
> *Por otra parte, el hecho de que las cámaras puedan ser vistas por los trabajadores o los clientes porque no se oculta su existencia y son apreciables a simple vista, tampoco se considera relevante por aquella doctrina del Tribunal Constitucional en orden a respetar los postulados expuestos.*
>
> *Y es que privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo fue también de su derecho fundamental a la protección de datos" (FJ 5º).*

Valoración.- Lo que resulta sorprendente es que se proceda a confirmar el despido disciplinario, cuando los hechos son constados mediante la prueba videográfica, y esta se ha anulado, ya que el reporte documental del ordenador central lo que refleja es un alto índice de devoluciones, no existiendo ni tan siquiera descuadres, y la testifical practicada nos viene a explicar únicamente el mecanismo de reporte de los incidentes. Parece que la Sala ha quedado "*contaminada*" por el resultado de la prueba que ella misma ha declarado ilícita y aplica su "*reproche moral*" a un despido que desde el punto de vista estrictamente procesal y formal considero habría de calificarse como improcedente por falta de prueba*:*

Prescindiendo por tanto de la prueba que hemos declarada ilícita, debemos ver si existen otras pruebas invocadas por la empresa para acreditar los hechos en que basa el despido disciplinario del recurrente. Y entendemos que sí ha quedado probado.

(...) Pues bien, en uno de los controles que se realizaron por el departamento de control interno saltó información que desde la caja NUM002 del establecimiento de Avendaño se había producido un ticket cero (anulado) el día 11 de agosto de 2012. Y así la empresa realizó un chequeo de las transacciones realizadas por el actor en línea de cajas desde el día 11 de agosto encontrándose gran número de

anulaciones en el registro de su caja. Tales operaciones aparecen descritas con detalle en la carta de despido, indicándose el día y hora exacta de la transacción y la operación y productos anulados y lo que el trabajador reflejaba en el ticket. Por tanto, tales operaciones se prueban con los informes diarios electrónicos de la caja registradora. Por otra parte, los arqueos de la caja no muestran excedente alguno de dinero como sería lo normal de haberse anulado operaciones.

También ha valorado la instancia la prueba testifical de Dª Melisa, responsable del departamento de control interno de la empresa quien ha explicado cómo se efectúa el control de las cajas registradoras desde el ordenador central siendo en uno de estos controles cuando se detectaron las anomalías en la caja en la que trabajaba el Sr. José Pablo. Y fue una vez comprobadas las anomalías cuando se visionaron las imágenes grabadas por las cámaras de videovigilancia . Pero entendemos que prescindiendo de esta prueba que hemos declarado ilícita los hechos alegados por la empresa quedan suficientemente acreditados.

Entendemos que la empresa ha probado las irregularidades cometidas (….) "(FJ 6º).

Con este "*encaje de bolillos*", la sentencia califica dudosamente el despido como procedente, habiendo la Sala quedado viciada con el resultado de lo que se ha desprendido de una prueba declarada nula.

P) Conclusiones

Q)

Ante la falta de regulación legal en materia de videdovigilancia y la "pereza" del legislador en la materia, cabe antes, a todas luces, esperar una pronta rectificación de la doctrina constitucional tras la STC 39/2016, de 3 de marzo.

La referida última sentencia constitucional, no ha hecho otra cosa que introducir confusión e inseguridad jurídica en la materia objeto de análisis, como ya se puede observar en la doctrina del TS y de algún TSJ, y lógicamente cabe esperar resoluciones difíciles de "*digerir*" desde el punto de vista doctrinal porque la doctrina constitucional no es clara sino ambigua, por lo que de ella no cabe vaticinar buenos resultados.

Es lamentable que cuestiones que estaban delimitadas de una manera más o menos clara en videovigilancia, se hayan difuminado, produciéndose un retroceso en los derechos fundamentales reconocidos al trabajador.

2. Detectives privados

El mercado de trabajo ha dado lugar a prestaciones de servicios de caracteres muy diferentes, donde el control empresarial no resulta sencillo al ser el lugar de trabajo variable o el horario flexible y, por ello, no es extraño que se busquen medios que no son usuales en lo ordinario como la contratación de un detective privado, algo que cuenta con un enorme potencial lesivo pues permite conocer datos relativos a la vida privada del trabajador[909]. Cuando el empresario sospecha que la conducta extralaboral del empleado es susceptible de dañar los intereses de la empresa, es frecuente que contrate los servicios de una agencia de detectives para vigilar si este cumple o no con su cometido en los términos y forma pactados, pues como sabemos, tiene prohibido encomendar estas funciones a sus propios empleados.

En principio, la vigilancia de los trabajadores mediante detectives privados es una fórmula más entre las diversas posibles, no contraria por sí misma al ordenamiento jurídico. Es inexistente el "*derecho a no ser vigilado fuera del trabajo*", pero también la facultad ilimitada de fiscalizar la conducta extralaboral del empleado[910].

A) Regulación legal

Ley 5/2014.- La Ley 5/2014, de 4 de abril, de Seguridad Privada (LSPr) ha derogado la Ley 23/1992, de 30 de julio, y regula de manera mucho más detallada y completa que la anterior la función del detective. Se trata de una norma extralaboral; sin embargo, como sucede muchas veces, de su contenido se extraen ciertas pautas que

[909] RODRÍGUEZ CARDO, I, A.: «Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador», *Actualidad laboral*, núm.12, 2014, pág.3.

[910] SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCCONI, C.: «Implicaciones prácticas de la nueva ley de Seguridad Privada». *Gestión de Conocimiento. Noticias Jurídicas*. GÓMEZ ACEBO & POMPO, abril 2014, pág. 1 del original impreso.
http://www.gomezacebo-pombo.com/media/k2/attachments/implicaciones-practicas-de-la-nueva-ley-de-seguridad-privada.pdf

pueden afectar a las relaciones laborales[911]. El ámbito objetivo de proyección de la actividad de detectives no varía mucho de la anterior norma, así el art, 5.1 h LSPr recoge que pueden investigar" *a personas, hechos o delitos sólo perseguibles a instancia de parte*", no abarca por tanto los posibles delitos perseguibles de oficio.

Limitaciones.- Lo que constituye una novedad es, sin duda, el art. 8.4 que regula limitaciones genéricas expresas, referidas a todo el personal de seguridad:

> *a) No podrán intervenir ni interferir, mientras estén ejerciendo los servicios y funciones que les son propios, en la celebración de reuniones y manifestaciones, ni en el desarrollo de conflictos políticos o laborales.*
>
> *b) No podrán ejercer ningún tipo de control sobre opiniones políticas, sindicales o religiosas, o sobre la expresión de tales opiniones, ni proceder al tratamiento, automatizado o no, de datos relacionados con la ideología, afiliación sindical, religión o creencias.*
>
> *c) Tendrán prohibido comunicar a terceros, salvo a las autoridades judiciales y policiales para el ejercicio de sus respectivas funciones, cualquier información que conozcan en el desarrollo de sus servicios y funciones sobre sus clientes o personas relacionadas con éstos, así como sobre los bienes y efectos de cuya seguridad o investigación estuvieran encargados.*

Parece razonable impedir la intervención de detectives privados para solventar problemas o "*conflictos laborales*" y que en su caso actúen las fuerzas del orden público.

Encargo investigador.- Un elemento importante lo constituye la previsión del art. 25.1 a) cuando exige *"Formalizar por escrito un contrato por cada servicio de investigación que les sea encargado, comunicando su celebración al Ministerio del Interior o, en su caso, al órgano autonómico competente en la forma que reglamentariamente se determine. Dicha obligación subsistirá igualmente en los casos de subcontratación entre despachos"*. Este contrato es el documento por el cual se legitima "*el encargo investigador*" y es además el instrumento que delimita el ámbito objetivo, subjetivo y material de la investigación desde el punto de vista empresarial[912].

Funciones.- Establece el art. 37 las funciones inherentes de los detectives privados derivados de dicho encargo investigador, tanto a solicitud de personas físicas como jurídicas:

> *1. Los detectives privados se encargarán de la ejecución personal de los servicios de investigación privada a los que se refiere el artículo 48, mediante la realización de averiguaciones en relación con personas, hechos y conductas privadas.*
>
> *2. En el ejercicio de sus funciones, los detectives privados vendrán obligados a:*
>
> *a) Confeccionar los informes de investigación relativos a los asuntos que tuvieren encargados.*

---

[911] SEMPERE NAVARRO, A. V. y ARIAS DOMÍNGUEZ, A.: *Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014),* ed. Francis Lefebvre, 2014, pág. 17.

[912]ARIAS DOMINGUEZ, A.: «Detectives privados, jurisdicción social y proyecto de ley de seguridad privada», Comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social de la AEDTSS, mayo 2014, pág. 9 del original impreso, *http://www.aedtss.com/images/stories/documentos/XXIV_CONGRESO_NACIONAL/pdf/4.1.pdf*

b) Asegurar la necesaria colaboración con las Fuerzas y Cuerpos de Seguridad cuando sus actuaciones profesionales se encuentren relacionadas con hechos delictivos o que puedan afectar a la seguridad ciudadana.

c) Ratificar el contenido de sus informes de investigación ante las autoridades judiciales o policiales cuando fueren requeridos para ello.

3. El ejercicio de las funciones correspondientes a los detectives privados no será compatible con las funciones del resto del personal de seguridad privada, ni con funciones propias del personal al servicio de cualquier Administración Pública.

4. Los detectives privados no podrán investigar delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento, y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido hasta ese momento.

3. El ejercicio de las funciones correspondientes a los detectives privados no será compatible con las funciones del resto del personal de seguridad privada, ni con funciones propias del personal al servicio de cualquier Administración Pública.

4. Los detectives privados no podrán investigar delitos perseguibles de oficio, debiendo denunciar inmediatamente ante la autoridad competente cualquier hecho de esta naturaleza que llegara a su conocimiento, y poniendo a su disposición toda la información y los instrumentos que pudieran haber obtenido hasta ese momento".

Obligaciones.- El régimen jurídico de las obligaciones que asumen los detectives viene determinado por dos premisas esenciales: la confección de los informes de investigación (art. 37.1 apto. a) LSPr.) y la ratificación del contenido de los mismos ante las autoridades (art. 37.1. apto.c) LSPr.). Dichos informes no solo son un derecho sino que la ley ha preferido configurarlo como uno de los deberes que pesan sobre el ejercicio de la actividad profesional.

El conjunto de las actividades a desarrollar por los detectives privados está delimitado por los preceptos citados, siendo por tanto un rasgo fundamental de la actividad el que sus informes puedan ser trasladados al proceso como prueba, con la finalidad de conseguir la convicción de un juez sobre la existencia de un determinado hecho o dato relevante para la solución de un litigio[913].

Informe.- La LSPr ha venido a alterar significativamente el marco de realización del informe del investigador, que desde ahora debe elaborarse con mayor pulcritud, conteniendo menciones muy específicas de las que antes carecía:

- Por cada encargo, por cada actividad profesional, que se elabore un informe.
- Se deberán reflejar los aspectos formales del encargo, número de registro asignado al servicio, datos del contratante, así como las circunstancias materiales de la investigación abarcando el ámbito objetivo de actuación del detective, el objeto de contratación así como los "*medios*" los

[913] MORENO GARCÍA, J. A.: «Informes de los detectives privados y prueba en el proceso», *Revista de Jurisprudencia El Derecho,* núm. 1, 2007, pág. 1.

"*resultados*" y las actuaciones realizadas incluyendo el elenco de los "*detectives intervinientes"* [914].

- El informe del detective puede servir para preconstituir la prueba testifical: bien presenciando el mismo unos determinados hechos, bien acompañando al empresario en la apreciación de los mismos[915].

Limitaciones.- Por su parte, el art. 48 LSPr. regula las obligaciones inherentes al ejercicio del encargo al detective. Existen tres tipos de limitaciones distintas en la actividad del detective privado, a saber:

- *Funcional.* Con carácter previo, debe existir y acreditarse que hay un interés legítimo por quien realice el encargo. Existen unas limitaciones funcionales a la actividad investigadora, en el ámbito laboral, que son: no podrán intervenir en huelgas o conflictos colectivos, ni podrán realizar averiguaciones que pretendan saber la afiliación política o sindical de los trabajadores.
- *Objetiva*. Pues existen ámbitos no investigables, ámbitos en los que no se puede abrir una investigación porque está prohibido.
- *Operativa.* En la realización de las operaciones propias de la función de detective se deben emplear medios y mecanismos respetuosos con los derechos de los investigados y proporcionados con el carácter de la investigación[916].
- Singularización del encargo investigador[917].

Vale la pena recordar que la prescripción de las faltas laborales cometidas por los trabajadores, el conocimiento empresarial de lo investigado, se adquiere cuando se recibe el informe investigador o cuando el empleador adquiere alguna información concreta del detective, el plazo de prescripción se inicia de ese día[918].

B) El principio de proporcionalidad

Planteamiento.- Los tribunales suelen dar validez como prueba al informe elaborado por los detectives privados, en la medida que el seguimiento en lugares públicos no se considera lesivo del derecho a la intimidad como regla general[919]. Las investigaciones de los detectives están amparadas en la Ley de Seguridad Privada, pero

---

[914] SEMPERE NAVARRO, A. V., y ARIAS *DOMÍNGUEZ,* A.*: Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014), op. cit*. , pág. 38.

[915] *Ibídem*, pág. 58.

[916]ARIAS DOMINGUEZ, A.: «Detectives privados, jurisdicción social y proyecto de ley de seguridad privada», *op.cit.*, pág. 7 del original impreso.

[917] SEMPERE NAVARRO, A. V. y ARIAS DOMÍNGUEZ, A.: *Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014), op. cit*., pág. 42.

[918] *Ibídem*, pág. 57.

[919] RODRÍGUEZ CARDO, I. A.: «Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador»», *Actualidad laboral*, núm.12, 2014, pág. 5.

el problema que plantea la utilización de este medio de control radica en determinar si con él se respeta o no la dignidad del trabajador.

Regla general.- Como regla general, el poder de dirección empresarial y en su caso las facultades disciplinarias no pueden alcanzar a las actividades extralaborales del trabajador que precisamente por estar amparadas por derechos constitucionales quedan fuera del radio de acción de los poderes empresariales; y cuando el empleador interfiere, lo hace con afectación de los derechos pero esta intervención sólo está permitida cuando se sospeche fehacientemente que la conducta empresarial es contraria al interés profesional y dicha conducta presente un potencial riesgo grave para la empresa y no meramente hipotético[920].

Restricciones.- Por tanto, la utilización de los servicios de los detectives privados y el apoyo gráfico de su investigación, como medio de prueba se acepta cuando las imágenes se concretan a espacios públicos y se trata de controlar la actividad del trabajador fuera del establecimiento empresarial, o de verificar si se encuentra incapacitado[921].

La doctrina parece mantener una postura homogénea a la hora de analizar la ilicitud o no de las pruebas sobre incumplimientos contractuales de los trabajadores obtenidas a través de los detectives, sin embargo esta postura no resulta tan clara cuando se trata de controlar el crédito horario por los representantes de los trabajadores, porque en estos supuestos el potencial lesivo es más intenso, pues además del derecho a la intimidad, se encuentra afectado el derecho a la libertad sindical. En el imprescindible análisis cabría preguntarse si la empresa utiliza esos mismos métodos de vigilancia en relación con otros trabajadores cuya prestación se desarrolle[922].

Intimidad.- Como ya expresamos, el derecho a la intimidad de la persona implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de lo demás que pese a ello, no tiene carácter absoluto. Para el TC en cada caso concreto habrá de apreciarse en los medios de vigilancia y control establecidos en el ejercicio del poder del empresario y en la injerencia en el derecho a la intimidad del trabajador.

---

[920] FERNÁNDEZ VILLAZÓN, L.A.: «Las facultades empresariales de control de la actividad laboral», ed. Aranzadi, 2003, págs. 173 y ss.

[921] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op.cit*, pág. 35.

[921] STSJ Madrid Sala de lo Social de 5 octubre 2016 (EDJ 2016/206328).

[922] RODRÍGUEZ CARDO, I. A.: «Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador», *Actualidad laboral*, núm.12, 2014, pág.5.

Doctrina constitucional.- La doctrina de las SSTC 98/2000 y 186/2000,ya analizadas, es perfectamente aplicable a este ámbito respecto al principio de proporcionalidad, que ha de cumplir con los siguientes requisitos:

a) Justificación: requiere la existencia de sospecha de un comportamiento irregular del trabajador que va a ser objeto del seguimiento del detective.

b) Idoneidad: debe permitir verificar si el trabajador realiza actividades incompatibles con su situación.

c) Necesidad: no es posible utilizar otros medios de vigilancia alternativos igualmente eficaces.

d) Equilibrio: existirá cuando el seguimiento se realice durante un período limitado, suficiente para confirmar las sospechas.

C) El control sobre uso de " horas sindicales"

a) Delimitación

El art. 37.3.e) ET prevé que el trabajador pueda ausentarse de su puesto de trabajo, sin pérdida de remuneración para realizar funciones sindicales o de representación del personal en los términos establecidos legal o convencionalmente. Esta categoría del crédito de horas se ubica en el art. 68 ET, y el permiso para negociar convenios colectivos, en el art. 9.2 LOLS. Entre esas garantías se encuentra el derecho al crédito horario reconocido por el artículo 10 de la Ley Orgánica de Libertad Sindical, al equiparar las garantías de los representantes sindicales a las establecidas legalmente para los miembros de los Comités de Empresa o de los órganos de representación existentes en las Administraciones Públicas. Así lo ha dispuesto, entre otras, la Sentencia del Tribunal Constitucional (Sala Segunda) de 16 de mayo de 2000[923] que reconoce que "*el derecho que tienen determinadas secciones sindicales de empresa a estar representadas por delegados sindicales, con las competencias y garantías del art. 10.3 LOLS, que conllevan paralelas obligaciones y cargas para el empleador*" (FJ 1º)[924].

---

[923] STC 132/2000, de 16 mayo (RTC 2000\132).

[924] MORALES DE LABRA, E.*:* «Crédito horario sindical, un derecho limitado». *Revista Doctrinal Aranzadi So*cial núm. 58, 2011 (BIB 2010\2489).

b) Derecho a no ser vigilado singularmente

La sentencia que marcó un precedente, es la STS de 29 de septiembre de 1989[925], que declara el derecho de los representantes de los trabajadores a no ser "*sometidos a vigilancia singular*", como refuerzo a las acciones legales entabladas por representantes de trabajadores frente a empresas[926]. La imposibilidad de sometimiento a control singular, limita la actuación profesional del detective y pretende proscribir un seguimiento tan intenso y meticuloso que no deje lugar ni espacio a la privacidad, lo que entronca con los derechos constitucionales del trabajador[927].

Poco tiempo después y recogiendo esta doctrina, aparece otra relevante sentencia que marcó un hito en la materia[928]; es la STS de 14 de junio de 1990[929], que afirma que los representantes de los trabajadores han de utilizar el crédito horario en interés de la colectividad de los trabajadores de la empresa y no en beneficio propio, pues lo contrario es un doble fraude, a los trabajadores que representan y a la propia empresa: *"Es de significar que la no utilización del denominado crédito horario sindical en las tareas representativas para las que, legalmente, aparece concedido, a la par que constituye una actitud de deslealtad respecto al colectivo de trabajadores representados, comporta, asimismo, una manifiesta actitud de fraude para la empresa que, únicamente, en función de dicha actividad representativa, abona el salario sin contraprestación del trabajo*"(FJ 11º).

Se declara que el uso del crédito sindical no es un derecho absoluto, cuando es manifiesto que no se está realizando un correcto uso del mismo; por tanto no se puede someter a la absoluta libertad del trabajador*: "(…) Si bien el ejercicio de ese derecho inherente al*

---

[925] STS de 29 septiembre de 1989 (RJ 1989\6553).

[926] DÍAZ RODRÍGUEZ, J. M.: «Intimidad y privacidad sindical frente al control empresarial». Comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social de la AEDTSS, mayo 2014, pág. 13 del original impreso. *http://www.aedtss.com/images/stories/documentos/XXIV_CONGRESO_NACIONAL/pdf/2.6.pdf*

[927] SEMPERE NAVARRO, A. V. y ARIAS DOMÍNGUEZ, A.: «Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014)», *op. cit*., pág. 72.

[928] Doctrina seguida por los siguientes Tribunales: STSJ C. Valenciana, núm. 156/1996, de 23 enero.(AS 1996\129). STSJ C. Valenciana núm. 2133/1996, de 10 septiembre. (AS 1996\2868) STSJ Cataluña, sentencia núm. 2616/1997, de 7 abril. (AS 1997\1417). STSJ País Vasco, núm. 745/1998, de 3 marzo. (AS 1998\1289) STSJ Andalucía, Málaga , sentencia núm. 1561/2002, de 12 septiembre. (AS 2002\3796), STSJ Cataluña, núm. 9447/2009, de 29 diciembre. (AS 2010\1218.) STS 13 marzo 2012. RJ 2012\5242 .STSJ C. Valenciana, núm. 1015/2012, de 10 abril. (AS 2012\1711). STSJ Madrid, núm. 120/2012, de 27 febrero. (AS 2012\702)

[929] STS Sala Social, 14-6-1990. (RJ 1990\5075).

desempeño de función representativa no permite una interpretación restrictiva que lo coarte o someta a controles indebidos o contrarios a la imprescindible libertad de acción que le debe ser inherente, sin embargo cuando se llegue a advertir un manifiesto uso del crédito horario en cuestión, que contradice la finalidad a que, legalmente responde, lógicamente, ha de rechazarse tal anómalo desenvolvimiento, tanto desde la perspectiva del colectivo laboral representado como de la empresa que coopera al desarrollo de la actividad de representación colectiva" (FJ 8º).

De aquí que no quepa excluir absolutamente a la empresa del control sobre el ejercicio de dicha actividad representativa sindical y del consiguiente crédito horario, pues: "(…)*si es evidente que un mal uso de este último transgrede la buena fe y lealtad debida al colectivo de trabajadores representado, también lo hace en relación a la lealtad debida a la empresa, cuyo sacrificio de horas de trabajo debido no se ve adecuadamente correspondido o compensado*" (FJ 6º)

Declara la Sentencia del Alto Tribunal que "*la concesión de este crédito horario no está sometida a la previa autorización del empresario*". De tal manera, que dentro de la libertad que se le otorga al representante, el empleo del crédito horario para atender los intereses individuales del trabajador titular de este derecho constituye una conducta fraudulenta que puede ser objeto de sanción por parte de la empresa[930]. Por otro lado, el seguimiento que realiza el detective necesariamente tiene que ser discriminado, en el sentido de que debe ir dirigido únicamente a concretos trabajadores; no se puede ejercer un control sistemático de todos los representantes[931].

En consecuencia, forma también parte del contenido del derecho a la libertad sindical del art. 28.1 CE, el derecho del trabajador a no sufrir, por razón de su afiliación o actividad sindical, menoscabo alguno en su situación profesional o económica en la empresa, garantía de indemnidad que veda cualquier diferencia de trato por tales razones y que determina el menoscabo del derecho a la libertad sindical si la actividad sindical tiene consecuencias negativas para quien la realiza, o si éste queda perjudicado por el desempeño legítimo de la actividad sindical[932].

---

[930] INDA ERRERA, M.: «Despedido por atender un negocio particular en horas sindicales», *Revista Aranzadi Doctrinal*, núm. 4, 2012.

[931] SEMPERE NAVARRO, A. V, y ARIAS DOMÍNGUEZ, A.: *Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014*), *op. cit*., pág. 72

[932] STSJ de Madrid de 25 de abril de 2014 (EDJ 2014/68963).

c) Naturaleza y requisitos de la vigilancia (STS de 15 de octubre de 2014[933])

Resuelve el recurso de casación interpuesto por el trabajador contra sentencia del TSJ de Cataluña que estimó el recurso de suplicación de la empresa en el que se formuló un voto particular, el Alto Tribunal desestima formulándose asimismo voto disidente. Los hechos declarados probados son los siguientes:

- La trabajadora era ayudante de dependienta en un supermercado y representante legal de los trabajadores.
- La empresa sospechaba que la trabajadora no cumplía de manera correcta con las horas destinadas a crédito sindical y la somete a la vigilancia de un detective privado.
- Del resultado del informe del detective, se acordó la apertura de expediente contradictorio disciplinario. La instructora formuló pliego de cargos del que se dio traslado a la trabajadora concediéndole un plazo de cinco días para presentar escrito de descargo, reclamando aquélla la unión al expediente de la documentación que estimó conveniente. De la incoación del expediente y del pliego de cargos se entregó copia al Comité de Empresa para que, si lo consideraba oportuno, pudiera emitir informe.
- La actora presentó alegaciones en su descargo exponiendo que el primero de los días imputados realizó las actividades sindicales durante toda la jornada prevista. En cuanto al segundo día imputado reconoció que fue suspendida la sesión del curso de formación sindical prevista para esa mañana, lo que le fue comunicado telefónicamente el día anterior, fijándose al mismo tiempo una reunión informativa para dicha tarde en el Sindicato para tratar asuntos sindicales. También añadía que si posteriormente, no concretó lo sucedido ese día fue precisamente para evitar equívocos por parte de la empresa, considerando que lo fundamental era que realizó actividad sindical aunque no coincidiera con la franja horaria inicialmente prevista.
- La instructora dio por concluido el expediente valorando los hechos como constitutivos de dos infracciones, una grave y otra muy grave, se notificándose a la trabajadora carta de despido disciplinario.
- La sentencia del Juzgado de lo Social de Figueras estima improcedente el despido dando la opción de ser indemnizada o readmitida a la trabajadora.
- La STSJ de Cataluña de 19 de febrero de 2013[934] acepta la revisión de los hechos declarados probados en base a la documental de la prueba del detective y procede a declarar el despido procedente.

El Informe no es prueba documental.- El primer motivo de casación que por parte de la representación de la trabajadora se plantea es que no procede considerar la prueba del detective como documental sino como testifical, por lo que la estimación de la suplicación no era válida, la Sala contesta que respecto al carácter de esta prueba de informe del detective privado " *No es dable configurarlos como prueba documental a los efectos de fundamentar la revisión fáctica en suplicación - ni tampoco el error de hecho en casación ordinaria (art. 207.d LRJS) -, al no tratarse de un auténtico documento sino de meras manifestaciones testimoniales formuladas por escrito que por ello no pierden su verdadero carácter de prueba testifical o de una denominada prueba testifical*

[933] STS de 15 octubre 2014 (RJ 2014\5807).
[934] STSJ Cataluña de 19 febrero de 2013 (AS 2013\2287).

impropia, que solo habría adquirido todo su valor procesal como tal prueba testifical de haber sido ratificada en juicio por sus firmantes, cuya valoración queda a la libre apreciación del juzgador de instancia" (FJ 4º). Por lo que procede a estimar el motivo.

Revisión fáctica.- Como segundo motivo de recurso se plantea la ilicitud de la vigilancia o control singular a que fue sometida en el ejercicio de su crédito horario respecto a la procedencia o no de la prueba de detectives, y el derecho de los representantes de los trabajadores a desempeñar sus funciones "sin ser sometidos a vigilancia singular", señala que no se entrará a resolver este segundo motivo, pues habiendo prosperado el primero de los motivos del recurso, y habiéndose eliminado de los hechos probados la adición fundada en la testifical a cargo de detective privado, y al no estar basados los restantes hechos probados de la sentencia de instancia en tal prueba, carece de interés a los fines de este recurso sentar en abstracto doctrina sobre esta cuestión.

Libertad de uso.- Como tercer motivo del recurso, plantea la recurrente la cuestión relativa a que no puede exigirse a los representantes de los trabajadores un cómputo escrupuloso del tiempo establecido en el uso del crédito horario, la Sala contesta:

"El presunto incumplimiento, en todo o en parte, de las funciones propias de la representación de los trabajadores durante el uso del crédito horario, detectada incluso por la petición previa del mismo y la posterior justificación inexacta aportada, no constituye por sí solo una trasgresión de la buena fe contractual que pueda justificar despido, puesto que la presunción de que las horas solicitadas para el ejercicio de las tareas representativas son empleadas correctamente conduce a interpretar de modo restrictivo la facultad disciplinaria del empresario, que sólo podrá alcanzar el despido en supuestos excepcionales en los que el empleo en propio provecho del crédito horario concedido por el art. 68.e) ET a los representantes de los trabajadores sea manifiesto y habitual, es decir con una conducta sostenida que ponga en peligro el derecho legítimo de la empresa a que los representantes formen cuerpo coherente con los representados y que esta conducta esté acreditada con pruebas que no hayan empleado una vigilancia que atente a la libertad de su función" (FJ 10).

Por lo que en consecuencia se casa y anula la sentencia de la segunda instancia declarándose improcedente el despido. El voto particular, formulado por la Magistrada Calvo Ibarlucea, se dirige frente a la admisión del recurso al carecer de un presupuesto como es la contradicción entre las resoluciones sometidas a comparación.

d) Realización de actividades privadas (STS de 13 de marzo de 2012[935])

El caso.- Resuelve el recurso de casación para la unificación de doctrina que resulta desestimado y que plantea el conflicto de la irregularidad de la prueba del

[935] STS de 13 de marzo de 2013 (RJ 2012\5242).

detective privado. El supuesto de hecho versa sobre un empleado que es representante de los trabajadores, al que se despide, imputándole un uso indebido de su crédito horario, por la ausencia de dos días, previamente anunciada a la empresa. La titular de la relación laboral contrató con un detective privado la investigación de las actividades que el trabajador realizaba durante este tiempo, concluyéndose que había realizado actividades en un negocio particular relacionado, además, con la actividad de la empresa. Por lo que se confirma el despido disciplinario declarado en la STSJ de Murcia de 22 de septiembre de 2010[936].

La doctrina.- Se alude al principio de proporcionalidad a la hora de ponderar la prueba del detective: "Hay que atender a las circunstancias concurrentes, para considerar si la vigilancia mediante detectives fue proporcionada o no , por ejemplo ya que no se trató de una vigilancia indiscriminada de la actuación sindical del trabajador sino que se limitó a los unos días concretos y previas sospechas previas" (FJ 2º).

En definitiva, esta sentencia sigue la teoría general sobre la materia aludida anteriormente, y en ella se admite que los representantes de los trabajadores tienen derecho a desempeñar sus funciones "sin ser sometidos a vigilancia singular", en tanto supone "una traba o limitación a su derecho de libertad o libre ejercicio del cargo", pero esto no significa la proscripción de la prueba de detectives, que sólo constituye un obstáculo para el ejercicio de tales funciones en los supuestos de desproporción de la medida, cuando se lleva a cabo con vulneración de derechos fundamentales.

e) Doctrina judicial sobre uso ilegítimo de la prueba del detective

La STSJ de las Islas Canarias de 25 de septiembre de 2015[937].- El TSJ de Canarias estima el recurso de suplicación interpuesto por el demandante, contra la sentencia de la instancia, dictada en autos promovidos en materia de impugnación de sanción, revocándola en el sentido de anular totalmente la sanción de dos meses de suspensión de empleo y sueldo impuesta, con todas las consecuencias jurídicas y económicas inherentes a tal declaración.

---

[936] STSJ de Murcia de 5 de mayo de 2010 (AS 2010\1886).

[937] STSJ de Islas Canarias de 25 septiembre de 2015(AS 2016\160).

Con cita expresa de la doctrina de la STS de 13 de marzo de 2012[938], se declara la sanción improcedente por utilización abusiva del crédito horario, declarando la nulidad de la prueba de detective privado al no constar dato alguno del que quepa inferir la concurrencia de particulares circunstancias que hubieran podido llevar a la empresa a sospechar que se estaba realizando por parte del trabajador un uso abusivo del crédito horario en provecho propio. Incluso, el control se había realizado fuera del horario laboral, considerándose de forma errónea que únicamente son actividades sindicales amparadas por el crédito horario las que se desarrollan en la sede del sindicato y durante su horario de atención al público:

> *"En primer lugar, la sumisión al representante sindical a vigilancia singular mediante su seguimiento por un detective, resulta absolutamente desproporcionada, por cuanto, no refleja el histórico dato alguno del que quepa inferir la concurrencia de particulares circunstancias que hubieran podido llevar a la empresa a sospechar que estaba haciendo un uso abusivo del crédito horario en provecho propio, es más, el control de su actividad se llevó a cabo incluso fuera de su horario laboral, y, como corolario de ello dicha prueba debe reputarse nula de pleno derecho, por haberse obtenido ilegítimamente, vulnerando el derecho a la libertad de la función sindical.*
>
> *- En segundo término, se parte de la errónea concepción de que únicamente son actividades sindicales amparadas por el crédito horario las que se desarrollan en la sede del sindicato y durante su horario de atención al público, obviando que las mismas pueden desplegarse en múltiples ámbitos comprendiendo un amplio y variado abanico de actividades que no solo pueden realizarse en los locales de la organización sindical o visitando centros de trabajo, sino en otros muchos lugares y en cualquier horario.*
>
> *- Finalmente, el que D. Manuel no hubiera realizado funciones sindicales en una franja horaria no coincidente de su horario de trabajo, que, como decimos se iniciaba a las 22 horas, que es lo único que la sentencia de instancia declara probado, en modo alguno permite concluir a que a partir de dicha hora y en el tramo correspondiente a su jornada laboral hubiera llevado a cabo actividades de carácter sindical, pues no solo la utilización que de dicho permiso realiza el representante está legalmente investida de una presunción de probidad" (FJ 3º).*

En base a estos tres presupuestos, concluye la sentencia que los representantes de los trabajadores tienen derecho a desempeñar sus funciones sin ser sometidos a vigilancia singular, ya que ello "*supone una traba o limitación a su derecho de libre libertad o libre ejercicio del cargo*". Por lo que, las pruebas obtenidas por la empresa con desconocimiento del derecho a no ser sometidos a vigilancia singular han de considerarse nulas por ilícitamente obtenidas, sin que ello suponga una proscripción de la prueba de detectives que solo constituye un obstáculo para el ejercicio de tales funciones en los supuestos de desproporción de la medida cuando se lleva a cabo con vulneración de derechos fundamentales. De manera que, cuando, atendiendo a las concretas circunstancias concurrentes en cada caso, ese control o vigilancia empresarial resulte proporcionado, idóneo y razonable, ningún reproche merecerá la obtención de dicho medio de prueba desde la perspectiva constitucional.

[938] STS de 13 de marzo de 2013 (RJ 2012\5242).

En definitiva se ha sometido la prueba del detective al juicio de proporcionalidad y no se ha considerado tal medida proporcionada, por lo que la prueba es nula y al no haber hechos imputables no hay lugar sanción ni por tanto suspensión de empleo y sueldo

STSJ de Madrid 25 de abril de 2014[939].- Se desestima el recurso de suplicación planteado por la Real Federación Española de Natación, que entre otros extremos impugna que no se le haya dado relevancia a la prueba practicada por el detective, consistente en seguimientos en las horas sindicales del recurrido, pues ni tan siquiera era proporcionado acordarla:

"Por tanto, este motivo también se rechaza, por cuanto que, amén de que nada se ha justificado sobre el especial control y seguimiento por la empresa de la acción sindical realizada por el actor, lo cierto es que su actuación los días a que se refiere la comunicación escrita de despido disciplinario no demuestran la existencia de ninguna actividad incompatible con la función sindical que tiene asignada." (FJ 5º)

STSJ Cantabria de 19 de marzo de 2014[940].- Esta sentencia es un claro ejemplo de la tendencia actual, en la que despedir por el uso ilegítimo del crédito sindical se concibe como *ultima ratio*, y solamente para los trabajadores que realicen esta práctica de manera habitual y manifiesta. Estamos ante un despido disciplinario basado en utilización irregular de crédito horario. El TSJ desestima el recurso de suplicación de la empresa y confirma la nulidad del despido. La sanción de despido solo podrá imponerse en los supuestos excepcionales en los que se justifique un empleo en provecho propio que sea manifiesto y habitual, pues existe una presunción de que las horas solicitadas para el ejercicio de las tareas representativas son empleadas correctamente:

"(...) la jurisprudencia, tras un inicial criterio sobre la utilización irregular del crédito horario , ha experimentado un giro interpretativo restrictivo, de acuerdo con el cual el crédito horario está configurado como una garantía de la función representativa y la actividad de los representantes debe comprender actuaciones de diferente signo, por lo que tienen derecho a no estar sometidos a vigilancia en el ejercicio de las mismas, existiendo una presunción de lealtad y de probidad en el cumplimiento de aquellas (...).

Además, como razona la STS de 21-1-1991 el tiempo de inasistencia al trabajo, derivado del uso del crédito horario sindical, normalmente es superior al de duración estricta de los actos representativos que van a llevarse a cabo, dada la necesidad de efectuar desplazamientos, o preparar las reuniones o las intervenciones. De ahí que, como recogen las SSTS de 2-11-1989, 28-6-1990 o 21-9-1990, la sanción de despido por esta causa sólo pueda imponerse en los supuestos excepcionales en los que se justifique un empleo en provecho propio que sea manifiesto y habitual, existiendo una presunción de que "las horas solicitadas para el ejercicio de las tareas representativas son empleadas correctamente". Ello determina que deba interpretarse de un modo restrictivo la facultad disciplinaria del empresario, que sólo podrá imponer el despido "en supuestos excepcionales en los que el empleo en propio provecho del crédito horario concedido por el art. 68.e) a los representantes de los trabajadores sea manifiesto y habitual, es decir, una

---

939 STSJ de Madrid de 25 de abril de 2014 (JUR 2014\134454).

940 STSJ de Cantabria de 19 de marzo de 2014 (EDJ 2014/57935).

conducta sostenida que ponga en peligro el derecho legítimo de la empresa a que los representantes formen cuerpo coherente con los representados" (FJ 3º).

STSJ Cataluña de 29 de octubre de 2013[941].- Aborda la comprobación de la realidad de las " *horas sindicales".* Declara el uso legítimo del crédito horario en domicilio. El TSJ estima el recurso de suplicación y declara la improcedencia de la sanción impuesta al trabajador. El domicilio es considerado lugar idóneo para el desarrollo de funciones representativas y está amparado por la presunción de uso legítimo del crédito horario de forma habitual, para poder entender que procede la imposición de sanción:

"Tampoco puede exigirse al trabajador la carga de probar las funciones que realiza, pues ello podría menoscabar la libertad sindical y constituir una injerencia desproporcionada y disuasoria en su función representativa. Al contrario, corresponde a la empresa dicha carga probatoria, que en el caso de autos no se ha cumplido.

Acompañar a la hija a la escuela e ir a dejar la basura, junto a la visita durante menos de una hora de un concesionario no puede considerarse en el lapso de tres días como incumplimiento de labores representativas, cuando consta que la mayor parte del tiempo el trabajador permaneció en su domicilio, amparado por la presunción de uso legítimo del crédito horario, siendo, como hemos dicho, el domicilio un lugar idóneo para el desarrollo de las funciones representativas"(FJ 3º).

Por tanto, no puede presumirse que por el hecho de estar en el domicilio propio no se realicen funciones representativas, cuando las mismas abarcan formación, información, comunicación, denuncia, vigilancia de cumplimiento de normativa, y un largo etcétera de actividades (*vid* art. 64 ET) que pueden realizarse desde un ordenador.

STSJ de Valencia de 16 de mayo de 2013.- La sentencia de suplicación resuelve el recurso planteado por la empresa en el sentido de desestimarlo, confirmando con ello la sentencia de la instancia. Los antecedentes del caso son los siguientes: a un delegado sindical, que era trabajador de una ITV, con una antigüedad considerable, se le imputaba el uso indebido del crédito horario, considerando que los hechos eran constitutivos de una falta de trasgresión de la buena fe contractual, a través de la prueba del detective privado. La sentencia de la instancia estimó la pretensión de despido nulo y la Sala confirmó el pronunciamiento pues, a pesar de estimar la revisión de hechos declarados probados, solo constaban cuatro días de realización de funciones ajenas:

"En el presente supuesto, de los hechos probados, con las revisiones admitidas, lo único que consta es la realización por el actor de actividades ajenas a su función sindical en cuatro días determinados, en los que también consta que contactó con otras personas por lo que no puede concluirse que no dedicase parte del tiempo a actividades propias de su representación sindical (...)debiéndose tener en cuanta que tal como señala el Tribunal Supremo en Sentencia de 13-3-12 , "Respecto a la procedencia de la prueba de detectives, y el derecho de los representantes de los trabajadores a desempeñar sus funciones "sin ser sometidos a vigilancia singular", esta Sala Cuarta del Tribunal Supremo tiene señalado, en sentencia de 10 de febrero de 1991 "(FJ 2º).

[941] STSJ de Cataluña 29 de octubre 2013 (EDJ 2013/252910).

Por tanto la falta del criterio de "*habitualidad"* es lo que hace que el representante sindical, no sea merecedor de la sanción máxima del ordenamiento jurídico.

STSJ de Baleares de 16 de marzo de 2013[942].- En esta sentencia se desestima el recurso de suplicación planteado por la empresa. Los hechos son los siguientes: se despide a una delegada sindical que debía reunirse los días indicados en la sede del sindicato, en horario de tarde, lo que le coincidía con su horario de trabajo, pero no acude ni a su trabajo ni a las reuniones. Se le realiza un seguimiento por detective privado que constata que los días y horas comunicados, la trabajadora no asistió a reunión alguna en la sede del sindicato. Pero los hechos no ocurren tal y como sostiene la empresa.

En aquellos casos en que no coincidan las horas destinadas a la actividad representativa con el horario de trabajo del representante, éste tiene derecho a que aquellas horas se consideren como parte del crédito horario y se deduzcan de las horas de trabajo efectivo; pues, en otro caso se estaría produciendo un incremento de las horas de trabajo en perjuicio del trabajador, como consecuencia del desarrollo de la actividad representativa:

> *(…)"Esta es la idea que guió al Tribunal Supremo en la sentencia de 18 de marzo de 1986 y aunque allí se resolvía sobre un representante que tenía asignado turno de noche, no coincidiendo su jornada laboral con la de sus representados, estableciéndose una excepción a la regla general de que el tiempo dedicado a actividades representativas debe coincidir con el tiempo de trabajo real y efectivo, esta misma idea debe extenderse a otros supuestos y en general a todos aquellos casos en que no hay coincidencia entre la actividad sindical y el horario de trabajo del representante, como se hace en las anteriores sentencias"(FJ 2º).*

f) Doctrina judicial que declara el uso legítimo de crédito sindical

STSJ de Andalucía de 14 de noviembre de 2013[943].- Se desestima el recurso de suplicación planteado por el representante de los trabajadores por utilización de su crédito horario sindical para actividades personales de ocio. Se declaró probado a través de la prueba del detective que durante varios días que fue objeto de seguimiento se iba a la playa. Se impugna por la recurrente con resultado negativo; la nulidad de la prueba del detective y se entiende vulnerado el derecho a la libertad sindical. La Sala resuelve

[942] STSJ de Baleares 16 de mayo de 2013 (EDJ 2013/112419).

[943] STSJ de Andalucía de 14 de noviembre de 2013 (AS 2014\570).

estimando la licitud de la prueba de detectives privados, al no estar ante una prueba ilegal sino proporcional a la finalidad pretendida:

> *"(….) el empleo de detectives a la vista de las circunstancias concurrentes que se exponen en la sentencia recurrida es un ejercicio regular y correcto de las facultades directivas y organizativas de la empresa demandada así como posteriormente de las facultades sancionadoras al comprobar el uso indebido y desviado del crédito horario, y que tal empleo de detectives en el presente caso no constituye una prueba ilegal vulneradora de derechos fundamentales ni del derecho de libertad sindical del actor, quedando demostrados y acreditados los hechos imputados y motivadores de la decisión sancionadora que se relatan que describen en el ordinal octavo de los hechos probados" (FJ 3º).*

Sobre la inexistencia de vulneración de derechos fundamentales, al impugnarse el derecho a la libertad sindical, la Sala declara:

> *" (…) pero la protección de los derechos fundamentales también se extiende a no permitir que encuentre amparo y protección la utilización indebida y desviada de tales derechos, y en concreto debe llegar a extenderse a no procurar la protección al uso incorrecto, fraudulento y en beneficio propio y no de la función representativa que le es propia del crédito horario reconocido al actor como miembro del Comité de empresa, es decir al contrario de lo que el actor dice la falta de amparo de su pretensión es correcta protección de los derechos fundamentales que invoca, y por otro lado tampoco puede entenderse que la empresa sea ajena al uso del crédito horario que se desarrolla en el ámbito de la propia empresa y que supone la no prestación de servicios por conceder horas para el ejercicio de una actividad representativa que realmente no se realizó sino que el actor disfrutó de estas horas de crédito representativo en lugar de realizar dicha actividad representativa en actividades privadas de ocio, recreo y playa, por lo que por la misma consideración indicada de protección de los derechos fundamentales esta Sala no puede amparar tal conducta del trabajador recurrente pues con ello también se está protegiendo el derecho fundamental de libertad sindical y también se está protegiendo el derecho de los trabajadores a que sus representantes ejerciten sus créditos horarios de forma debida y correcta y lo hagan en el ejercicio de la función representativa que les es encomendada y para la cual han sido nombrados y para la cual les ha sido concedido el crédito horario" (FJ 5º).*

Ciertamente, como razona la Sala, el que ha vulnerado el derecho a la libertad sindical es el recurrente, y es también necesario velar por los derechos de los trabajadores que a su vez este representaba pues sus libertades sindicales también han de ser protegidas.

STSJ de Canarias de 24 de abril de 2013[944].- El Tribunal desestima el recurso de suplicación planteado por la empleada, confirmando la procedencia de su despido. La sentencia de instancia consideraba que se había realizado un mal uso de las horas sindicales que regula el art. 68 e) del Estatuto de los Trabajadores por parte de la representante sindical, que solicitó permiso para hacer uso de esas horas sin que realmente las empleara para ese cometido, sino para un uso particular (un día se queda en su domicilio, otro día acude a una exposición de pintura y varios días ayuda a regentar el bar de su compañero sentimental).

[944] STSJ de Canarias de 24 de abril de 2013 (EDJ 2013/134832).

El motivo de la denegación es que cuando se invoque por un trabajador que un despido es discriminatorio o lesivo de cualquier derecho fundamental, ha de al menos aportar por su parte una prueba indiciaria y en el presente caso no se ha aportado ningún indicio[945]. Se cuestiona por la recurrente la falta de proporcionalidad de la prueba del detective, sosteniendo que ha sido objeto de seguimiento por el detective como represalia por parte de la empresa, al haber participado días antes en una huelga. La Sala contesta:

> *"En cuanto a que la vigilancia efectuada por un detective fue desproporcionada, hay que indicar que la misma se inició desde el 14 de julio de 2011, fecha en que la actora y su compañero inauguraron el bar la Cafeína, que es lo que llevó a la empresa a sospechar del uso que hacía la misma del crédito sindical sin que tal vigilancia vulnere su derecho a la intimidad, quedando acreditado por la Juzgadora que sólo fue a la actora a quien le pusieron el detective y no al resto de trabajadores que secundaron la huelga en la empresa, acaecida en 2010"(FJ 4º).*

STSJ de Madrid de 11 de febrero de 2013[946].- Se desestima el recurso de suplicación y se confirma por la Sala de lo Social la sentencia de instancia, que declara que existe transgresión de la buena fe contractual por parte de los representantes de los trabajadores, que han utilizado de forma indebida el crédito horario sindical solicitado para los días 24 y 31 de diciembre, pues en esos días su sindicato estaba cerrado y eran días de trabajo a pleno rendimiento.

> *Se estima procedente la prueba del detectives al existir indicios relevantes de que no se iba a desarrollar la actividad sindical, la empresa sabía que el Sindicato al que pertenecían las representantes permanecía cerrado en esas fechas de Navidad, se rechaza que la vigilancia haya sido abusiva, y no se admite una posible compensación de la actividad sindical desempeñada otros días por tratarse de fechas en que la actividad comercial de la empresa es muy superior a la ordinaria y no haberse utilizado ni una mínima parte del crédito horario solicitado en actividades sindicales:*
>
> *Respecto a la procedencia de la prueba de detectives, entiende esta Sala que la sentencia recurrida no ha cometido la infracción denunciada, pues la empresa contrató a los detectives al haberse solicitado el crédito horario los días 24 y 31 de diciembre de 2011, días especialmente señalados al tratarse de Nochebuena y la víspera de año nuevo, en los que la empresa sabía que el Sindicato al que pertenecían las actoras permanecía cerrado, no habiéndose solicitado el crédito horario por ningún otro representante de los trabajadores, por lo que existían ya unos indicios relevantes de que no se iba a desarrollar la actividad sindical, tratándose además de días*

---

[945] La distribución de cargas probatorias propia de la prueba indiciaria alcanza a supuestos en los que esté potencialmente comprometido cualquier derecho fundamental. En cuanto al canon de control constitucional, es sabido que la prueba indiciaria se articula en un doble plano, el primero consiste en la necesidad por parte del trabajador de aportar un indicio razonable de que el acto empresarial lesiona su derecho fundamental, principio de prueba o prueba verosímil dirigidos a poner de manifiesto el motivo oculto que se denuncia. El indicio no consiste en la mera alegación de la vulneración constitucional, sino que debe permitir deducir la posibilidad de la lesión Sólo una vez cumplido este primer e inexcusable deber, recaerá sobre la parte empresarial la carga de probar que su actuación tuvo causas reales absolutamente extrañas a la pretendida vulneración.

[946] STSJ de Madrid de 11 de febrero de 2013 (AS 2013\2283).

en los que la empresa demandada tiene un importante incremento de actividad al dedicarse al comercio -en otros sectores en esas fechas es público y notorio que la actividad está en mínimos- y le es aplicable concretamente, el Convenio colectivo del comercio de confitería, pastelería, bollería repostería heladería y platos cocinados y además la vigilancia guarda relación con la imputación formal de la carta despido, no se interfirió en actividades representativas de las actoras y se circunscribió a determinados periodos, no excesivamente largos" (FJ 1º).

E) Control de trabajadores en situación de incapacidad temporal

a) Delimitación

Esta es probablemente la causa más común para el empleo de detectives. Los abundantes pronunciamientos jurisprudenciales analizan las circunstancias particulares de cada caso y son difícilmente reconducibles a categorías homogéneas. Se pretende detectar actividades laborales concurrentes y, si el trabajador investigado no las realiza, comprobar si la actividad desempeñada es acorde o no, puede o no perjudicar su recuperación profesional[947]. Un aspecto importante a tener en cuenta es que en el informe técnico no puede deducirse la incompatibilidad de la lesión que sufre el trabajador[948], es decir que el informe ha de ser lo más objetivo posible.

b) Actividad contraindicada (STSJ Extremadura de 26 noviembre 2015[949])

El caso.- La Sala de Extremadura desestima el recurso interpuesto por la empresa contra la sentencia de Instancia en la que se declara improcedente el despido disciplinario del actor, que vio extinguida su relación laboral por transgresión de la buena fe contractual debido a haber realizado actividades incompatibles con su situación de IT.

Los hechos.- La empresa procede al despido del trabajador, teleoperador de profesión, en base a la prueba videográfica y fotográfica realizada por detective privado: había llevado a cabo sin dificultad alguna actividades cotidianas como viajes, conducción de vehículo, de ocio, cargar objetos pesados, y además por la información que se

[947] SEMPERE NAVARRO, A. V. y ARIAS DOMÍNGUEZ, A.: Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014), *op.cit.*, pág. 74.
[948] *Ibídem*, pág. 77.
[949] STSJ Extremadura de 26 noviembre 2015 (EDJ 2015/233444).

desprendía de una grabación en la que el trabajador acudía a un programa de tele-Extremadura a una sección dedicada a la actividad de peluquería en calidad de tertuliano y colaborador como peluquero. Por otro lado, se declara probado que el actor estaba en proceso de IT por trastorno ansioso- depresivo, secundario a su conocimiento de que era portador del VIH.

Razonamientos jurídicos.- La Sala entiende, respecto al informe de investigación privado lo siguiente: "*En cuanto a la carga y descarga de material pesado en fecha 31 de Enero, parece referirse a bolsas de compra y a tablas, hechos sin relación alguna con el problema psíquico que justificó la situación de IT, tampoco acreditan las fotografías incorporadas a dicho Informe que el vehículo (…) estuviera estacionado en la calle Sauceda de Sevilla y que en ésta existan pubs de ocio, ni que consumiera el demandante junto a un grupo de amigos varias copas, así como que le estuviera prescrito al actor no conducir y no salir o distraerse*" (FJ 1º).

Igual razonamiento se aplica respecto a las colaboraciones en la televisión extremeña. El segundo fundamento de derecho se dedica a resolver la consideración de las conductas realizadas por el actor como transgresoras de la buena fe, en base a la teoría gradualista, a lo que la Sala contesta: *"El TS (…) ha establecido dos categorías distintas: por un lado, aquéllas que, por resultar incompatibles con el proceso patológico en que se ha fundado la baja laboral, evidencian la simulación del mismo y el propósito fraudulento con que su reconocimiento y efectos subsiguientes se han obtenido, y, por otro lado, aquéllas que son incompatibles no con las disminuciones funcionales inflingidas por los padecimientos indicados, sino con la eficacia de los tratamientos prescritos, retrasando o impidiendo el resultado de éstos y la recuperación del afectado con daño tanto de los intereses públicos del sistema asistencial, como de los privados de su empleadora. Y evidentemente, teniendo en cuenta la narración fáctica de la resolución recurrida, es obvio que no concurren los requisitos exigidos jurisprudencialmente para calificar como conducta grave y culpable merecedora de la sanción de despido, siendo que, teniendo en cuenta la índole de la enfermedad que originó la baja laboral del trabajador, no se olvide, con la categoría profesional de teleoperador, no consta sea susceptible de perturbar su curación, ni evidencia la aptitud laboral de éste, con la consiguiente simulación en perjuicio de la empresa, sino todo lo contrario habiendo contribuido la actividad desarrollada a la curación del demandante, como hemos visto"* (FJ 1º).

Con ello concluye que procede desestimar el recurso de la empresa, pues el despido disciplinario de trabajadores en situación de baja por enfermedad, según la constante doctrina jurisprudencial, es la repercusión que en la evolución o curación del proceso patológico puedan tener las actividades desarrolladas por los trabajadores durante ese período.

c) Caza desaconsejada (STSJ Galicia de 23 de Junio de 2014[950])

La Sala desestima el recurso de suplicación planteado y confirma el despido disciplinario del recurrente. El actor estuvo de baja por incapacidad temporal aproximadamente tres semanas. Durante ese tiempo la empresa contrató a un detective y lo graba realizando durante todo un día actividades de caza, del todo incompatibles con su estado: " *En primer lugar, la actividad realizada por el trabajador durante su incapacidad temporal -salir a cazar en varias ocasiones, hasta 3 veces en 8 días- tiene un componente físico importante -estar a la intemperie hasta 8 horas diarias y a veces hasta oscurecer, andar subir y bajar laderas de montañas, agacharse, arrodillarse y otras posturas forzadas, realizar todo ello cargando la escopeta, a veces coger en brazos a un perro para meterlo en el remolque, según se deduce del Hecho Probado Cuarto-, lo que, de manera fuertemente indiciaria -y salvo prueba médica de contrario que, dicho sea de paso, no existe en los autos-, demuestra o bien la capacidad del trabajador para realizar sus labores como oficial primera en un taller mecánico -que es la profesión del trabajador, Hecho Probado Primero-, o bien la incompatibilidad con el proceso curativo -de hecho, la gota con otras manifestaciones, que es el diagnóstico de la baja médica, aconseja reposo relativo con la pierna en alto los dos primeros días, posteriormente introducción de actividades habituales, Hecho Probado Tercero*" (FJ Único).

d) Tareas inconvenientes (STSJ de Islas Baleares de 30 de enero de 2014[951])

La parte demandante formula recurso de suplicación contra la sentencia dictada por el Juzgado de lo Social, en la que se desestimó su demanda por realizar actividades incompatibles con su situación de IT. Vía recurso solicita la nulidad respecto de la prueba del informe del detective privado y su declaración en juicio por vulnerar el derecho a la intimidad del recurrente. La Sala recuerda la doctrina constitucional de las conocidas SSTC 98/2000 y 186/2000, y somete la prueba del detective al principio de proporcionalidad, y la declara ajustada y proporcional. Además no cabe apreciar lesión a su intimidad puesto que pudo ser visto por los detectives trabajando, como por cualquier persona, pues estaba en la vía pública: (…)*Efectivamente, el sometimiento a vigilancia del demandante por parte de detectives privados era adecuada para conseguir el fin pretendido, que no era*

[950] STSJ de Galicia de 23 de junio de 2014 (EDJ 2014/128618).

[951] STSJ de Islas Baleares de 30 de enero de 2014 (JUR 2014\89248).

otro que el de constatar si el demandante estaba vulnerando las obligaciones que impone la buena fe dentro del contrato de trabajo. Sin duda, la decisión de someter al demandante a vigilancia se adoptó por la existencia de sospechas de que estaba trabajando durante su baja. La medida era además necesaria, pues no se sabe de qué otro modo podía la empresa acreditar el incumplimiento del trabajador si no era comprobando que efectivamente realizaba durante su baja servicios de jardinería en una finca. Por último, en cuanto a la proporcionalidad, no debe perderse de vista el hecho de que el trabajador fue observado en un lugar no reservado, pudiendo ser observado cambio, la medida igualmente por cualquier persona que pasara por el lugar, lo cual incluso desdibuja la idea de intromisión en la vida privada o esfera personal y, en sirvió para evidenciar el incumplimiento y adoptar las medidas adecuadas"(FJ 1º).

Tampoco se acepta que la conducta del demandante no constituya un incumplimiento contractual, grave, y culpable sancionable con despido. Puesto que existe un hecho probado no revocado según el cual el trabajador durante su baja estuvo realizando trabajos de jardinería en una finca privada. Durante la IT el trabajador se ve exonerado de su obligación de trabajar, pero se mantienen el resto de sus deberes, en particular y en lo que aquí atañe, el de fidelidad, cuya vulneración justifica el despido. Y, concretamente, si el trabajador está impedido para consumar la prestación laboral a que contractualmente viene obligado tiene vedado cualquier otro tipo de quehacer, sea en interés ajeno o propio, sobre todo si se tiene en cuenta que su forzada inactividad le es compensada económicamente por la empresa y por la Seguridad Social, a las que perjudica, incurriendo así en la causa de transgresión de la buena fe en el desarrollo del contrato constitutiva del incumplimiento contractual grave y culpable del trabajador que justifica su extinción por decisión del empresario mediante despido.

F) Control de la concurrencia desleal

a) Delimitación

El deber de no concurrencia simple, sin pacto alguno que lo refrende o garantice de manera privilegiada, ha sido tradicionalmente vigilado, empleando a detectives. Los tres elementos de la concurrencia desleal son: 1) Realización de labores esencialmente idénticas a las contratadas. 2) Sin conocimiento ni consentimiento empresarial. 3) Causando un daño real o potencial al empleador[952].

[952] *Ibídem*, pág. 69.

La ilicitud existe cuando se produce la competencia económica con el empresario, aunque no haya generado un perjuicio objetivado, son suficientes los meros actos preparatorios, como recoge la STS 5 de junio de 1990[953]: *"No se requiere la existencia de un perjuicio real, bastando que sea potencial", llegando incluso a "adelantarse" su consumación por los meros actos de preparación, en la Sentencia de esta Sala de 7 de octubre de 1987 , que afirma existir "un principio de ejecución" dotado de intencionalidad suficiente, a efectos de establecer una acción contraria a la prohibición del artículo 21.1 del Estatuto... con lo que queda patente la realización de actos "preparatorios" de una competencia desleal"* (FJ 4º).

Si bien la doctrina judicial parte de la presunción de lesividad de la concurrencia, en actividades o análogas, la presunción se destruye cuando el empresario consiente, aunque sea de manera tácita[954].

b) Especialista de confección (STSJ de Cataluña 5 de marzo 2014[955])

La recurrente, especialista de confección, que trabajaba para la marca *Lacoste* es despedida por haber llevado a cabo operaciones de comercio en beneficio propio aprovechándose de las ventajosas condiciones económicas que permitía que los empleados y sus familiares pudieran adquirir las prendas fabricadas y comercializadas, revendía lo que compraba (recoge la carta de despido que se le imputa "*llevar a cabo actos de comercio o venta a terceros de artículos y prenda*s"). De la prueba se desprende incluso la venta de prendas de la firma al propio detective, se somete la medida al principio de proporcionalidad, y se llega a la conclusión por la Sala de lo Social de Cataluña, de que el seguimiento es proporcional pues se llevó a cabo porque existían sospechas fundadas sobre la trabajadora y el seguimiento se limitó únicamente a un par de días.

G) Apropiación de bienes empresariales y gastos indebidos

a) Delimitación

Constituye también un supuesto muy usual. En contra de lo que pudiera pensarse aquí se actúa con independencia del valor de lo sustraído o los servicios indebidamente

---

[953] STS de 5 junio 1990 (RJ 1990\5020).

[954] *Ibídem*.

[955] STSJ de Cataluña de 5 de mayo de 2014 (EDJ 2014/98795).

utilizados. No hay que asociar la presencia del detective con la de una elevada cantidad de dinero pues, lo que se enjuicia respecto a la actuación del trabajador, es la transgresión de la buena fe contractual. En ocasiones son requeridos por presuntas apropiaciones indebidas, que parten de sospechas en determinado turno laboral, o en determinado puesto de trabajo; y el detective viene a confirmar la sospecha que tenía el empleador. En otras ocasiones se les requiere para certificar cómo y de qué manera se emplea el dinero. Lo que suscita más interés para el empresario es el uso que se hace del mismo[956].

Dentro de todas las modalidades posibles (sustracción de dinero, control de gastos y fiscalización de las minutas de kilometraje y manutención, etc.), la actividad del detective debe sustentarse en una sospecha legítima del empresario[957].

b) Limpiador de coches (STSJ Cataluña de 26 mayo 2014[958])

El TSJ resuelve lo que podríamos denominar hurto a través de la "*prueba de la honestidad*". La Sala de lo Social desestima el recurso de suplicación del trabajador, limpiador de coches, y se confirma la procedencia del despido. Como ya venimos afirmando, se exige que los medios de control de la actividad laboral por parte de las empresas sean justificados, idóneos, necesarios y proporcionados para evitar la lesión de los derechos fundamentales del trabajador, como intimidad, honor, propia imagen o dignidad: "*En primer lugar la prueba parte de unos indicios, que no meras sospechas, consistentes en que un cliente reclama en enero de 2012 que le faltan unas monedas de su vehículo tras la limpieza efectuada por la empresa. (HP3ª); en segundo lugar el interés empresarial en el control está justificado y no es de mera conveniencia, por cuanto había recibido ya quejas de clientes por tal razón. En tercer lugar, los medios que se emplean son la grabación por un detective de la imagen en el lugar de trabajo , con el fin de obtener pruebas ante los razonables inicios de infracción laboral, por lo que en tal caso no se vulnera ni la intimidad ni el derecho a la propia imagen del trabajador STSJ Catalunya 22/11/04; en cuarto lugar, el control oculto podría incidir en la dignidad del trabajador y en su derecho al honor, en tanto que integra la reputación profesional que podrían verse afectados por un control oculto dirigido a "testar" su honestidad*."(FJ 2).

---

[956] SEMPERE NAVARRO, A. V. y ARIAS DOMÍNGUEZ, A.: «Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014*), op. cit*., pág. 62.

[957] *Ibídem*, pág. 85.

[958] STSJ de Cataluña de 26 de mayo de 2014 (EDJ 2014/98863).

En definitiva, la admisión como lícita de la prueba de honestidad (en concreto se le introduce dinero en dos coches que debía limpiar) realizada por el detective está condicionada sustancialmente por las circunstancias del caso y por la sumisión de la misma a dos límites claros: el test de proporcionalidad, en tanto se incida los derechos fundamentales del trabajador, y la buena fe.

H) Conclusiones

Como primera conclusión cabe afirmar que el empleo de los detectives constituye una excepción al funcionamiento ordinario de control empresarial que suele hacerse por otro tipo de medios.

La justificación de esta prueba reside en la existencia de indicios de actividad irregular y con los otros diferentes mecanismos de control existentes no será posible llegar a los resultados que puede aportar la prueba del detective. Se concibe así como un último recurso.

Las cuestiones más problemáticas parecen suscitarse respecto al control de los créditos sindicales de los que gozan los representantes de los trabajadores, pues nos encontramos, con el derecho a la libertad sindical que ha de ser objeto de tutela; asimismo ha de ser protegido el derecho construido por la jurisprudencia del representante de los trabajadores a "*no ser sometido a vigilancia singul*ar". Salvo casos muy flagrantes, en esta materia, se suele declarar la nulidad del despido o de la sanción.

La utilización del detective en cada supuesto concreto ha de ponderarse con arreglo al principio de proporcionalidad.

Por la propia idiosincrasia de las materias sobre las que se proyecta la actividad de los detectives: despidos, IT, etc., es infrecuente que haya pronunciamientos sobre unificación de doctrina[959].

En la apreciación de concurrencia desleal, se abarca desde su enunciación básica, que son , recordemos, actos meramente preparatorios, hasta la más singular derivación de clientes en la empresa en la que trabaja el empleado.

[959] SEMPERE NAVARRO, A. V. y ARIAS DOMÍNGUEZ, A. *Detectives en las relaciones laborales. Impacto de la Ley de Seguridad Privada (L5/2014), op. cit.*, pág. 85.

En el análisis de las actividades incompatibles con la IT, se ha de diferenciar entre las que sean laborables en sí mismas (concurrentes y no concurrentes) y otras de ocio, esparcimiento o meramente privadas[960].

Haciendo nuestras las palabras de un sector doctrinal, concluimos afirmando que ante la ausencia de regulación expresa y de criterios del Tribunal Supremo, es aconsejable extremar la prudencia en la adopción de la decisión de recurrir a la vigilancia de detectives, motivándola previamente, reduciendo su ámbito y sabiendo cuál es su valor procesal[961]

2. Sistemas de localización

A) Elementos comunes

Origen.- La caída del llamado "*telón de acero*" y el fin de la Guerra Fría supusieron en el denominado mundo occidental la liberación de muchos efectivos militares, y de los servicios de espionaje oficiales, y, sobre todo, la incorporación de muchas de las innovaciones técnicas empleadas antes para espiar, como el GPS y GMS, que han pasado a usarse en la lucha, principalmente, contra la criminalidad organizada, el terrorismo y las manifestaciones grupales de delincuencia. Pero se han convertido también en posibles métodos de control método del empresario a sus trabajadores[962].

Conflicto de derechos.- Los sistemas de localización pueden colisionar con el derecho a la intimidad. Así el art. 7.2 de la LO de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen considera "*como intromisiones ilegitimas la utilización de aparatos de escucha, dispositivos ópticos o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas así como la grabación , registro o reproducción*", siempre que el titular del derecho no haya otorgado el consentimiento expreso a tal efecto.

---

[960] *Ibídem.*

[961] SEMPERE NAVARRO, A. V. y SAN MARTÍN MAZZUCCONI, C.: «Implicaciones prácticas de la nueva ley de Seguridad Privada», *op. cit.*, pág. 4 del original impreso.
http://www.gomezacebo-pombo.com/media/k2/attachments/implicaciones-practicas-de-la-nueva-ley-de-seguridad-privada.pdf

[962] VELASCO NUÑEZ, E.: «Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías», *Revista de Jurisprudencia El Derecho*, núm. 4,2011 (EDB 2011/112).

Los datos de localización constituyen sistemas de vigilancia emergentes aunque la LOPD no haga referencia a ellos. El art. 2 de la Directiva Europea 20002/58/CE, de 12 de julio de 2002, sobre el tratamiento de datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas, define los sistemas de geolocalización como "*cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público*".

Tipología.- La geolocalización, los sistemas de proximidad y los controles biométricos poseen en común la creación de un fichero de datos[963] en el que se identifica a la persona y en él se incluyen nombre, apellidos y DNI de la misma. De forma genérica, estas bases de datos deben estar sometidas a lo que establece la LOPD, en cuanto al registro del fichero de datos, que ha de estar controlado por la AEPD[964]. Por lo que podemos concluir que los datos de localización constituyen datos personales, y por tanto, son de aplicación las disposiciones la LOPD, aunque no exista alusión expresa. Es más, la definición de datos de carácter personal se basa en la existencia de una información, el dato, que, a su vez, puede vincularse a una persona identificada o identificable, se conoce como la personalización del dato[965].

Conocimiento previo.- En el ejercicio legítimo de sus derechos, el trabajador ha de conocer con antelación que se le va a realizar un control de su actividad a través de las tecnologías instauradas en su empresa de geolocalización, así como la finalidad del mismo. Entre otros extremos, el empresario debe identificar al responsable del fichero, e informar sobre la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Ya existen pronunciamientos al respecto de los tribunales menores, que entienden que es perfectamente extrapolable la doctrina de la STC 29/2013, de 11 de febrero, sobre la aplicación del derecho a la autodeterminación informativa del art. 18.4 CE (que, como sabemos, resuelve un supuesto de prueba videográfica), salvo en los concretos mecanismos de control que de manera expresa se diga que constituyen un

[963] Art. 26.1 LOPD: «Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos».

[964] Informe AEPD núm. 0324/2009.

[965] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op .cit*, pág. 73.

dato personal, pero no se encuentran especialmente protegidos (así sucede con la huella dactilar, como veremos).

Control excesivo.- Las conclusiones alcanzadas por el TC en el supuesto de la STC 29/2013, de 11 de febrero[966], resultaron perfectamente trasladables al sistema de vigilancia por geolocalización, por tanto si una empresa cedía a un trabajador un vehículo o un móvil para que fuera usado por el mismo en el ejercicio de las funciones propias de su trabajo, los datos que se conectasen a su manejo así como a sus desplazamientos y ubicaciones a lo largo de la jornada laboral, no cabe duda que vendrían a reflejar la forma de proceder del trabajador; permitiendo de ese modo conocer una parcela de su vida personal. Eso quedaba indicado como se indica en la Sentencia de la Sala de lo Social del TSJ de Madrid de 21 de marzo de 2014 [967]: "*El permanente conocimiento de parcelas de la vida del trabajador que por muy imbricadas que estén en el desarrollo de la relación laboral con la empresa inciden potencialmente en la esfera de su derecho a la intimidad personal y, de ser objeto de tratamiento como aquí sucede, del que igualmente le asiste a la protección de datos de tal carácter*".

Por lo cual la empresa debía proporcionar la información previa a los trabajadores, afectados por el control, de estos dispositivos de localización, sobre los siguientes aspectos: 1) La instalación de los dispositivos de localización de datos. 2) La finalidad los mismos. 3) Las características y alcance del tratamiento de datos que se iban a realizar; en qué casos los datos de localización podían ser examinados; durante cuánto tiempo y con qué propósitos. 4) Se debía de expresar, de manera muy detallada y precisa qué información podía utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

Se habla en pasado porque esta doctrina entendemos que queda desfasada con la STC 39/2016, pero hasta la fecha no hemos encontrado jurisprudencia sobre despidos disciplinarios basados en la prueba del GPS que la aplique [968].

[966] STC 29/2013, de 11 febrero(RTC 2013\29).

[967] STSJ Madrid de 21 marzo de 2014 (AS 2014\823).

[968] En las últimas sentencias sobre la materia, los recurrentes no plantean un posible conflicto con el art. 18. 4 CE, *vid*. STSJ Madrid de 18 julio de 2016 (JUR 2016\210690) STSJ Islas Baleares de 12 mayo de 2016 (JUR 2016\169106) y STSJ Islas Canarias de 9 mayo de 2016 (JUR 2016\153183).

B) La geolocalización

a) Panorama jurídico

La geolocalización, basada fundamentalmente en los sistemas GPS[969] y GSM[970], transmite de forma constante y activa el posicionamiento actual de un dispositivo, a través de tecnología basada en módulos de satélite independiente, que acota sectores de vigilancia en función de la cobertura que estos tengan.

Los servicios de geolocalización permiten el seguimiento en tiempo real de los objetivos marcados, y facilita su control en circunstancias adversas como la alta velocidad, los trayectos largos, la nocturnidad, etc[971]. Se trata de tecnología de vanguardia que permite ubicar un objeto receptor de señales de radio sobre la superficie de la tierra, gracias a una red de 24 satélites que orbitan el planeta. Al identificar la señal del cuerpo por localizar, desde el punto de vista geométrico, basta contar con los datos de hora y proximidad a tres satélites para encontrar su posición. Con la sincronización de relojes se puede obtener la distancia por triangulación, denominada *trilateración espacial*[972]. La resolución en la ubicación del cuerpo de interés sobre la tierra tiene un margen de error menor a 15 metros[973].

La información sobre la posición geográfica es una tecnología emergente, que ofrece la posibilidad de conocer la ubicación geográfica de una persona y hacerle un seguimiento en tiempo real[974], bien para localizar permanentemente el vehículo usado por el empleado, o al propio trabajador si el dispositivo va insertado en el teléfono móvil que le facilita la empresa. La posibilidad de que esta medida de control afecte a derechos

---

[969] *Global Positioning System.*

[970] *Global System Mobiles.*

[971] VELASCO NUÑEZ, E.: «Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías», *op. cit.*

[972] Método matemático para determinar las posiciones relativas de objetos, usando la geometría de triángulos, de manera análoga a la triangulación, pero en lugar de utilizar medidas de ángulo usa las localizaciones m más conocidas de dos o más puntos de referencia.

[973] ELIZALDE MEDRANO, A., ROJAS RAMÍREZ, J.A, TEJEIDA PADILLA, R. «Medición Sistémica del Desempeño en el Transporte de Carga con GPS», *Revista Científica ConCiencia Tecnológica* núm. 45, 2013, pág. 25.

[974] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos» *op.cit.* pág.20.

fundamentales nos parece evidente, pese a que en realidad lo que se geolocaliza es el objeto en el que se ha instalado el dispositivo[975].

c) Avances técnicos

Los datos de tiempo- localización son una de las fuentes del Big Data más sensibles a la privacidad de los usuarios; por ello tienen una enorme aplicación práctica, además de la oportunidad del uso de grandes volúmenes de datos, traen consigo enormes riesgos para la privacidad y son una enorme fuente creciente de datos[976].

Aplicaciones populares tales como *Foursquare*[977], *Google Places*[978], Facebook Places, etc., registran la posición geográfica en la que se encuentra un usuario en un momento dado. Existen otras que pueden registrar la posición de movimientos, como por ejemplo, la aplicación *Glympse*[979] para *Iphone* y *Ipad*, que permite compartir la posición del usuario a la velocidad que se va moviendo[980].

Hasta la aparición de estos dispositivos, las empresas del sector del transporte solían controlar diariamente las circunstancias de la circulación de su vehículos, respecto a las horas de arranque, parada, duración de la circulación, velocidad, mediante tacógrafos, los cuales poseen una doble finalidad: mejorar las condiciones de trabajo y aumentar la seguridad en carretera. Dicho mecanismo carece de la capacidad de conocer en todo momento la posición del vehículo y tampoco proporciona datos sobre las rutas específicas que va realizando el conductor, por lo que su colisión con el derecho a la intimidad es mínima; además de venir justificado por la normativa europea[981].

---

[975] FERNÁNDEZ GARCÍA, A.: «Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial» *Revista Doctrinal Aranzadi Social* núm. 17, 2010 (BIB 2009/1901)

[976] JOYANES AGUILAR, L.: *Big Data*. *Análisis de grandes volúmenes de datos en organizaciones*, ed. Marcombo Ediciones Técnicas, 2014, págs.36 y 37.

[977] Aplicación con lanzamiento el 11 de marzo de 2009 creada por Foursquare Labs Inc., dentro el género de los servicios de red social, oferta al usuario un servicio basado en localización web aplicada a las redes sociales, basándose en la geolocalización, se obtienen recomendaciones personalizadas de restaurantes establecimientos comerciales, etc. donde los contactos del usuario han estado. *http://foursquare.com*

[978] Directorio gratuito ubicado en *Google Maps* donde se registran las empresas y negocios que a través de la geolocalización conecta directamente con usuarios, posibles clientes.

[979] *App* desarrollada por Apple para compartir la posición GPS con otros usuarios.

[980] JOYANES AGUILAR, L. *Big Data*. *Análisis de grandes volúmenes de datos en organizaciones*, *op.cit.*

[981] FERNÁNDEZ GARCÍA, A. « Sistemas de geolocalización como medio de control del trabajador :un análisis jurisprudencial», *Revista Doctrinal Aranzadi Social* núm. 17, 2010 (BIB 2009/1901)

d) Derechos afectados

Desde la óptica de la regularidad de la obtención de las informaciones del GPS, con el objeto de que puedan servir de prueba en un posible juicio, hay que entender que nos encontramos, en muchos casos, ante datos sensibles de la vida privada (art. 8.1 CEDH), por lo que en algunos países de nuestro entorno se ha optado por una regulación expresa. Así, en Italia, el art. 4 del *Statuto dei lavoratori* exige un acuerdo entre los representantes de los trabajadores para poder usar mecanismos de control a distancia y en caso de que no se llegue a un acuerdo, dirimirá la controversia un Inspector de Trabajo[982].

e) El modelo francés

En Francia se han elaborado unas pautas para el empleo concreto de estos dispositivos de geolocalización, a través de una Recomendación de fecha 16 de marzo de 2006 de la Comisión Nacional de Libertades e Informática. Dicha Comisión estableció que el uso de la geolocalización en los vehículos de los empleados solo puede justificarse para un número justificado de finalidades:

a) Como medida de seguridad del propio empleado o de las mercancías que tiene a su cargo.

b) Para una mejor asignación de los medios que permita cumplir con las prestaciones que deben realizarse en los lugares dispersos.

c) Para el control de la facturación.

d) Para el seguimiento del tiempo de trabajo, cuando este no pueda realizarse por otros medios[983].

e) Pautas de buenas prácticas

La Recomendación CM/rec(2015)5 relativa al tratamiento de datos personales en el entorno laboral[984] se pronuncia sobre este tipo de dispositivos en el apto. 18 donde afirma, respecto a los datos biométricos, que su utilización sólo se permite en el supuesto

---

[982] FERNÁNDEZ GARCÍA, A.: «Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial», *op. cit*

[983] *Ibídem.*

[984] *https://wcd.coe.int/ViewDoc.jsp?id=2306625*

de imposibilidad de utilizar "otros métodos alternativos de tratamiento menos intrusivos para la vida privada" [985].

¿Pero ha de estar localizable y disponible un trabajador las 24 horas del día para la empresa? Es obvio que la tecnología lo permite, pero que tal control lesiona, entre otros, el derecho del trabajador a su descanso. La Recomendación aborda la cuestión en su apto. 16[986], y consiente la utilización estos aparatos pero siempre primando por encima de cualquier otra consideración el derecho del trabajador a su descanso y a no estar siempre disponible. Es decir, derecho a no permanecer controlado de manera permanente por el empleador. Por consiguiente, se acepta la posibilidad de que las empresas puedan contactar permanentemente con sus trabajadores, pero siempre y cuando el control no sea la finalidad principal, "sino únicamente una consecuencia indirecta de la acción tendente a la protección de la producción, la salud, la seguridad o la gestión eficaz de una organización". En su utilización los empleadores deberán mostrarse especialmente cuidadosos con los derechos de los trabajadores, y respetar los principios generales de "minimización y proporcionalidad".

---

[985] 18.1. *The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of employers, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards, including the additional safeguards provided for in principle*.

18.2. *The processing of biometric data should be based on scientifically recognised methods and should be subject to the requirements of strict security and proportionality.*

[986] *16. Equipment revealing employees' location*

16.1. Equipment revealing employees' location should be introduced only if it proves necessary to achieve the legitimate purpose pursued by employers and their use should not lead to continuous monitoring of employees. Notably, monitoring should not be the main purpose, but only an indirect consequence of an action needed to protect production, health and safety or to ensure the efficient running of an organisation. Given the potential to violate the rights and freedoms of persons concerned by the use of these devices, employers should ensure all necessary safeguards for the employees' right to privacy and protection of personal data, including the additional safeguards provided for in principle 21. In accordance with principles 4 and 5, employers should pay special attention to the purpose for which such devices are used and to the principles of minimisation and proportionality.

16.2. Employers should apply appropriate internal procedures relating to the processing of these data and should notify the persons concerned in advance about them.

f) El caso español

En nuestro marco normativo, la necesidad de uso del GPS en determinados vehículos corresponde a una obligación impuesta por el RD 640/2007, de 18 de mayo, por el que se establecen excepciones a la obligación de las normas sobre los tiempos de conducción, descanso y el empleo del tacógrafo en transporte por carretera.

La información que se desprende del GPS puede ser tratable automatizadamente y ello afecta a los arts. 18.1 y especialmente art. 18.4 CE[987]. A este respecto hemos de señalar la ausencia de previsión de este sistema de control laboral en la LOPD, ni existe tampoco a través de instrucción de la Agencia Española de Protección de Datos. Pero sí que existen varias resoluciones de la AEPD respecto a los dispositivos GPS como medida de control laboral, que por su interés con la materia queremos destacar.

g) Criterios de la AEPD

R 1208/2014 de 13 de septiembre de 2016[988].- Con fecha 7 de enero de 2016 tuvo entrada en la AEPD un escrito de denuncia de un representante sindical y secretario general de un sindicato contra el Ayuntamiento de Vigo. Por existir otras actuaciones ya en curso, la presente resolución que cometamos se ciñe a la denuncia efectuada respecto al sistema de geolocalizadores de los vehículos policiales del Ayuntamiento. Con respecto a los sistemas de geolocalización GPS, la AEPD declara lo siguiente: "(…) instalados en los vehículos policiales cabe decir, según manifestaciones al respecto, que por medio de expediente de contrato de servicios el Concejal Delegado de Seguridad y Movilidad autorizó el 17 de abril de 2015 la contratación de un servicio de localización y gestión mediante tecnología GPS de los vehículos de Policía Local, cuya finalidad es la optimización de la función policial mediante la inmediata, eficiente y eficaz asignación de servicios a las unidades móviles en función de su proximidad al lugar demandado y conseguir así una máxima eficacia en protección de la seguridad ciudadana. Asimismo, el sistema cumple una función de autoprotección respecto de las unidades en servicio en

[987] VELASCO NUÑEZ, E.: «Investigación procesal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba electrónica», *Revista La Ley* núm. 8, 2013.

[988] Proc. núm.PS/00593/2016 de la AEPD. Resolución disponible en *http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2016/common/pdfs/E-00593-2016_Resolucion-de-fecha-13-09-2016_Art-ii-culo-6-LOPD.pdf*

la vía pública, permitiendo su constante localización y apoyo en caso de sucesos que pudiesen comprometer la vida o integridad física de los funcionarios actuantes. El sistema permite el acceso al histórico de posicionamiento de los vehículos (sin que consten qué funcionarios los ocupaban) y de la implantación del nuevo sistema se dio cuenta en sucesivas reuniones en el orden del día del Cuerpo".

Por tanto, la AEPD siguiendo el criterio de la citada Instrucción 1/2006, no considera, en el presente caso, que la instalación de geolocalizadores en los vehículos, en los términos expuestos vulnere los principios de calidad, proporcionalidad y finalidad del tratamiento.

R 1208/2014 de 29 de mayo de 2014[989].- En el procedimiento sancionador instruido por la AEPD, esta resuelve estimar la denuncia efectuada por tres ex-trabajadores de una empresa de seguridad que fueron despedidos de manera disciplinaria por los datos que se desprendieron del dispositivo GPS, que se instaló en el vehículo que utilizaban en el trabajo, con ausencia de información previa a los interesados, respecto a su instalación, si bien ese mismo día se puso en conocimiento a los representantes de personal su implantación[990].

En consecuencia, se sancionó a la empresa, a pesar de que la mercantil había esgrimido en su defensa la excepción del art. 6.2 LOPD, que excusa la aplicación de la necesaria comunicación al interesado -que establece el artículo 5 de la LOPD- argumentando que el GPS se instaló no con una función de control horario, sino para detectar deficiencias en el servicio por parte de los denunciantes y otro personal de la empresa, a consecuencia de las quejas manifestadas por un cliente; es decir para realizar "*un seguimiento oculto*" . La AEPD resume su doctrina sobre el GPS, concluye diciendo que al estar ante la presencia inequívoca de datos personales, debe cumplirse el deber de información al afectado, exigido en el artículo 5 de la LOPD. Pero la resolución va más allá y añade, que en base al art. 4.1 LOPD se ha de explicitar la finalidad del uso de esos datos que ha de ser *"determinada, explicita y legítima".*

---

[989] Proc. núm.PS/00558/2013 de la AEPD. Resolución disponible en *http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2014/common/pdfs/PS-00558-2013_Resolucion-de-fecha-29-05-2014_Art-ii-culo-5.1-LOPD.pdf*

[990] Pero con una información un tanto escueta, que decía «*esta empresa ha decidido: 1.- Colocar un dispositivo de localización mediante GPS, en el vehículo de la empresa y que tiene base en el Parque, contratándolo con una empresa especialista en estos dispositivos. 2.- Contratar a una Agencia de Detectives, para que de fe de estos supuestos incumplimientos*».

Respecto al consentimiento, se declara que al estar ante una relación contractual de carácter laboral, esto no es necesario: "*está exceptuado del consentimiento preceptivo del artículo 6 de la LOPD porque en esta ocasión se tratan datos que se refieren a las partes de un contrato de una relación negocial, laboral o administrativa y son necesarios para su mantenimiento o cumplimiento, toda vez que se trata de datos personales de los trabajadores*". Esta excepción, sin embargo no exime del deber de información al sujeto afectado que no se realizó, por lo que se sanciona a la empresa como autora de una infracción leve *ex* art. 44.2.c) de la LOPD: *"El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado"*

Esta Resolución fue recurrida en reposición y confirmada a través de Resolución de la AEPD de 25 de julio de 2014[991], se alegó sustancialmente la empresa que había notificado a los representantes de los trabajadores que iban a ser fiscalizados por GPS, pero la AEPD respondió que se requirió información previa a los propios afectados, por lo que se ratificó en su anterior resolución.

AP/00032/2013 Infracción de la Guardia Civil por no informar instalación GPS en vehículos[992].- La Asociación Unificada de Guardias Civiles en Burgos tuvo conocimiento de que la Dirección General de la Guardia Civil dio orden por la cual se debían de revisar los movimientos realizados por los vehículos oficiales, a través de los datos almacenados por los GPS, al objeto de controlar y vigilar si el servicio de los trabajadores resultaba ser correcto y se habían realizado todas las presentaciones y cometidos asignados, así como si habían permanecido mucho tiempo parados en algún punto.

La Asociación manifestó que no se tenía constancia de que la Dirección General de la Guardia Civil haya informado a los trabajadores sobre dicho control a través de los GPS de vehículos oficiales. Asimismo, se denuncia la carencia de inscripción del correspondiente fichero, donde se almacena la información y, por otro lado, la falta de información a los afectados. Se concede trámite de Alegaciones a la Guardia Civil y ésta

[991] Resolución disponible en: *http://www.agpd.es/portalwebAGPD/resoluciones/recursos_reposicion/rr_sobre_procedimientos_sancionadores/common/pdfs/REPOSICION-PS-00558-2013_Resolucion-de-fecha-25-07-2014_Art-ii-culo-5.1-LOPD.pdf*

[992] Proc. núm. AP/00032/2013 de la AEPD. Resolución disponible en: AEPD.*http://www.agpd.es/portalwebAGPD/resoluciones/admon_publicas/ap_2014/common/pdfs/AAPP-00032-2013_Resolucion-de-fecha-23-01-2014_Art-ii-culo-5.1-LOPD.pdf*

responde que considera que los datos contenidos en los dispositivos GPS no constituyen un tratamiento de datos a los efectos previstos en la LOPD.

Tras la oportuna tramitación, se declara probado por la AEPD que no consta que la Dirección General de la Guardia Civil haya informado previamente a sus trabajadores de que los datos obtenidos a través de los dispositivos GPS instalados en los vehículos oficiales podrían ser utilizados para el control laboral de sus trabajadores. Tampoco consta acreditado que haya informado a sus agentes que los dispositivos GPS recaban datos de carácter personal.

Asimismo, se declara que sí se está ante un tratamiento automatizado de datos de carácter personal porque es posible, sin un esfuerzo desproporcionado, asociar la posición de los vehículos oficiales, su localización, con los miembros de la Guardia Civil que estén haciendo uso de tales vehículos, su identidad. Los dispositivos instalados en los coches oficiales emiten señales que controlan la hora de puesta en marcha y parada, recorrido efectuado, paradas intermedias, lugares exactos de situación y, en definitiva, su localización efectiva, obteniendo así́ por medio de los dispositivos instalados datos del lugar en que se encuentra cada una de las personas.

También advierte la AEPD que en caso de haber previsto que utilizaran los datos personales asociados a los GPS para el control laboral de sus trabajadores, la D. G. de la Guardia Civil deberá́ proceder a informar previamente y de forma fehaciente a sus agentes de este extremo, con el alcance que corresponda, tal y como se establece en la Sentencia del Tribunal Constitucional 29/2013.

En definitiva, se declaró por parte de la AEPD a la Dirección General de la Guardia Civil que ha infringido lo dispuesto en el artículo 5.1 de la LOPD, -tipificada como leve en el artículo 44.2.c) de la citada Ley Orgánica- ¡, se requiere a dicho organismo, para que acredite en el plazo de un mes desde este acto de notificación las medidas de orden interno, que impidan que en el futuro pueda producirse una nueva infracción del artículo 5.1 de la LOPD.

C) Requisitos para la instalación de dispositivos GPS

Tal y como recoge la STSJ de Galicia de 17 de enero de 2014[993]: "*el uso de medios y dispositivos tipo GPS no se pueden considerar ilícitos, pues la empresa tiene un claro interés en tener localizados sus vehículos, lo que no incide en la violación de ningún derecho fundamental*". *A priori* el uso del GPS por parte de la empleadora no es de por si ilícito de manera automática, pero sí lo es en caso de incumplir una serie de requisitos que desglosamos a continuación:

a) Proporcionalidad en el tratamiento de datos de localización

Según el Informe Jurídico de la AEPD núm. 0090-2009[994], la proporcionalidad consagrada en el art. 4.1 de la LOPD, se concreta con respecto a esta tecnología en la necesidad de que el tratamiento de un determinado dato que se desprende el GPS debe ser proporcionado a la finalidad que lo motiva. Por ejemplo, en el caso sometido a esta consulta de la AEPD, la finalidad que ocasiona el tratamiento de datos de localización del escolta es garantizar la seguridad de la persona escoltada, por lo que el principio de proporcionalidad se cumple.

Ahora bien, debe tenerse en cuenta que el tratamiento de los datos de localización fuera del tiempo de la prestación laboral resulta excesivo en relación a la finalidad perseguida, por lo que vulneraría el principio de proporcionalidad y resultaría contrario a la LOPD.

b) Conocimiento previo del trabajador de la instalación del dispositivo GPS

No es preciso el consentimiento del trabajador[995], pero sí el conocimiento del empleado afectado, con respecto a todos los extremos aludidos en el art 5.1 LOPD. Los interesados a los que se les soliciten datos personales deben ser informados de modo expreso, preciso e inequívoco:

---

[993] STSJ Galicia de 6 junio de 2014 (AS 2014\1782).

[994] En el caso que se analiza por la AEPD, se trata de una empresa de seguridad que obtiene datos de localización de los escoltas a través de los teléfonos con el GPS, la geolocalización se considera proporcionada a la finalidad de garantizar la seguridad del escoltado.

[995] Informe Jurídico de la AEPD núm.2009-0090: Proporcionalidad en el tratamiento de datos de localización.

a) De la existencia de un fichero o tratamiento de datos de carácter personal.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.
c) De las consecuencias de la obtención de sus datos o de la negativa a sumunistrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición .
e) De la identidad y dirección del responsable del tratamiento o en su caso de su representante."

En caso de incumplimiento del art. 5.1 LOPD, los datos que emplea la empresa para sancionar tienen un carácter personal y por lo tanto, el haberlos obtenido y utilizado sin el conocimiento del trabajador vulnera la intimidad personal del trabajador, art. 18.1 CE, así como su derecho a la protección de datos personales, art. 18.4 CE.

c) Facultad del trabajador de disponer en todo momento de la información

El trabajador debe conocer en todo momento, así como ha de tener identificado a quien tiene sus datos personales y ha de saber qué finalidad va a someter el control de los mismos. Las obligaciones específicas de información y las autorizaciones necesarias en los casos de tratamiento de datos, se refieren siempre a casos en los que se quiere utilizar la información en cuestión para usos distintos de los inicialmente previstos.

La aplicación de un uso diverso requiere de las correspondientes garantías específicas, en caso contrario, no resultaría válida. Por ejemplo cuando la empresa hubiera comunicado al trabajador sobre la existencia del GPS, pero declaró que la finalidad de su instalación era otra, como por ejemplo, evitar el robo de los coches, no se podría, entonces, utilizar posteriormente la información para sancionar al propio empleado.

A modo de resumen, podemos afirmar que el problema que plantean estos sistemas de localización en el ámbito laboral, deriva de su posible colisión con los derechos fundamentales del trabajador, pues los mismos no sólo ofrecen la posibilidad de ser medios de localización, sino medios de información, los riesgos que comportan para la intimidad son evidentes[996]. Asimismo, para el pleno cumplimiento del derecho a la protección de datos, el trabajador ha de tener la facultad de saber, en todo momento, quién dispone sus datos personales y a qué uso los está sometiendo. Ya que a través del GPS se puede tener el permanente conocimiento de parcelas personales de la vida del empleado y que, aunque conozca y acepte por parte del mismo la existencia del GPS, este complemento de información resultaría indispensable.

[996] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos» o*p.cit,* pág.22.

D) Valoración judicial de la información obtenida mediante GPS

a) Viajes falseados (STSJ de Galicia de 14 de febrero de 2013[997])

Esta sentencia revoca la sentencia de instancia y declara procedente el despido disciplinario del actor, viajante de profesión, por constar que no había realizado en realidad desplazamientos y visitas, que decía haber efectuado. Dicha conducta fue detectada mediante un programa de localización de dispositivos móviles, llamado *Bdlocaliza*[998], que consiste en una aplicación que se descarga en el dispositivo móvil con GPS y transmite cada cierto tiempo su posición.

La Sala de lo Social de Galicia otorga validez a la prueba con el siguiente argumento: "*La empresa realizó un comunicado interno al recurrido que decía que la empresa podrá adoptar las medidas que estime oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales*" (FJ 2º). Sin embargo, consideramos cuestionables dichas razones, ya que los términos de la comunicación al trabajador, resultan en exceso imprecisos y genéricos; entendía que en ellos estaba comprendida la posibilidad de utilizar sistemas de control como el dispositivo GPS. Sin embargo, a nuestro juicio, no puede estimarse que constituya la obligada comunicación al trabajador de la utilización del GPS.

Sorprendentemente, la sentencia, trae a colación la doctrina de la STC 186/2000[999], de 10 de julio, que sabemos que hace referencia a la videovigilancia oculta. El contenido de la misma es reproducido en parte, para concluir con lo siguiente: *"Por tanto, los hechos indicados en la relación fáctica no suponen violación de derechos fundamentales o libertades públicas. El artículo 20.3 del ET señala 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 adopción y aplicación la consideración debida a su dignidad*

---

[997] STSJ de Galicia 14 de febrero de 2014 (AS 2013/906).

[998] *BDlocaliza* es un sistema de localización desarrollado por Ayco y dirigido a sectores en los que es preciso realizar un seguimiento de las personas que forman parte del equipo de trabajo para mejorar la eficiencia del servicio. Según la información corporativa *http://www.bdlocaliza.com/bdlocaliza_y_tu_actividad.php#.U_I_ARYlNow*

[999] STC 186/2000 de 10 de julio (RTC 2000\186).

humana, y el seguimiento establecido por la empresa máxime cuando existe conocimiento previo de los trabajadores o de sus representantes legales, como es el caso " (FJ 5).

c) Encargado de suministros (STSJ de Cataluña de 5 de marzo de 2012[1000])

La Sala de lo Social de Cataluña, desestima el recurso de suplicación entablado por el trabajador ante la sentencia que le había sido denegada en la instancia, y confirma el despido disciplinario de un encargado de suministros, basado en la información de un GPS.

El recurso no prosperó, pues no se tuvo en cuenta que se había alegado por parte del recurrente infracción del derecho a la protección de datos y que la única información previa que recibió fue de carácter muy genérico:

"*Por la presente, le recordamos su deber de cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia, así como de realizar el trabajo convenido bajo la dirección del empresario o persona en quien delegue, y 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 adopción y aplicación la consideración debida a su dignidad humana*" (AH 12º).

Y a este respecto, la Sala declaró de manera que nos resulta llamativa, que dichos datos no revisten el carácter de personales: *"Como dice la STC de 30 de noviembre de 2000 el derecho fundamental a la protección de datos tiene por finalidad garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado.*

La instalación por parte de la empresa de un dispositivo GPS en un vehículo propio que pone a disposición del trabajador para realizar su trabajo con la finalidad de comprobar donde se encuentra el vehículo durante el tiempo en que el trabajador lo utiliza dentro de su jornada laboral, no es propiamente una recogida de datos de carácter personal que pueda afectar a la intimidad del trabajador, sino un medio de vigilancia y control para comprobar que el mismo cumple sus obligaciones laborales, sin que en el presente caso existan indicios de que la empresa haya hecho un uso indebido de los datos obtenidos, más allá de la finalidad perseguida de controlar la jornada laboral del actor"(FJ 2º).

El argumento de la Sala en nuestra opinión resulta bastante cuestionable, ya que dato personal es toda una información que pueda relacionarse con una persona, obviamente los datos del GPS son datos personales, ello deja claro que la lesión del art. 18.4 CE es del todo evidente.

[1000] STSJ de Cataluña de 5 de marzo de 2012, rec. 5194/2011 (EDJ 2012/80659).

d) Monitorización selectiva (STSJ de Andalucía de 15 de julio de 2015[1001])

El TSJ andaluz desestima el recurso de suplicación del trabajador y confirma la procedencia del despido. El uso de medios y dispositivos tipo GPS no se puede considerar ilícitos a pesar de lo que alega el recurrente pues la empresa comunicó la existencia del dispositivo al empleado haciéndole firmar que era conocedor de la monitorización del vehículo. La argumentación del empleado despedido hace suya la doctrina de una sentencia de la Sala de lo Social de Madrid[1002], en la que un trabajador no había suscrito documento en el que daba su conformidad al tratamiento de datos que se desprendían de su GPS. Pero la Sala de lo Social del TSJ con sede en Granada contesta que la conformidad o consentimiento del mismo es irrelevante, argumentando lo siguiente: *"Los datos GPS utilizados son única y exclusivamente los generados por el movimiento del vehículo utilizado por el trabajador solo en jornada de trabajo y a los exclusivos efectos de realizar las funciones propias de la categoría. Cuestión distinta es que implantado el sistema GPS en un vehículo puesto a disposición del trabajador de manera permanente, por ejemplo, en caso de directivos o comerciales, resultara luego que se intentaran hacer valer los datos obtenidos en relación a tramos horarios ajenos a la jornada laboral y a la prestación de servicios. Sin embargo si el sistema GPS se instala en el vehículo asignado precisamente para el desarrollo del servicio y para poder realizar las rutas de vigilancia, entonces no acertamos a discernir cómo puede separarse conceptualmente el control de posición de tal vehículo, de la comprobación del cumplimiento de sus obligaciones por parte del trabajador"*(FJ 2º).

En definitiva, el hilo del razonamiento reside en que la monitorización del vehículo de empresa se realizaba durante la jornada laboral y no era permanente; por tanto, no se revelan datos de la vida privada; por tanto, no incidía en la intimidad; y respecto al derecho a la autodeterminación informativa, no requiere el consentimiento pero sí el conocimiento. El extremo que no queda claro y es el punto débil de la misma, es el alcance de dicho conocimiento del trabajador si se le informó de manera expresa de la finalidad disciplinaria con la que podían usarse los datos que se desprendían del GPS; aspecto que como no se detalla no queda claro si se ha dado cumplimiento al art. 18.4 CE.

[1001] STSJ de Andalucía de 15 de julio de 2015, rec.1.264/2015 (EDJ 2015/159359).

[1002] La Sala contesta que no posee el valor de jurisprudencia a efectos de revisión del derecho aplicado, la STSJ de Madrid de 21 de marzo de 2014 (AS 2014\823) que *ut infra* se comenta.

d) Visitas imaginarias (STSJ de Madrid de 22 de mayo de 2015[1003])

Los antecedentes de hecho de esta sentencia de la Sala de lo Social de Madrid son los siguientes: una empresa en el balance económico de los últimos meses detecta una disminución en el nivel de sus ingresos, sospecha de posibles abusos por parte de sus empleados y decide someter a control GPS la actividad de sus comerciales, comunicándolo previamente a los afectados.

De la fiscalización del vehículo del recurrente se desprende que los tres días que fue objeto de seguimiento, el reporte de visitas que por correo electrónico derivó a la empresa no se correspondían con la información del GPS. El trabajador afectado había declarado un mayor número de visitas a clientes que realmente realizó, por lo que es despedido de manera disciplinaria. En la instancia se desestimó la demanda, el trabajador recurrió en suplicación solicitando la revisión de los hechos declarados probados y cuestionando la validez de la prueba del GPS, interesando su nulidad, a ello se le contesta: "(…) *Se aprecia que teniendo conocimiento el actor de la instalación del sistema de control empresarial a través del GPS, (hecho probado tercero 1), omitió las visitas a una serie de clientes que, sin embargo, anotó como visitados en los partes por él emitidos (hecho probado tercero 4), y demoró el inicio efectivo de su trabajo y el tiempo efectivo dedicado al mismo"* (FJ 3º).

Por tanto, si el trabajador conocía que el vehículo que utilizaba en su trabajo, había estado sometido a control GPS, no cabe ampararse en la nulidad de la prueba del GPS. Si bien es cierto que determinados extremos se desconocen (como si se informó o no de la finalidad del control disciplinario del GPS), pero lo que cabe pensar es que no fueron planteados por el recurrente puesto que se tenía que haber dado respuesta a los mismos. En definitiva, la doctrina de autodeterminación informativa en esta sentencia se aborda de manera muy superficial.

[1003] STSJ de Madrid de 22 de mayo de 2015 (JUR 2015\161186).

e) Vigilante de seguridad (STSJ de Castilla La Mancha 28 de abril de 2015[1004])

Los antecedentes de hecho son los siguientes: un vigilante de seguridad que debía encontrarse de servicio deja su vehículo aparcado y de manera casual por su ruta aparece un superior jerárquico, reconoce el coche aparcado y observa que no hay nadie dentro. Llama por teléfono al recurrente y este sale de una casa que confiesa que es la de unos amigos y a la que había ido a comer. Ante tales hechos se somete a fiscalización el GPS de todos los vehículos de empresa que usaban los trabajadores.

Del GPS del actor y de su compañero de trabajo se desprende que durante sus jornadas no realizaban el itinerario nocturno que debían, por ello los dos empleados son despedidos. En la instancia se declara que se desoyó el mandato de la empresa, que era estar en permanente guardia durante la noche, de manera itinerante, entre las tres estaciones de ferrocarril de ADIF de las que existía la encomienda de velar por la seguridad de las misma, y el mandato de la empresa de visitar cada estación al menos en dos ocasiones por noche. Los datos del GPS revelaron que el vehículo durante muchos días, estaba parado sin circular durante largos intervalos de la noche.

La demanda es desestimada en la instancia, pero posteriormente, la Sala estima el recurso de suplicación del trabajador, pues, aunque el empleado conocía la existencia del GPS, no había sido informado de manera suficiente de la finalidad disciplinaria del control del mencionado dispositivo: "*En el presente caso no existe esa constancia clara y expresa de que se hubiera informado al trabajador, no ya de la instalación del GPS, que cabe deducir que pudiera tener un conocimiento general de ello, sino de la eventualidad de poder ser dicho dispositivo utilizado por la empresa para tener un conocimiento y control de su ubicación, a todos los efectos laborales, incluido sancionadores en su caso. (...) más especialmente, sobre la posibilidad de utilizar los datos que de dicho dispositivo se pudieran obtener, como medio de prueba de alcance disciplinario en contra del trabajador, debe considerarse que la utilización de tal medio probatorio, y los datos obtenidos de ello, lo fueron ilícitamente. Y que por lo tanto, en cuanto fueron obtenidos de modo ilícito, no eran datos que pudieran ser aportados como medio de prueba, al quedar contaminados por ese origen* " (FJ 4º).

Vemos que el aspecto esencial es no haber informado de manera suficiente no sobre la existencia del GPS, sino sobre el uso con fines disciplinarios que se da a la

[1004] STSJ Castilla-La Mancha de 28 de abril de 2015 (EDJ 2015/76914).

información que se desprende de este. En consecuencia, se revoca la sentencia de Instancia, que declaró la procedencia del despido, pues no quedó acreditado lo manifestado en la carta de despido por estar basado en una prueba nula.

Se deduce que no es suficiente, por tanto, cumplir formalmente con una información básica, sino que esta ha de ser completa de manera que el empleado sea consciente de forma plena de lo que implica la fiscalización del vehículo de empresa por un GPS.

f) Vigilante de seguridad (STSJ de Castilla La Mancha 31 de marzo de 2015[1005])

Lo llamativo de esta sentencia es que los antecedentes de hecho son sustancialmente los mismos que los descritos en el apartado anterior, variando la Ponente[1006]. Pero, en lugar de como en aquel caso declararse nula la prueba, en base a la misma doctrina aquí se declara válida y conforme al 18.4 CE. Se sigue la tesis sostenida en la STC 29/2013, de 11 de febrero[1007], a la que menciona expresamente y concluye que la previa información que poseía el trabajador, sobre la existencia de un GPS instalado en su vehículo, hace que no se menoscaben ni restrinjan sus derechos fundamentales, pues "*tenía un cabal conocimiento sobre la finalidad y la utilidad de la información que recababa el dispositivo de localización*".

Sorprende esta argumentación en los Fundamentos de Derecho cuando en los hechos declarados probados esto no se desprende. Por otro lado, se argumenta que aunque el trabajador no había suscrito un documento sobre el tratamiento de datos, (como si sucede en la STSJ de Castilla La Mancha 23 de marzo de 2015[1008], en la que el trabajador expresaba su conformidad), se aplican los mismos razonamientos aquí que en la sentencia aludida y se considera irrelevante la inexistencia del documento del tratamiento de datos del trabajador: *"(…) entendemos que en el caso que ahora se valora, no era necesario un consentimiento específico del trabajador, razón por la cual los datos obtenidos del sistema GPS del vehículo podían utilizarse por la empresa para la comprobación del cumplimiento de los deberes laborales del interesado. En*

[1005] STSJ de Castilla-La Mancha de 31 de marzo de 2015 (EDJ 2015/47653)

[1006] En este caso Gómez Garrido, M.L. y en anterior, Rentero Jover, J.

[1007] STC 29/2013, de 11 febrero (RTC 2013\29).

[1008] STSJ de Castilla-La Mancha de 23 de marzo de 2015 (EDJ 2015/47653).

consecuencia la prueba debió en efecto valorarse, para extraer de ella las consecuencias oportunas." (F.Jº.4º)

Se consideran argumentos suficientes para validar el uso de los datos obtenidos por lo siguiente:1) El hecho de haberse obtenido del GPS solo datos de la jornada de trabajo, y no datos fuera de horario de trabajo, y que estarían relacionados con la vida privada del empleado. 2) El conocimiento de la instalación del GPS, la conducta de la empresa y entender que era legítimo el uso que se hizo del GPS. 3) En este razonamiento resulta irrelevante que exista consentimiento del trabajador para ser sometido a control GPS; aspecto que consideramos acertado. Enfatiza la Sala de lo Social que lo relevante era que el trabajador conociera que su vehículo llevaba un GPS. Podríamos decir que se aplica de manera parcial y sesgada la doctrina de la STC 29/2013 de 11 de febrero[1009]; no se profundiza en el art. 18.4 CE, respecto a la finalidad del uso de la información del GPS con efectos disciplinarios, y no existe pronunciamiento, cuando esto debe considerarse un aspecto esencial.

g) Gestor de cuentas (STSJ de Madrid de 21 de marzo de 2014[1010])

Esta sentencia desestima el recurso de la empresa confirmando la sentencia de instancia que declaró improcedente el despido del actor, gestor de cuentas, por la ilicitud de la prueba en la que se basaban los hechos de la carta de despido, concretamente se declaraban vulnerados los art. 18. 1 CE y 18.4 CE. Cabe destacar la sólida argumentación jurídica de la sentencia, que a lo largo de su dilatada extensión, pasa a realizar un prolijo estudio de la jurisprudencia constitucional y la europea[1011].

Como hechos anteriores destacables a la extinción de la relación laboral, merece mencionarse que tres meses antes de la misma, se procedió a cambiar de coche al trabajador y se le instaló un GPS, meses más tarde se le notificó al actor la política de empresa respecto al uso del vehículo de su propiedad que facilitaba al trabajador, debía

[1009] STC 29/2013, de 11 febrero (RTC 2013\29).
[1010] STSJ de Madrid de 21 de marzo de 2014 (AS 2014\823).
[1011] STEDH de 2 septiembre 2010. Caso Uzun contra Alemania. (JUR 2010\301139).Vigilancia del demandante a través de GPS en el marco de la investigación de diversos delitos de intentos de asesinatos reivindicados por un movimiento terrorista: medida que constituye una injerencia grave en la vida privada del demandante, prevista por Ley, violación inexistente.

ser exclusivamente laboral, y un mes después de esta comunicación recibió otra, manifestándole que en su vehículo se le había instalado un GPS. Los hechos sancionados por la empresa se refieren todos a fechas a anteriores a tener conocimiento el trabajador sobre la presencia del dispositivo GPS. Razona la Sala lo siguiente: "*Como dice el documento aportado por la demandada (…), se trata de sistema de seguridad dirigido a la "localización de vehículos robados" que "localiza, hace seguimiento y recupera tu vehículo ". En otras palabras, nada más lejos de la finalidad para la que, a la postre, se destinó "*(FJ 5º) (…) "*quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida*". (FJ 17º).

La línea argumental de la empresa pivota sobre una misma invocación, los datos en que la empresa se funda para el despido disciplinario no tienen el carácter personal que se les atribuye, sino exclusivamente profesional. A esto la Sala responde que es información que se ubica en la parcela de la intimidad del trabajador: *"(…)Si el vehículo que la demandada cedió al trabajador para uso exclusivamente profesional sólo podía ser utilizado por él y, además, debía permanecer siempre bajo su custodia, mantenimiento y cuidado, cuantos datos se conecten a su manejo y, por ende, a su localización y desplazamientos fuera del centro de trabajo, se proyectan refleja, pero ineluctablemente, sobre la forma de proceder del usuario, que no es otro que el conductor, permitiendo de este modo conocer en todo momento durante su uso parcelas de la vida del trabajador que por muy imbricadas que estén en el desarrollo de la relación laboral con la empresa inciden potencialmente en la esfera de su derecho a la intimidad personal y, de ser objeto de tratamiento como aquí sucede, del que igualmente le asiste a la protección de datos de tal carácter* "(FJ 16º).

También se resalta el rasgo claramente intrusivo del dispositivo GPS en la esfera personal del trabajador: "*Otro tanto cabe decir en el caso de autos en cuanto a los cánones constitucionales de enjuiciamiento del dispositivo de localización utilizado, que en modo alguno supera los juicios de necesidad, idoneidad y proporcionalidad, por cuanto que si lo que quería demostrar la empresa era que algunos días el trabajador no agotó la duración de su jornada laboral, o utilizó en una ocasión para uso propio el vehículo que le había facilitado, o no tenía que haber pasado gastos de comida otros días en que después de comer regresó sin más a su domicilio, se trata de hechos que pudieron ser probados sin ninguna dificultad por otros medios mucho menos aflictivos e intrusivos en la esfera de su intimidad personal y vida privada"*(FJ 21º 6º).

Por tanto, la intrusión es clara ante la ausencia de información previa acerca del uso del GPS, el trabajador no era conocedor de la dimensión de los actos por los que podía ser sancionado; lo que vulneraba su derecho a la autodeterminación informativa.

h) Viajante defraudador (STSJ de Castilla la Mancha de 17 de junio de 2014[1012])

El tribunal resuelve en sentido estimatorio el Recurso de Suplicación del trabajador que fue despedido de manera disciplinaria, declarándolo improcedente y no nulo, como se pedía de manera principal. Porque lo que determina la nulidad es la prueba que consistente en un GPS oculto en el móvil de empresa proporcionado, en la que dicho despido se había basado. La causa no es ajena al contrato de trabajo y se sustenta directamente en la vulneración de un derecho fundamental.

Los antecedentes de hecho son los siguientes: el recurrente vendedor viajante hacía creer que realizaba una serie de visitas presenciales a clientes, detalladas en los partes de trabajo diario que confeccionaba cuando gran número de las mismas no se llevaron realmente a cabo. Tales hechos fueron constatados, pero, a pesar de su gravedad, no deberían ser tenidos en cuenta en base a la doctrina ya marcada por la STC 29/2013 de 11 de febrero[1013]: "*Trasladando dicha doctrina constitucional al caso que ahora se enjuicia, resulta claro que no existió la adecuada información, en los términos de claridad y suficiencia que son exigibles a los efectos de evitar actuaciones sorpresivas, y que en todo caso, no consta la existencia de la expresa autorización del trabajador, que no puede ser objeto de seguimiento durante todos los días de su vida laboral, y tanto durante la jornada como fuera de ella (al no tener prohibida la utilización del teléfono móvil fuera del tiempo de actividad laboral). Intromisión claramente contraria al artículo 18,1 del texto constitucional, y a los demás preceptos orgánicos y sustantivos que han sido mencionados*" (FJ 4º).

Estamos de acuerdo con el sentido del fallo pero enfatizar en el hecho de que el trabajador haya consentido de manera expresa o no lo haya hecho es irrelevante, pues no se infringe con ello la proporcionalidad, como ya ha manifestado al respecto la AEPD. No obstante, este aspecto no debe estar del todo claro pues la STC 39/2016, de tres de marzo[1014], insiste sobre este extremo.

[1012] STSJ de Castilla-La Mancha de 17 de junio de 2014 (EDJ 2014/114292).

[1013] STC 29/2013, de 11 febrero. (RTC 2013\29).

[1014] STC 39/2016, de 3 marzo. (RTC 2016\39).

I) Comercial financiera (STSJ de Madrid de 29 de septiembre de 2014[1015])

El TSJ desestima el recurso de suplicación de la empresa y confirma la improcedencia del despido en la instancia. Los antecedentes de hecho, son los siguientes: la empresa comunicó por escrito, a la parte recurrida, con solicitud de firma como acuse de recibo, un documento que denominó "*de uso de vehículo*", en el que sustancialmente se exhortaba a la trabajadora a realizar una correcta utilización del mismo, únicamente con fines de trabajo, pero no se mencionaba que el vehículo incorporaba un dispositivo GPS. El cometido de su trabajo era visitar estaciones de servicios con el motivo de promocionar la venta de tarjetas VISA. Se la despidió de manera disciplinaria por usar el vehículo para fines particulares, cuando solo se podía utilizar de manera exclusiva para fines profesionales.

La Sala de lo Social, en el FJ 4º, reitera su doctrina ya expresada en su STSJ de 21 de marzo de 2014[1016], anteriormente comentada. La posibilidad de conocer en todo momento, mediante un sistema de geolocalización, que permite un continuo y permanente seguimiento del vehículo cedido al trabajador, durante su uso, no solo posicionamiento de este por razones de seguridad, sino también muestra el lugar exacto en donde se halla y, a su vez, el posterior tratamiento de los datos obtenidos con una finalidad completamente distinta de la anunciada y sin conocimiento del conductor. Las conclusiones extraídas, a merced de este dispositivo tecnológico y su aportación como medio de prueba en sede judicial para demostrar un pretendido incumplimiento contractual, constituyeron un procedimiento que lesiona los derechos fundamentales del trabajador, en concreto la trabajadora no ha cedido de manera expresa su consentimiento para la cesión de sus datos personales, lo cual vulnera su derecho a la autoprotección informativa del art. 18.4 CE.

[1015] STSJ de Madrid de 29 de septiembre de 2014 (EDJ 2014/212693).

[1016] STSJ de Madrid de 21 de marzo de 2014 (AS 2014\823).

J) Repartidor (STSJ Cantabria de 22 de enero de 2016[1017])

La Sala de lo Social desestima el recurso del trabajador que vio denegada su demanda en la instancia. Los hechos probados son los siguientes: un repartidor, que tenía instalado un GPS en el vehículo que conducía y era conocedor de esta instalación, permaneció en los lugares que concretan en la carta de despido sin realizar labores de conductor-repartidor estuvo parado, o bien dentro del coche, o bien visitando a terceros, etc. No obstante, comunicó a la empresa que había realizado visitas que en la realidad eran inexistentes. Por hechos similares ya fue sancionado con anterioridad.

En el recurso de suplicación, la parte recurrente como primer motivo intenta la revisión de los hechos probados de manera infructuosa. Se argumenta también como segundo motivo de suplicación la revisión del derecho aplicado, concretamente alegando infracción de los arts. 54 y 55 ET, dentro de este alegato se impugna, expresamente, la prueba documental basada en GPS, dada la posibilidad de falta de precisión y fiabilidad. Destacan que es un modelo de 2012, pero no sin aportan las especificaciones técnicas del mismo, ni certificación técnica acreditativa de su correcto funcionamiento. La Sala de lo Social de Cantabria contesta que esta apreciación no es controlable en suplicación, sino en la Instancia: "*Sin que pueda ahora revisarse la tecnicidad del GPS (…). Concluyendo el magistrado de instancia, también de forma clara, respecto de lo imputado, que el actor voluntariamente y contra la voluntad empresarial, incumple su obligación de trabajar en los momentos de su jornada que se detallan en la carta, pues no estaba ni conduciendo ni en su reparto ordinario de mercancía.*

En especial, cuando se trata de conductor-repartidor, alejado del control inmediato del empresario, que carece de modo efectivo de otro control que el disciplinario.

Pues si, en modo alguno, precisa la empresa prueba fehaciente en la instancia -que sí precisa el recurrente en suplicación-. Lo acreditado, es la disminución voluntaria del rendimiento, o hechos también calificables (los mismos) como deslealtad o abuso de confianza en las gestiones encomendadas que se le imputa" (FJ 3º).

[1017] STSJ Cantabria de 22 de enero de 2016 (EDJ 2016/4703).

Por todo lo cual, la Sala concluye que tal actitud constituye una deslealtad y una actuación contraria a los especiales deberes de conducta que han de presidir la ejecución de la prestación de trabajo y la relación entre las partes y en consecuencia valida la procedencia del despido declarado en la instancia. No hay constancia de que el trabajador tuviera conocimiento respecto al uso del GPS con fines disciplinarios. Creemos que se debía haber incidido en este extremo y luego, en caso de inexistencia del mismo, plantear una nulidad de la prueba. Por lo que parece que el planteamiento de la parte actora no estuvo del todo acertado.

K) Encargado de mantenimiento (STSJ de Castilla la Mancha de 17 de septiembre de 2015[1018])

La Sala de lo Social de Castilla la Mancha confirma el despido declarado como procedente en la Instancia. A la parte recurrente, que era de profesión encargado de mantenimiento, se le imputó haber abandonado su puesto de trabajo, así como no haber atendido averías que le habían sido notificadas.

Al trabajador se le informa de la colocación en su coche de un GPS; este le permitía a la empresa efectuar un seguimiento exhaustivo del vehículo empleado por él para la ejecución de su trabajo. Pero, un dato importante a tener en cuenta es que no se le había advertido de manera expresa que dicho dispositivo había sido introducido con la finalidad de que los datos que se desprendan del mismo puedan ser usados con fines disciplinarios, que pudieran constituir el fundamento de su despido.

El trabajador planteó dos motivos de recurso, el primero consiste en la revisión de los hechos declarados probados, que se desestima; y el segundo, la infracción del derecho aplicado, al considerar el trabajador demandante que no había transgredido la buena fe contractual, porque la empleadora no acreditó el incumplimiento contractual imputado y que ciertas prácticas que se le imputaban, eran *de facto* toleradas por la empresa. La Sala contesta que se han declarado probadas la existencia de diversas actuaciones por parte del trabajador indicativas de una manifiesta falta grave de cumplimiento de sus obligaciones laborales carente de toda justificación. No se ha acreditado tampoco la existencia de actos

[1018] STSJ Castilla-La Mancha de 17 de septiembre de 2015 (EDJ 2015/237914).

tolerados por parte de la empresa, en relación con los hechos imputados, que pudiera justificar su conducta.

Se desprende de los hechos declarados probados que el trabajador no fue informado de manera suficiente sobre la finalidad de instalación del GPS, por lo que podía haber planteado la nulidad de la prueba y, en consecuencia, que la información que se desprendía del GPS no fuera parte de los hechos declarados como probados. En el supuesto de haberse formulado la petición de nulidad de la prueba por violación del art. 18.4 CE en la instancia, se hubiera obtenido otra clase de pronunciamiento, que probablemente declarara el despido como improcedente.

E) Conclusión

El silencio normativo sobre el uso de las nuevas tecnologías y en concreto sobre los dispositivos GPS provocaba cierta dispersión doctrinal. Pero tras la aparición de la STC 29/2013 la doctrina se unificó en su mayor parte[1019], podemos comprobar la influencia de la sentencia constitucional en la jurisprudencia sobre el uso de los dispositivos GPS, con respecto a la información previa, que fue seguida por las diferentes Salas de lo Social de los TTSSJ. Pero los efectos de la STC 39/2016, de tres de marzo[1020] y las sentencias que bajo su cuestionada doctrina puedan dictarse, hacen temer que se divida la doctrina y los pronunciamientos pasen a ser de variada índole, con la consiguiente inseguridad jurídica que ello supone.

[1019] Pero todo tiene matices, ya en ocasiones, el mero conocimiento de la instalación del GPS por parte del trabajador parecía ser "*una carta en blanco*" para el empresario, para validar una fiscalización sin información suficiente, y todo porque no se profundizaba ni analizaba con detenimiento, doctrina del derecho a la autodeterminación informativa.

[1020] STC 39/2016 de 3 marzo (RTC 2016\39).

6. Sistemas de proximidad (RFID)

A) Delimitación

La identificación por radiofrecuencia es la tecnología que permite la lectura y/o escritura de datos a distancia. Se define como el uso de ondas electromagnéticas radiantes o del acoplamiento del campo reactivo en la porción del espectro correspondiente a las radiofrecuencias, para comunicarse en ambas direcciones con una etiqueta a través de diversos sistemas de modulación y codificación a fin de leer unívocamente la identidad de una etiqueta de radiofrecuencia o de otros datos almacenados en ella[1021]. Por tanto, la RFID permite procesar datos, incluidos los datos personales, a cortas distancias, sin contacto físico, ni interacción visible entre lector y grabador y la etiqueta, de manera que dicha interacción puede producirse sin que la persona se dé cuenta.

Con este sistema se logra un control del cumplimiento del horario de trabajo a través de la dispensación de tarjetas de identificación a los trabajadores que contienen un microchip con los datos identificativos del mismo. Las tarjetas de identificación, se insertan en unos relojes electrónicos situados a la entrada de la empresa, registrándose de esta manera la entrada y salida[1022].

[1021] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: *Control informático, videovigilancia y protección de datos en el trabajo, op .cit*, pág. 72.

[1022] 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». Comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social. AEDTSS. 2014, págs.4-5. *http://www.aedtss.com/images/stories/documentos/XXIV_CONGRESO_NACIONAL/pdf/1.19.pdf*

B) Posible colisión con el derecho a la autodeterminación informativa

La información que se recaba a través de esta tecnología revela datos sobre el comportamiento; esta información puede vincularse a una persona identificada o identificable, a un portador o bien *ad hoc* sobre alguien previamente no identificado[1023].

El Grupo de Trabajo del art.29, recomienda que la tecnología permita al portador del chip desactivarlo fácilmente y que el sistema de transmisión utilice soluciones de criptografía[1024].

La AEPD se ha pronunciado sobre los sistemas RFID recomendando en la *Guía sobre Seguridad y Privacidad de la Tecnología RFID de la AEPD* [1025] que los trabajadores afectados por el uso de estas etiquetas de manera directa o indirecta deben ser informados de la existencia del tratamiento en los términos del art. 5 LOPD; en la información, que ha de ser clara y accesible, se debe indicar el uso de etiquetas, su localización en el producto, la existencia de lectores y si las etiquetas serán objeto de monitorización. Asimismo admite que se incluya una tarjeta del trabajador en su etiqueta identificativa del centro de trabajo, considerándolo pertinente, adecuado y no excesivo en relación con la finalidad, que es la posibilidad de identificarlo mientras por motivos de seguridad desarrolla sus funciones[1026].

Estos mecanismos, tienen su riesgo, respecto a la cesión de datos a terceros, prohibida por la LOPD ya que pueden revelar datos a personas ajenas, pues cabe la posibilidad de que se produzca la pérdida o robo de alguna tarjeta, y alguien la pueda utilizar y llegar a averiguar datos profesionales o identificativos del trabajador afectado, o incluso, si por ejemplo el trabajador lleva encima la tarjeta identificativa de su centro de trabajo, cuando acude a otra empresa, que tenga también el sistema de radiofrecuencia,

---

[1023] LLÁCER MATACÁS, M.R.: «La autodeterminación informativa en la sociedad de la vigilancia: ubiquitous computing» en AA. VV. LLÁCER MATACÁS M.R.: (Coor). *Protección de datos personales en la sociedad de la información y la vigilancia*, ed. La Ley. 2011, pág.65.

[1024] COLIN, C. y POULLET, Y. «Sociedad de la Información y Marketing: Case Study» en AA.VV. LLÁCER MATACÁS (Coor). *Protección de datos personales en la sociedad de la información y la vigilancia.* Ed. La Ley. 2011.Pág.245

[1025] *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_RFID.pdf*

[1026] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C. Las TIC's en el ámbito laboral, *op.cit.* Pág. 66.

se puede realizar una lectura a través de este medio, dando lugar a una pérdida de dominio de los datos personales[1027].

C) Tipología judicial

a) **Director de calidad (**STSJ de Asturias de 27 de marzo de 2015[1028])

Los antecedentes del caso son los siguientes: un trabajador, director de calidad, con casi 30 años de antigüedad, es despedido porque la empresa ha descubierto que en ocasiones no registra su entrada en una máquina RFID situada a la entrada de las instalaciones, sino que lo hace desde su ordenador una vez en su puesto, empleando para ello sus claves personales de acceso al sistema informático de fichajes que le permiten introducir datos en él; claves de las dispone para su cometido laboral de calidad y control de tiempos de producción, pero que usa irregularmente para fines para los que no le fueron facilitadas (eludir el fichaje a la entrada), y de manera fraudulenta, pues se ha comprobado que en esos días en los que registra su entrada no en la máquina de fichaje de la entrada, sino desde su ordenador, en lugar de consignar en el sistema su hora real de entrada, lo que hace es introducir en el mismo una hora próxima a la que debía entrar a trabajar, cuando en realidad, había acudido mucho más tarde, en algunos casos incluso con más de una hora de retraso.

No se impugna el sistema de control de accesos. La versión ofrecida en el recurso como justificación es que se le había concedido la facultad de realizar una jornada inferior a la pactada por la que se le retribuía. Lo cual es contrario a la lógica empresarial, pues ¿qué necesidad tenía, entonces, de falsear los fichajes?

[1027] 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», *op.cit.*, pág.9 del original impreso.

[1028] STSJ Asturias de 27 marzo de 2015 (JUR 2015\109545).

b) Gerocultora (STSJ del País Vasco de 10 de septiembre de 2013[1029])

La Sala de lo Social del País Vasco confirma la sentencia de la instancia, en el sentido de desestimar el recurso de suplicación planteado por la empresa y confirmar la improcedencia del despido, precisamente porque los hechos no se pudieron probar por la poca fiabilidad de los datos que se revelaban del sistema de proximidad. Por esta causa, la posible controversia constitucional ni tan siquiera se plantó.

Los antecedentes de hecho son los siguientes: A la parte recurrida, de profesión gerocultora, se le extingue de manera disciplinaria su contrato. La carta de despido está basada en información obtenida de las tarjetas de radiofrecuencia, consistente en una serie de irregularidades que se le imputaban sobre todo omisiones; pues en base a su plan de trabajo debía ejecutar a lo largo de la madrugada una serie de cambios posturales a ancianos imposibilitados, y no los realizó durante varios días.

El sistema de acceso a cada una de las habitaciones se controlaba con un lector de tarjeta RFID a la entrada de la misma, dicho lector estaba conectado a una placa que se encuentra en el falso techo del pasillo (justo encima de la puerta de la habitación). En caso de pasar una tarjeta con permisos por el lector de tarjetas RFID, se activa un relé que acciona la electrocerradura que da acceso a la habitación.

La Sala de lo Social no asume el resultado que ofrecen los lectores de entrada y permanencia en las habitaciones, al cuestionar los sensores porque existía cierta desconexión o incongruencia en los resultados, que ya se había puesto en evidencia en la sentencia de Instancia y en consecuencia se desestima el recurso y se confirma la resolución del Juzgado de lo Social.

c) Impuntualidades (STSJ de Galicia de 25 de noviembre de 2011[1030])

En esta sentencia, la Sala de lo Social de Galicia confirma el despido disciplinario de un trabajador que a través de los sistemas RFID, la empresa se percató de que accedía al trabajo mucho más tarde de la hora que reflejaba en los partes de trabajo que entregaba

[1029] STSJ del País Vasco de 10 de septiembre de 2013 (JUR 2014\158598).

[1030] STSJ de Galicia de 25 noviembre de 2011 (JUR 2011\427793).

a la empresa, datos que asimismo se habían contrastado mediante prueba videográfica; lo que confirma la procedencia del despido en su día acordado.

CAPÍTULO III. CONTROL DE CONDUCTAS PRIVADAS

1. Plataformas sociales

A) Delimitación

Las redes sociales en línea son servicios basados en la Web que permiten a sus usuarios relacionarse, compartir información, coordinar acciones y, en general, mantenerse en contacto. Estos servicios y aplicaciones representan la red social, permiten la construcción de una identidad digital y facilitan la difusión de actividades en la Red[1031]. Asimismo, no cabe desconocer, la servidumbre que comportan, al exigir como condición de acceso a las mismas el deber de facilitar información personal, datos que pueden revelar información del entorno, la familia, sobre los hábitos, estilos de vida o la salud[1032].

Desde el punto de vista jurídico, una red social ha de definirse como un servicio de la sociedad de la información porque cumple con los cuatro requisitos exigidos por el Anexo de la Ley 34/2002, de 22 de julio, de Servicios de la Sociedad de Información y del Comercio Electrónico, a saber: servicio prestado a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario[1033].

El Dictamen 5/2009, sobre redes sociales en línea[1034], adoptado el 12 de junio de 2009 por el Grupo de Trabajo sobre protección de datos del artículo 29, define los "servicios de redes sociales" como "*plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes*", destacando tres características sobre las mismas: en primer lugar, que el usuario proporciona unos datos personales para generar su perfil o descripción; en segundo lugar, que la red social proporciona al usuario unas herramientas a efectos de que este coloque su propio contenido en línea (fotografías, comentarios, vídeos, enlaces, etc.); en tercer lugar, que el

---

[1031] ORIHUELA COLLIVA, J. L: «Internet: la hora de las redes sociales», *Nueva Revista de Política Cultura y Arte*, núm. 119, 2008, pág. 58.

[1032] GOÑI SEIN, J.L.: «Los límites de las potestades empresariales vs. Derecho a la intimidad de las personas trabajadoras en el entorno de las TIC. El control empresarial en el espacio virtual. Problemática laboral de las redes sociales», *op.cit.*

[1033] DÁVARA RODRÍGUEZ, M.Á.: Manual de Derecho Informático, *op. cit.*, pág. 603.

[1034] *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf*

funcionamiento de las redes se efectúa gracias a la utilización de unas herramientas que proporcionan una lista de contactos para cada usuario con quienes se puede interactuar.

La Web 2.0[1035] ha supuesto una revolución dentro del campo virtual en tanto en cuanto los internautas son los generadores del contenido de la Red[1036], y su carácter abierto hace posible la publicación de información por múltiples personas, tradicionalmente, sin acceso habitual a los medios de comunicación y carentes de los mecanismos de control de estos[1037]. Como poéticamente señalaron los tribunales americanos, en Internet un ciudadano tiene los mismos derechos que el periódico *New York Times*, esa es su grandeza[1038].

Los datos son esclarecedores: Población mundial: 7.210M. Usuarios de Internet: 3.010M (42%). Usuarios de Redes Sociales: 2.078M (29%). En Europa, el 70% de 837M de personas acceden a Internet. Y de éstos, el 46% son usuarios de redes sociales[1039]. Y en España los porcentajes son similares. Con estos datos, no prestar atención a lo que sucede fuera de nuestras organizaciones y no protegerse puede ser temerario. Y es que la irrupción y expansión de las redes sociales ha determinado que surjan múltiples problemas de trascendencia jurídica, que afectan a los diferentes sectores del ordenamiento jurídico, entre ellos, penal, civil y en lo que ahora nos ocupa, laboral.

[1035] Término acuñado por Tim O'Reilly (presidente de O'Reilly Media empresa impulsora de los movimientos de software libre y código abierto) y pronunciado por primera vez en una conferencia organizada sobre *brainstorming* (lluvia de ideas, también denominada tormenta de ideas, es una herramienta de trabajo grupal que facilita el surgimiento de nuevas ideas sobre un tema o problema determinado) del 5 al 7 de octubre 2004 en San Francisco (EEUU).

[1036] Espacio de transformación producido por los cambios en Internet: un sitio Web 2.0 permite a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual.

[1037] Ciertos autores señalan que la Web 2.0 es "*un término con obsolescencia programada*", ya que pronto encontraremos dinámicas 3.0. *Vid.* ROVIRA COLLADO, J.: «Redes sociales en la universidad: profesionales, académicas y de lectura», *Álabe: Revista de Investigación sobre Lectura y Escritura,* núm. 13, 2016, pág. 3.

[1038] MARTÍNEZ, R.: «¿Controlar las redes sociales?» *Actualidad Jurídica Aranzadi*, núm. 886, 2014. (BIB 2014\1805).

[1039] KPMG (2015, 17 de febrero) «Ciberinteligencia en las redes sociales», *http://www.kpmgciberseguridad.es/ciberinteligencia-en-las-redessociales/#sthash.8tiD410i.0eTmbiyM.dpuf*

El hecho cierto es que en los últimos años, las plataformas sociales se han convertido en un fenómeno casi omnipresente. Proporcionan un nuevo escenario donde la inmediatez, la transparencia y el concepto de comunicación aportan nuevas oportunidades para las habituales formas de comunicación[1040]. No solo representan una auténtica revolución por la manera de entender las redes interpersonales sino por el rol que protagoniza el internauta que ha pasado de ser mero sujeto pasivo a ser uno activo[1041]. Todo ello, además, se ha visto reforzado por la aparición de los "*smartphones*" que permiten la conexión a Internet y que multiplican las posibilidades de realizar comentarios a través de las redes sociales en cualquier momento y lugar[1042].

B) Clasificación

Las redes sociales *on line* son muy dispares y presentan muchas diferencias de contenido, desde las que tienen un carácter general, hasta aquellas otras que proporcionan unos contenidos más específicos o concretos[1043]:

a) A través de las primeras, que podrían denominarse como redes sociales de comunicación "*generalistas*" (Facebook, Tuenti o Google +.), los usuarios comparten sus fotografías, videos, reflexiones, aficiones y preferencias de todo tipo.

b) Una segunda categoría podría ser la correspondiente a las redes sociales de comunicación "*especializadas*" en atención a sus contenidos. Al igual que en la anterior se comparten una serie de informaciones vía comentarios, videos o fotografías, solo que hay un hilo argumental determinado (la fotografía, el arte, los viajes, la gastronomía, etc.). Y muy próximas a estas, se encuentran una serie de plataformas que, sin ser exactamente

---

[1040] ORTIZ LÓPEZ, P.: «Redes sociales: funcionamiento y tratamiento de información personal», *Revista Derecho y Redes sociales*, 2013, pág.21.

[1041] BEL ANTAKI, J.: «Redes sociales y su incidencia jurídico laboral en los derechos fundamentales del trabajador», Comunicación al XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social de la AEDTSS 2014: *Los Derechos Fundamentales Inespecíficos en la Relación Laboral y en Materia de Protección Social*, pág. 2 del original impreso. *http://www.aedtss.com/images/stories/documentos/XXIV_CONGRESO_NACIONAL/pdf/1.8.pdf*

[1042] TÁLENS VISCONTI, E.E.: «La libertad de expresión de los representantes de los trabajadores y sus nuevas tecnologías. Su alcance en las redes sociales» Comunicación al Congreso Nacional de Derecho del Trabajo y de la Seguridad Social de la AEDTSS 2014: *Los Derechos Fundamentales Inespecíficos en la Relación Laboral y en Materia de Protección Social*, pág. 1 del original impreso. *http://www.aedtss.com/images/stories/documentos/XXIV_CONGRESO_NACIONAL/pdf/2.11.pdf*

[1043] ORTIZ LÓPEZ, P: «Redes sociales: funcionamiento y tratamiento de información personal», en AA. VV. RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R. (Coords.): *Derecho y redes sociales*, Ed. Civitas-Thomson Reuters, 2013, pág. 24.

redes sociales *on line* , funcionan de un modo muy similar, así twitter o instagram, para imágenes o fotografías.

c) Redes sociales "*profesionales*" y cuyo objeto es facilitar que los individuos puedan encontrar empleo o entrar en contacto con compañeros de profesión u oficio. Aquí, cabe citar a Linkedin.

Una vez creadas por un sujeto o por una entidad, y establecidas sus condiciones de uso, el funcionamiento de unas redes y otras presenta una serie de pautas, más o menos comunes.

C) Trascendencia laboral

Las redes sociales son una herramienta de expresión, para algunos internautas algo incluso indispensable (rozando en ocasiones lo patológico), que crean un perfil bibliográfico personalizado dentro de la comunidad virtual, ello genera que el perfil personal de cada usuario y el modo en que se interactúa, se conviertan en una "*huella digital*", un escaparate del propio ser[1044]. La huella digital es enorme, y eso que sólo acabamos de empezar. Pensemos que el 80% de la población en España no lleva más de 5 años utilizando redes sociales o smartphones[1045], ¿cómo estaremos a este ritmo dentro de 10 o 20 años? Con la cantidad de información que una persona ha podido compartir, consciente o inconscientemente, sobre sí mismo, existen algoritmos capaces de generar patrones sobre su comportamiento, gustos o preferencias, de manera que puedan ofrecerle servicios, productos o experiencias completamente ajustadas a su perfil.

Estos mismos algoritmos que estudian en detalle comportamientos, son capaces de reproducir el siguiente movimiento de manera predictiva, serían capaces de, según las preferencias, escribir el próximo *tuit* o el siguiente estado en facebook, con las gotas adecuadas de inteligencia artificial y la información que se ha ido compartiendo, incluso serían capaces de actuar como el usuario real[1046].

Por otro lado, cada vez es más frecuente la utilización de las redes sociales por parte de la empresa como herramienta de difusión de sus servicios y productos, desempeñando un papel beneficioso para la misma por la rapidez a la que puede llegar la

---

[1044] 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, pág. 53.

[1045] *Ibídem.*

[1046] KMPG (2015, 18 de marzo) «Los límites de la privacidad: mi vida sin mí». http://www.kpmgciberseguridad.es/los-limites-de-la-privacidad-mi-vida-sin-mi/#sthash.ezYbStYB.dpuf

información a un gran número de usuarios. Según el último informe disponible del INE, cerrado a fecha 28 de junio de 2016, el 42,9% de las empresas utilizan alguno de los medios sociales por motivos de trabajo. Los principales usos están dirigidos la presentación de la empresa (89,3%), la declaración de la política de intimidad o certificación de la seguridad del sitio web (69,3%) y el acceso a catálogos y listas de precios (49,8%). El 91,5% de las empresas que usan los medios sociales creen que son útiles en mayor o menor medida para desarrollar su negocio[1047].

Pero si esta utilización de las redes sociales no se encuentra gestionada o regulada correctamente por parte de la empresa, determinados comentarios realizados por sus propios empleados pueden repercutir negativamente en la imagen de la empresa, consiguiendo el efecto contrario del pretendido además de poder suponer una vulneración de la materia en protección de datos o propiedad intelectual, industrial, etc.[1048]. En este punto puede adquirir un papel determinante que la empresa tenga redactado y divulgado entre sus empleados un código de uso sobre la utilización de las redes sociales.

Como tuvimos ocasión de reseñar, la información de los candidatos a un puesto de trabajo, obtenida por la presencia de los mismos en las redes sociales es, en ocasiones, utilizada como criterio de selección, por lo que está incidiendo en la relación laboral, antes incluso de su inicio, y esta información puede de igual modo afectar a su mantenimiento, llegando a fundamentar un despido disciplinario. De ahí que la existencia de las plataformas sociales deba considerarse un hecho de innegable relevancia en la aplicación del Derecho del Trabajo.

Por otro lado, también cabe destacar la óptica penal de las redes sociales, son nuevas formas de socialización que están dando una magnitud diferente de violencia que antes se ejercía por otros procedimientos. El punto débil de las redes es la salvaguardia de la intimidad, porque el usuario publica su información personal, sus fotografías y sus pensamientos en la red. Esto hace al navegante vulnerable a la manipulación, a las infamias y al descrédito. Un caso frecuente es el del individuo que busca el resguardo de las redes sociales para actuar de forma anónima y ejercer este tipo de violencia[1049].

[1047] INE (2016, 28 de Junio) «Encuesta sobre el uso de Tecnologías de la Información y las Comunicaciones (TIC) y del comercio electrónico en las empresas», *op. cit.*

[1048] ARMENTIA MORILLAS, P.: «La importancia de un "Código de uso" de las redes sociales», *Actualidad Jurídica Aranzadi*, núm. 888, 2014 (BIB 2014/2243).

[1049] VARGAS GALLEGO, A. I.: «Nuevas formas de violencia contra las mujeres. Redes sociales. Delitos de descubrimiento y revelación de secretos», *Revista de Jurisprudencia El Derecho*, núm. 2, 2013 (EDB 2013/50).

D) Virtualidad como medio probatorio

a) En general

Un tribunal federal de Richmond, en Virginia, EEUU, declaró que teclear la opción "*me gusta*" en Facebook constituye un acto de libertad de expresión y nadie puede ser despedido como represalia por tal acción[1050] y, por tanto, debe estar amparado por la Primera Enmienda de la Constitución[1051]. ¿Sería ello trasladable a nuestros Juzgados de lo Social? No cabe duda de que estamos ante unos medios probatorios cuya proposición y práctica en el proceso social debe ser admitida, por lo que, en principio, si se consigue probar que la causa del despido fue esa, entendemos que sí.

Uno de los problemas que plantean las redes sociales, es el relativo a la utilización de las publicaciones que en dichos medios aparecen para tratar de demostrar las alegaciones que se formulan en el juicio, esto es, el recurso a las redes sociales como fuente probatoria. Pues bien, en general, el uso de las redes sociales como medio de prueba en el proceso laboral suscita diversas dudas que resulta interesante analizar. Para empezar hay que cuestionar su propia admisibilidad, sobre todo desde la perspectiva de su eventual obtención con violación de derechos fundamentales[1052].

b) En la LRJS

Respecto a la admisibilidad de la práctica de la prueba documental de lo publicado en redes sociales el art. 90 LRJS establece que las partes "*podrán servirse de cuantos medios de prueba se encuentren regulados en la Ley, incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de*

[1050] La sentencia tiene su origen en una denuncia presentada por varios empleados de un sheriff, uno de los cuales señaló que había sido despedido por dar "*Me gusta*" en la campaña del rival de su jefe.

[1051] LÓPEZ ANTUÑA, J.:«Pulsar "Me gusta" en Facebook: despido nulo y riesgos del uso de WhatsApp en la comunicación abogado cliente», *Revista del Consejo General de Graduados Sociales*, núm. 29, 2014, pág. 24.

[1052] NORES TORRES, E.: «La utilización de las redes sociales como medio de prueba en el proceso laboral», *op. cit*., pág.3.

datos", es decir, reconoce en términos muy amplios los medios de prueba utilizables en el proceso laboral y en esta definición se incluyen las redes sociales. Asimismo, a la misma conclusión se llega por la vía del art. 299 LEC, de modo particular a su apartado tercero, cuando reconoce la posibilidad de utilizar "*cualquier otro medio no expresamente previsto en los apartados anteriores*" a través de los cuales "*pudiera obtenerse certeza sobre hechos relevantes*".

Si acudimos analizar la doctrina judicial, comprobamos cómo, de hecho, existen diferentes pronunciamientos judiciales en los que se evidencia su utilización para demostrar diferentes cuestiones y en muy pocos casos se ha cuestionado su admisibilidad: tan es así, que la negativa judicial a su aportación, si bien autónomamente considerada no es susceptible de ser recurrida, salvo en el supuesto excepcional regulado en el art. 90.2 LRJS, puede justificar la interposición de un ulterior recurso contra la sentencia que en su día se dicte basado, precisamente, en el rechazo de este medio probatorio[1053].

Por otro lado, en función de cómo se presente, la misma puede precisar el apoyo instrumental de otros medios de prueba (art. 382 LEC), como el reconocimiento judicial, la pericial informática, testifical o interrogatorio de parte para acreditar la autenticidad de la información y la identidad del autor (si corresponde o no con el titular del perfil) o concretar el lugar y momento de los hechos relatados, o servir a su vez de apoyo a otros medios de prueba, como por ejemplo, la testifical practicada por el detective[1054].

E) Respeto a la libertad de expresión

a) Planteamiento

[1053] NORES TORRES, L.E.: «Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales: aspectos individuales, colectivos y procesales», *Revista de Información Laboral*, núm. 7, 2016 (BIB 2016\4160).

[1054] FERRANDO GARCÍA. F.: «Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías», *op. cit.*, pág. 63.

El centro de trabajo, como lugar en el que la persona desarrolla su actividad laboral, no puede constituir un espacio ajeno o vetado a los derechos y libertades que le son inherentes. Sin perjuicio de la delimitación de sus contornos y la compatibilidad con los de otros sujetos, el trabajador debe poder expresar sus opiniones libremente, como predica el art. 20.1 CE, en tanto no atente contra el honor de la empresa, sus superiores, compañeros o clientes.

Así se ha entendido por los tribunales. En este sentido, la STSJ de Cataluña de 1 de abril de 2014[1055], respecto a las expresiones vertidas sobre la Universidad en la que trabajaba en twitter y en un blog, han de ser valoradas teniendo en cuenta que ejercía el libre ejercicio del derecho a la libertad de expresión e ideológica en cuanto a los llamamientos a la huelga han de ser puestos en relación con ese derecho.

No obstante, el complejo de derechos y obligaciones que genera el contrato de trabajo modula el ejercicio de los derechos fundamentales, puesto que la buena fe en esta relación contractual comporta un límite adicional al ejercicio de la libertad de expresión (STC 241/1999[1056]), las expresiones que en otro contexto pudieran resultar legítimas, no tienen por qué serlo en el ámbito de la relación laboral.

Conforme al art. 7 LO 1/1982, el derecho al honor y a la propia imagen resultan lesionados cuando se obtiene, graba o reproduce información relativa a la vida íntima de las personas, se divulgan hechos de la vida privada de una persona, se divulgan informaciones que difaman a una persona o la hacen desmerecer la consideración ajena, e Internet se vuelve un medio apto para esta divulgación a la que hace referencia dicho artículo, cuando la información se incluye en redes sociales o páginas web[1057].

[1055] STSJ Cataluña de 1 de abril de 2014 (EDJ 2014/104160).

[1056] STC (Sala 2ª) de 20 de diciembre de 1999 (EDJ 1999/40224). Se cuestiona en la demanda de amparo si el ejercicio legítimo del derecho a la libertad de expresión ampara el contenido del escrito que el recurrente remitió al director del hospital en el que presta servicios aquél con ocasión de haber solicitado un permiso horario para asistir a un curso de formación, que fue finalmente denegado. El TC entiende que las manifestaciones del recurrente en el escrito que remitió al hospital con motivo de la denegación de tal permiso, entrañaron una intención vejatoria y ofensiva para el destinatario y para los que con él forman el equipo gestor del hospital referido, por lo que procede desestimar el recurso.

[1057] DE MIGUEL ASENSIO, P.A: «Servicios de la Sociedad de la Información», *Revista de Derecho Privado de Internet*, núm. 1, 2015, pág. 30 (BIB 2015/7).

Como siempre, se ha de buscar el necesario equilibrio entre la libertad de expresión y lo que resulte adecuado conforme a ésta, dentro del marco del contrato de trabajo.

b) Ejercicio del derecho

Las distintas opiniones expresadas en las redes sociales por un trabajador respecto a posibles comentarios relacionados con su trabajo, deben ser interpretadas dentro del contexto en el que han sido vertidas, teniendo en cuenta el plus de gravedad que supone la forma escrita[1058] y la difusión pública de la red social[1059]. Con respecto al ejercicio de la libertad de expresión, por parte de los trabajadores, sirvan a título de ejemplo, las siguientes sentencias.

La **STSJ de Asturias de 31 de marzo de 2016** declara nulo y no improcedente, el despido de un trabajador que utilizó las redes sociales para llevar a cabo una intensa actividad propagandística y de difusión de una reivindicación seguida por los trabajadores de Gijón de la cadena Burger King para que se procediera al abono de los salarios atrasados, en un contexto social de huelga[1060].

La **STSJ de Cataluña de 30 de enero de 2013**[1061] confirma el pronunciamiento de improcedencia de un despido de una trabajadora del Hotel "*W*" de Barcelona que había publicado en su cuenta privada de Twitter un mensaje desvelando la estancia en el citado hotel de lujo de dos famosos personajes del mundo del espectáculo [1062].

c) Extralimitaciones

El ejercicio de la libertad de expresión no puede justificar sin más el empleo de expresiones o apelativos insultantes, injuriosos o vejatorios que exceden del derecho de crítica y son claramente atentatorias para la honorabilidad de aquél cuyo comportamiento

---

[1058] El carácter oral se ha venido justificando por el carácter irreflexivo de las expresiones proferidas de este modo, por el acaloramiento de una situación de conflicto. A *sensu contrario*, los agravios por escrito son realizados con una mayor serenidad y cavilación.

[1059] TALENS VISCONTI, E.E.: «La libertad de expresión en los representantes de los trabajadores y nuevas tecnologías», *op.cit.*, pág. 9

[1060] STSJ Asturias de 31 marzo de 2016 (JUR 2016\86339).

[1061] STSJ de Cataluña de 30 de enero de 2013 (EDJ 2013/45938).

[1062] En concreto Ricky Martín y Justin Bieber.

o manifestaciones se critican[1063] (STC 204/1997[1064]). No existe un "*pretendido derecho al insulto*", en soporte digital, como no cabe admitirlo en papel y el límite se encuentra en la propia dignidad de la persona o empresa de la que se habla.

En este sentido, la **STSJ de Galicia de 23 de febrero de 2012**[1065] confirma el despido de un trabajador que cuelga en la red un vídeo manipulado en el cual se identifica al empleador con la figura de Hitler, la Sala de Galicia declara procedente el despido por el específico ánimo injurioso. Por el contrario, entendemos que no se puede amparar en la libertad de expresión actos contrarios a la buena fe que ha de presidir la relación de las partes.

La **STSJ de Madrid de 26 de septiembre de 2012**[1066]; declara que constituye una deslealtad grave y culpable publicar en una página web un relato parcial y sesgado de una realidad percibida de forma marcadamente subjetiva, con el único objeto de perjudicar, lesionar, agraviar o deshonrar a la empleadora, en un medio de divulgación y difusión pública, de amplio espectro, cual es Facebook, y referido a un archivo en formato *pdf* denominándolo "*Hospital Valdemoro denunciado*" con el comentario adjunto "*Anceraf apoya a este trabajador. Podéis dejarnos vuestros comentarios en Facebook"*.

La **STSJ de 25 de diciembre de 2015**[1067], confirma la decisión de la instancia pues "los comentarios realizados por el actor en la página de Facebook de CGT , que reproduce no están amparados en el derecho a la libertad sindical ni de expresión , ya que constituyen insultos que quedan fuera de esta protección por ser frases y expresiones

[1063] LLUCH CORELL, F.J.: «Las ofensas verbales como causa de despido disciplinario. Respuesta de los tribunales» *Revista de Jurisprudencia El Derecho*, núm. 3, 2005, pág. 6.

[1064] STC 204/1997, de 25 de noviembre (EDJ 1997/8135). Se interpone rec. de amparo contra sentencia que declaró procedente el despido del recurrente por ofensas verbales a la empresa, TVE, y a sus directivos, efectuadas durante unas entrevistas radiofónicas. Para el TC parte de las manifestaciones realizadas por el recurrente, las relativas a la situación del Ente público recurrido y a la actuación de algunos de sus directivos, están amparadas por el derecho a la libertad de expresión; pero hizo también otras declaraciones en las que emitió juicios de valor claramente ofensivos, innecesarios para expresar su opinión sobre los hechos denunciados, y proferidos en descrédito de los directivos y responsables de la empresa, y que no están justificadas, por lo que procede denegar el amparo solicitado.

[1065] STSJ Galicia de 23 de febrero de 2012 (JUR 2012\108833).

[1066] STSJ de Madrid de 20 de diciembre de 2012 (EDJ 2012/320382).

[1067] STSJ de Madrid de de 21 diciembre de 2015 (JUR 2016\41445).

objetivamente ultrajantes y ofensivas innecesarias para narrar lo hechos, ideas u opiniones que se expongan" (FJ 5º).

F) Dudas jurídicas

Son muchas las cuestiones sin resolver alrededor de estos problemas, tanto en general cuanto respecto de su traslación al ámbito laboral.

Por ejemplo se discute sobre el día inicial para cómputo de los plazos de prescripción o caducidad aplicables a las acciones de resarcimiento que entablen los perjudicados. A nivel europeo, el TEDH en su Sentencia de 10 de marzo de 2009[1068], en el caso *Times Newspapers Ltd*[1069] *v. The United Kingdom,* ha considerado que cada transmisión que realiza un usuario de los artículos de un archivo de un periódico digital implica un acto de publicación del mismo[1070]. Por su parte la práctica judicial española, (sirva de ejemplo la SAP de Barcelona de 29 de enero[1071]) inicia el plazo de caducidad del art. 9.5 LO 1/1982 desde la publicación en Internet.

Por otro lado, en relación a una posible indemnización por daño moral en las redes sociales respecto una publicación que pueda suponer una difamación, esta ha de valorarse con arreglo al alcance de la difusión que la misma haya tenido en la Red. La tecnología de Internet puede facilitar el conocimiento del número de usuarios que ha accedido a una determinada información disponible en la malla mundial (con mayor precisión que los lectores de un periódico de prensa escrita) pero el problema son los otros servidores en los que a su vez pueda reproducirse, pues respecto a estos, no es sencillo conocer cuántas veces la información fue copiada y difundida[1072].

[1068] STDH de 10 de marzo de 2009 (EDJ 2009/16021).
[1069] Propietario y editor del periódico *The Times*.
[1070] DE MIGUEL ASENSIO, P.A.: «Servicios de la Sociedad de la Información», *op. cit*., pág. 30.
[1071] SAP Barcelona núm. 30/2014 de 29 de enero. Rec. 421/2013 (EDJ 2014/29531).
[1072] DE MIGUEL ASENSIO, P.A.; «Servicios de la Sociedad de la Información», *op cit*., pág. 31.

G) Derecho a la intimidad

Esta posible colisión no se plantea en todas las redes sociales; así, Twitter o Linkedin tienen un perfil público y, por tanto, disponer de la información que procede de tal perfil no genera este tipo de conflicto.

Un caso diferente lo constituye la red social Facebook. Cierto sector de la doctrina considera que para entender o no lesionado el derecho a la intimidad el elemento determinante reside en las condiciones de uso que haya establecido el titular de la cuenta si es de acceso público o restringido; a saber existen varios niveles de difusión "*público*" en general, "*amigos*", "*amigos de amigos*" o establecer una configuración personal o "*solo yo*". Si el acceso fuera restringido sí existe un derecho a la intimidad que puede resultar lesionado[1073].

Probablemente la clave no reside en la cuestión de tener la cuenta restringida o con un acceso público, sino en el hecho de que quien interactuase sea o no consciente de que está haciendo público un comentario, con independencia de que haya mantenido una cierta privacidad en su cuenta. Recordemos se trata de una plataforma social cuya función esencial es compartir contenidos en la comunidad virtual, con unas características peculiares que suscribe el usuario al abrir y crear su cuenta y por tanto es conocedor de las mismas. Lo único que sí estaría protegido por el derecho a la intimidad y el secreto de las telecomunicaciones serían los mensajes privados a un destinatario concreto[1074].

[1073] LLORENS ESPADA, J. «El uso de Facebook en los procesos de selección de personal y la protección de los derechos de los candidatos», *op.cit.*, págs. 4-5.

[1074] TALENS VISCONTI, E.E.: «La libertad de expresión en los representantes de los trabajadores y nuevas tecnologías», *op.cit.*, págs.. 9-10.

G) Derecho a la autodeterminación informativa

1. La "exención doméstica" (Dictamen del GT29)

El GT29 emitió el 12 de junio de 2009 el Dictamen 5/2009, sobre las redes sociales en línea[1075]. Este documento aborda el funcionamiento de los servicios de redes sociales y la posibilidad de satisfacer las exigencias de la legislación sobre protección de datos de la Unión Europea. En particular, se pone de manifiesto cómo muchos usuarios de las redes sociales se mueven dentro de una esfera puramente personal, entrando en contacto con gente como parte de la gestión de sus asuntos personales, familiares o domésticos.

Según destaca el GT29, la citada Directiva no impone las obligaciones de un responsable de datos a un individuo que procesa datos personales "*en el transcurso de actividades estrictamente personales o domésticas*". Siguiendo este precepto, el GT29 estima que, con carácter general, en la mayor parte de las actividades realizadas por los usuarios de un servicio de redes sociales, debe aplicarse lo que denomina "*exención doméstica*", en lugar de la normativa de protección de datos.

2. Casos al margen de la "exención doméstica"

Existen tres supuestos en los que las actividades desarrolladas en las redes sociales, no estarían cubiertas por la "*exención doméstica*":

1º. Uso de la red social como plataforma de colaboración para una asociación o una empresa.- Si un usuario de redes sociales actúa en nombre de una sociedad o asociación, o utiliza el servidor, principalmente, como una plataforma para conseguir objetivos comerciales, políticos o benéficos, la exención no se aplica.

En este caso, el usuario asume todas las obligaciones de un responsable de datos que está revelando datos personales a otro responsable de datos y a terceros. En estas circunstancias, se necesita el consentimiento de las personas concernidas o algún otro fundamento legítimo dispuesto en la Directiva de Protección de Datos. El GT29 expone

[1075] Adoptado el 12.6.2009 por el Grupo del art. 29 de la Directiva. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/2009/common/wp163_en.pdf*

que los prestadores del servicio de la red social deben garantizar la instauración de configuraciones por defecto gratuitas y que respeten la privacidad, restringiendo el acceso a los contactos seleccionados.

En estas condiciones, cuando el acceso a la información del perfil se amplía hasta más allá de los contactos seleccionados, como cuando se facilita el acceso al perfil a todos los miembros del servicio de la red social o cuando los datos son indexables por motores de búsqueda, el acceso se sale de la esfera personal o doméstica. De igual manera, si un usuario toma una decisión informada de ampliar el acceso más allá de los "*amigos"* seleccionados, las responsabilidades inherentes a un responsable de datos se activan.

2º. Uso de la red social por cualquier persona que utiliza otras plataformas tecnológicas para divulgar datos personales en Internet. Se aplicará el mismo régimen legal que en el supuesto anterior. Aunque la "*exención doméstica*" no se aplique, el usuario de SRS puede beneficiarse de otras exenciones como la exención "*con fines periodísticos o de expresión literaria o artística*". En dichos casos, se ha de llegar a un equilibrio entre la libertad de expresión y el derecho a la privacidad.

3ª. Supuestos en los que es preciso garantizar los derechos de terceros, particularmente en relación con "*datos sensibles*". Son "*datos sensibles*" aquellos que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, la pertenencia a un sindicato o datos relativos a la salud o a la vida sexual. Los datos personales sensibles sólo se pueden publicar en Internet con el consentimiento explícito del sujeto de datos o si el sujeto de datos ha hecho que los datos sean manifiestamente públicos.

El GT29 expone que en algunos Estados Miembros de la UE, las imágenes de los sujetos de datos se consideran una categoría especial de datos personales, ya que se pueden utilizar para distinguir entre orígenes raciales o étnicos o bien que puedan utilizarse para deducir las creencias religiosas o los datos sobre la salud. El GT29, en general, no considera que las imágenes en Internet sean datos sensibles, a menos que éstas se utilicen claramente para revelar datos sensibles acerca de los individuos.

En este sentido, a título ejemplificativo, sirva la Resolución de la AEPD R/00369/2012, de fecha 16 de febrero de 2012[1076], que versa sobre la denuncia de una

[1076]*http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2012/common/pdfs/PS-00434-2011_Resolucion-de-fecha-16-02-2012_Art-ii-culo-6.1-LOPD.pdf*

trabajadora efectuada sobre una publicación de un parte médico suyo en el perfil de Facebook de su empresa[1077].

H) Datos del trabajador compartidos por su empresa

Mención especial debe hacerse al tratamiento de los datos en la red social de los empleados de empresas, la comunicación de datos de los trabajadores por el empleador tanto a la red social como a otros usuarios. Según el Informe 0184/2013 de la AEPD[1078] constituye una cesión de datos de carácter personal definida en el artículo 3. i) de la LOPD como "*toda revelación de datos realizada a una persona distinta del interesado*"[1079].

El Dictamen 8/2001 de 13 de septiembre de 2001[1080], sobre tratamiento de datos personales en el contexto laboral, adoptado por el GT29, en cuanto a la legitimación del tratamiento señala expresamente que por lo que respecta al "*Consentimiento*", el Grupo del artículo 29 considera que si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, no debería legitimar este tratamiento a través del consentimiento. Por el contrario, *"el recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello*". Concluye dicho informe que el consentimiento para la comunicación por

---

[1077] El mencionado parte de incapacidad temporal, contiene su nombre y apellidos, junto con su número de tarjeta sanitaria, número de afiliación a la Seguridad Social, número de DNI y domicilio. Asimismo se incluye el nombre de la empresa y los datos asociados a la baja médica: "*60 días*", "*fecha de baja: 08/09/2010*". La empresa efectuó alegaciones manifestando que desconocía al autor de tal acto, por lo que no podía sancionar a ningún trabajador, eso si no explica, quizás porque no quepa justificación alguna al respecto, los comentarios a la mencionada foto del parte de IT, que realizaron desde el administrador del perfil social de la empresa, jactándose de la posible prolongación de la baja médica se recoge lo siguiente:

"*El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos*".

[1078] El Informe 0184/2013 de la AEPD, recoge la consulta plantea diversas dudas respecto a la aplicación de lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, a la creación de una red social en la que, según señala el consultante, existirán 3 tipos de perfiles (personas físicas, profesionales o autónomos y empresas, que podrán dar de alta a empleados). Señala que en la Red social además de interaccionar unas personas con otras se crean contenidos por parte de los usuarios y empresas (conversaciones, mensajes, debates, consultas, publicaciones, etc.).

[1079] *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2013-0184_Red-social-y-creaci-oo-n-de-perfiles-de-empleados..pdf*

[1080] *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf*

Internet de los datos de sus empleados, no podría entenderse válidamente prestado en el contexto de la relación laboral si su negativa a darlo llevase aparejada algún tipo de consecuencia adversa o discriminatoria, no pudiendo hablarse de consentimiento libre, por lo que la comunicación de los datos de los empleados en Internet no puede ampararse en el consentimiento del trabajador.

De este modo, en cuanto que el consentimiento no vendría a legitimar una cesión de datos de los trabajadores en una red social, habría que examinar si, en cada caso, dicha comunicación forma parte del contrato de trabajo[1081] (por ser precisamente el objeto de dicho contrato como ocurriría, por ejemplo, en el supuesto del trabajador contratado para ser la imagen de la empresa) así como si se ajusta a los principios de protección de datos y en particular al de proporcionalidad, para determinar si la misma es conforme a la LOPD [1082].

El tratamiento de datos sin consentimiento del afectado constituye un límite al derecho fundamental a la protección de datos, pues, son elementos característicos del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos, y en especial aquellos que revisten carácter especialmente sensible. Por lo que se estima vulnerado por la empleadora de la denunciante el artículo 6.1 de la LOPD y la empresa, subsumible en el artículo 44.3.b) de la LOPD como infracción grave.

Por lo que podemos concluir que el empleador no debe usar ningún tipo de dato de sus empleados para "colgarlos" en una red social, porque el consentimiento los trabajadores, no vendría a legitimar una cesión de datos en una red social.

[1081] Esta es también la postura del Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), cuyo considerando 34 recoge lo siguiente: «*El consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal cuando exista un desequilibro claro entre el interesado y el responsable del tratamiento. Así sucede especialmente cuando el primero se encuentra en una situación de dependencia respecto del segundo, por ejemplo, cuando los datos personales de los trabajadores son tratados por el empresario en el contexto laboral*».

[1082]*http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2013-0184_Red-social-y-creaci-oo-n-de-perfiles-de-empleados..pdf*

I) Redes sociales y procesos de selección

1. La experiencia estadounidense

En una época de "*striptease informativo*", en la que las informaciones personales se cuelgan casi sin pudor y se muestran en la Red sin más protección que la que uno decide, en el bienio 2012/2013 doce estados de EEUU aprobaron sus leyes para la protección del acceso a la contraseña en las redes sociales, con el objetivo de prohibir a los empresarios solicitar a los candidatos, e incluso a sus propios trabajadores, la contraseña de acceso a Facebook o Twitter[1083].

La estrategia empresarial estadounidense es siempre sorprendente, es una práctica habitual que para acceder al perfil privado de un aspirante, se solicite durante la entrevista al candidato, que acceda a su cuenta de la red social que use para que el empresario supervise su perfil en su presencia, práctica conocida como *shouldersurfing*[1084], bien solicitar amistad en los perfiles de los virtuales candidatos[1085] o requerir al trabajador para que proceda a modificar la configuración de acceso a su página y en lugar de tenerla privada, configurarla como pública.

El legislador se ha visto obligado a abordar estos excesos, en un intento de evitarlos. Así sucede con el art. 980 del *Labor Code* del Estado de California. Esta norma refiere su aplicación al llamado "*social media*", o redes sociales en una concepción amplia, en el que incluye los servicios y cuentas de correo electrónico, todo tipo de servicios online, y perfiles en sitio web o localizaciones, en una lista que se declara no exhaustiva. En este contexto de manera general[1086], se impone al empleador el deber de no requerir:

[1083] BEL ANTAKI, J.: «Redes sociales y su incidencia jurídico laboral en los derechos fundamentales del trabajador», *op. cit*., pág. 2.

[1084] En seguridad informática "*surfear sobre el hombro*", se refiere a la utilización de técnicas de observación directa , como mirar por encima del hombro de alguien, para obtener información. Se utiliza, comúnmente, para obtener contraseñas, números PIN, códigos de seguridad y datos similares.

[1085] LLORENS ESPADA, J.: «El uso de Facebook en los procesos de selección de personal y la protección de los derechos de los candidatos», *op.cit.* ,pág.12

[1086] Se plantean excepciones realmente relevantes. Primero, cabría este acceso cuando se trate de la investigación de acusaciones de mala conducta del empleado, de una violación de leyes y reglamentos aplicables, a condición de que el acceso se realice para los fines de la investigación o el procedimiento

1) La revelación del usuario y contraseña con la finalidad de acceder a ámbitos personales en redes sociales.
2) Acceder a redes sociales en presencia del empleador.
3) Dar a conocer ámbitos personales en redes sociales[1087].

c) Postura eurocomunitaria

En nuestro continente, el acceso a los datos publicados por los candidatos a un empleo en redes sociales también comporta peligros para las posibilidades de empleo y contratación, lo que ya advirtió el Dictamen 5/2009[1088], sobre redes sociales en línea.

La Recomendación CM/rec(2015) relativa al tratamiento de datos personales en el entorno laboral, señala que el empleador debería evitar solicitar acceso a aquella información que los candidatos compartan *online*, concretamente en redes sociales el apartado 5.3 reza así, los empleadores deberán abstenerse de exigir o solicitar a un trabajador o a un candidato a un empleo "*tener acceso a informaciones que este comparta con otros en línea, en especial en las redes sociales*".

Asimismo, los datos de los candidatos deberían eliminarse en el momento en que se tome la decisión de no contratarlos[1089] aunque será posible conservarlos para futuras convocatorias si se advierte de ello y se permite a los candidatos solicitar la cancelación de sus datos en cualquier momento.

---

correspondiente. También se admite el requerir el usuario y contraseña para acceder a instrumentos electrónicos facilitados por el empresario. Por último, en los casos en los que se protege al empleado frente al control empresarial se prohíbe adaptar medidas disciplinarias ante su negativa o resistencia a revelar datos.

[1087] MARTÍNEZ MARTINEZ, R.: «¿Controlar a los trabajadores?» *Actualidad Jurídica Aranzadi* núm. 864, 2013 (BIB 2013\1209).

[1088] Adoptado el 12-6-2009 por el Grupo del art. 29 de la Directiva. http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/2009/common/wp163_en.pdf

[1089] Art.13.1." *Personal data should not be retained by employers for a period longer than is justified by the employment purposes outlined in principle 2 or is required by the interests of a present or former employee"* . (*Los datos personales de los trabajadores no deben ser retenidos por los empleadores por un período más largo que el de la contratación de acuerdo con lo señalado en el principio 2 o por ser requerimiento por los intereses de un trabajador antiguo o actual).*

d) El caso alemán

En Alemania la influencia de Internet como canal de información de candidatos a un empleo ya se ha dejado sentir a nivel normativo. El 25 de agosto de 2010 se modificó la normativa sobre protección de datos con la aprobación de la conocida comúnmente como la Ley Facebook[1090]. En esta norma se establece que las empresas sólo podrán consultar los datos de candidatos que aparecen en redes sociales profesionales como LinkedIn, pero no podrán consultar los datos de sus empleados o de los candidatos que estén contenidos en redes sociales de uso particular como Facebook.

Con esta regulación se pretende restringir la práctica de buscar en las redes sociales información acerca de candidatos a un puesto de trabajo. Ahora bien, en Derecho la cuestión se reduce con harta frecuencia a la capacidad de poder probar lo alegado, y este es el principal problema que plantea esta modificación; la forma de acreditar en un procedimiento judicial cuándo una empresa ha consultado y tenido en cuenta los datos de una red social.

d) Situación en España

En nuestro país no existe normativa específica al respecto, tan solo el artículo 16. 2 de la Ley de Infracciones y Sanciones en el Orden Social (LISOS)[1091], considera tales actitudes, una infracción muy grave en materia de empleo; está prohibida la solicitud de datos de carácter personal en los procesos de selección, el empleador no puede basar su decisión de declinar una candidatura por la información obtenida en la Red.

Sería recomendable la implantación por parte de las empresas de una política interna respecto al uso de las redes sociales, en las que la empleadora realizara una declaración de intenciones proscribiendo las selecciones discriminatorias en los procesos de selección.

[1090] elpais.com (2010, 27 de agosto) «Alemania prohíbe al jefe buscar datos del empleado en Facebook»
http://elpais.com/diario/2010/08/27/sociedad/1282860003_850215.html

[1091] Reza así: «*Solicitar datos de carácter personal en los procesos de selección o establecer condiciones, mediante publicidad, difusión o por cualquier otro medio, para el acceso al empleo por motivos de sexo, origen, incluido el racial o étnico, edad, estado civil, discapacidad, religión o convicciones, opinión política, orientación sexual, afiliación sindical, condición social y lengua dentro del Estado*».

Pero la realidad es que en la actualidad, los sujetos que intervienen en la colocación de trabajadores (empresas de selección, agencias de colocación, etc.) pueden acceder a datos de los candidatos volcados en redes sociales en Internet que fueran determinantes para su contratación o no contratación. En muchas ocasiones, se producirá una discriminación en el acceso al empleo en virtud de aquellos datos (religión, convicciones, orientación sexual, estado de salud, etc.) sin que el potencial candidato ni siquiera sea consciente de ello[1092]. La red social amplifica el espectro de informaciones que la empresa puede valorar a la hora de tomar su decisión y facilita, por tanto, el camino hacia discriminaciones silenciosas difícilmente combatibles[1093].

J) Las redes sociales como instrumento para la acción colectiva

1. Planteamiento de la cuestión

Los nuevos medios sociales son muy potentes, de ahí que los sindicatos, los utilicen para mantener conversaciones personales y contactos diversos con miles de afiliados, potenciales afiliados y simpatizantes. Los sindicatos ya no pueden limitarse exclusivamente a los medios tradicionales (periódicos, televisión, radio) o las visitas de los sindicalistas a los trabajadores. Los medios tecnológicos permiten una conversación directa sin mediadores, sin importar la distancia o la hora del día o la noche. Los sindicatos pueden utilizar las diversas y eficaces herramientas de medios sociales en red, pero como a todo usuario le es exigible un uso a la vez adecuado para el ejercicio de su función, pero responsable y sometido a las exigencias legales. Herramientas como Facebook y Twitter no deberían ser un elemento secundario[1094].

En este sentido, la web de CCOO, en su gaceta sindical, recoge que la presencia en redes sociales tiene como principales objetivos atraer, convencer, convertir y fidelizar;

[1092] Están prohibidos los ficheros que tengan como finalidad exclusiva almacenar datos que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual (art. 7.4 LPD)

[1093] TASCÓN LÓPEZ, R.: «El trabajo humano (y su derecho) ante el imparable fenómeno de las redes sociales en Internet», *Revista de Trabajo y Seguridad Social*, núm. 340, 2011, pág.143.

[1094] *http://blog.comfia.net/gallery/1/awhite-sindicatos%20y%20redes%20sociales.pdf*

"*incrementar la cultura del trabajo en red en el seno de CCOO en el funcionamiento cotidiano y a través del grupo de ciberactivistas del sindicato*[1095]".

Dentro de este ámbito de las redes sociales, la cuestión a delimitar es si cabe reconocerles un mayor ámbito de intervención a los representantes de los trabajadores por la expresiones vertidas en estas redes, pues si bien se les protege como a cualquier trabajador el derecho a la libertad de expresión, tienen también un plus añadido el derecho a la libertad sindical. Cierto sector de la doctrina, es constante a la hora de afirmar que cuando la libertad de expresión e información se desarrolla por sujetos sindicales, en realidad, nos situamos en el terreno de la libertad sindical. Así, el derecho eventualmente vulnerado será el del art. 28 CE y no el art. 20 CE del cuya invocación será meramente instrumental y quedará subsumida en el primero[1096].

Ante la práctica inexistencia de asuntos que han llegado a los tribunales sobre esta cuestión entendemos ha de aplicarse por analogía la doctrina que ha ido configurándose para resolver otra serie de manifestaciones propias de la actividad sindical: configuración de carteles, reparto de octavillas, etc.

2. Doctrina del TEDH (caso Palomo Sánchez)

Un elemento delimitador por el que comenzar, lo constituye la STEDH de 12 de septiembre de 2011 dictada en Gran Sala, asunto Palomo Sánchez y otros[1097]. Los hechos sucedieron de la siguiente manera: los reclamantes trabajaban como repartidores para una empresa, contra la cual habían interpuesto diversas acciones solicitando que se reconozca la especialidad de sus condiciones laborales. En mayo de 2001 constituyeron un sindicato solicitando ayuda en este sentido.

Dicho sindicato publicaba un folleto mensual, el cual, en abril de 2002 se hacía eco del fallo de una sentencia, que otorgaba parcialmente la razón a los interesados en relación a sus reenvidicaciones, acompañado de una caricatura del director de recursos humanos y varios trabajadores en actitud poco ortodoxa para quejarse del hecho de que

[1095] *http://www.ccoo.es/comunes/recursos/1/pub106003_Gaceta_Sindical_(Edicion_especial_n_176)__CCOO_y_las_redes_sociales.pdf*

[1096] NORES TORRES, L.E.: «Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales: aspectos individuales, colectivos y procesales», *Revista de Información Laboral* núm. 7, 2016 (BIB 2016\4160).

[1097] STEDH de 12 septiembre 2011 (EDJ 2011/195062).

varias de estas personas habían testificado a favor de la empresa. En consecuencia, en junio de 2002 los interesados fueron despedidos por falta grave, por lo que acuden posteriormente ante los tribunales. Se consideraba que no puede considerarse un despido nulo puesto que está basado en una falta grave.

En desacuerdo con este fallo interponen recurso de apelación que es desestimado, interponiéndose recurso de casación. Tras nuevas audiencias, en mayo de 2004, el Tribunal Supremo desestima el recurso. Se acude al Tribunal Constitucional a través de un recurso de amparo, en enero de 2006 es denegado. Los demandantes consideran que la sanción impuesta implica una injerencia en su libertad de expresión, ya que el despido es consecuencia de la publicación del boletín de su sindicato.

El TEDH, recuerda que el art. 10 CEDH exige de una disposición jurídica formulada con precisión para permitir a las personas implicadas prever con claridad las consecuencias de realizar un acto determinado, cosa difícil de conseguir, especialmente en un ámbito tan sensible como es la protección del honor y la reputación de una persona, por lo que a veces es difícil establecer una línea clara y precisa entre informaciones y opiniones. El TEDH debe valorar, además, si la injerencia criticada corresponde a una necesidad social imperiosa, si está en proporción con un interés legítimo y si los motivos alegados por las autoridades nacionales para justificarla son pertinentes y suficientes.

El TEDH entiende que, en este caso, la pena infringida a los demandantes puede entenderse como respuesta a una necesidad social imperiosa, ya que es consecuencia de la protección a intereses legítimos que se persigue, por lo que, teniendo en cuenta la extrema importancia del debate de interés general en el que el litigio se enmarca, la condena debe considerarse proporcionada, desestimando así la violación del art. 10 CEDH interpretado a la luz del art. 11 CEDH.

3. Doctria del TS (caso El Corte Inglés)

En España, nuestro Alto Tribunal en STS de 20 de abril de 2005[1098], estima el recurso de casación para la unificación de doctrina interpuesto por la empresa demandada frente a la sentencia que declaró que los actores estaban ejercitando la libertad sindical y la libertad de expresión y, en consecuencia, sus despidos por tal conducta merecían la

[1098] STS 20 de abril de 2005 (EDJ 2005/83714).

calificación de nulidad. El TS señala que la distribución del folleto sindical por parte de los actores no estaba amparada por el ejercicio de la libertad sindical y de expresión, ya que tal distribución constituyó transgresión del deber de buena fe contractual. La conducta de los recurrentes que originó el litigio y constituye el hecho objeto de enjuiciamiento, fue la distribución "*entre los empleados*" de un "*comunicado de la sección sindical de Madrid de CCOO*" en dos días distintos, en tres establecimientos diferentes de la empresa El Corte Inglés. El comunicado o panfleto sindical distribuido narra en un folio escrito por las dos caras el desarrollo de la concentración reivindicativa convocada por CCOO ante la Fundación Ramón Areces, e invita al final a los lectores, en los términos que luego se verán, a unirse al sindicato a fin de cambiar las condiciones laborales en la empresa.

El comunicado, además de abundar en otras manifestaciones despectivas, incluye las siguientes expresiones, dirigidas a consejeros, vocales, directores de centro, jefes de personal, accionistas y *"demás fauna (que) pasaban ante nosotros*":

> *a) "Mafias fascistas que controlan la empresa".*
>
> *b) "El capo di tutti capi se reunía con la familia para repartir los territorios y los esbirros custodiaban la fortaleza, realmente era una visión de Chicago años 20".*
>
> *c) "Al otro lado estaban los terroristas de cuello blanco que campan a sus anchas por la empresa y que utilizan cualquier medio para seguir manteniendo el estado de terror que impera en la empresa".*
>
> *d) "A los únicos que echamos en falta en el sarao fue a los pistoleros a sueldo de FASGA y FETICO" (siglas de sindicatos con implantación en la empresa).*
>
> *e) "Banda terrorista que es el Corte Inglés". La rúbrica o titular de la hoja distribuida es "Junta de accionistas: demócratas y terroristas"; y la invitación con la que concluye plantea de nuevo la disyuntiva "¡tú decides el bando !: con los demócratas o con los terroristas" (FJ 2º).*

La Sala razona lo siguiente respecto al contenido del comunicado: "*El comunicado o panfleto objeto de enjuiciamiento no contiene una denuncia mínimamente concreta de hechos de relevancia pública, sino una serie de descalificaciones. La consideración de las expresiones descalificatorias incluidas en dicha hoja o panfleto como apelativos insultantes, injuriosos o vejatorios que atentan a la honorabilidad de la empresa y de sus dirigentes y directivos parece fuera de toda duda. Prescindiendo de otros términos despectivos, las calificaciones reiteradas de "mafia" y de "banda terrorista", y la afirmación de imponer o mantener "el estado de terror que impera en la empresa" tienen con seguridad tal carácter.*

Por otra parte, no podemos coincidir con la afirmación de la sentencia recurrida de que la distribución de información sindical convierte a los distribuidores en simples mensajeros de la entidad sindical a los que vendría a ser de aplicación por analogía la doctrina del reportaje neutral. El representante de los trabajadores que está afiliado y es cargo orgánico del sindicato cuya información distribuye no es un mensajero o medio transmisor que actúa por cuenta ajena; efectúa la labor de distribución, sin dejar de ser trabajador de la empresa, en cuanto representante de los trabajadores y en cuanto miembro del sindicato. En cualquiera de estas condiciones está obligado a conocer el contenido de la comunicación difundida (conocimiento que expresamente consta en el caso), y no está facultado para proceder a su distribución cuando incluye apelativos insultantes, injuriosos o vejatorios" (FJ 10º).

Aplicando esta doctrina, conforme con la mantenida también en la STS de 12 de febrero de 2013[1099], la libertad de expresión no es ilimitada, el ejercicio de los derechos

[1099] STS de 12 de febrero de 2013 (EDJ 2013/18827) .

de libertad sindical puede comportar la exigencia de una publicidad especial dirigida a las propias partes del conflicto o a terceros afectados, pero debe ajustarse a los estrictos términos de los derechos e intereses que se debaten, y aunque encajen en ella actos de crítica en sentido amplio, no pueden ampararse los contenidos tendentes a desprestigiar a la empresa; y sin que, a la inversa, quepa justificar actos empresariales desproporcionados que puedan limitar el ejercicio de la libertad de expresión o el de libertad sindical bajo el pretendido amparo del ejercicio de las facultades organizativas del empleador o de la libertad de expresión.

Por lo que podemos concluir que el art. 28.1 CE resulta totalmente aplicable, para estos supuestos, comporta la exigencia de una publicidad especial e incluso en algunos casos, un plus o una mayor permisividad otorgada a los comentarios proferidos por parte de los representantes de los trabajadores[1100].

4. Doctrina judicial (caso Unipost)

Como botón de muestra sirva la STSJ de Murcia de 14 de mayo de 2012[1101], que desestima el recurso de suplicación planteado por la empresa, contra la sentencia de la instancia que declara la nulidad de su despido por vulneración del derecho a la libertad sindical. Los hechos son los siguientes: la actora afiliada al sindicato CGT venía prestando sus servicios para la empresa UNIPOST S.A, desarrollando las tareas propias de conductor, fue despedida por transgresión de la buena fe contractual, por haber difamado a la empresa en Facebook[1102].

[1100] TÁLENS VISCONTI, E.E.:«La libertad de expresión de los representantes de los trabajadores y sus nuevas tecnologías. Su alcance en las redes sociales», *op. cit*., pág. 7

[1101] STSJ de Murcia de 14 de mayo de 2012 (EDJ 2012/131972).

[1102] *"(…) nos darán a todos las cartitas con nuestro nombre de usuario y nuestra contraseña para que la nobleza sepa lo que se cuece en los mentideros. en beneficio para ellos camuflándolo como beneficiosos para nosotros... SEREMOS OBREROS, PERO NO GILIPOLLAS COÑO!!! Y otra cosita, Leandro, en Murcia somos cuatro (literalmente) afiliados a CGT, y el año pasado dos compañeros (no liberados, por supuesto) nos visitaron (de sus días de vacaciones), nos guiaron en cómo y cuándo abrir fuego y además mantienen el contacto telefónico con nosotros preocupados de los temas que nos afectan a todos los compañeros y los que solo afectan a la delegación de Murcia... así que... para mi tiene bastante valor lo que hacen. Ahora cada uno sabrá a que le huele la boca, yo le que se es que a mi jamás me olerá a culo. Salud compañeros"*(HP 4º).

La empresa, tras calificar los hechos constitutivos de un despido disciplinario, al final de la carta, reconoce la improcedencia del mismo, no conforme la trabajadora recurre ante el Juzgado de lo Social, que declara la nulidad del despido, tesis que es avalada por la Sala:

> *"Con independencia del lenguaje utilizado, que es ocioso analizar o calificar respecto de su corrección o incorrección formal, en el fondo, lo que se quiere decir es que se echaba de menos la capacidad crítica, lo que estaría protegido por el derecho de libertad de expresión , al no ser una afirmación insultante.*
>
> *Es por ello que, existiendo suficientes indicios de que la reacción de la empresa fue como consecuencia de que conocía que la trabajadora estaba afiliada al sindicato de CGT y que había sido elegida y designada representante de la Sección Sindical"(FJ 3º).*

4. Facebook

A) Planteamiento

a) Relevancia

Este sitio web de redes sociales constituye un fenómeno mundial tan notorio que no requiere una caracterización previa para poder examinar los problemas que plantea desde la óptica aquí asumida. Por ser la red que tiene mayor tráfico en el mundo, con 130 millones de usuarios, líder en tiempo de uso, los usuarios pasan en Facebook una media de 42 minutos diarios y uno de cada siete minutos que los usuarios de todo el mundo pasan en la Red está dedicado a mirar Facebook[1103]. Y por otro lado, por tener una configuración de la privacidad distinta respecto a las otras redes, merece un estudio diferenciado. Es más, dada su relevancia, el 96,43% de empresas del IBEX 35 publica información sobre sus productos y servicios (los contenidos que generan más interacción con los seguidores son las publicaciones relacionadas con información corporativa y con productos) u ofrece atención al cliente en Facebook[1104].

Esta red permite que cada usuario que se registra pueda construir un pequeño sitio web estandarizado, con varias páginas para colgar documentos, citas, imágenes,

---

[1103] GUREVICH, A.: «El tiempo todo en Facebook». *Aposta Revista de Ciencias Sociales núm. 69, 2016. http://www.apostadigital.com/revistav3/hemeroteca/gurevich.pdf*

[1104] ACED, C. y LALUEZA BOSH, F.: «¿Qué contenidos publican las empresas en los medios sociales? Análisis crítico del discurso de las compañías del IBEX 35 y del Fortune 500 en blogs corporativos, Facebook y Twitter». *Revista Internacional de Relaciones Públicas*, núm.11, 2016.

música, enlaces, etc. La gestión de la privacidad hace referencia a las opciones de configuración que hacen los usuarios en Facebook, para controlar la información que quieren mostrar en su perfil y su visibilidad; como sabemos, las opciones son cuatro: *público*, *amigos*, *sólo yo*, y *personalizado*, en consecuencia, el usuario puede decidir qué partes de ese sitio web quedan abiertos a la lectura pública y qué partes quedan restringidas a las personas a quienes él autorice (llamados "amigos") y en qué partes otras personas, con o sin autorización previa, pueden hacer comentarios o colgar a su vez otros archivos.

A nivel técnico, podemos afirmar que la plantilla de Facebook es compleja; opera y crea significados como uno de los puntos clave del interfaz de Facebook, acumulando e integrando el tráfico online mediante un diseño llamado *Facebook Platform*[1105], cuyo eje es el *Facebook Open Graph protocol*[1106], este sistema de captura es la clave para entender los intereses económicos de Facebook y sus fines comerciales. Esta implementación es automática, y personalizada, esta red permite a su vez otras páginas mejorar su visibilidad recomendando su perfil, su conectividad u otros sistemas. El botón "*me gusta"* y la opción "sigue *a esta página"* son ejemplos clave, los dueños de páginas ajenas a Facebook tienen la posibilidad de generar nuevos flujos de noticias y recomendaciones en el interfaz de aquellas personas que se han registrado en su red social o que le han dado a "*me gusta"* a su página. En este proceso, Facebook aumenta el enfoque y el rango del análisis de datos de los usuarios para monitorear sus actividades y sugerir potenciales estrategias de marketing a las marcas[1107].

[1105] Conjunto de servicios, herramientas y productos proporcionados por Facebook para terceros que acceden a estos datos.

[1106] Plataforma basada en aspectos sociales de los usuarios de Facebook y que puede ser usada por terceros.

[1107] CROGAN, P.:«La automatización y digitalización de la vida cotidiana», *adComunica: Revista Científica de Estrategias, Tendencias e Innovación en Comunicación*, núm. 12, 2016.

http://dx.doi. org/10.6035/2174-0992.2016.12.8

b) Problemas jurídicos

La brevedad temporal que conlleva la aceptación de las condiciones necesarias para crear una cuenta en Facebook y el entusiasmo por poder acceder a los servicios de estas redes sociales hace que no se repare en la cantidad de información de tipo personal que voluntariamente se vuelca. Desde el ámbito de la Psicología Social parece ser que esta cesión gratuita de datos personales se realiza sin tener consciencia de ello y sin ningún tipo de crítica por parte de los usuarios[1108].

La difusión considerable de contenidos que dan a conocer los internautas de Facebook y su descontextualización puede generar consecuencias negativas, como contactos indeseados, divulgación indeseada de información y malentendidos, lo que supone una amenaza a la privacidad[1109].

La fascinación de las redes sociales hace que miles de usuarios regalen información de tipo personal a estas compañías que a su vez venden esos datos a otras empresas a un alto precio (en otras situaciones se habría generado el rechazo de la persona) [1110]; de hecho, las condiciones de Facebook explicitan que las imágenes que se suban a su plataforma se licencian gratuitamente para la red social, pudiendo hacer la empresa un uso comercial de las mismas (se concede una licencia no exclusiva, transferible, con derechos de sub-licencia)[1111].

[1108] MEJÍAS PELIGRO, J.F. y DURÁN SEGURA, M. : «Protección de la privacidad en Facebook: ¿cómo nos ciberprotegemos?» en Aportaciones a la investigación sobre mujeres y género al V Congreso Universitario Internacional Investigación y Género 2014 Sevilla, págs. 893-902. *https://idus.us.es/xmlui/bitstream/handle/11441/41041/Pages%20from%20Investigacion_Genero_14-2-4.pdf?sequence=1&isAllowed=y*

[1109] CHAMARRO LUSAR, A. y BELTRÁN I MARTÍNEZ, A.: «Gestión de la privacidad de los perfiles de Facebook de adolescentes». *Pixel-bit:Revista de Medios y Educación*, núm. 48, 2016. *http://acdc.sav.us.es/pixelbit/images/stories/p48/13.pdf*

[1110] *Ibídem.*

[1111] PASCUAL, A. : «Fotografías e Internet, derechos y deberes». *Actualidad Jurídica Aranzadi*, núm. 914, 2015 (BIB 2015\18231).

En fin, la utilización de estas redes puede ser más o menos intensa y resultar más o menos trascendente, pero, normalmente, va dejando un rastro sobre la identidad del sujeto actuante y su personalidad[1112].

c) Perspectiva de género

Si esta actitud se analiza desde una perspectiva de género; la población femenina suele ser más consciente de los riesgos de aportar información en las redes sociales por lo que su cuenta suele tener una configuración restringida que impide el acceso público, mientras que el sector masculino suele tener un acceso más abierto, pero al mismo tiempo esta población es la que más información privada muestra en los muros de la Red[1113].

Estos patrones de comportamiento entre hombres y mujeres, relacionados con la publicación de información y la protección de su privacidad, en la población española, desprenden resultados similares. Según un estudio realizado en 2014, en la Universidad de Sevilla[1114]:

a) Existen diferencias de género en la lectura de la política de privacidad de Facebook por parte de los usuarios; los resultados pusieron de manifiesto que el porcentaje de hombres que aceptó la política de privacidad de Facebook sin haberla leído previamente era superior al de mujeres[1115].

[1112] NORES TORRES, L.E.: «Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales: aspectos individuales, colectivos y procesales», *op.cit.*

[1113] Estos resultados se han obtenido en estudios realizados fundamentalmente con población estadounidense *vid*. MEJÍAS PELIGRO, J.F. y DURÁN SEGURA, M. «Protección de la privacidad en Facebook: ¿cómo nos ciberprotegemos?», *op.cit.*

[1114] Participaron en este estudio, de manera voluntaria, 190 jóvenes de ambos sexos (68 hombres y 122 mujeres) de entre 20 y 35 años de edad, con una media de edad de 24 años (D.T. = 4.00). Todos los participantes, que manifestaron ser en su totalidad de nacionalidad española, eran usuarios de la red social Facebook. En cuanto a su nivel educativo, el 93% eran estudiantes universitarios, el 3% estaba haciendo un ciclo superior, el 2% un ciclo medio y el 2% cursaban estudios de bachillerato.

[1115] Un total de hombres (71.6%) frente a mujeres (59.8%) que nunca ha leído la política de privacidad de Facebook.

b) Respecto a las conductas dirigidas a proteger la privacidad en la red Facebook; los resultados ponen de manifiesto una frecuencia media superior en la realización de conductas de protección por parte de las usuarias[1116].

B) Incidencia del derecho a la autodeterminación informativa

a) Planteamiento

Las redes sociales son empresas a las que concedemos autorización para disponer de nuestros datos personales que no están radicadas en nuestro país, y las más de las veces tampoco en la Unión Europea, y desconocemos el nivel de protección que la normativa de estos países dispensa a la protección de los datos personales y las razones de seguridad pública o de otra índole que justifican su acceso o utilización por terceros. La confianza de que nuestros datos personales van a ser tratados de una forma segura y únicamente para los fines que justificó su entrega se convierte en una exigencia en nuestros días, no solo porque la protección de los datos personales es un derecho fundamental, sino porque la desconfianza de los usuarios influiría en el uso de las nuevas tecnologías[1117].

Por esta razón, se han establecido normas comunes en la UE para garantizar que los datos personales gocen de un elevado nivel de protección "*equivalente*" en cualquier parte de la Unión. Los ciudadanos tienen derecho de reclamación y de reparación si sus datos son objeto de un uso indebido en cualquier país de la UE[1118]. Pero el problema

---

[1116] Respecto al ítem "*he publicado información personal falsa en mi perfil*" los hombres (M = 2.04) manifestaban haber publicado más información falsa en su perfil que las mujeres (M = 1.60). Respecto al ítem "*soy precavido con las personas que acepto como amigas*", las mujeres informaban ser más precavidas con la gente que aceptan como contactos en Facebook (M = 4.67) que los hombres (M = 4.21). Por último, respecto al ítem "*configuro la privacidad de mi perfil para que solo pueda ser visto por mis amigos*" las mujeres (M = 4.64) utilizan esta medida significativamente más que los hombres (M = 4.05).

[1117] CÓRDOBA CASTROVERDE, D.: «¿Es segura la transferencia de datos personales a EE.UU.?»,*Revista de Jurisprudencia El Derecho*, núm. 1, 2016 (EDB 2016/55).

[1118] A tal efecto, el art. 25 de la vigente Directiva 95/46/CE de 24 de octubre relativa a la protección de datos de las personas físicas establece que la transferencia de datos a un tercer Estado deberá garantizar un "nivel de protección adecuado". La constatación de que un Tercer Estado garantiza un nivel de protección adecuado debe hacerse tanto por los Estados miembros como por la Comisión, y en este último caso, de conformidad con el art. 25.6 de la Directiva, se podrá adoptar una Decisión que, tras la investigación pertinente, constate que el Tercer Estado es seguro a los efectos de transferir los datos, en

trasciende el ámbito de la Unión Europea y se sitúa a nivel mundial, por lo que la normativa europea sobre protección de datos prevé normas específicas para la transferencia de datos personales fuera de la Unión, con el fin de garantizar la mejor protección posible de los datos cuando estos se exporten al extranjero. Pero es posible que acontecimientos sobrevenidos y malas prácticas posteriores evidencien que no se está haciendo un uso adecuado de nuestros datos lo que permitiría a un ciudadano cuestionar la transferencia de sus datos a ese tercer Estado.

b) Exigencias de la UE (caso Safe Harbor)

Estos problemas han sido abordados por la STJUE dictada en Gran Sala de 6 de octubre de 2015[1119], a raíz de una cuestión prejudicial planteada por la High Court de Irlanda, en relación con la transferencia de datos a EEUU de un usuario de Facebook[1120].

cuyo caso pueden transferirse datos personales desde los Estados miembros sin que sea necesaria ninguna garantía adicional

[1119] STDH 6 de octubre de 2015 , Maximillian Schrems contra Data Protection Commissioner. (EDJ 2015/171779).

[1120] Los hechos eran los siguientes: el Sr. Schrems, austriaco residente en Austria, usuario de la red Facebook desde 2008. Toda persona residente en el territorio de la Unión que desee utilizar Facebook está obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos. Los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento. El Sr. Schrems presentó ante el comisario una reclamación en la que le solicitaba en sustancia que ejerciera sus competencias estatutarias, prohibiendo a Facebook Ireland transferir sus datos personales a Estados Unidos. Alegaba que el Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las actividades de vigilancia practicadas en él por las autoridades públicas. El Sr. Schrems hacía referencia en ese sentido a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la National Security Agency. Sin embargo la Comisión había adoptado la Decisión 2000/520, en la que se afirmaba que había quedado constatado que Estados Unidos garantizaba un nivel adecuado de protección, lo que limitaba las posibilidades de control que podía ejercer las autoridades independientes de protección de datos de Irlanda sobre la consideración de EEUU como puerto seguro a efectos de un nivel de protección adecuado.

Esta sentencia invalida el denominado *Safe Harbor*[1121] en relación con las transferencias internacionales de datos realizadas entre Europa y Estados Unidos. Una cuestión que sin duda afecta a gran parte de los responsables de ficheros, entre los que se encuentran aquellos que traten datos en servicios *cloud*, demanden servicios prestados por empresas norteamericanas o transmitan datos a empresas establecidas o participadas por entidades estadounidenses[1122]. Hasta la sentencia, se consideraba que las empresas adheridas a los principios del *Safe Harbor*, ofrecían garantías adecuadas en materia de protección de datos.

Los antecedentes del caso son los siguientes: El tribunal irlandés resuelve una reclamación de un usuario austriaco de Facebook, que pretendía prohibir el trasvase de sus datos a EEUU, ante las noticias que aparecieron en todos los medios sobre Edward Joseph Snowden[1123]. En un determinado momento del proceso, se aprecia que la vigilancia electrónica y la interceptación de los datos personales transferidos desde la UE a EEUU servían a finalidades necesarias e indispensables para el interés público. No obstante, el referido tribunal añade que las revelaciones de Snowden habían demostrado que los organismos federales estadounidenses habían cometido "*importantes excesos*"[1124] por lo que planteó una cuestión prejudicial; cuestiona si un acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de

[1121] Los principios internacionales *safe harbor* (*puerto seguro*) están pensados para prevenir pérdidas o filtraciones no autorizadas de información. Para adherirse al *Safe Harbor*, las empresas debían certificar ante el Departamento de Comercio de Estados Unidos que cumplían con los estándares de protección de datos exigidos por la Unión Europea, debiendo renovar este certificado anualmente. Pensado para organizaciones que operen entre Estados Unidos y la Unión Europea y que alojen datos personales de sus clientes y/o usuarios.

[1122] LÓPEZ CARBALLO, D.: «Safe Harbor: de aquellos polvos, estos barros», *Actualidad Jurídica Aranzadi* núm. 915, 2016 (BIB 2016\486)

[1123] Consultor tecnológico estadounidense, informante, antiguo empleado de la CIA y de la NSA (Agencia de Seguridad Nacional). En junio de 2013, hizo públicos, documentos clasificados como alto secreto incluyendo programas de vigilancia masiva de la NSA llamados *PRISM* y *XKeyscore*, cuyo propósito era permitir a los analistas buscar metadatos, contenido de correos electrónicos, historial de navegación, nombres, números de teléfono, direcciones IP, idioma y ciertas palabras claves de cualquier actividad que se haya realizado en Internet.

[1124] La supervisión de las acciones de los servicios de información se realizaba a través de un procedimiento secreto y no contradictorio. Una vez transferidos los datos personales a Estados Unidos, organismos federales, como el FBI, podían acceder a ellos en el contexto de la vigilancia y de las interceptaciones indiferenciadas que ejecutan a gran escala.

proporcionalidad y a los valores fundamentales protegidos por la Carta de los derechos fundamentales de la Unión Europea[1125].

El problema surgía por la existencia de una Decisión de la Comisión 2000/520 por la que se constataba que EEUU dispensaba un nivel de protección adecuado, por lo que se cuestionaba la validez de la misma a la luz arts.7 y 8 de la Carta Europea de Derechos Humanos. Se preguntaba al Tribunal europeo si la autoridad independiente de control de datos de Irlanda estaba vinculada por la constatación realizada por la Comisión en esa Decisión o bien si el art. 8 de la Carta autorizaba al comisario a separarse, en su caso, de esa constatación y si puede o debe realizar dicho comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520[1126].

La sentencia comentada sienta unos importantes criterios respecto de lo que debe entenderse como el "*nivel adecuado de protección*" que han de proporcionar los terceros Estados a los que se transfieren datos desde la Unión Europea, pueden sintetizarse en los siguientes:

- Al tercer Estado destinatario de los datos personales no es exigible un nivel idéntico de protección al existente en la Unión Europea, pero sí un nivel "*sustancialmente equivalente*" de protección de los derechos y libertades garantizados en la normativa comunitaria, interpretada a la luz de la Carta Europea de Derechos Fundamentales. Este nivel de protección puede ser alcanzado por diferentes medios a los aplicados por el ordenamiento jurídico de la UE.

- Para determinar ese nivel adecuado no solo han de tomarse en consideración la legislación y los compromisos internacionales asumidos por el tercer Estado destinatario de los datos personales, sino también la práctica seguida por ese país para asegurar el cumplimiento de esas reglas.

- Debe realizarse un seguimiento periódico del nivel de protección, incluyendo las circunstancias sobrevenidas a las decisiones en las que se constataba su existencia.

[1125] Y ello por entender que el derecho al respeto de la vida privada garantizado por el art.7 de la Carta y por los valores esenciales comunes a las tradiciones de los Estados miembros quedaría privado de alcance alguno si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que esas prácticas se rodeen de garantías adecuadas y comprobables.

[1126] CÓRDOBA CASTROVERDE, D.: «¿Es segura la transferencia de datos personales a EE.UU.?», *op.cit.*

- Este nivel de protección es exigible no solo a las empresas a las que se transfieren los daños sino también frente a injerencias procedentes de la actividad de las autoridades del Estado.

-No se considera un nivel adecuado de protección el que las autoridades del Estado destinatario puedan acceder de forma generalizada a los datos personales transferidos y a las comunicaciones electrónicas, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido.

- Tampoco respeta ese nivel de protección una legislación que no permite que el ciudadano afectado pueda ejercer acciones para acceder a los datos que le conciernen, su rectificación o supresión[1127].

C) Sanción empresarial por lo publicado

Veamos seguidamente diversos casos resueltos por nuestros Tribunales con un común denominador: la supervisión de la información reflejada en la red social se utiliza por parte de la empresa como forma de probar que el empleado ha transgredido sus obligaciones laborales. En general, consideran lícita la conducta del empleador consistente en utilizar la información y opiniones del trabajador vertidas en las redes sociales o blogs para adoptar medidas disciplinarias contra ellos aplicando el criterio gradualista.

a) Denuncia exagerada (STSJ Murcia 31 marzo 2014)

La STSJ de Murcia de 31 de marzo de 2014[1128] resuelve en sentido contrario al trabajador el recurso planteado por este, confirmando su despido disciplinario. El trabajador, transportista de profesión, publicó en su cuenta de Facebook que su empresa no le abonaba los salarios (en concreto, tres nóminas), y llega a acusar a su jefe de haberlo agredido físicamente, de acosar a los trabajadores y de apropiarse indebidamente el importe de su IT. En tanto en cuanto, estamos ante la falsa imputación al empresario de hechos que constituirían delitos o faltas, la respuesta, no puede tener favorable acogida a

[1127] CÓRDOBA CASTROVERDE, D.: «¿Es segura la transferencia de datos personales a EE.UU.?», *op.cit.*

[1128] STSJ de Murcia de 31 de marzo de 2014(EDJ 2014/58714).

la pretensión del trabajador, puesto que se trata de una clara transgresión de la buena fe contractual:

"El contenido del mensaje de referencia no se limitaba a poner de manifiesto el incumplimiento de la obligación de pago de salarios, sino que acusaba a la empresa de acoso a sus trabajadores, de agresión física por parte de Moisés y de apropiación por parte de la empresa de la prestación por IT . Tales acusaciones, en el presente caso, se producen intencionadamente y no solo afectan a la buena marcha del trabajo, sino también tiene por objeto crear una imagen negativa de la empresa; las imputaciones citadas no solo tienen un contenido injurioso en tanto pretenden menoscabar o degradar la reputación y buen nombre del empresario e, incluso, calumnioso en cuanto contienen una falsa imputación de conducta ilegal, irregular o deshonesta, con independencia de que tales imputaciones puedan tener o no relevancia penal" (FJ 3º).

c) Quejas por impago (STSJ Galicia 23 abril 2014)

La STSJ de Galicia de 23 de abril de 2014[1129] confirma el despido declarado improcedente en la instancia, desestimándose así el recurso de la empresa. La trabajadora fue despedida por causas disciplinarias, imputándosele la publicación en Facebook de hechos falsos y que considera injuriosos para la empleadora.

Las manifestaciones de la trabajadora, en cuenta personal de Facebook, camarera de profesión y en proceso de IT, en ese momento, tenían que ver con un hecho cierto que era que no se abonaba el salario: "*llevo doce años de mi vida entregados y completamente dedicados a ciertos empresarios venidos a menos y su última gran hazaña, no pagarme mi sueldo, porque dicen no tener dinero*". Calificando a sus empleadores de indecentes "*¿acaso se puede caer más bajo*?" *Quizás hablo desde la rabia y la impotencia de tener que seguir trabajando para esos personajes, que no saben lo que es la decencia, que no han sabido, ni saben valorar la dedicación hacia ellos...*" La publicación de estas afirmaciones provocó multitud de comentarios por terceras personas, hasta trascender, finalmente, a la empresa.

La sentencia declara, de forma acertada, que las manifestaciones de la recurrida, están protegidas por el derecho a la libertad de expresión, porque la trabajadora no falta a la verdad cuando habla sobre la falta de abono de los salarios, y las expresiones no revisten la gravedad suficiente para justificar un despido, sino que son fruto de la tensión de la situación de impotencia: impago de nóminas, baja médica, etc.

[1129] STSJ de Galicia de 23 de abril de 2014 (EDJ 2014/126294).

d) Divulgar imágenes de compañeros (STSJ Castilla y León 30 abril 2014)

La STSJ de Castilla y León de 30 de abril de 2014[1130] afronta el recurso de suplicación de una trabajadora. La conducta sancionada fue la difusión por parte de la empleada de unas imágenes propiedad de la empresa, extraídas de sus cámaras de seguridad, y su divulgación en la red Facebook, con la realización de comentarios "*dando así acceso a las mismas a una pluralidad de personas, alguna de las cuales las hizo llegar a la empresa*". Concretamente, eran dos vídeos en los que se recogía como unas compañeras tropezaban y caían al suelo. Se solicita la revisión del derecho aplicado entendiendo infringido el art. 18 en sus apartados 1 y 4 CE y la doctrina de la STC 29/2013, de 11 de febrero[1131]. Hábilmente la Sala contesta:

" (…) *llama poderosamente la atención que la demandante recurra alegando la vulneración de los derechos fundamentales, cuando en realidad ella ha conculcado los de sus compañeras de trabajo, siendo indiscutido el hecho de que las imágenes grabadas aparecían en su cuenta de facebook, habiendo sido extraídas previamente de la cámara de vigilancia de la empresa*.

(…), *difícilmente puede resultar violada la intimidad de una trabajadora que sin autorización de la empresa publica en una red social accesible (...) a múltiples personas las grabaciones de unas compañeras de trabajo en situaciones que pueden resultar perjudiciales para su imagen "* (FJ 2º).

Son tres actitudes las laboralmente sancionables: realizar una copia prohibida, difundirla y hacerlo burlándose de las compañeras. No se entiende que se alegue infracción del derecho a intimidad y a la protección informativa, cuando la recurrente es la que incurre en una vulneración de derechos fundamentales sobre sus compañeros, en definitiva, la viabilidad de la suplicación era prácticamente nula.

[1130] STSJ Castilla y León de 30 de abril de 2013 (AS 2014\1202).
[1131] STC 29/2013, de 11 de febrero (RTC 2013\29).

d) Empleado del Obispado (STSJ Galicia 8 octubre 2014)

La STSJ de Galicia de 8 de octubre de 2014[1132] se pronuncia sobre los siguientes hechos: un trabajador que presta servicios en una casa sacerdotal de la Diócesis de Ourense, publica en Facebook expresiones injuriosas de todo calibre[1133] asegurando haber sido víctima de humillaciones, amenazas y engaños por ser negro e inmigrante. Al trascender tales expresiones y llegar a conocimiento de la empresa el trabajador es despedido.

La Sala de lo Social de Galicia, declara no amparar esta conducta bajo un pretendido derecho a la libertad de expresión, afirma que no es tampoco un argumento válido la configuración privada de su cuenta de Facebook, abierta a amigos:

" Es evidente que la libertad de expresión ampara la crítica, pero no las injurias ni, mucho menos, comportamientos que bien pudieran integrarse en la calumnia; porque lo que el Sr. hace es faltar al respeto debido a su empleadora, lanzando unas duras acusaciones, genéricas invectivas, que lo único que tratan es de desprestigiarla y vulnerar su imagen de cara al público. Integra, pues, una actuación muy grave. (…) y por otra parte, el ánimo del actor no era -empleando una terminología penal- iocandi -que es la propia del ingenio popular-, sino iniuriandi directamente; aparte de que en su «muro» no colgó un dicho, un refrán, un aforismo o una canción, sino afrentas o imputaciones atentatorias contra el buen nombre de su empresaria. Además, no cabe argüir que su cuenta estaba cerrada y sólo abierta a amigos, ya que dicho dato no consta entre los hechos probados" (FJ 4º).

Tras esto, somete la conducta a la teoría gradualista: *"La actuación de las partes ha de ser enjuiciada a la luz de los principios de individualización y de proporcionalidad: a) individualización, en cuanto ha de estarse a las peculiaridades de cada caso sometido a decisión, con sus específicos elementos, entre los cuales cobra especial relieve el factor personal y humano; y b) proporcionalidad, en cuanto ha de establecerse un criterio gradualista para que exista la adecuada coherencia entre las conductas enjuiciadas, la sanción y las personas afectadas"* (FJ 4º).

Finalmente, considera que la calificación del despido ha de ser la de procedente, por cuanto la medida adoptada por el empresario es proporcionada en atención a las condiciones concurrentes y a las expresiones proferidas, aparte del medio empleado de rápida difusión al ser una red social.

[1132] STSJ de Galicia de 8 octubre de 2014 (AS 2014\2738).

[1133] Tales como: "*condenan el homosexualismo y entre sus jerarcas hay pedófilos*", se refiere a "*la perversión de esta religión*", "*viven de las mujeres y otros se van de prostitutas que yo los he visto*", "*es inmoral e ilegal eso hace la iglesia católica romana*", etc.

e) Ofensas a compañero de trabajo (STSJ Cataluña 30 septiembre 2015)

La STSJ de Cataluña de 30 de septiembre de 2015[1134] confirma el despido declarado en la instancia de una trabajadora, auxiliar de enfermería, que dirigió ofensas verbales y escritas a compañeros de trabajo (en concreto, en el transcurso de una jornada de trabajo pidió a un colega de planta hablar "*a solas*" y al negarse este lo llamó, "*tullido*", "*flojo*" e "*hijo de puta*", acto seguido llamó a una compañera de trabajo por teléfono, y al no coger ésta el móvil, comenzó a mandarle whastapp insultándola, e incluso, posteriormente, a la hija de esta por Facebook[1135]). La Sala entiende que la recurrente estaba en un momento de tensión, inmersa en un proceso judicial por mobbing frente a la empresa, y las conversaciones verbales que tuvo en tono subido, pudieron ser fruto del acaloramiento. Pero respecto a los insultos proferidos de manera escrita, estos carecen de toda justificación "*por ir acompañados de una mayor reflexión y comprensión de su alcance y significado, por más que lo fueran a través de medio de comunicación personal"* (FJ 5º) rompieron el clima laboral normal de convivencia y respeto.

Por tanto, la demandante es merecedora de la sanción disciplinaria que corresponde decidir al empresario, por lo que al haber decidido éste la de despido, correctamente declarado procedente por el magistrado de instancia, la Sala no aprecia desproporción alguna.

f) Injuria a mando intermedio (STSJ Cataluña 6 noviembre 2015)

La STSJ de Cataluña de 6 de noviembre de 2015[1136] desestima el recurso de suplicación del trabajador apelante, oficial primera electricista, que fue despedido por trasgredir la buena fe contractual, al injuriar a un mando intermedio de la empresa en el muro de su perfil virtual de una red social. Los antecedentes de hecho son los que siguen: una trabajadora, responsable de obra de la empresa donde prestaba servicios el recurrente, tuvo conocimiento de que estaban publicadas en el muro de Facebook del trabajador

[1134] STSJ de Cataluña de 30 septiembre de 2015 (JUR\2015\281582).
[1135] Tildando de "golfa" a su madre.
[1136] STSJ Cataluña de 6 de noviembre de 2015 (EDJ 2015/231303).

despedido toda clase de ofensas hacía su persona[1137]. Ese mismo día se dirigió a la Jefa de Recursos Humanos poner en su conocimiento lo publicado, entrando en su Facebook y constatando que dicha publicación seguía expuesta. Al día siguiente el empleado fue llamado por Recursos Humanos, admitiendo que tenía expuesta dicha publicación y por ello fue despedido. La empleada injuriada, denunció por la vía penal y se dictó sentencia condenando al demandante como responsable de una falta de injurias.

Se solicita la revisión de los hechos probados que se desestima, también se solicita la revisión del Derecho aplicado, el recurrente sostiene que el pantallazo de su perfil de Facebook, ha podido ser manipulado por la empresa, a lo que la Sala contesta:

> *"Son ya numerosos los casos en los que la doctrina judicial del orden social acepta como medio válido de prueba las publicaciones de empleados en redes sociales. Prueba que es válida en el presente caso, pues no consta que se haya obtenido de manera ilícita, sin que exista prueba alguna de falseamiento o manipulación de la publicación por parte de la empresa. La parte actora pudo presentar prueba pericial técnica al respecto. (...)En todo caso, esta alegación de falsedad no casa con el hecho de que el actor reconociera ante la Jefa de Recursos Humanos tener expuesta dicha publicación en Facebook" (FJ 3º).*

g) Instar cambios en la política de contratación (STSJ Madrid 15 enero 2016)

La STSJ Madrid de 15 enero de 2016[1138] estima el recurso de una empresa aérea en el sentido de revocar la nulidad del despido con indemnización de daños y perjuicios declarado en la instancia, estimando la pretensión de improcedencia. Los hechos declarados probados son los siguientes: la empleada, de profesión tripulante de cabina de pasajeros, con contratos eventuales de duración determinada por acumulación de tareas, se adhirió a una plataforma virtual de trabajadores eventuales de Air Europa, aunque en los hechos no consta la fecha de adhesión de la actora a dicha plataforma, se pedía que se cambiara la política de contratación de la empresa, los firmantes eran más de 2.500 personas y la actora compartió esta opinión, al igual que otras muchas personas realizando

---

[1137] El texto del perfil de Facebook era el siguiente: "*Mirar la sinvergüenza de mujer, junto al Rogelio y la otra Teodora. Desayunando en el Toro en horario de trabajo, y es capaz la muy Zorra de despedirnos a mí y al Jose Daniel por ir a buscar un bocadillo al comedor de Repsol, se le tendría que caer la cara de vergüenza. Por desgracia en la viña del señor hay muchas mujeres que por las razones que se desconocen son capaces de joder al hombres, pues me quedo más tranquilo o me quedaré más tranquilo cuando la pille fuera del trabajo y le diga lo zorra que es, y que no tenemos que pagar si es una mala follada o si tiene un mal día, pero que sepa que nos ha jodido por lo menos mil euros porque le ha salido del coño. Siento las palabras utilizadas, pero esa cosa no merece menos. Es una zorra*".

[1138] STSJ Madrid de 15 enero de 2016 (JUR 2016/40104).

comentarios en Facebook, así como también realizó unos comentarios genéricos en una página web de acceso público llamada www.change.org sobre política de contratación de la empresa compartidos por más de dos mil trabajadores.

Posteriormente, la Inspección de Trabajo realiza un requerimiento a la empresa para que transforme en indefinidos los contratos de trabajo de los tripulantes de cabina de pasajeros con contratos eventuales sucesivos que han venido prestando servicios de forma periódica. La empresa, durante los meses de septiembre y octubre del año 2014, ha suscrito contratos de interinidad saltándose el orden establecido en el escalafón, incluso contratando a través de esta modalidad a personas que no estaban siquiera en el escalafón con contratos de duración determinada.

Un sindicato interpuso demanda de conflicto colectivo ante la Audiencia Nacional por este asunto, solicitando que se obligara a la empresa a cumplimentar y garantizar el orden establecido en el escalafón regulado en el convenio para las ofertas de contratación en relación con los contratos de sustitución o interinidad. En la Audiencia Nacional finalizó el proceso por conciliación judicial, comprometiéndose la empresa a cumplimentar y garantizar el orden establecido en el escalafón regulado en el Convenio Colectivo para las ofertas de contratación en relación con los contratos de sustitución o interinidad con fecha de efectos del día de la conciliación.

Posteriormente, al no efectuarse el llamamiento, estando en su escalafón, demanda por despido nulo, argumentando que no la habían llamado atacando su derecho a la libertad de expresión, por reivindicar lo que era legítimo en Internet. En la instancia se estima íntegramente la demanda y se declara nulo el despido, porque se entiende por el Juzgador que en paralelo al conflicto entre la empresa y los trabajadores, se procedió a no efectuar el llamamiento de la trabajadora como represalia por la actitud de apoyo al conflicto que mostró en redes sociales, lo que vulneraba sus derechos fundamentales.

La Sala del TSJ de Madrid, tras desestimar varios motivos que tratan de modificar los hechos declarados probados, estima el motivo de vulneración del Derecho aplicado y declara que el despido no es nulo. Se argumenta que tal motivo debe tener favorable acogida, porque no pueden considerarse como indicios mínimamente relevantes de represalia lo datos que existen, no consta la fecha de adhesión de la actora a la plataforma de Facebook virtual de trabajadores eventuales de Air Europa. Por consiguiente, el despido de la demandante es improcedente y no nulo.

Excluida la nulidad del despido por vulneración de derechos fundamentales, procede absolver a la empresa demandada del abono de la cantidad condenada, en concepto de daños morales que venían acordados en la sentencia de instancia.

h) Recapitulación

Parece que la solución a estos conflictos vendrá de la mano de considerar la gravedad de la conducta, teniendo en cuenta la capacidad de difusión del medio empleado para manifestarla[1139]. Desde el punto de vista de obtención de la información públicamente disponible y su posible y posterior uso por parte de la empresa, no puede tener reproche más allá de lo éticamente aceptable[1140].

C) Acceso a redes sociales durante la jornada de trabajo

Este supuesto abarca los problemas más clásicos de la navegación por Internet[1141], en ellos se aplica la misma doctrina que la expresada en la Parte General sobre la existencia o no de una prohibición de usar los medios de la empresa para fines particulares, de acuerdo con el criterio de la expectativa razonable de confidencialidad y partiendo de la existencia de una tolerancia social hacia un uso moderado.

a) Despido por utilizar FB (STSJ Andalucía 14 noviembre 2013)

La STSJ de Andalucía de 14 de noviembre de 2013[1142] estima el recurso de suplicación de la empresa y declara procedente el despido de las tres trabajadoras que accedieron a la red social Facebook. Es doctrina mayoritaria que si no hay derecho a utilizar los medios informáticos para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las

---

[1139] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCCONI, C.: *Las TIC's en el ámbito laboral*, *op. cit.*, pág. 77.

[1140] LLORENS ESPADA, J.: «El uso de Facebook en los procesos de selección de personal y la protección de los derechos de los candidatos», *op.cit.*, pág. 66.

[1141] *Ibídem.*

[1142] STSJ de Andalucía de 14 de noviembre de 2013 (EDJ 2013/277305).

comunicaciones, porque, al no existir una situación de tolerancia al uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo:

> *"La respuesta parece clara: 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 existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo*" (FJ 4º).

b) Acceso a FB vedado previamente (STSJ Madrid 26 enero 2015)

La STSJ de Madrid de 26 de enero de 2015[1143]. con expresa alusión a la STS de 6 de octubre de 2011[1144], revoca la sentencia de Instancia, estimando el recurso de suplicación de la empresa (INDRA), al considerar que existe una transgresión de la buena fe contractual por las visitas a internet por la trabajadora para usos personales:

> " *ha accedido a numerosas páginas web de contenido no profesional, sobre todo redes sociales (como, por ejemplo, Facebook.com y Twitter.com), (...) dedicando a estas actividades nada menos que 16 horas y 47 minutos en el mes de octubre (21 días laborables) y 10 horas 43 minutos en el mes noviembre (16 días laborables)".*

Ello a pesar de que cuando se inició la relación laboral la parte recurrida firmó un anexo al contrato de trabajo del que se desprendía la existencia de una prohibición absoluta sobre el uso de medios de la empresa (ordenadores y acceso a Internet) para fines ajenos a la actividad laboral asimismo que la empleadora se reservaba el derecho a controlar o limitar el conjunto de servicios de Internet accesibles a sus usuarios por motivos de seguridad o rendimientos de la red y que su uso inapropiado sería sancionado con eliminación del acceso y la aplicación de sanciones disciplinarias. Se solicita la revisión del derecho aplicado en relación a la jurisprudencia relativa a la inaplicación de la teoría gradualista para faltas consistentes en transgresión de la buena fe contractual. Así: "*la existencia de una prohibición absoluta que válidamente impuso el empresario sobre el uso de medios de la empresa (ordenadores y acceso a Internet) para fines ajenos a la actividad de la empresa, sin que conste de otro lado la posibilidad del uso personal del mismo, y que la actora ha utilizado un medio cuya propiedad no le pertenece y cuyo uso está sujeto a las instrucciones del empresario, incumpliendo por ello con las normas dictadas a tal fin por el empleador, trasgrediendo la buena fe contractual*" (FJ 4º).

[1143] STSJ Madrid de 26 de enero de 2015 (EDJ 2015/16515).
[1144] STS 6 de octubre de 2011 (RJ 2011\7699).

H) Control indirecto de la Incapacidad Temporal

Las redes sociales, son foros ajenos a la organización empresarial, espacios abiertos de amplia difusión, a los que pueden acceder terceros[1145] y existe en ellos una clara tendencia o moda, o incluso a veces una cierta patología, a "*subir*" imágenes con amigos en situaciones de diversión, de la información recogida en ellos se puede justificar un despido disciplinario por simulación de IT, como observaremos la conductas enjuiciadas, se someten a la teoría gradualista[1146].

a) Camarera en despedida de soltera (STSJ Asturias 14 junio 2013)

La STSJ de Asturias Sala de 14 de junio de 2013[1147] desestima el recurso de suplicación planteado, y se confirma el despido disciplinario, por desarrollar actividades incompatibles con su situación de IT. Por la información obtenida de la página de Facebook de la recurrente, se declara probado que la trabajadora de baja médica por contractura cervical al día siguiente de iniciar el proceso de IT, con motivo de la despedida de soltera de una compañera, viajó a Madrid en avión y estuvo con unas amigas en un parque de atracciones y en dos días salió por varios pubs y discotecas hasta altas horas de la madrugada, siendo procedente el despido al mostrar la conducta de la trabajadora la aptitud laboral para el desempeño de los cometidos propios de su profesión de camarera.

Se alega infracción del art. 18.3 CE por la recurrente, la Sala declara que no se ha vulnerado la intimidad de la trabajadora al haber sido obtenidas las fotografías de páginas de Facebook sin necesidad de utilizar clave ni contraseña alguna:

> "*En este caso se alega la violación del artículo 18-3 de la Constitución al haberse obtenido dicha prueba a través de paginas de redes sociales y al efecto cabe decir con la sentencia de instancia que no se ha vulnerado la intimidad de la trabajadora al haber sido obtenidas las fotografías sin necesidad de utilizar clave ni contraseña alguna para acceder a las mismas dado que no estaba limitado el acceso al público, de modo que se obtuvieron libremente pues al estar "colgadas" en la red pudieron ser vistas sin ningún tipo de limitación con lo que no hay una intromisión en la intimidad de la trabajadora que además aparece en las instalaciones de un parque de atracciones de Madrid y por tanto en un lugar público*" (FJ 2º).

[1145] GRANDE ESTURO, C. y GORDILLO, C. «El uso de las redes sociales en la jurisprudencia social», Actualidad Jurídica Aranzadi núm. 855, 2013 (BIB 2013\191).

[1146] STSJ País Vasco de 12 de julio de 2011(EDJ 2011/368538).

[1147] STSJ Asturias de 19 de abril de 2013 (JUR 2013\245751).

b) Migrañas y trasnochar (STSJ Galicia 17 noviembre 2015)

La STSJ de Galicia 17 de noviembre de 2015[1148] confirma el despido de la parte recurrente que se encontraba en su proceso de IT por migrañas, cuando trasciende a la empresa que trasnocha saliendo a bares pubs hasta altas horas de la madrugada, como se desprende de las fotos perfil público de Facebook de una cafetería- pub en el aparece en dos noches distintas en la zona de baile y de la testifical de un detective privado que le realizó un seguimiento de día, manifestando que pudo realizar un trayecto de más de 50 kilómetros conduciendo y por la noche que manifestó que estuvo con amigos hasta las tres de la mañana en unos cinco establecimientos hoteleros distintos:

> "*Conductas contrarias a las exigencias de la buena fe contractual todas aquellas actividades que, o bien resultan contraindicadas para el curso de la enfermedad, o simplemente exponen al que las hace a una recaída en la misma, pues quien desarrolla esa conducta está defraudando a la empresa, a la Seguridad Social y a sus propios compañeros de trabajo; suponiendo una contravención palpable del deber fundamental de colaborar en su curación que tiene el trabajado*" (FJ 5º).

c) Limpiadora y guitarrista (STSJ Las Palmas 22 enero 2016)

En el caso de la STSJ Las Palmas de 22 de enero de 2016[1149] una limpiadora fue despedida disciplinariamente por transgresión de la buena fe contractual imputándosele que había desarrollado una actividad normal durante la baja de IT por traumatismo en miembro superior derecho, que era apta para el trabajo y que tales actividades contravenían el tratamiento médico indicado y dilataban su curación. La sentencia de instancia calificó de procedente el despido considerando acreditado, a través de fotos colgadas por la propia trabajadora y su marido en Facebook, que esta tocó la guitarra en público y que realizó labores de bricolaje de lijado y barnizado de puertas de su casa.

Planteado recurso de suplicación por la trabajadora, se descarta, en primer lugar, vulneración del derecho a la intimidad, pues son imágenes compartidas por ella mismo que permitió ser fotografiada en el momento de su realización. En efecto, ella misma consintió la reproducción de la imagen propia y procedió a la exposición pública de las

[1148] STSJ Galicia de 17 noviembre de 2015 (EDJ 2015/229342).
[1149] STSJ Las Palmas de 22 enero de 2016 (JUR 2016\43168).

fotos en una red social de libre entrada a todo el que quiera tomar conocimiento de lo en ella expuesto. Tampoco vulnera este derecho fundamental la investigación empresarial que supone la búsqueda en Facebook de las fotos, pues no se trata de una actividad que exceda de las facultades de control del empresario que puede hacer seguimiento también durante la suspensión del contrato por enfermedad (art.20.3 ET), debiéndose respetar la buena fe contractual. En efecto, cuando un trabajador está de baja médica y por tanto fuera del ámbito de control directo del empresario, es legítimo y necesario el seguimiento de su estado y actividad a través de un medio idóneo como es el acceso a una red social, publicitada por la propia trabajadora, sin vulnerarse su derecho a la intimidad.

Finalmente, declara el despido improcedente, al entender el TSJ que no que existe comportamiento desleal por incompatible con la situación subsidiada de IT

I) Valoraciones conclusivas

No nos encontramos ante un nuevo problema o ante un nuevo reto para el Derecho del Trabajo, sino que, más bien, se trata de una serie de problemas comunes o habituales de la disciplina solo que ahora se presentan con unos ropajes distintos o parcialmente distintos[1150].

Es muy importante la configuración de la privacidad en el perfil de las redes sociales por parte del trabajador, porque si no existe restricción alguna, terceros podrán acceder a toda clase de detalles de los usuarios.

La Red Social es un medio probatorio cuya proposición y práctica en el proceso social es claramente admitida. Los Tribunales consideran lícita la conducta del empleador de utilizar la información y opiniones del trabajador manifestadas en redes sociales para adoptar medidas disciplinarias contra ellos. Salvando siempre la validez del modo de obtención de esa prueba.

En relación, a la posible colisión con la libertad de expresión, las diversas manifestaciones vertidas en las redes sociales por un empleado en relación a posibles comentarios relacionados con su empresa, deben ser contextualizadas dentro del marco

[1150] NORES TORRES, L.E.: «Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales: aspectos individuales, colectivos y procesales», *op.cit.*

especial en el que se encuentran que es el contrato de trabajo, teniendo en cuenta el plus de gravedad que supone la forma escrita y la difusión pública de la red social. Asimismo, de ningún modo el ejercicio de la libertad de expresión justifica sin más el empleo de expresiones insultantes en las redes sociales.

En relación al derecho a la intimidad, el conflicto es inexistente pues el trabajador que interactúa es consciente de que está haciendo público un comentario, con independencia de que haya mantenido una cierta privacidad en su cuenta, con la excepción de los mensajes enviados de forma privada.

El derecho que sí debe respetar el empresario de forma totalmente escrupulosa, es el del derecho a la autodeterminación informativa, en cuanto que el consentimiento no vendría a legitimar una cesión de datos de los trabajadores en una red social. Por tanto no se pueden difundir ni imágenes ni datos de los trabajadores en la plataforma social de la empresa, salvo que dicha comunicación forme parte del objeto del contrato de trabajo.

El uso por parte de los representantes sindicales de las plataformas sociales, puede comportar la exigencia de una publicidad especial dirigida a las propias partes del conflicto o a terceros afectados, pero habrá de atenerse a los estrictos términos de los derechos e intereses que se debaten, y aunque encajen en ella actos de crítica en sentido amplio que en caso de simples trabajadores, no se tolerarían por no estar amparados por la libertad sindical, son injustificables los contenidos tendentes a desprestigiar a la empresa.

3. Otras redes, blogs y foros de Internet

A) Twitter

a) Planteamiento

Twitter es una red social de sistema de intercambio de pequeños mensajes de texto llamados *tweets* en los que se expresan de forma muy breve opiniones, se dan informaciones, se proporcionan enlaces o se hacen propuestas. La persona registrada crea sus mensajes y estos son distribuidos automáticamente a todas aquellas otras personas que se han suscrito a los mismos (siendo posible decidir si el usuario debe autorizar las suscripciones o éstas son libres). La distribución puede llegar a la página de twitter del destinatario, a su correo electrónico o incluso, muy frecuentemente, a sus teléfonos móviles mediante SMS. El envío también puede hacerse a través del teléfono móvil. El

uso del móvil convierte el sistema de twitter en un medio de propagación rápida de comentarios e información muy eficaz, también para la organización de eventos masivos.

El objetivo es lograr que los contenidos se conviertan en "*virales*". Twitter funciona a velocidad de vértigo; los mensajes caducan con gran rapidez, por lo que es necesaria cierta frecuencia para impactar de algún modo. Como punto positivo, la capacidad de generar viralidad es mucho mayor que la de otras redes, como Facebook[1151].

c) Vertiente jurídica

Con respecto a una posible colisión del derecho a la intimidad o secreto de las comunicaciones, como ya se expuso, no se plantea conflicto; el perfil es público y, por tanto, disponer de la información que procede de tal perfil supone un dilema inexistente.

En su caso los problemas que se planteen serán en relación con el derecho a la libertad de expresión, en este punto cabe traer a colación la reciente STS de 13 de julio de 2016[1152] ,dictada por la Sala Segunda, que ha condenado a un año de prisión a una joven por un delito de enaltecimiento del terrorismo y humillación a las víctimas cometido al difundir a través de twitter, bajo el perfil de "*Madame guillotine*", mensajes que atentaron a la dignidad de Irene Villa y Miguel Ángel Blanco. La sentencia, considera que las expresiones se enmarcan dentro del discurso del odio[1153] que no están protegidas por la libertad ideológica o de expresión. [1154]. Los magistrados rebajan de dos años a un

---

[1151] SICRE, L.: «5 claves para usar (bien) Twitter si eres abogado», *Actualidad Jurídica Aranzadi* núm. 920, 2016 (BIB 2016\3982).

[1152] STS de 13 julio de 2016 (JUR 2016\155482)

[1153] "*La alabanza o justificación de acciones terroristas que no cabe incluirlo dentro de la cobertura otorgada por el derecho a la libertad de exposición o ideológica en la medida que el terrorismo constituye la más grave vulneración de los Derechos Humanos de aquella Comunidad que lo sufre, porque el discurso del terrorismo se basa en el exterminio del distinto, en la intolerancia más absoluta, en la pérdida del pluralismo político y en definitiva en la aterrorización colectiva como medio de conseguir esas finalidades*" (FJ 3º).

[1154] Según los hechos probados, la joven, nacida en 1991, publicó comentarios y expresiones desde su perfil de Twitter, donde tenía 790 seguidores, con el fin de denigrar la memoria de la víctima de la organización terrorista ETA, Miguel Ángel Blanco, y despreciar a Irene Villa, víctima también de un atentado, así como ensalzar las actividades de miembros de la citada organización. La sentencia afirma que no se trata de criminalizar opiniones discrepantes sino de combatir actuaciones dirigidas a la promoción pública de quienes ocasionan un grave quebranto en el régimen de libertades y daño en la paz de la comunidad con sus actos criminales, atentando contra el sistema democrático establecido. Asimismo, indica

año de prisión la pena que le impuso la Audiencia Nacional al estimar parcialmente el recurso de casación interpuesto por la acusada, acogiendo el motivo en el que alegaba la desproporción de la condena.

d) Primeras sentencias

Con respecto al conflicto con la libertad de expresión, cabe traer a colación la STSJ de Navarra de 21 de febrero de 2014[1155] que resuelve el recurso de suplicación planteado por la empresa frente a la sentencia de instancia de un trabajador que fue despedido por verter determinadas expresiones que la empleadora consideraba injuriosas[1156], por la Sala procede a desestimar el recurso, confirmando la improcedencia del despido, se alude la escasa trascendencia que tuvo la publicación de twitter:

> *"La irregularidad imputada al trabajador no se produce en el ámbito de su propia función profesional, y los twitter referidos no se ha dicho cuantos días permanecieron publicados, pero no parece que los comentarios del trabajador hayan llegado a tener la publicidad y extensión suficiente para haber llegado a ser conocidos del gran público y llegar a dañar la imagen de la compañía ante proveedores y clientes. No hay lucro personal y tampoco se acredita el daño. Y excepto el último en que se dice que los trabajadores están hartos (no sic) de la opresión, no parecen especialmente injuriosos o calumniosos, sino que reflejan un trabajador indignado por causas que ni siquiera se concretan, en un contexto que parece que tiene un enmarque ciertamente*

---

que la humillación o desprecio a las víctimas afecta directamente a su honor y a su dignidad, perpetuando su victimización, que es actualizada a través de esa conducta.

[1155] STSJ Navarra de 21 de febrero de 2014 (JUR\2014\101739).

[1156] Los antecedentes de hecho son los siguientes, un trabajador oficial administrativo de un grupo de empresas dedicado a actividades funerarias (Grupo Memora), con motivo del proceso de I.T de un compañero ha de asumir más responsabilidades puesto que su puesto no se va a cubrir, y para agravar más la situación, por motivos económicos se había despedido a varios empleados de la misma categoría profesional. Estos hechos provocan en el actor un enfado hacia la empresa que le lleva a publicar en su cuenta de Twitter personal expresiones varias referidas a su empleadora tales como: "*Memora si quéreis guerra la vais a tener*", " *Grupo Memora os voy a reventar la venta*", "*Grupo Memora juega con fuego , lástima que no se puso guantes* " y " *Memora es una estafa no tiene recorrido y sus empleados están hasta los cojones de la opresión* ". Al día siguiente de esto, la empresa despide al trabajador, de manera disciplinaria, entendiendo que se está públicamente menoscabando la imagen de la empresa así como interpretan los hechos como unas amenazas. En la instancia el Jugado de lo Social entendió amparado en la libertad de expresión las manifestaciones. Se alza la empresa en segunda instancia y el resultado fue que se desestima su Recurso de Suplicación planteado, confirmando la improcedencia del despido disciplinario del que fue objeto.

explicable por la situación de conflicto laboral ante el cambio de la distribución de los servicios y agravamiento de las condiciones laborales" (FJ 3º).

También se argumenta en que dichas se realizan en una situación específica y concreta de reajustes presupuestarios y trabajadores despedidos por motivos económicos con la consiguiente sobrecarga de trabajo, contexto con el que parece ampararse y justificarse su conducta. Se admite que *" desde luego es una conducta injustificable"* pero la Sala, finalmente, aplica la teoría gradualista para entender que no cabe imponer la máxima sanción*: "no llega a ser de gravedad extrema para merecer la sanción extrema del despido, en un trabajador que en sus años de servicio no se le achaca amonestación alguna, y ello sin perjuicio de que pudo ser sancionada con una pena inmediatamente inferior"* (FJ 3º).

B) Redes profesionales

a) Planteamiento

Una red profesional es un tipo de servicio de red social que se enfoca en la interacción y relacionamiento de naturaleza comercial y profesional, en vez de las relaciones personales. Ejemplos destacados son LinkedIn, Viadeo, Xing y Johume.

b) Problemas jurídicos

Respecto a los derechos fundamentales, al ser una red de difusión pública no se plantea conflicto con el derecho a la intimidad o el secreto de las comunicaciones, y por el marcado carácter profesional de este tipo de red social es bastante improbable que existan colisiones con el derecho a la libertad de expresión.

Los problemas que se plantean en relación con este tipo de redes son los relacionados con una supuesta competencia desleal[1157], como sabemos, el trabajador responde de los daños que haya podido causar por este motivo a la empleadora por las gestiones realizadas para captar clientes para su propia empresa o su nueva empleadora, mientras la relación laboral está viva en relación con este período y el salario percibido,

[1157] Actividad económica o profesional que entra en competencia económica con el empresario por incidir en un mismo ámbito el mercado en el que se disputa un mismo potencial de clientes.

e incluso en conductas posteriores si se estipula un pacto de no competencia; durante un tiempo no puede ya concurrir en el libre mercado contra su empresario anterior. Tanto en uno, competencia desleal, como en otro supuesto, pacto de no concurrencia, el empresario puede reclamar al trabajador los daños y perjuicios que éste le haya causado por incumplimiento laboral y con independencia de las medidas disciplinarias que haya adoptado al respecto.

c) Primeras sentencias

En el caso de la **STSJ de Madrid de 25 de noviembre de 2014**[1158] el trabajador firma como un anexo a su contrato de trabajo un pacto de no competencia post contractual en el sector dedicado a la instalación y comercialización de aparatos eléctricos con duración de18 meses contados a partir de cuando finalizara su relación laboral. Dos años después solicita la baja voluntaria en la empresa y un mes después publica en LinkedIn que trabaja en una empresa del mismo sector, tal información trasciende a su antigua empleadora que le solicita el abono de la cantidad pactada por no haber respetado el pacto. La Sala confirma la indemnización de daños y perjuicios declarada en la instancia, sin considerar válido el argumento de que la cláusula era abusiva cuando se firmó el anexo del contrato de trabajo (*pacta sunt servanda*).

La **STSJ de Madrid de 23 de septiembre de 2015**[1159] declara que el perfil profesional del trabajador que figura en la red profesional de LinkedIn no supone una deslealtad y no es incompatible con la cláusula de confidencialidad que había firmado al inicio del contrato, la Sala entiende que "*La lealtad a la empresa obliga al empleado, entre otras cosas, a no aprovecharse indebidamente de su reputación o esfuerzo(…)Pero ese deber de lealtad no puede inhibir la propia libertad profesional y de trabajo del trabajador, ni puede exigir una noticia inmediata y detallada de lo que es un mero proyecto, cuya viabilidad o realización están en estudio (…) el tener colgado en Internet el perfil profesional por si un día quiere y desea cambiar libremente de trabajo no tiene entidad suficiente para la procedencia del despido*" (FJ 5º). Por tanto, carece de entidad en este supuesto la publicitación en la red profesional a efectos del despido.

La **STSJ de Cataluña de 16 de marzo de 2016**[1160] admite la revisión de los hechos probados incorporando a los mismos el pantallazo del perfil profesional de

[1158] STSJ de Madrid de 25 de noviembre de 2014 (JUR\2015\47880).

[1159] STSJ de Madrid de 23 de septiembre de 2015, rec. 307/2015 (JUR\2015\242034).
[1160] STSJ Cataluña de 16 marzo de 2016, rec.5867/2015 (JUR 2016\123428).

LinkedIn del trabajador por competencia desleal y declara procedente el despido puesto que había firmado un pacto de exclusividad en el sector del marketing que había incumplido: "(…) *en la red social Linkedin él mismo lo afirmaba, por lo que, aunque consta en el hecho probado tercero que el propósito del actor era el de ayudar a su pareja sentimental en construir una pág. web para realizar un trabajo académico, también lo es que el propósito de dicha pág. web era dar a conocer una empresa que se dedicaba a ofrecer servicios de publicidad por Internet a otras empresas y que él figuraba como parte del equipo de trabajo, por lo que es claro que la creación de dicha pág. web era claramente la creación de una empresa con ánimo de lucro y no únicamente un trabajo académico"* (FJ 4º).

d) Valoración conclusiva

Los conflictos de fondo que plantean las redes profesionales son los clásicos lo que difiere es el medio a través del cual se publicitan los trabajadores que actúan de manera desleal, que es novedoso; la propia red profesional que hace que transcienda la conducta a la empresa. Como hemos analizado un "pantallazo" de un perfil profesional es un documento válido a los efectos de solicitar la revisión de los hechos declarados probados en el recurso de suplicación. No se cuestiona la importante carga probatoria del contenido de las redes profesionales en las que el conflicto, a diferencia de otras no versa sobre derechos fundamentales sino sobre legalidad ordinaria, en este caso, existencia de un quebrantamiento o no del pacto de no competencia.

C) Blogs

a) Descripción

Las nuevas tecnologías han permitido que la comunicación sea más fácil, más sencilla y, sobre todo, más directa. Y entre todas las herramientas y oportunidades al alcance de todos los internautas, y por tanto del trabajador, destaca una: el blog o lo que es lo mismo, un diario personal del autor o autores con contenidos de su interés, actualizados con frecuencia y a menudo comentados por los lectores. Sirve como

publicación en línea de historias con una periodicidad muy alta, que son presentadas en orden cronológico inverso, es decir, lo más reciente que se ha publicado es lo primero que aparece en la pantalla. Es muy frecuente que los blogs dispongan de una lista de enlaces a otros blogs, a páginas para ampliar información, citar fuentes o hacer notar que se continúa con un tema que empezó otro blog.

b) Tipología

Propios.- Los cauces electrónicos usados por el trabajador creados y gestionados por él mismo. El trabajador puede disponer de un espacio web para colgar su página o crear un blog en un sitio especializado y allí puede escribir comentarios, transmitir informaciones, colgar enlaces, vídeos, música o sonido, aplicaciones y programas, etc. Ese sitio web puede estar protegido, de manera que solamente puedan acceder quienes dispongan de claves proporcionadas por el propio trabajador o administrador del sitio, o puede estar abierto a cualquier persona que navegue por Internet. A su vez las claves pueden ser proporcionadas de forma personalizada por una persona física, discriminando entre las peticiones recibidas, o pueden ser proporcionadas por la máquina a cambio de un registro de los datos, registro en el cual habitualmente solamente se comprueba la veracidad de la dirección de correo electrónico proporcionado (se exige un mensaje de confirmación en respuesta a un mensaje enviado a esa dirección). En este segundo caso (claves generadas automáticamente a cambio de un registro) el acceso no puede ser considerado estrictamente como restringido o privado, siendo más similar a un acceso público.

Ajenos.- El trabajador puede hacer comentarios al pie de documentos o en zonas de las páginas web que así lo permitan, como suele suceder en las de muchos periódicos, blogs, etc. La forma de proporcionar las claves puede ser personalizada o automática, pero incluso si es personalizada, al ser una página web ajena al trabajador, normalmente éste no tendrá control sobre las personas que pueden acceder a la página.

Foros de Internet.- Se analizan en capítulo aparte, el siguiente.

c) Vertiente laboral

En cualquiera de los supuestos descritos anteriormente, estamos obviamente, ante foros ajenos a la organización empresarial, espacios abiertos de amplia difusión, a los que pueden acceder terceros. Por ello, a pesar del derecho fundamental de libertad de

expresión y opinión, lo cierto es que la existencia de una relación laboral modula el ejercicio de tales derechos, gracias al principio de buena fe contractual que debe presidir toda relación de trabajo[1161].

Cierto sector de la doctrina considera recomendable incluir un apartado en la normativa interna de la empresa en la que se ponga de manifiesto que, sin ánimo de limitar el derecho de información y libertad de expresión de los empleados, siempre se deberá respetar el buen nombre y reputación de la empresa, de sus compañeros de trabajo y de los clientes en las opiniones y manifestaciones publicadas en redes sociales o blogs[1162], aunque desde mi punto de vista es algo que resulta obvio y por tanto, es intrascendente tal regulación expresa.

d) Límites a la libre expresión

El problema que se plantea es el de la colisión entre la privacidad y/o libertad de expresión y la potestad sancionadora del empresario, como ya se indicó anteriormente, no existe un derecho al insulto. Las SAP de Cantabria de 2 de junio de 2016[1163] condena a un representante sindical de UGT a pagar una multa de 2.520 euros y a indemnizar con 6.000 euros a dos dirigentes del mismo sindicato al considerarle autor de un delito de injurias graves con publicidad.

El sindicalista condenado creó un blog, amparándose en el anonimato, para "*lesionar y menoscabar gravemente la dignidad personal*" de dos dirigentes de su sindicato[1164]. Por este motivo, se confirma la condena si bien rebaja la indemnización que la magistrada del Juzgado de lo Penal núm. 3 de Santander le impuso en primera instancia: de 20.000 euros de indemnización para cada uno de los dirigentes injuriados a 3.000 euros. La Audiencia Provincial de Cantabria también confirma la decisión de la juez de absolverle del delito de calumnias del que venía siendo acusado, al no encontrar elementos suficientes para considerar que cometió tal ilícito penal. Se incide en que los comentarios son "*altamente ofensivos e injuriosos, incluyendo calificativos que no se*

[1161] GORDILLO, C. y GRANDE C.: «El uso de las redes sociales en la jurisprudencia social», *op.cit.* (BIB 2013\191).

[1162] *Ibídem.*

[1163] SAP Cantabria de 2 junio de 2016 (JUR 2016\141760).

[1164] En este sentido, subraya que el acusado se refiere a los dos dirigentes de su sindicato "*de forma reiterada y sistemática con calificativos tales como fachas, tragones beneficiados, pandilla de sinvergüenzas, impresentables, indecentes, corruptos o mierda de personajes*".

compadecen con el ánimo de criticar o informar alegado por el recurrente", "*La naturaleza de tales comentarios unida al gran periodo de tiempo durante el que dicho blog permaneció activo pone de manifiesto que el acusado actuó guiado por un inequívoco ánimo de injuriar*".

Además, responde a la alegación del acusado de que había creado el blog para servir de medio de comunicación entre seis u ocho conocidos destacando que tuvo una "*publicidad inusitada*" al registrar más de 57.000 entradas, tal y como el acusado se encargaba de destacar en el blog. Finalmente, en relación a la indemnización, la Audiencia entiende que la conducta del condenado "*tuvo que provocar un lógico y humano sufrimiento personal o daño moral*", atendiendo a que las injurias se prolongaron en el tiempo y que además el blog tuvo gran difusión en el ámbito del sindicato. Sin embargo, señala el tribunal que ninguno de los dos dirigentes injuriados ha acreditado los padecimientos que manifestaron en el juicio, por lo que la sala entiende proporcionada una indemnización para cada uno de 3.000 euros.

e) Tipología judicial.

1º) Imputaciones genéricas

A veces a empresa reacciona frente a manifestaciones de carácter genérico que realiza el trabajador y que constituyen expresiones descalificadoras genéricas, vertidas en la web-blog personal de un trabajador, que no están dirigidas de forma clara y directa a un directivo o compañero de trabajo constituyen un despido improcedente[1165].

En este sentido, difundir información incierta de la empresa a través de un comunicado a los usuarios donde se presta el servicio no reviste la gravedad suficiente para proceder a extinguir la relación laboral la filtración[1166].

[1165] STSJ Cataluña de 16 mayo de 2007 (AS 2007\2400).
[1166] STSJ Galicia de 23 mayo de 2011 (AS 2011\2249).

2º) Diseños industriales en Infojobs (STSJ Cataluña 22 febrero 2016)

La STSJ de Cataluña 22 de febrero de 2016[1167] estima el recurso de suplicación planteado por el trabajador despedido por publicar en su perfil profesional información que la empresa entendía contraria a su política de confidencialidad y de datos. Como antecedentes de hecho relevantes, merece destacarse que con anterioridad al despido el actor publicó en la bolsa de trabajo INFOJOBS de Internet su perfil profesional en el que incluía, en el apartado últimas experiencias profesionales, la referencia a que era diseñador gráfico de la empresa demandada y en los datos personales del su *curriculum vitae* incluía el enlace a la página que contenía su blog. Cuando se accedía a dicho enlace se visualizaban diseños de autoría del trabajador que eran propiedad de la marca de la demandada (diseños de cajas de lápices, de etiquetas de felicitación, posters, ilustraciones para parking, sobres de imitación de la marca F, incluido un tríptico referido a las nuevas instalaciones de la empresa en que constaba una fotografía de uno de los administradores y gerentes de la empresa demandada, etc.)[1168.]

La Sala razona que se está ante un acto de mera información sobre su actividad laboral previa, pero no supone ni realizar actividades de la misma naturaleza para otras empresas de la competencia, ni sacar de los locales de la empresa o enviar códigos de fuentes de programa o de cualquier otro tipo, ni tampoco apropiarse de unas marcas o diseños que son propiedad de la empresa. Por otro lado la información que se ofrecía en el blog no era distinta de la que oferta la propia empresa en su publicidad o a través de

[1167] STSJ Cataluña de 22 febrero de 2016(JUR 2016\67683).

[1168] Lo que se imputaba al empleado en la carta de despido era literalmente lo siguiente: "*En fecha 04 de febrero esta empresa ha tenido conocimiento que es poseedor de un blog personal con la dirección www.emedoble.glogspot.com.es, en el cual ha publicado una serie de productos propiedad de esta empresa, ha usado nuestro nombre así como la imagen de uno de nuestros administradores y gerentes de la empresa, sin nuestro consentimiento expreso , encaminado a realizar actividades de la misma naturaleza para otras empresas de la competencia, ejerciendo usted una grave competencia desleal, lo que se ve reflejado en el contacto del mismo blog en el que dice textualmente: "si te gusta lo que has visto y quieres contratarme para tu empresa/proyecto gráfico. Ponte en contacto conmigo y hablemos de negocios*..."

los mismos productos que comercializa, por lo que no cabe hablar de un grave perjuicio para la misma al facilitar a la competencia la realización de copias de sus productos.

3º) Blog anónimo de profesor (STSJ Madrid 29 noviembre 2013)

La STSJ de Madrid de 29 de noviembre de 2013[1169] confirma el despido procedente de un profesor de literatura que es identificado como el autor de un blog anónimo en el que a modo de diario, relataba las experiencias en su trabajo todo bajo un tinte subjetivo con todo tipo de expresiones desafortunadas (racistas, machistas, xenófobas, etc.) respecto a alumnos, padres y compañeros de profesión. En el mencionado blog se explicitaban datos que hacían que se identificara claramente el instituto de referencia y el posible autor. Se trató la cuestión en un claustro y el recurrente admitió ser el autor del mismo. Poco después, el recurrente, procedió a borrar el blog, contenido que fue recuperado por un perito informático y un notario que dio fe del mismo y lo protocolizó; con sustento en esta prueba fue despedido.

Sostiene en síntesis el recurrente que el despido vulnera el derecho a la libertad de expresión, pues no habría quedado acreditado que se refiera a personas del centro escolar, tratándose de una creación literaria, habiendo ya calificado el demandante en uno de los pasajes al "*blog*" como irracional. La Sala califica como procedente el despido y recuerda que la libertad de expresión no ampara insultos ni menosprecios:

> *Entiende esta Sala que las expresiones que el actor recoge en el "blog " y que se recogen en el relato fáctico, entre las que figuran aquellas a las que nos hemos referido en el fundamento jurídico anterior*[1170]*, no están amparadas en la libertad de expresión, pues en el mismo figuran insultos, menosprecios y faltas de respeto, incluidas expresiones que afectan al aspecto físico de las personas, que son gratuitas y que no tienen ninguna justificación, lo que lleva consigo que deba desestimarse este motivo del recurso"* (FJ 6º).

[1169] STSJ de Madrid de 29 de noviembre de 2013 (EDJ 2013/266591).

[1170] «*Es correcta la afirmación de que alguna de las personas a las que se refiere el "blog " está perfectamente identificada, debe reseñarse que esta Sala entiende que resulta irrelevante que no figuren identificadas todas las personas por su nombre y apellidos, pues en todo caso se está refiriendo a profesores, padres de familia y alumnos del colegio en los que presta servicios el demandante, a los que se refiere de forma claramente despectiva e insultante, siendo alguno de ellos perfectamente identificable por la disciplina que enseña en el colegio o por tareas que desempeña, como sería el caso de la profesora de matemáticas a la que denomina "Bruja*"» (FJ 5º).

4º) Blog del administrador (STSJ Cataluña 14 febrero 2012)

Si por el contrario, es el trabajador el que reclama a la empresa por menoscabo al honor, se exige que por la relación laboral esté vigente; no se puede plantear la reclamación de tutela del derecho al honor frente al contenido y opiniones expuestas en el blog personal en Internet del administrador y socio de la empresa, con posterioridad a la extinción contractual, por incompetencia de la jurisdicción laboral[1171].

f) Conclusión

La doctrina judicial considera lícita la conducta del empleador que utiliza la información y opiniones del trabajador vertida en blogs tanto porpios como ajenos y foros de Internet. La adopción de medidas empresariales a partir de la información proporcionada en estos recurso tecnológicos no exige el establecimiento de códigos de conducta o protocolos que regulen las manifestaciones de los trabajadores en dichos medios para utilizar las mismas como medio de prueba válido en un procedimiento disciplinario, pues la libertad de expresión no ampara el derecho a menoscabar la dignidad de otro.

D) Foros de Internet

a) Planteamiento

Un foro en Internet es una página web, creada habitualmente, a partir de la programación en el lenguaje HTML[1172], y que tiene como características fundamentales el poder mostrar, al usuario de Internet que accede a ella, información variada utilizando una interfaz gráfica, atractiva y sencilla de utilizar gracias a un mecanismo de hiperenlaces con otras págin as web (*links*) o con otras partes de la misma página web (*tags*). La protección del código fuente de la página web implica su consideración como

[1171] STSJ Cataluña de 14 febrero de 2012 (AS 2012\265).

[1172] Siglas de *HyperText Markup Language*, hace referencia al lenguaje de marcado para la elaboración de páginas web. Es un estándar que, en sus diferentes versiones, define una estructura básica y un código para la definición de contenido de una página web, como texto, imágenes, etc.

programa informático y, por lo tanto, queda sometida a lo dispuesto por el TR Ley de Propiedad Intelectual sobre la protección de los programas de ordenador[1173].

Pese a que las páginas web son sólo uno de los servicios que ofrece Internet (otros son: ftp, irc, telnet; news, correo electrónico...), lo cierto es que es uno de los servicios más utilizados por los usuarios y, desde luego, es el más propicio para configurar todo tipo de plataformas. El carácter abierto de la Red hace posible la publicación de informaciones por múltiples personas tradicionalmente sin acceso habitual a los medios de comunicación carentes de los mecanismos de control de estos[1174].

Los chats o foros sociales de Internet no suelen ofrecer ningún tipo de restricción para que las conversaciones puedan ser conocidas por otras personas; son comunicaciones públicas en las que participan simultáneamente y en tiempo real varios internautas, pudiendo su contenido ser conocido por cualquier otro sujeto que desee acceder a la misma a través de la red pública, salvo en caso de que se utilice la opción de comunicación bidireccional cerrada entre dos usuarios[1175]. En muchas páginas se puede acceder a foros sobre diversas materias, en la que los participantes pueden leer los comentarios de los demás y además hacer comentarios propios siguiendo el hilo de otros comentarios anteriores, además de proporcionar enlaces a páginas web. El acceso a los foros puede ser libre para la lectura o exigir alguna clave, respecto a lo cual solamente cabe repetir lo ya dicho anteriormente. Puede ocurrir que se exija clave para poder escribir comentarios, pero no para la lectura de los mismos.

Por lo que no es de extrañar que Internet sirva para que los ciudadanos de todo el mundo, sin distinciones, barreras ni fronteras, tengan o puedan tener acceso a la información, al ocio, a la cultura, al trabajo, a los servicios, a la salud, en definitiva, a más y mejor calidad de vida.

b) Problemas jurídicos

Lo expuesto no impide que Internet presente inconvenientes, como puede ser el de propiciar la comisión de determinados delitos, algunos especialmente graves, como la pornografía infantil o la prostitución, o el de aumentar las posibilidades de vulnerar derechos fundamentales, señaladamente los derechos al honor, la intimidad y la propia

[1173] SAN JUAN DELGADO, I. D. : «La página web», *Boletín de Legislación*, núm. 262, 2003.

[1174] DE MIGUEL ASENSIO, P.A.: «Servicios de la Sociedad de la Información», *op. cit.*, pág. 26

[1175] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op.cit.*

imagen. Por otra parte, el propio funcionamiento de este medio dificulta enormemente la identificación, la localización y, en consecuencia, la posibilidad de exigir responsabilidad a los autores de dichos delitos y vulneraciones.

Son dos los derechos fundamentales que pueden sufrir colisión: 1º) La libertad de expresión, aspecto ya analizado en el capítulo de las redes sociales, por lo que se realiza una remisión remitimos a lo manifestado en ese epígrafe. 2º) El derecho a la intimidad, en el caso de que se fiscalice el ordenador del empleado y través de la carpeta de archivos temporales, se acceda a la información sobre qué tipo de páginas visita, que quedaría anulado, como sabemos por la existencia de prohibiciones expresas.

a) Difusión de conversación laboral (STSJ Cataluña 11 marzo 2013)

La STSJ de Cataluña de 11 de marzo de 2013[1176]aborda el caso de trabajadores que proceden a la difusión pública de forma continuada de una grabación privada de una conversación mantenida por tres mandos de la empresa a través de los teléfonos móviles de los trabajadores, que procede a colgarse en una página web, con un enlace desde dónde puede escucharse íntegramente el contenido de las conversaciones. La Sala no puede amparar tal actitud:

> *"(...) la conducta en que los actores incurrieron es...reprobable pues tiene mal encaje en los derechos de libertad de expresión e información general e incluso en el propio ámbito del derecho de representación (pues) actúan sobre una grabación cuya ilícita procedencia conocen, a las que dan difusión a través de web...sin que conste que hayan verificado la autenticidad de su contenido y la responsabilidad de la fuente..."; no habiéndose limitado a "la mera denuncia o al ofrecimiento de información sino que se orienta a promover la hostilidad frente a otros compañeros mediante su identificación (…) e imputación de coparticipación en una conducta empresarial que es criticada abiertamente..." Pudiera cuestionarse la responsabilidad de los sancionados en un ámbito diverso al que es propio de la jurisdicción social, pero -en lo que se refiere al enjuiciamiento de su conducta desde una perspectiva sancionatoria/laboral- la conclusión que se obtiene no puede razonablemente diferir de la judicialmente alcanzada en favor de la procedencia de la sanción impuesta" (FJ 2º).*

Quien graba una conversación de otros atenta, independientemente de otra consideración, al derecho reconocido en el artículo 18.3 de la Constitución, por el contrario quien graba una conversación con otro no incurre, por este solo hecho, en conducta contraria al precepto constitucional citado, pues si se impusiera un genérico deber de secreto a cada uno de los interlocutores o de los corresponsables *ex* artículo 18.3 CE, se terminaría vaciando de sentido el contenido del referido artículo.

[1176] STSJ de Cataluña de 11 de marzo de 2013 (EDJ 2013/72102).

La presencia de un elemento ajeno a los interlocutores entre los que media el proceso de comunicación es indispensable para configurar el ilícito constitucional aquí analizado que es, en efecto, el que motiva su sanción disciplinaria bajo la correcta y adecuada cobertura de la norma colectiva que previene frente aquellas conductas que vulneren derechos de su personal, como lo es el relativo al secreto de sus comunicaciones, con el agravante añadido de su difusión en una web, por eso la Sala deja entrever que la conducta pudiera llegar a ser un ilícito no solo laboral sino penal.

b) Descrédito de compañeros (STSJ Navarra 19 julio 2013)

La STSJ de Navarra de 19 de julio de 2013[1177] afirma que el hecho de que un trabajador acuda a un foro de Internet y realice comportamientos éticamente reprochables hacia un compañero de trabajo no es motivo de despido disciplinario, por no guardar conexión alguna con la relación laboral, a pesar de haberse acreditado su autoría.

Los hechos transcurren del siguiente modo: el empleado había insertado en un foro de Internet, en concreto en una página web en la que se ofertaba la prestación de servicios sexuales de tendencia homosexual, varios anuncios gratuitos solicitando relaciones de naturaleza sexual e introdujo en los mismos, el número de teléfono privado del domicilio de uno de sus compañeros de trabajo, lo que conllevó que aquél recibiera continuas llamadas telefónicas, tanto durante el día como durante la noche.

La carta de despido menciona que el compañero de trabajo se vio obligado a presentar denuncia ante la policía y que, tras realizar las investigaciones pertinentes, se encontró la página web en la que estaba inserto el número de teléfono de denunciante, que llevó a la dirección IP del domicilio del actor. Por este motivo se incoaron asimismo diligencias penales que acabaron en un una condena por una falta de vejaciones. Consta que anteriormente a estos hechos, la relación entre ambos empleados era cordial, no había existido nunca, ningún tipo de problema previo.

La carta de despido afirma que los hechos que imputaba al demandante, demuestran su actuación maliciosa y consciente, con ocultación y persistencia, y con el

[1177] STSJ de Navarra de 19 de julio de 2013(JUR\2014\43706).

único objetivo de hacer daño al compañero de trabajo, afectando a su derecho a la intimidad y al honor. La Sala resuelve:

> *"Las ofensas verbales o físicas para que constituyan una conducta sancionada con el despido tienen que estar relacionadas con el contrato de trabajo, esto es, el conflicto debe traer necesariamente su causa en la relación laboral, y no en aspectos particulares o ajenos a la misma, de modo que si se originan fuera del trabajo y se causan por razones ajenas al mismo, no existe fundamento suficiente para convalidar la decisión extintiva disciplinaria». Esto es lo que ocurrió en el caso enjuiciado, habiendo considerado con acierto el Magistrado de instancia que el despido era improcedente porque los hechos que lo motivaron, consistentes en insertar en una página web de contactos sexuales el número de teléfono privado de un compañero de trabajo y el hacer pedidos en su nombre, y contra reembolso, de productos eróticos, carecen de naturaleza laboral no sólo porque tuvieron lugar fuera de las dependencias de la empresa sino, sobre todo, porque tampoco sucedieron en el desarrollo como consecuencia de la relación laboral" (FJ 4º).*

El criterio delimitador es, por tanto, que la situación conflictiva ha de tener su origen en la relación de trabajo, y no en aspectos ajenos a la misma (como en el supuesto que nos ocupa), si la publicación en la página web hubiera sido a consecuencia o como represalia de un problema o pelea de ambos empleados, en el centro de trabajo por motivos de trabajo, si guardaría relación causal.

c) Piloto rebajado (STSJ Madrid 16 diciembre 2013)

La STSJ de Madrid de 16 de diciembre de 2013[1178] resuelve el recurso de suplicación de un piloto de *Air Europa*, que actuó de una manera "*despechada*", tras ser relevado de su cargo de comandante. Fruto del acaloramiento "*excesivo"* por tal decisión de la compañía aérea, publica en un foro de Internet opiniones que dañan considerablemente el prestigio de la empresa al imputarle graves irregularidades incluso con presunta responsabilidad penal, todo con base en unas informaciones no contrastadas e inciertas. Llegó a escribir que "*había comandantes que volaban con la licencia de vuelo caducada*", o a que un comandante a "*le tuvieron que falsificar los datos del simulador de vuelo porque no superó el entrenamiento e hicieron la vista gorda*", que Air Europa era subcontrata del Ministerio de Defensa para determinados desplazamientos y con ello "*ponía en peligro a los militares puesto que no era una aerolínea segura*", e incluso llega atribuir la responsabilidad a la empleadora en el conocido accidente de Katowiche (Polonia)[1179].

[1178] STSJ Madrid de 16 diciembre de 2013, rec. 1231/2013. (AS 2014\113).

[1179] ABC.es (2006, 30 de enero) Concluyen las tareas de rescate en el accidente de Katowice con un saldo provisional de 67 muertos. *http://www.abc.es/hemeroteca/historico-30-01-2006/abc/Internacional/concluyen-las-tareas-de-rescate-en-el-accidente-de-katowice-con-un-saldo-provisional-de-67-muertos_1314077105238.html*

El recurrente alega la infracción del art. 10 del Convenio para la Protección de los Derechos Humanos y Libertades Fundamentales que protege la libertad de expresión, en relación con los arts. 20.1.a) y 16 de la Constitución , que protegen la libertad de expresión y la libertad ideológica, sostiene, en síntesis, que ha obrado en ejercicio de su derecho a la libertad de expresión y no puede ser despedido por ello, habiendo manifestado no hechos sino "*opiniones*", "*o más bien preguntas comparativas*", derivadas además de su estado anímico "*conturbado"* a raíz de la reciente destitución de su puesto de comandante, añadiendo que no había efectuado imputaciones concretas a personas determinadas sino alusiones genéricas y que, en todo caso, los destinatarios no se han considerado ofendidos, por lo que desde la óptica del mencionado Convenio internacional citado la sanción es excesiva. Resuelve la Sala:

> *"Distinta consideración merece la publicación del actor en los siguientes días en la página web "aviacióndigitalglobal.com" de los comentarios que se transcriben en el hecho probado 5º En este momento el demandante ya no se halla en uso de su libertad de expresión dentro de la empresa, sino que está transmitiendo al exterior opiniones que desprestigian a la empresa basadas en informaciones no debidamente contrastadas y que han resultado infundadas.*
>
> *(...) el derecho a comunicar información veraz aunque no requiere una exactitud absoluta de lo afirmado, sí exige una comprobación razonable de las fuentes de las que proviene, como declaran entre otras las STC 10 , 223/93 y 4/96 . No solamente se imputan graves irregularidades con quiebra de la seguridad en vuelo, no contrastadas, sino incluso delitos. El daño injustificado que se produce al honor y la imagen de la empresa es innegable, debido a las imputaciones que realiza el trabajador de forma pública y con trascendencia incluso penal, aparte de quebrantar la buena fe contractual también al recomendar a las empresas de la competencia frente a su empleadora. Es relevante en estos aspectos la doctrina de la STC 126/03 (RTC 2003, 126) al considerar que en el marco del contrato de trabajo es exigible que antes de trasladar a los medios de comunicación denuncias sobre el mal funcionamiento de la empresa con notable menoscabo de su imagen pública, se haya dado ocasión a que los organismos públicos competentes hayan podido verificar la realidad de los hechos que se denuncian" (FJ 3º).*

Por tanto, para realizar este tipo de comentarios, el piloto debía haber denunciado los hechos ante las autoridades competentes y una vez comprobada su veracidad, posteriormente, se podría, en su caso, realizar las manifestaciones en base a su autenticidad. Al no haber actuado de la manera antes descrita, los actos del trabajador no pueden quedar amparados ante el derecho a la libertad de expresión. Va más allá la Sala, afirmando que el reproche va más allá del ámbito laboral, pues cabe incluso pensar que la empleadora en este caso, podría haber ejercido acciones penales contra el actor por difamar de manera pública, hay argumentos para ello, aunque no consta tal extremo.

d) Vulneración de código empresarial (STSJ Castilla y León 2 julio 2105)

La STSJ de Castilla y León de 2 de julio de 2015[1180] resuelve el caso de un trabajador de profesión oficial primera de mantenimiento de carreteras, que tuvo una macabra conducta; en dos ocasiones distintas, mientras se encontraba despejando la carretera de obstáculos por dos accidentes de tráfico que ocurrieron en dos días distintos, realizó fotos y posteriormente, colgó las mismas en una página web de difusión pública. Las fotos de las imágenes que el empleado subió a un foro de Internet se correspondían a dos siniestros graves; en uno de ellos existía una persona fallecida y en el otro había un herido en estado de inconsciencia, estas imágenes se hicieron virales en la Red.

Tan virales fueron las fotos que trascendieron a la Guardia Civil, que a su vez acudió a la empresa de mantenimiento de carreteras con motivo del inicio de una investigación al objeto de determinar la autoría y difusión de las citadas fotografías para en su caso incoar diligencias penales. El trabajador en esa visita de la autoridad pública, reconoció la autoría de las fotos y posterior divulgación, a modo de curiosidad apuntaremos, que llegó a manifestar "*¿y qué pasa*?" al parecer creyendo en su impunidad respecto a lo acontecido. En consecuencia, fue despedido de manera disciplinaria. EL razonamiento judicial clave dice así:

> *"En cuanto a ello, en los contratos del actor se ha consignado, expresamente, una cláusula adicional 7ª de confidencialidad, en el modo que recoge el ordinal cuarto, que se da por reproducido. A sabiendas y con conocimiento de la misma, realiza unas fotos de un accidente en el que tuvo que intervenir, con posterioridad, el día 14-12-14, publicitando las mismas en las páginas web, de la forma que recoge el ordinal quinto, que se da por reproducido. Dicha conducta acreditada, supone una vulneración de la buena fe contractual exigible, a los efectos del Art. 54.2. d) ET y del Art. 102 del Convenio aplicable, por lo que el despido efectuado debe ser considerado como procedente" (FJ 2º).*

Se insiste para justificar la procedencia del despido, en la firma de un anexo al contrato de trabajo que el trabajador había aceptado y en consecuencia, no debía revelar nada de lo que conociera por su trabajo y como lo incumplió pues es correcto extinguir la relación laboral. Pero no encontramos el reproche ético de la conducta, no se apunta por ningún lado la grave falta cometida en base a la conducta irrespetuosa con las más mínimas y elementales normas de convivencia humana. Tampoco se alude a las violaciones flagrantes de la intimidad y al derecho a la autodeterminación informativa de

[1180] STSJ de Castilla y León de 2 julio de 2015 (JUR 2015\180207).

los heridos de los accidentes de tráfico, dada la gravedad de lo acontecido la argumentación es sorprendentemente ligera.

e) Conclusión

Debemos partir de que respecto a los comentarios vertidos en páginas web o foros de Internet, por parte de los empleados, la situación a enjuiciar ha de tener su origen en la relación de trabajo, y no en aspectos ajenos a la misma. Y tras ello que bajo el derecho a la libertad de expresión, no cabe amparar conductas tales como: imputar ilícitos a la empleadora, insultar, difundir conversaciones privadas de compañeros grabadas sin el consentimiento de los mismos, etc.

5. Mensajería instantánea (Whatsapp)[1181]

A) Delimitación

En las sociedades modernas el teléfono móvil se ha erigido como el más importante reflejo de la manifestación del pensamiento íntimo, o instrumento sobre el que se proyectan los factores que permiten reconocer la individualidad. El *smartphone* debe ser entendido como una proyección de la quintaesencia de lo que confiere su singular idiosincrasia a cada individuo y *lege ferenda* sería aconsejable marcar una línea roja en cuanto a su defensa[1182]. A día de hoy, whatsapp ha venido sustituyendo los servicios tradicionales de mensajes cortos o sistema de mensajería multimedia en los teléfonos móviles.

[1181] Capítulo publicado *vid.* CUADROS GARRIDO, M.E.: «El uso del WhatsApp en las Relaciones Laborales». *Nueva Revista Española de Derecho del Trabajo* núm. 171, 2014. (BIB 2014\4506).

[1182] RODRÍGUEZ MAGARIÑOS, F. G.: «Réquiem por el derecho a la intimidad en los smartphones: análisis de la última Jurisprudencia del TC contrastada con la del TEDH». *Revista Aranzadi Doctrinal* núm. 9, 2014 (BIB 2013\2696).

WhatsApp fue fundada en 2009 por Jan Koum y Brian Acton, exempleados de Yahoo!, es una aplicación de mensajería para enviar y recibir mensajes mediante Internet, complementando servicios de correo electrónico, mensajería instantánea, servicio de mensajes cortos o sistema de mensajería multimedia. Además de aprovechar la mensajería en modo texto, los usuarios pueden crear grupos y enviarse mutuamente, imágenes, videos y grabaciones de audio. Tiene más usuarios que Twitter[1183], cuenta con más de 600 millones de usuarios activos mensuales y debido a su alta productividad la aplicación ha sido comprada por Facebook.

Dada su presencia por doquier su uso se ha ido normalizando en el ámbito laboral. Como botón de muestra puede citarse que el art. 24 de Convenio Colectivo del sector de Industrias de Aderezo, Relleno, Envasado y Exportación de Aceituna de Sevilla[1184] establece que las llamadas al trabajo se podrán realizar por WhatsApp.

B) Problemas jurídicos

a) Secreto de las comunicaciones

Esta nueva fórmula de comunicación reviste los mismos patrones que el resto de sistema de "*mensajería instantánea*" y "*SMS*"; los mensajes enviados al destinatario pero aún no leídos por éste deben entenderse protegidos por el derecho al secreto de las comunicaciones. En este sentido puede citarse de la Sala Segunda la STS de 27 de junio de 2002[1185] , en conexión con la STC 70/2002 de 3 de abril[1186] , que considera tales mensajes son "*auténticas y genuinas comunicaciones personales, similares a las que se remiten y reciben por correo o telégrafo, pero cuyo vehículo de transmisión en este supuesto es el teléfono*", por lo que, de hecho, se trata de una especie de comunicación de una misiva personal efectuada vía telefónica, que no se "*oye"* por su destinatario, sino que se "*lee*" al aparecer en la pantalla del aparato y mediante esa lectura se conoce el

[1183] abc.es (2013, 23 de octubre) WhatsApp adelanta a Twitter con sus 350 millones de usuarios. *http://www.abc.es/tecnologia/moviles-aplicaciones/20131023/abci-whatsapp-twitter-usuarios-activos-201310231452.html*

[1184] BOP Sevilla 12 junio 2014, núm. 134

[1185] STS Sala Penal de 27 de junio de 2002 (RJ 2002\7219).

[1186] STC 70/2002, de 3 de abril (RTC 2002\70).

contenido del mensaje o de la misiva, por lo que resulta incuestionable que esta clase de comunicaciones se encuentran tuteladas por el secreto que establece el art. 18.3 CE[1187]. Razón por la cual debe hacerse extensible por analogía la protección constitucional que establece el art. 18 de la CE a la comunicación por whatsapp, tutelándose desde el comienzo hasta el final los derechos a la intimidad y al secreto de las comunicaciones[1188].

Así es, por mucho que varíe la realidad social, la base del derecho debe permanecer inalterable y adaptarse a las nuevas circunstancias. De lo contrario el Derecho se verá abocado a la caducidad y a su desaparición[1189].

b) Riesgos genéricos

Con respecto al derecho a la protección de datos, en febrero de 2014 el director de la oficina alemana de regulación de la privacidad, desaconsejó el uso de WhatsApp por no estar sujeto a la legislación europea en materia de seguridad y privacidad de la información, quedando desprotegidos los datos de los usuarios[1190].

La AEPD ha participado, en el análisis coordinado para examinar las condiciones de privacidad de las aplicaciones móviles más populares organizado por la Red Global de Control de la Privacidad (GPEN). Esta iniciativa tiene como objetivo fomentar el cumplimiento de la legislación de protección de datos y privacidad, promover la concienciación de los usuarios y obtener una visión integral y conjunta[1191]. Las entidades

---

[1187] Circular 1/2013, de 11 enero, de la Fiscalía General del Estado, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Apto. 5.-6 Acceso a mensajes de texto o SMS.

[1188] MONEREO PÉREZ, J.L y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *op. cit.*

[1189] JOSSERAND, L.: «El espíritu de los Derechos y su relatividad» en AA. VV. MONEREO LÓPEZ (Dir.): *Teoría del abuso de Derecho: El abuso de los Derechos Fundamentales*, ed. Comares, 2012, pág. 237.

[1190]elmundo.es (2014, 24 de febrero) Alemania desaconseja el uso de WhatsApp. *http://www.elmundo.es/tecnologia/2014/02/24/530b1a8fca4741c3388b456d.html*

[1191] AEPD (2014, 10 de septiembre) Nota de prensa: Resultados del análisis coordinado sobre las condiciones de privacidad de las aplicaciones móviles.*https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/sep_14/140910_NP_Resultados_analisis_GPEN.pdf*

que han llevado a cabo el análisis han mostrado su preocupación por el hecho de que el 31% de las aplicaciones analizadas, entre las que se encuentra whatsapp, solicitaban permisos excesivos en relación a las funciones que presta la *app*. Por otra parte, el 43% de las apps no habían adaptado sus políticas de protección de datos para ser leídas en pequeña pantalla, incluyendo políticas extensas y que obligaban a desplazar el texto en la pantalla o hacer clic en varias páginas.

c) Eficacia probatoria

Es una cuestión prácticamente unánime en los Juzgados de lo Social el hecho de admitir como prueba documental la transcripción de las conversaciones de whatsapp; la propia aplicación establece la posibilidad de reenviar por correo electrónico el histórico de las conversaciones tenidas con un determinado contacto o en determinado grupo, en el caso de impugnación en sede judicial habrá que estar al resultado de la pericial informática. Enumeramos seguidamente tres ejemplos en los que en uno se declara la nulidad de actuaciones por no admitir tal prueba, y otros dos en los que la transcripción de la conversación de whatsapp ha sido determinante para el fallo estimatorio de la sentencia.

La **STSJ de Cataluña de 15 de julio de 2014**[1192] declara la nulidad de actuaciones por no haber sido admitida por el Juzgador de Instancia, la prueba documental consistente en la transcripción de varias conversaciones de whatsapp. La Sala de Lo Social de Cataluña anula dicha resolución ordenando que sean repuestas las actuaciones al momento de la admisión de la prueba en el acto de juicio, para que se acuerde la práctica de la prueba documental solicitada que fue indebidamente inadmitida.

En la **STSJ de Andalucía de 21 de mayo de 2014**[1193], la transcripción de los whatsapps entre la actora, empleada de hogar sin dar de alta en seguridad social, y la empleadora sirve para probar la relación laboral existente. Las conversaciones sobre las funciones propias de la profesión (la comida que había que hacer a los niños que cuidaba) o sobre una de las notas de la relación laboral que es la retribución (preguntaba con qué fecha se le abonaría el sueldo del mes), son un elemento determinante para el Juez de

[1192] STSJ de Cataluña de 15 de julio de 2014 (JUR 2014\243599).

[1193] STSJ de Andalucía de 21 de mayo de 2014 (JUR 2014\205827).

Instancia para determinar que existía una relación contractual entre las partes de naturaleza laboral.

En la **STSJ del País Vasco de 13 de mayo de 2014**[1194], se declara nulo con violación de derechos fundamentales, el despido de una empleada de hogar que sufre acoso sexual por parte del empleador en base a la prueba documental aportada consistente en informes de Urgencias y de Psiquiatría, y en la reproducción de varios mensajes de whatsapp enviados por su empleador, con proposiciones sexuales, y con preguntas fuera de todo lugar (como el tipo de lencería que utilizaba ese día).

C) Tipología judicial

a) Abandono del trabajo (STSJ Aragón 23 junio 2013)

La STSJ de Aragón de 23 de junio de 2013[1195] desestima el recurso interpuesto y confirma el despido disciplinario por abandono del puesto de trabajo, en la documental aportada se transcribe una conversación vía whatsapp entre el recurrente y su jefe, en la que se constata su intención de no volver al trabajo porque le molestaba la presencia de otro compañero de trabajo.

b) ATS en Geriátrico (STSJ Galicia 15 abril 2014)

La STSJ de Galicia de 25 de abril de 2014[1196] declara que no vulnera el derecho al secreto de las comunicaciones de una empleada, la utilización como prueba para justificar su despido la transcripción de una conversación a través de whatsapp entre ella y otra interlocutora, compañera de trabajo que lo puso en conocimiento de la empresa.

La actora trabajaba como ATS en una residencia geriátrica y fue despedida por negligencia en la distribución y administración de los medicamentos a los residentes de la misma. La empresa justificó dicho despido en una comunicación por whatsapp, que la trabajadora remitió a su encargada, de la que se deduce que delega la administración de los medicamentos en auxiliares sanitarios de los que además "no se fía del todo ", como

[1194] STSJ de País Vasco de 13 de junio de 2014 (JUR 2014\230183).

[1195] STSJ de Aragón de 23 junio de 2014 (JUR 2014\197005).

[1196] STSJ de Galicia de 25 de abril de 2014 (EDJ 2014/126515).

admite en la conversación que llega a la empresa, pero el hecho cierto es que la encargada de la administración y verificación de ingesta de los fármacos por parte de los ancianos era ella. La recurrente alega que la intervención de conversación privada por whatsapp, es fraudulenta y atentatoria contra su derecho a la intimidad, la Sala contesta: "la prueba documental aportada por la empresa (transcripción de un whatsapp) no se ha efectuando vulnerando el secreto de las comunicaciones, contemplado en el art 18.3 de la CE y ello por cuanto que el conocimiento de la conversación privada lo tiene la empresa por la revelación de la otra interlocutora" (FJ 4º).

En consecuencia, se confirma la procedencia del despido al haber incurrido la trabajadora del geriátrico en un grave quebrantamiento de la buena fe contractual exigible que justifica tal calificación de la extinción como proporcionada a la máxima sanción impuesta.

c) Uso de Whatsapp conduciendo (STSJ Cantabria 18 junio 2014)

La STSJ de Cantabria de 18 de junio de 2014[1197], declara procedente el despido de un conductor de autobús que enviaba mensajes de whatsapp mientras conducía. Los hechos fueron conocidos por la empresa en virtud de una reclamación de una usuaria del servicio que aporta varias fotos de tal acción. Es evidente que constituye una grave negligencia en el cumplimiento de las obligaciones el conductor de autobús que utiliza el teléfono móvil, para el envío de whatsapp, mientras conduce durante casi todo el trayecto de la ruta. El trabajador había firmado que era conocedor del protocolo de la empresa sobre el uso del teléfono móvil e incluso acudió a una sesión informativa sobre seguridad y rellenó un cuestionario de manera correcta lo que demuestra su conocimiento previo de la infracción que estaba cometiendo.

[1197] STSJ de Cantabria de 18 de junio de 2014 (JUR 2014\180053).

d) Directora de Guardería (STSJ Cataluña 11 julio 2014)

La STSJ de Cataluña de 11 de julio de 2014[1198] desestima el recurso de la directora de un centro de educación infantil, que vio desestimada su demanda en la instancia, que declaró su despido procedente. La recurrente y el resto de maestras de una escuela de educación infantil, habían creado un grupo en la plataforma whatsapp, donde todos los mensajes enviados por sus componentes eran recibidos por el resto del grupo y por tanto podían participar todas las integrantes del mismo en las conversaciones.

Un día, la directora del centro participó en una conversación iniciada en whatsapp por otra trabajadora que realizó una fotografía de los genitales de un menor de la escuela dando lugar a comentarios fuera de tono. El contenido de esta conversación trascendió y fueron despedidas la directora y la maestra que subió la foto del menor. Resultaron amonestadas el resto de las trabajadoras participantes en la conversación.

La sentencia descarta que pueda aplicarse aquí la tesis gradualista y concluye que el incumplimiento es grave y culpable. Asimismo descarta que se haya vulnerado el principio de igualdad pese a que no todas las implicadas en la conversación del grupo fueron despedidas. La Sala razona con algo que es obvio, su responsabilidad, en calidad de directora del centro, es mayor que la del resto ya que no debía haber permitido ese tipo de conversación, debiendo pedir la inmediata eliminación de la foto y no hizo eso sino que los comentarios más censurables fueron los suyos. Lo que es algo grave y culpable y justifica la procedencia del despido.

E) Valoración

Puede concluirse que la transcripción de los mensajes de whatsapp es una cuestión no controvertida, pues suele admitirse su práctica como documental en el acto de juicio. Se admite que uno de los comunicantes sea al que aporte tal información a la empresa pues en este caso no se vulnera el secreto de las telecomunicaciones pues uno de los interlocutores interviene, se vulneraría el derecho a la intimidad del trabajador denunciado ante la empresa pero el infractor es el interlocutor no la empresa.

[1198] STSJ de Cataluña de 11 de julio de 2014(JUR 2014\241700).

Respecto a la fiscalización del teléfono móvil de la empresa, si existe una política de prohibición de uso, tal mandamiento neutraliza cualquier expectativa. Otro supuesto sería el del teléfono móvil propio que no es posible fiscalizarlo y si se quiere demostrar que se usa la aplicación whatsapp, habrá que realizarlo a través de otros medios como la prueba videográfica y siempre bajo el juicio de proporcionalidad.

CAPÍTULO IV. MAGNITUDES BIOMÉTRICAS

1. Planteamiento

A) Especificidad

Un sistema tradicional de identificación personal efectúa la autenticación a través de algo que se posee (una llave, una tarjeta de identificación, etc), y/o se sabe (una clave, un PIN, etc.). Es la forma de proceder de los llamados *sistemas de autenticación por posesión y por conocimiento*, respectivamente. Sin embargo, un *sistema biométrico* es un método de reconocimiento en el que la identidad de un individuo es determinada a partir de alguna de sus características fisiológicas o de comportamiento[1199]. La creciente demanda de acceso a los servicios de la Sociedad de la Información ha dado lugar en las últimas décadas a la aparición de una nueva rama de la Tecnología denominada Autenticación biométrica o simplemente Biometría. Un sistema biométrico podría definirse como "*un sistema automático que permite el reconocimiento de seres vivos a través de sus rasgos inherentes*"[1200].

La biometría es la ciencia que se encarga de medir las propiedades físicas de los seres vivos. El término procede del griego donde *bios* significa vida y *metron*, medida. Puede definirse como el estudio de métodos ideados para el reconocimiento de forma

[1199] ZORITA SIMÓN, D.: «Reconocimiento automático mediante patrones biométricos de huella dactilar», Tesis doctoral, Universidad Politécnica de Madrid, 2003, Pág.11 del original impreso. *http://oa.upm.es/79/1/09200327.pdf*

[1200]PASCUAL GASPAR, J. M. : «Uso de la firma manuscrita dinámica para el reconocimiento biométrico de personas en escenarios prácticos», Tesis doctoral Universidad de Valladolid, 2010, pág 1 del original impreso. *https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?fichero=13741*

única de personas en base a uno o más rasgos físicos intrínsecos o de comportamiento[1201]. El control biométrico asegura la imposibilidad de suplantación de un individuo por otro, a través de una característica física e intransferible de la persona. Se caracteriza asimismo por la auditabilidad, que permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados[1202].

Los controles biométricos son métodos que se usan para reconocer a los trabajadores basándose en determinadas características físicas (huellas digitales, iris, patrones faciales…), de conducta o mixtos.

B) Clases y caracterización

Una clasificación sencilla de las tecnologías biométricas se realiza en función de las características de las mismas: 1º) Rasgos fisiológicos. Son aquellos que corresponden a características estáticas diferenciadoras del cuerpo humano de índole principalmente física. Ejemplos de ello son la huella dactilar, iris y retina, geometría de la mano, reconocimiento facial. 2º) Rasgos de comportamiento. Son rasgos que están más relacionados con la conducta de la persona corresponden a características dinámicas. A esta categoría pertenecerían, por ejemplo, firma manuscrita, tecleo, paso, voz…

Los principales componentes que se pueden identificar en un sistema biométrico son: 1º) El sensor. Es el dispositivo de captura de los rasgos o características biométricas[1203]. Para registrar y convertir los rasgos biométricos en datos de computador se necesitan sensores adecuados. 2º) El repositorio. Es la base de datos donde se almacenan las plantillas biométricas inscritas para su comparación. Estas plantillas, deberían protegerse en un área física segura, cifradas y firmadas digitalmente[1204]. 3º) Los algoritmos para extracción de características (procesamiento) y comparación[1205].

[1201] ARETIO BERTOLIN, J. y ARETIO BERTOLIN, M. T.: «Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación», *Revista española de electrónic*a, núm. 630, 2007, pág. 52 del original impreso .*http://www.redeweb.com/_txt/630/52.pdf*

[1202] FORMETÍN ZAYAS, Y.: «La unificación de criterios sobre la utilización de la firma digital en los contratos electrónicos». *Base de Datos de Bibliografía* núm.30, 2007 (EDB 2007/104337).

[1203] ARETIO BERTOLIN, J., ARETIO BERTOLIN M. T. «Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación», *op. cit*., pág. 54.

[1204] *Ibídem*, pág. 56.

[1205] *Ibídem.*

C) Enfoque jurídico

Para la AEPD, los datos biométricos son datos personales, porque cumplen las de notas definición de dato personal[1206]. Como norma general, el uso de la biometría para las exigencias generales de seguridad de los bienes y las personas no puede considerarse un interés legítimo que prevalezca sobre los intereses o los derechos y libertades fundamentales del interesado. Por el contrario, el tratamiento de datos biométricos solo puede justificarse como un instrumento necesario para asegurar los bienes o las personas cuando se disponga de pruebas, sobre la base de las circunstancias objetivas y documentadas, de la existencia de un riesgo considerable. Para ello, el responsable del tratamiento deberá probar que determinadas circunstancias plantean un riesgo considerable específico, que deberá evaluar con especial cuidado[1207].

Los avances tecnológicos han dado lugar a un reducido número de pronunciamientos judiciales en los que se alude a mecanismos de control mucho más sofisticados que las tradicionales cámaras y micrófonos. Esta clase de artefactos, se podrían considerar como emergentes y entre ellos se encuentran los denominados controles biométricos y las etiquetas de identificación[1208].

2. La huella dactilar

A) Delimitación

Las huellas dactilares son un identificador biométrico ampliamente utilizado, su uso se extiende desde aplicaciones forenses y policiales hasta aplicaciones civiles muy comunes, como el control de accesos. La huella dactilar consiste en la reproducción de la epidermis de la parte posterior de los dedos de la mano. Una huella dactilar está formada

---

[1206] Informe de la AEPD sobre Tratamiento de la Huella Digital de los Trabajadores.http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/1999-0000_Tratamiento-de-la-huella-digital-de-los-trabajadores.pdf

[1207] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de trabajo del artículo 29, pág.14

[1208] SAN MARTIN MAZZUCCONI, C.: «El derecho a la protección de datos personales de los trabajadores: Criterios de la Agencia Española de Protección de Datos» en AA.VV. SAN MARTIN MAZZUCONI, C. (DIR): *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, ed. Eolas Ediciones, 2014, pág. 232.

por un conjunto de líneas que se denominan crestas (líneas oscuras) y valles (líneas claras). Este conjunto de líneas, que forma la huella dactilar puede asemejarse a patrones o texturas que se pueden analizar de diferentes maneras dependiendo del grado de detalle. Las características más utilizadas para el análisis y comparación de huellas dactilares son las minucias, que son los puntos singulares que presentan las crestas[1209].

Para identificar una huella dactilar (biometría estática), con vistas a obtener las minucias, se utilizan sensores capacitivos, ópticos, térmicos, acústicos y de presión.

B) Valoración jurídica

La AEPD considera este sistema de control como recomendable por la inexistencia de margen de error así como que la información contenida en ese dato, no posee ningún aspecto concreto de la personalidad, de modo que los datos que se recaban no son de mayor trascendencia que un número personal[1210].

En consecuencia, y de acuerdo con la doctrina constitucional, los datos biométricos de la mano no están protegidos por el derecho a la intimidad y aunque sean datos personales no convierte su exigencia y posterior tratamiento automatizado en ilegítimos, pues no se trata de datos de los que el art. 7 LOPD considere como especialmente protegidos[1211].

[1209] LINDOSO MUÑOZ, A.: «Contribución al reconocimiento de huellas dactilares mediante técnicas de correlación y arquitecturas hardware para el aumento de prestaciones», Tesis Doctoral. Universidad Carlos III de Madrid. 2009, pág.20
http://earchivo.uc3m.es/bitstream/handle/10016/5571/Tesis_Almudena_Lindoso_Munoz.pdf?sequence=1

[1210] Informe 324/2009 de la AEPD.

[1211] Auto TC núm. 57/2007 de 26 febrero. Rec. Núm. 4243/2003.(RTC 2007\57).
«*No pueden entenderse como intromisiones forzadas en la intimidad aquellas actuaciones que, por las partes del cuerpo humano sobre las que se opera o por los instrumentos mediante los que se realiza, no constituyen, según un sano criterio, violación del pudor o recato de las personas*» (FJ 5º).

C) Tipología judicial

a) Costumbre empresarial (STSJ Cataluña 9 mayo 2011)

En ocasiones a la hora de resolver estos litigios por parte de los tribunales para enjuiciar el horario de entrada y salida de los trabajadores, se toma en consideración la costumbre extendida en la empresa que modula a veces el estricto control horario en una comunicación escrita de sanción. Sirva de ejemplo la STSJ de Cataluña de 9 de mayo de 2011[1212], en la se declara probado que existía un horario flexible en la mercantil dedicada a servicios financieros, ya que estaba generalizado que el horario para salir a la comida se hacía en función de las condiciones especiales "*del fluctuante mercado bursátil*", por lo que se rebajó la sanción impuesta.

b) Negativa a suministrarla (STSJ País Vasco 17 enero 2012)

En principio la negativa de un trabajador a facilitar su huella dactilar para impedir la aplicación del sistema de control de su hora de entrada y de salida al trabajo mediante el lector biométrico instalado al efecto, carece por sí sola de la gravedad exigida para ser subsumida en el incumplimiento contractual previsto en el artículo 54.2.b) del Estatuto de los Trabajadores, como así resuelve la STSJ País Vasco de 17 de enero de 2012[1213] en su FJ 2º:

> *"(...) aun aceptando que la negativa de la actora a facilitar su huella dactilar a los fines anteriormente reseñados carece de la gravedad exigida para ser subsumida en el incumplimiento contractual previsto en el artículo 54.2.b) ET, máxime si se tiene en cuenta que no medió sanción ni advertencia previa sobre las consecuencias de su decisión, subsisten las ausencias de los días 17 y 25 de enero de 2011 (media jornada), 7 y 28 de ese mismo mes (media jornada), y 15 a 18 de febrero siguiente, que, en defecto de regulación convencional específica, a la que no hacen referencia las partes, tienen la entidad y trascendencia suficiente para determinar, por sí solas, la procedencia del despido(...)".*

[1212] STSJ de Cataluña de 9 de mayo de 2011 (EDJ 2011/129389).

[1213] STSJ de País Vasco de 17 de enero de 2012 (EDJ 2012/96580).

c) Condición más beneficiosa (STS 16 septiembre 2015)

La implantación de sistemas RFID de lectura de huella dactilar no puede afectar a condiciones más beneficiosas existentes antes de su instalación para los trabajadores afectados. En este sentido la STS de 16 de septiembre de 2015[1214] confirma la sentencia de la AN sobre conflicto colectivo, respecto a la pausa del bocadillo. El origen de todo, resultó ser debido a que durante la pausa del bocadillo había trabajadores que salían fuera de las instalaciones de la empresa y otros que permanecían en su interior. Se producía así un descuadre en el control del acceso y salida de los mismos mediante huella dactilar, por esta razón acabó prohibiéndose tal descanso.

En consecuencia, el TS confirmó la declaración de nulidad de la decisión empresarial, en lo que respecta a los empleados que venían disfrutando de la pausa del bocadillo llevada a cabo por la AN; reconociendo el derecho a ser repuestos en sus anteriores condiciones, en que se les computaba ese período como tiempo de trabajo. Se trataba de una condición más beneficiosa cuando resulta clara la voluntad de la empresa de atribuir un derecho que no aparece reconocido ni en el Convenio de aplicación ni en la normativa de la empresa. Pero cualquiera que sea el título originario de la concesión, constituía un derecho adquirido y no un mero uso de empresa.

d) Implantación de control horario

La **STS-CONT de 2 de junio de 2007**[1215] resolvió el recurso de casación planteado por los sindicatos contra la Sentencia de la Sala lo Contencioso del TSJ, que confirmaba la decisión de la Consejería de la Presidencia de Cantabria sobre la implantación de un nuevo sistema de control horario consistente en la huella digital, pues no menoscaba el derecho a la integridad corporal. Así dice que *No es coextensa la intimidad corporal con la realidad física del cuerpo humano y que aquélla es un concepto cultural determinado por los criterios que prevalecen en materia de recato corporal de manera que no podrán apreciarse vulneraciones de ella ante actuaciones sobre partes*

[1214] STS de 16 septiembre 2015 (RJ 2015\5755).

[1215] STS, Sala de lo Contencioso-Administrativo, de 2 de julio de 2012 (LRJ 2007\6598) .

del cuerpo sobre las que no opera ese recato. Y nada de esto ocurre con la lectura biométrica de la mano.

En igual sentido, la **STSJ de Murcia de 25 de enero de 2010**[1216], confirmó el rechazo a la demanda por conflicto colectivo referida a la implantación de un sistema de control de acceso con huella digital en las instalaciones de la empresa HEFAME en lugar del anterior de fichaje a través de tarjetas, al no implicar este control una modificación sustancial de las condiciones de trabajo, a los efectos del art. 41 ET. La implantación de un control de acceso a las instalaciones, como el que la empresa demandada había establecido, no comportaba modificación sustancial de las condiciones de trabajo. Tampoco por la Sala se considera que este sistema que vinculaba la lectura de las huellas digitales a los datos de identidad de los trabajadores existentes revistiera los caracteres para considerarse una intromisión ilegítima en la esfera de la intimidad y, aunque es cierto que afecta a todos los trabajadores de la empresa, no se requiere para proceder a su adopción, un acuerdo con los representantes de los trabajadores:

> *"Del examen de las presentes actuaciones, no se aprecia que los trabajadores afectados por la entrada en funcionamiento del nuevo sistema de control de acceso hayan perdido "el poder de control y disposición sobre sus datos personales", integrado por los derechos que corresponden a los afectados a consentir la recogida y el uso de sus datos personales a conocer los mismos y, para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos", en los términos que previene la doctrina del TC" (FJ 4º)*

Recogiendo la doctrina anterior, la **STSJ de Canarias de 29 de mayo de 2012**[1217] afirma: "*un mecanismo de lectura biométrica de la mano mediante un escáner que utiliza rayos infrarrojos y que es inocuo para la salud no puede considerarse lesivo para el derecho a la integridad física y moral*." Y procedió a confirmar la sentencia de instancia, que rechazó la pretensión de un miembro del comité de empresa que impugnó el sistema de acceso al puerto de Gran Canaria a través de la huella digital.

[1216] STSJ de Murcia de 25 de enero de 2010 (EDJ 2010/18129).

[1217] STSJ de Islas Canarias de 29 de mayo de 2012 (AS 2012\1915).

3. El ADN

A) Delimitación

Para el control de acceso por el ADN[1218] se emplea un laboratorio químico o una unidad electrónica automatizada de análisis. La prueba del ADN no sólo tiene una finalidad de identificación, sino que además, y con mayor amplitud, nos determina toda la información genética de una persona y con ello facilita, datos y aspectos que afectan de forma clara y evidente a la intimidad de la persona[1219]. Los avances en el análisis del ADN presentan a su favor la ventaja de que los resultados están disponibles en cuestión de minutos.

Por otra parte, el ADN de necesaria obtención a efectos de identificación de una persona es el ADN no codificante o no expresivo, que no revela características fenotípicas[1220] de los individuos. Este hecho es de gran importancia en tanto se ve reducida la afectación de la esfera de intimidad del sujeto y, con ello, el ámbito de su cobertura constitucional, por lo que, si es necesario un control de identidad a través del ADN, lo recomendable es realizarlo a través del ADN no codificante.

B) Protección de datos

Los datos de ADN de una persona a menudo incluyen información sobre la salud o pueden revelar el origen racial o étnico. En este caso, los datos de ADN son datos sensibles y en su manejo deben aplicarse las garantías especiales previstas en el artículo 8 de la Directiva 95/46/CE además de los principios generales de protección de datos de la Directiva[1221].

[1218] El ácido desoxirribonucleico, abreviado como ADN, es un ácido nucleico que contiene instrucciones genéticas usadas en el desarrollo y funcionamiento de todos los organismos vivos conocidos y algunos virus, y es responsable de su transmisión hereditaria.

[1219] SIERRA FERNÁNDEZ, J.: «Bases de datos policiales sobre identificadores obtenidos a partir del ADN, la nueva normativa aplicable», *Revista de Jurisprudencia El Derecho*, núm. 4, 2008, pág. 2.

[1220] Término usado en bilogía y genética que se refiere a la expresión del genotipo (información genética que posee un organismo en particular en función de su ADN) en función de un determinado ambiente, son manifestaciones aparentes del patrimonio hereditario del individuo modificado por el medio ambiente.

[1221] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de trabajo del artículo 29. Pág.16
https://www.apda.ad/system/files/wp193_es.pdf

El nuevo Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos[1222], en su art.4 establece que por datos genéticos se entienden aquellos de carácter personal relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica suya. En el art 9.1 con la rúbrica "Tratamiento de categorías especiales de datos personales", recoge:

> "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física".

En el apartado 2 se excluye la aplicación del apartado anterior si media consentimiento expreso, concurren razones de interés público, etc. Y el apto. 4 del mismo art. se reserva a los estados miembros la capacidad de establecer una regulación más restrictiva en esta materia[1223].

De conformidad con el art. 3 j) de la Ley de Investigación Biomédica[1224] se considera dato genético de carácter personal el que proporciona información sobre las características hereditarias de una persona identificada o identificable obtenida por el análisis de ácidos nucleicos u otros análisis científicos. Este precepto ha venido a llenar una laguna que existía en nuestro ordenamiento, aproximándose a la que ya ofrecía la Declaración Internacional sobre Datos Genéticos Humanos[1225], aprobada por la Conferencia General de la Unesco de 16 de octubre de 2003[1226].

[1222] *https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf*

[1223] "Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud".

[1224] Ley 14/2007 de 3 de julio

[1225] GRAMUNT FOMBUENA, M.: El tratamiento de la investigación genética en la Ley de Investigación Médica en AA.VV. LLÁCER MATACÁS, J. (Coor): *Protección de datos personales en la sociedad de la información y la vigilancia,* ed. La Ley. 2011.Pág.179.

[1226] La regulación de la base de datos policial sobre identificadores obtenidos a partir de ADN para fines de investigación criminal se encuentra en la LO 10/2007 de 8 de octubre.

B) Derechos en presencia

Por tanto, la prueba del ADN puede afectar a la esfera íntima del trabajador, siendo válida su práctica si se han preservado todas las garantías para su obtención, debiéndose desarrollar sin que exista vulneración alguna de la dignidad humana (art. 10.1 CE); no se debe tampoco infringir el derecho a la integridad física que gozan todos los ciudadanos (art. 15.1 CE) ni el derecho a violar la propia intimidad (art. 18.1 CE) ni el vulnerar el derecho la autodeterminación informativa (art. 18.4 CE).

La recogida del ADN de una persona no implica automáticamente la vulneración de su integridad física; sobre todo porque su extracción puede llevarse a efecto en alguna parte del cuerpo que no suponga una intromisión a su intimidad; por ejemplo, la saliva[1227]. Las técnicas actuales nos llevan a entender que las muestras necesarias para la realización de análisis pueden obtenerse a partir de partes o elementos corporales mucho más sencillos de conseguir (pelo, uñas, etc.)[1228].

El problema de identificación por el ADN se encuentra en que a través del mismo se pueden obtener datos relativos a la salud del trabajador. Datos que en virtud del mandato del art.5 LOPD son "*sensibles*", por lo que es preciso que el empleado preste su consentimiento de manera expresa, para que se pueda proceder al tratamiento de estos datos. En igual sentido el art. 4 de la Ley 14/2007, acomoda la necesidad del consentimiento del informado. Por otro lado, y dado el carácter de esta información, se ha de estar ante una finalidad legítima que obligue a esta prueba de control tan sofisticada, por lo que se ha de ponderar su conveniencia en virtud del principio de proporcionalidad.

[1227] PORTAL MANRUBIA, J.: «La huella genética en la jurisdicción de menores», *Revista Aranzadi Doctrinal* núm. 9, 2010.

[1228] SIERRA FERNÁNDEZ, J.: «Bases de datos policiales sobre identificadores obtenidos a partir del ADN, la nueva normativa aplicable», *op.cit*., pág. 1.

4. Otras técnicas

A) Biométrica dinámica

La firma manuscrita efectuada en un dispositivo electrónico constituye el mecanismo no automatizado de verificación de la identidad de personas más usado en la actualidad y, según informes de mercado, es la segunda modalidad en importancia en Biometría conductual, justo detrás de la voz[1229].

Para reconocer la firma manuscrita (biometría dinámica) se emplea una tableta sobre la que escribir que detecte presión, aceleración del lápiz, inclinación, etc.

Es un sistema recomendable, por ser menos problemático y económico, pues, sólo necesita conectarse a una tableta[1230].

B) Estructura de la retina

El patrón de vasos sanguíneos en la retina se presenta como una característica biométrica relativamente joven pero muy interesante debido a sus propiedades inherentes. Para obtener la identificación por la estructura de la retina, se hace uso de una cámara de vídeo, TV o cámara web. La nota que presenta este importante sistema de identificación es que se trata de un patrón único para cada individuo. Además, al ser una característica interna es casi imposible crear una copia falsa. Por último, otra propiedad a destacar es que el patrón no cambia significativamente a lo largo del tiempo excepto en casos de algunas patologías médicas severas y no muy comunes[1231].

[1229] PASCUAL GASPAR, J. M. :«Uso de la firma manuscrita dinámica para el reconocimiento biométrico de personas en escenarios prácticos».*op. cit.*, pág 109.

[1230] 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», op. cit., pág.6

[1231] ORTEGA ORTAS, M.: «Automatic system for personal authentication using the retinal vessel tree as biometric pattern». Tesis doctoral Ed. Universidad de la Coruña. 2009.pág. 12 *http://ruc.udc.es/dspace/bitstream/2183/5678/1/OrtegaHortas_Marcos.tesis.pdf*

C) El iris ocular

El escaneo de iris se realiza analizando los patrones de color de los surcos de la parte coloreada de los ojos. Es uno de los sistemas biométricos más fiables debido a que posee alrededor de 266 puntos únicos mientras que la mayoría de sistemas biométricos poseen alrededor de 13 a 60 características distintas[1232]. Para obtener la identificación por la estructura del iris se emplea una cámara de vídeo, TV o cámara Web.

El problema reside en que a través de la lectura del iris, se pueden obtener datos relativos a la salud del trabajador, dándose, por tanto, el peligro de realizar actuaciones discriminatorias contra determinados trabajadores[1233].

Al existir la posibilidad de desprenderse de la lectura del iris datos "*sensibles*", en virtud del mandato del art.5 LOPD no solo es necesario que el trabajador conozca de la existencia de un fichero que incluye datos personales suyos, sino que es necesario que consienta de manera expresa, para que se puedan tratar estos datos[1234].

D) Reconocimiento de la voz

El reconocimiento de voz consiste, esencialmente, en el proceso de interpretación de una palabra pronunciada por una persona, perteneciente a un conjunto determinado de palabras, después de capturar la señal acústica que corresponde a la pronunciación de esta palabra a través de un micrófono.

Las palabras interpretadas o reconocidas son los resultados finales del proceso de reconocimiento de voz, que pueden usarse para iniciar diversas acciones en un sistema, a partir de la palabra reconocida como comando de voz. Y también, puede servir para introducir datos e información que corresponda justamente a la palabra reconocida[1235].

[1232] CORTES OSORIO, J.A. , MEDINA AGUIRRE, F.A. y MURIEL ESCOBAR , J.A.: «Sistemas de seguridad basados en Biometría» Scientia et Technica, Vol. 3, Núm. 46, 2010, pág. 100. *http://www.redalyc.org/pdf/849/84920977016.pdf*

[1233] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *op.cit*, págs. 53-54.

[1234] 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» *op. cit*., pág.12.

[1235] GARCÍA GARRIGOS. J.J.: «Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos». Proyecto Fin De Carrera. Escuela Técnica Superior de Ingeniería Electrónica. Universidad de Valencia, pág. 12.

E) Reconocimiento facial

Es considerado por el Grupo de Trabajo del 29[1236] incluido en el ámbito de la biometría, ya que contiene detalles suficientes para identificar a una persona de manera inequívoca, y transmitirlas a continuación a un servidor remoto para su tratamiento, lo que permite el establecimiento del perfil automatizado[1237].

El algoritmo de detección de caras está basado en una función que busca regiones rectangulares dentro de una imagen, regiones que contengan objetos que con una alta probabilidad se parezcan a otros de un conjunto de entrenamiento, devolviendo la región rectangular de la imagen donde se han encontrado. La función escanea varias veces la imagen y con diferentes escalas para encontrar objetos parecidos pero de diferentes tamaños[1238]. El proceso de identificación facial se divide básicamente en dos tareas: detección y reconocimiento La primera de ellas, la detección, comprende la localización de una o varias caras dentro de una imagen, ya sea fija o una secuencia de vídeo. La segunda tarea, el reconocimiento, consiste en la comparación de la cara detectada en el paso anterior con otras almacenadas previamente en una base de datos[1239].

https://www.researchgate.net/profile/Juan_Garcia_Garrigos/publication/259705766_Sistema_de_Autenticacion_Biometrica_de_Huella_Dactilar_asistido_por_Interfaz_de_Voz_para_el_Control_de_Accesos/links/02e7e52d69a04f3a57000000.pdf?inViewer=0&pdfJsDownload=0&origin=publication_detail

[1236] Ha emitido el Dictamen núm. 02/2012 sobre reconocimiento facial en los servicios en línea y móviles, de 22 de marzo, en el que señala que esta tecnología que ha sido integrada en los teléfonos para la identificación , autenticación (entiéndase verificación de la identidad) o categorización de las personas estando tanto a disposición de las organizaciones públicas como de las privadas, utilizándola las redes sociales y los fabricantes de teléfonos inteligentes. Se alerta de la posibilidad de la obtención ilícita de las imágenes , a través de un proceso de recuperación de sitios públicos como las memorias de caché de los motores de búsqueda, lo que suscita muchas preocupaciones en lo que respecta a la protección de datos de carácter personal.

[1237] DÁVARA RODRÍGUEZ, M.Á.: *Manual de Derecho Informático, op. cit.*, pág. 600.

[1238] MARTÍNEZ PÉREZ, J.V.: Sistemas de reconocimiento facial y realidad aumentada para dispositivos móviles. *TIC cuadernos de desarrollo aplicados a las TIC*, núm. 1,2012. pág. 5.

[1239] *Ibídem.*

7. Pautas comunes para la correcta aplicación

El registro formado por estos datos personales junto a los demás de este carácter incluidos en el fichero está sujeto a las previsiones de la LOPD, entre las cuales se hallan las relativas a la información a los afectados, prevista en el art. 5.1 y a la notificación del fichero a la Agencia Española de Protección de Datos.

El art. 6.2 de la LOPD excluye el consentimiento expreso del afectado cuando los datos de carácter personal se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. En general, el empleador está legitimado para tratar los datos biométricos de los empleados sin consentimiento de estos, salvo los controles que recaben datos especialmente sensibles, como hemos visto. En estos casos el consentimiento sólo es válido cuando se proporciona información suficiente sobre la utilización de los datos biométricos.

Dado que los datos biométricos pueden utilizarse como un identificador único y universal, el suministro de información clara y fácilmente accesible sobre cómo se utilizan los datos específicos debe considerarse absolutamente necesario para garantizar un tratamiento equitativo[1240]. Por tanto, este es un requisito esencial para un consentimiento válido en el uso de esa clase de datos.

El problema con respecto a los datos biométricos, es que existe el riesgo de que sean reutilizados con otros fines[1241] , incrementándose la vulnerabilidad del trabajador en estos casos, por lo que se recomienda que su uso sea valorado desde el principio de proporcionalidad, a partir de dos variables: 1º) Cabe preguntarse si es necesario e indispensable recurrir a su uso; si no existen otros medios alternativos. 2º) Debe elegirse

[1240] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de trabajo del artículo 29. Pág.12

https://www.apda.ad/system/files/wp193_es.pdf

[1241] La Directiva 95/46/CE prohíbe el tratamiento ulterior que fuera incompatible con los fines para los que se recogieron los datos.

el sistema biométrico idóneo, pues no todos entrañan el mismo riesgo para la intimidad de los trabajadores. En este sentido el Grupo de Trabajo del Grupo 29, mantiene una clara preferencia por las aplicaciones biométricas que no almacenan datos en un sistema centralizado, las que manejan datos identificativos básicos. Ello permite al interesado ejercer un mejor control sobre los datos personales tratados que le afectan[1242].

En el Informe 1999/000 de la AEPD, se planteó si la huella digital podía ser considerada un dato de carácter personal, y en su caso afirmativo, el tratamiento que correspondía aplicarle. La AEPD contesta que la huella digital es un dato personal y, dado que en la misma no se incluye ningún aspecto concreto de la personalidad, limitándose su función a identificar a un sujeto, no se requiere un almacenamiento de datos en una base centralizada[1243], pues son datos identificativos básicos[1244].

Por tanto las aplicaciones biométricas que no requieran almacenar la biometría en una base de datos centralizada, sino más bien sólo exclusivamente en un sop¡orte a disposición exclusiva para el usuario, son las más idóneas, por cuanto ello permite al afectado "*ejercer un mejor control sobre los datos personales que le afectan*"[1245].

En concordancia con todo ello, es lógico que una posible manipulación de la información que se desprende de los datos biométricos por parte del personal que pueda tener acceso a los mismos constituya una grave transgresión de la fe contractual, como entiende la STSJ de Asturias de 27 de marzo de 2015[1246].

[1242] Documento de trabajo sobre biometría del Grupo 29. Adoptado el 1 de agosto de 2003. pág. 12. Disponible en *https://www.apda.ad/system/files/wp80_es.pdf*

[1243]Tratamiento de la huella digital de los trabajadores, Informe 1999/000 de la AGPD. *http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/1999-0000_Tratamiento-de-la-huella-digital-de-los-trabajadores.pdf*

[1244] 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». *Op. cit*. Pág.11

[1245] GOÑI SEIN, J.L.: «Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», o*p.cit*., págs. 56-57.

[1246] STSJ de Asturias de 27 de marzo de 2015 (EDJ 2015/48601) En esta sentencia, se desestima el recurso de suplicación de un trabajador que fue despedido por manipular desde su ordenador los datos del fichaje de su propio acceso correspondientes a distintos días, al haber reconocido la autoría de los hechos, pretende que no se le sancione con el despido, en base a la teoría gradualista.

8. Reflexión conclusiva

Cierto sector de la doctrina considera que los sistemas de control de esta naturaleza son excesivamente rigurosos y exhaustivos, salvo que se justifique su carácter indispensable, por ser necesario para el desarrollo del proceso productivo deberían considerarse atentatorios de la dignidad del trabajador[1247].

El mayor problema que plantea el aspecto de la obtención de datos biométricos es su correcto control y tratamiento por parte de la empresa[1248]. En otro caso, resultan posibles por las infracciones de la LOPD, y es recomendable buscar un sistema de identificación que trabaje con datos identificativos básicos.

[1247] RODRÍGUEZ ESCANCIANO, S. *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op.cit*., pág.111.

[1248] SELMA PENALVA, A.: «El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores», *Revista Doctrinal Aranzadi Social* núm. 9, 2010 (BIB 2010\735).

CAPÍTULO V. SISTEMAS ESPECIALES DE TRABAJO

1.El teletrabajo

El teletrabajo como forma de prestación de servicios laborales brinda la posibilidad de desarrollar el trabajo fuera de las instalaciones de la empresa, a través de las tecnologías de la información y de las comunicaciones. Son frecuentes también otras denominaciones como trabajo a distancia, trabajo remoto, trabajo no presencial, trabajo en red, etc. No obstante, tal variedad terminológica no afecta a la delimitación conceptual de la realidad que se pretende identificar[1249].

A) Relevancia

La globalización económica ha producido como uno de sus principales efectos el proceso de deslocalización, que evoluciona aceleradamente: la transferencia total o parcial, física o virtual, de las actividades empresariales, a otras áreas geográficas, a través de la reestructuración de la cadena productiva, en busca de nuevos mercados potenciales, con menores costes de producción, con competencias tecnológicas o recursos abundantes y menor control social, fiscal, contable y ecológico[1250]. De sistemas de producción fijos se ha pasado de manera gradual a procedimientos flexibles y abiertos, según el llamado modelo del "*trébol*" en base al cual una parte de la actividad se desarrolla con personal interno, otra porción con empresas contratadas o subcontratadas (*outsourcing*[1251]), y el resto con trabajadores externos autónomos, personal de ETT´s, teletrabajadores, etc[1252].

[1249] ESCUDERO RODRÍGUEZ, R.: «Descentralización productiva y nuevas formas organizativas del trabajo» X Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Ministerio de Trabajo e inmigración, 2000, pág. 763

[1250] DE LIMA PINEL. M. F.: «Asimetría geográfica en la deslocalización: señal verde para las empresas y roja para los trabajadores». *Revista Universitaria de Ciencias del Trabajo*, núm. 11, 2010, págs. 225- 241.

[1251] Externalización de recursos y procesos.

[1252] GALLARDO MOYA, R.: *El viejo y el nuevo trabajo a domicilio: de la máquina de hilar al ordenador*, ed. Ibídem. 1998, pág. 9.

Por otro lado, la incorporación de la mujer al trabajo ha supuesto un cambio en el modelo de sociedad, esto ha repercutido en las empresas y en las familias[1253]. Algunos indicadores según los últimos datos oficiales disponibles nos ponen de relieve los marcadores sociales: natalidad 9%[1254], desempleo 18,91%[1255] , junto con otros indicadores empresariales como el índice de producción industrial situado en el porcentaje del 1,2%[1256] y el índice de competitividad con un 4,59% [1257] (somos economía 33 WEF[1258]), que nos indican que debemos adaptar la realidad actual a las exigencias de los tiempos. Entre los nuevos mecanismos de flexibilidad de la estructura empresarial se encuentra el teletrabajo[1259], que apareció por primera vez en EEUU, con motivo de la crisis del petróleo de los años 70 del siglo pasado.

[1253] AA. VV. FUNDACÍON MASFAMILIA (Coor).: El libro blanco del teletrabajo en España. Del trabajo a domicilio a los e-workers. Un recorrido por la flexibilidad espacial la movilidad y el trabajo en remoto. 2012. Pág.11. *http://www.teledislab.es/descargas/libroblancoteletrabajoespana.pdf*

[1254] INE (2016, 23 de junio) Nota de prensa sobre el Movimiento Natural de la Población. Indicadores Demográficos Básicos.

ño	acs.	dos.	Falleci	mortalidad	Tas a Natalidad	Índice de Fecund.
15	19.109	6	422.27	9,1%	9‰	1,33

http://www.ine.es/prensa/np976.pdf

[1255] INE (2016, 7 de noviembre) Nota de prensa sobre los Índices de producción industrial *http://www.ine.es/daco/daco42/daco422/ipi0916.pdf*

[1256] INE (2016, 23 de junio) Nota de prensa sobre el Movimiento Natural de la Población. Indicadores Demográficos Básicos.

ño	acs.	dos.	Falleci	mortalidad	Tas a Natalidad	Índice de Fecund.
15	19.109	6	422.27	9,1%	9‰	1,33

http://www.ine.es/prensa/np976.pdf

[1257] Datos 2016 *http://www.datosmacro.com/estado/indice-competitividad-global*

[1258] El Foro Económico Mundial (WEF=*WorldEconomicForum*) es organización una organización internacional e independiente comprometida a mejorar el estado del mundo mediante la participación de líderes empresariales, políticos, académicos, y otros representantes significativos de la sociedad para dar forma a las agendas globales, regionales e industriales.

[1259] Jack Nilles ingeniero y físico de profesión en 1972 se unió a la Universidad del Sur de California como Director de investigación interdisciplinaria y comenzó su investigación formal sobre teletrabajo, término que acuñó en 1973.

El teletrabajo aumenta en todo el mundo, abandonando definitivamente su fase embrionaria[1260], la media europea que está en un 35% en nuestro país, aunque en nuestro país los datos del INE reflejan que sólo el 27% de las empresas permiten el teletrabajo[1261]. Asimismo, en el mismo periodo, el 21 por ciento de las grandes empresas y el 16 por ciento de las pequeñas dispondrá de algún tipo de programa o iniciativa que promueva esta forma de trabajo, según datos del Instituto Nacional de Estadística. Sin embargo, en la actualidad, muchos empresarios y empleados continúan mirando con recelo la propuesta, pues según la última Encuesta de Población Activa señala, el 91,8 por ciento de los ocupados no trabajó ni un solo día en casa[1262]. Según los expertos, las causas son varias: el temor al aislamiento profesional, la dificultad para concentrarse en casa, y determinados aspectos de índole cultural, como la necesidad de estar físicamente en el lugar de trabajo y "*dejarse ver*"[1263].

En España, en el trabajo, prima principalmente la relación y la confianza; mientras que en Estados Unidos, el país donde más desarrollado está el teletrabajo, lo es la tarea, y el éxito en el trabajo se consigue alcanzando los objetivos marcados. En nuestro país existe un problema cultural asociado con el estilo de gestión basado en la relación y el corto plazo de los gestores españoles[1264]. En nuestro país la empresa de publicidad de las páginas amarillas propietaria del conocido número de información telefónica 11888, procedió a despedir de manera colectiva a muchos de sus trabajadores, lo que llevó al

---

[1260] THIBAULT ARANDA, J.: «Teletrabajo: ¿retorno al pasado esperanza de futuro?» *http://www.unizar.es/centros/eues/html/archivos/temporales/08_AIS/AIS_08_11.pdf*

[1261] (2016, 4 de marzo). *http://www.computerworld.es/tendencias/solo-el-27-de-las-empresas-espanolas-apuesta-por-el-teletrabajo*

[1262] INE (2016, 23 de junio) Nota de prensa sobre Encuesta de Población Activa. http://www.ine.es/daco/daco42/daco4211/epa0316.pdf

ño	acs.	dos.	mortalidad	a Natalidad	de Fecund.
15	19.109	422.276	9,1%	9‰	1,33

http://www.ine.es/prensa/np976.pdf

[1263] AA. VV. FUNDACÍON MASFAMILIA (Coor). El libro blanco del teletrabajo en España. Del trabajo a domicilio a los e-workers. Un recorrido por la flexibilidad espacial la movilidad y el trabajo en remoto, *op.cit.*, pág.10.

[1264] MILLÁN TEJEDOR, R. J.: «El teletrabajo como solución a la insostenibilidad de los parques empresariales españoles», *Bit* núm. 189, 2012.

cierre de centros de trabajo en varias provincias, y la empresa a los trabajadores que estaban adscritos a tales centros que se vieron extinguidos, les ofreció el traslado a la sede social que estaba en Madrid o pasar su modalidad de trabajo al teletrabajo. Todos los trabajadores optaron por esta última opción, por lo que tal alternativa, se ofrecía como una opción al traslado de domicilio, lo que en definitiva, beneficiaba a al trabajador[1265]. Sería deseable que en los supuestos de crisis económica fuera escogido el teletrabajo por otras empresas, en lugar de optar por trasladar al trabajador.

Pero el hecho cierto es que el teletrabajo incrementa en al menos un 15 por ciento la productividad de los empleados, contribuye a la sostenibilidad, por lo que conlleva el ahorro en desplazamientos, y facilita la conciliación de la vida laboral y familiar[1266].

B) Delimitación conceptual

El teletrabajo se caracteriza por su localización fuera del ámbito de la empresa desde la que se presta la actividad laboral[1267]; es aquella particular forma de organización del trabajo que se realiza a través del uso intensivo[1268] de las nuevas tecnologías[1269], y se materializa con el consentimiento del trabajador, mediante un acuerdo escrito (*requisito ad solemnitatem*) con el empresario. No es, por tanto, una profesión o un estatuto jurídico de las personas[1270]. Se ha dicho que estamos ante un fenómeno "*proteiforme*", por lo que hay por consiguiente diferentes tipos de teletrabajadores, desde el más sofisticado y autónomo, hasta el que lleva a cabo un trabajo tedioso y repetitivo[1271]. El trabajador a distancia tiene los mismos derechos que los que prestan sus servicios en el centro de

---

[1265] SAN de 23 diciembre de 2015 (JUR 2016\16114).

[1266] Europa Press (2016, 25 de enero) «El teletrabajo facilita la conciliación y aumenta un 15% la productividad» , *vid.* http://elprogreso.galiciae.com/noticia/494925/el-teletrabajo-facilita-la-conciliacion-y-aumenta-un-15-la-productividad

[1267] QUINTANILLA NAVARRO, R.Y.: «El Teletrabajo: Delimitación, Negociación colectiva y conflictos» en AA. VV. SAN MARTÍN MAZZUCONI, C. (DIR.): *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, ed. Eolas, 2014, pág. 335.

[1268] El uso de las TIC debe ser continuado e intenso y no accesorio o esporádico.

[1269] SEMPERE NAVARRO, A.V. y KAHALE CARRILLO, D.T.: *Teletrabajo*. Claves Prácticas, ed. Francis Lefebvre, 2014, pág. 31.

[1270] ESCUDERO RODRÍGUEZ, R.: «Descentralización productiva y nuevas formas organizativas del trabajo», *op.cit.*, págs. 769-770.

[1271] PÉREZ DE LOS COBOS ORIHUEL, F.: «Prólogo» en THIBAULT ARANDA, J. *El teletrabajo. Análisis jurídico laboral*, ed. CES, 2001, pág. 15.

trabajo, salvo los inherentes al trabajo presencial[1272] (dietas, desplazamientos, plus penosidad, etc.)

Por primera vez una actividad laboral que se ejecuta fuera de la empresa, puede ser supervisada como si el trabajador estuviera en los locales de la misma[1273] y a diferencia de otros ordenamientos jurídicos de nuestro entorno, como el italiano, nuestro ET no prohíbe la utilización de medios de control a distancia, pues ello sería tanto como "*ir en contra el signo de los tiempos*"[1274].

El poder directivo no se atenúa por la distancia, sino que se acentúa por los instrumentos de trabajo[1275]. Los avances informáticos, cuando se utilizan como herramientas de trabajo consiguen intensificar al máximo el control empresarial y crean nuevos indicios de laboralidad, hasta hace poco tiempo desconocidos[1276]. Por ejemplo, la utilización de un *software in accounting*[1277], que permite un control del tiempo de la prestación, el registro de la hora de encendido y apagado del ordenador, los errores, las interrupciones[1278], *boss everyware*[1279], *sniffers*[1280], etc.

En definitiva, se convierte al empleado en lo que se ha denominado "*trabajador transparente*"[1281]; las nuevas tecnologías aumentan el poder de control no ya sobre la

---

[1272] PURCALLA BONILLA, M.A. y DE PRECIADO DOMENECHQ, C.H.: «Trabajo a distancia vs. teletrabajo: estado de la cuestión a propósito de la reforma laboral de 2012», *Actualidad Laboral*, núm. 2, 2013 (LA LEY286/2013).

[1273] THIBAULT ARANDA, J.: *El teletrabajo. Análisis jurídico laboral*, *op. cit.*, pág. 122.

[1274] DEL VALLE VILAR, J.M. :«El derecho a la intimidad del trabajador durante la relación de trabajo en el ordenamiento laboral español» en AA. VV. *Estudios sobre el derecho a la intimidad*, ed. Tecnos, 1992, pág. 172.

[1275] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI,C.: *Nuevas tecnologías y Relaciones Laborales*, *op. cit*, pág. 116.

[1276] SELMA PENALVA, A.: «Propuestas y reconsideraciones sobre el teletrabajo», *Anales de Derecho* núm. 18, 2010, Universidad de Murcia, págs. 20-45.

[1277] Programa que registra y procesa contabilidad; funciona como un sistema de evaluación contable, procesa transacciones como pagar, cobrar, gestionar nóminas, realizar balances de comprobación, etc.

[1278] GARCÍA ROMERO, B.: *El teletrabajo*, Civitas, ed. Thomson Reuters, 2012, pág. 93.

[1279] *Boss Everyware* es un programa comercial que ayuda a supervisar los empleados en los ordenadores; permite ver qué sitios web visitan, qué tiempo tardan en escribir correos electrónicos qué aplicaciones ejecutan. Cada registro contiene información como nombre del equipo supervisado, nombre del usuario actualmente conectado y nombre del archivo de aplicación. *Vid. http://boss-everyware.software.informer.com/*

[1280] Programa informático que registra información que le envían los ordenadores periféricos, así como la actividad realizada en un determinado ordenador.

[1281] GAETA, L.: «Trabajo y derecho: la experiencia italiana», *Documentación Laboral*, núm. 49, 1996, ed. Cinca, pág. 45.

prestación sino sobre el empleado mismo[1282], pero la introducción de las nuevas tecnologías no altera, en esencia, la naturaleza de los poderes de dirección, sino su forma de manifestarse[1283]. Los sistemas son muy variados: utilización de seguidores URL[1284] que permiten rastrear los movimientos de los trabajadores en la red, tecnología ASP[1285] que conoce la ubicación de los trabajadores mediante el teléfono móvil, o identificadores de radiofrecuencia (RFID)[1286].

C) Regulación Internacional

La noción legal del teletrabajo en el Convenio núm. 177 de la OIT[1287], es bastante extensa, a pesar de su aparente limitación. Al igual que el art. 13 del ET rehúye el término "*teletrabajo*", pero, a diferencia de la elección del legislador español ("trabajo a distancia"), se apuesta por el término "trabajo a domicilio"[1288]. A los efectos del Convenio, la expresión "trabajo a domicilio" significa el trabajo que una persona, designada como trabajador a domicilio, realiza, en su domicilio o en otros locales que escoja, distintos de los locales de trabajo del empleador, a cambio de una remuneración, con fin de elaborar un producto o prestar un servicio conforme a las especificaciones del

[1282] Los datos recogidos pueden bastar para llegar a conclusiones convincentes sobre el perfil del trabajador, e incluso pueden ir mucho más allá, dar información sobre su perfil moral, político, social. Para profundizar en este aspecto, véase GARCÍA ROMERO, B.: *El teletrabajo*, o*p. cit*., pág.117.

[1283] SIERRA BENITEZ, E.M.: *El contenido de la relación laboral en el teletrabajo,* ed. Junta de Andalucía Consejo Económico y Social, 2011, pág. 299.

[1284] Responde a las siglas en inglés de *Uniform Resource sLocator*, significa localizador uniforme de recursos, es la dirección de internet.

[1285] Microsoft introdujo esta tecnología llamada *Active Server Pages*, en el año 1996. Es una parte de Internet Information Server (IIS) desde la versión 3.0; tecnología de páginas activas que permite el uso de diferentes scripts y componentes en conjunto con el tradicional HTML para mostrar páginas generadas dinámicamente, traduciendo la definición de Microsoft: "*Las Active Server Pages son un ambiente de aplicación abierto y gratuito en el que se puede combinar código HTML, scripts y componentes ActiveX del servidor para crear soluciones dinámicas y poderosas para el web*".

[1286] SIERRA BENITEZ, E.M.: *El contenido de la relación laboral en el teletrabajo*, *op.cit*., pág. 305.

[1287] C177 - Convenio sobre el trabajo a domicilio OIT, 1996 (núm. 177) (Entrada en vigor: 22 abril 2000) Adopción: Ginebra, 83ª reunión CIT 20 junio 1996.*Vid. http://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:312322*

[1288] USHAKOVA, T.: «El teletrabajo en el Derecho de la OIT» *Revista de Información Laboral*, núm. 9, 2015 (BIB 2015\4881)

empleador, independientemente de quién proporcione el equipo, los materiales u otros elementos utilizados para ello, a menos que esa persona tenga el grado de autonomía y de independencia económica necesario para ser considerada como trabajador independiente en virtud de la legislación nacional o de decisiones judiciales[1289].

Por tanto, el Convenio núm. 177 hace "*visibles*" a los trabajadores a domicilio[1290]. Impone a los Estados partes que adopten, apliquen y revisen periódicamente su política nacional en la materia, e introduzcan mejoras en la regulación de esta modalidad de trabajo (art. 3). En particular, la política nacional a la que se refiere tiene que promover la igualdad de trato entre los trabajadores a domicilio y los otros trabajadores asalariados, teniendo en cuenta todas las características de este tipo de trabajo (art. 4).

La Recomendación núm. 184 de la OIT[1291], desarrolla todos los aspectos del Convenio y añade otros campos de regulación de relevancia para mejorar la situación de los trabajadores a domicilio. Siendo de por sí un instrumento flexible, no impone obligaciones, sino que "recomienda" a los Estados establecer y aplicar un régimen más favorable a los trabajadores. Entre los derechos que incluye este instrumento complementario, destacan: el derecho a ser informado sobre las condiciones de empleo específicas, y el deber correspondiente del empresario para con el trabajador a domicilio y la autoridad nacional competente; las horas de trabajo, los períodos de descanso y licencias comparables con los derechos similares de otros trabajadores; la protección en los casos de terminación de la relación de trabajo, y el derecho a disponer de un mecanismo de solución de conflictos asegurado por la autoridad competente.

Para la delimitación y encuadramiento jurídico del teletrabajo, podemos recurrir a la búsqueda de nuevos indicios de laboralidad. Sobre la base de los criterios creados por la doctrina y la jurisprudencia, se puede precisar cuándo se presentan los rasgos típicos de una relación laboral por la existencia de una "*dependencia tecnológica o virtual*" en cuanto existe "*heterodirección*", pues la propiedad del *know-how* es del empresario, que es quien opera sobre los medios o herramientas ajenos para la prestación de servicios, el

---

[1289] Art. 1 (a) del C117.

[1290] *Ibídem.*

[1291] R184 - Recomendación sobre el trabajo a domicilio OIT, 1996 (núm. 184) Adopción: Ginebra, 83ª reunión CIT (20 junio 1996) *Vid. http://www.ilo.org/dyn/normlex/es/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:R184*

empleado lo hará mediante su integración en la unidad productiva del titular[1292]; así como el uso de un programa informático normalizado en el que el trabajador ha de realizar sus informes en su ordenador personal, para cuya realización ha sido instruido mediante cursillos de formación, o la firma en el contrato de trabajo de una cláusula para escoger o cambiar en cualquier momento el software aplicativo[1293], la conexión interactiva que es el instrumento de trabajo del operario y asimismo, de control para el empresario, en los supuestos en los que no existe conexión *on line,* pero sí un determinado horario en el que el teletrabajador puede ser controlado a través de llamadas, fax, o el hecho de la situación de *teledisponibilidad* (estar disponible y localizable incluso festivos en situaciones de urgencia).

D) Regulación y Jurisprudencia eurocomunitaria

En el contexto europeo del teletrabajo se ha puesto énfasis en la necesidad de preservar la privacidad del teletrabajador en el Acuerdo Marco Europeo sobre el Teletrabajo[1294]. Conforme al mismo *El teletrabajo es una forma de organización y/o de realización del trabajo, utilizando las tecnologías de la información en el marco de un contrato o de una relación de trabajo, en la cual un trabajo que podría ser realizado igualmente en los locales de la empresa se efectúa fuera de estos locales de forma regular*".

El Tribunal de Justicia de la Unión Europea, en la sentencia de 18 de septiembre de 2014 C- 549/13[1295] resuelve una cuestión judicial planteada por un tribunal alemán

---

[1292] SIERRA BENITEZ, E.M.: *El contenido de la relación laboral en el teletrabajo, op. cit.,* pág. 121

[1293] GARCÍA ROMERO, B.: *El teletrabajo, op. cit.,* págs. 81-82.

[1294] Acuerdo Marco sobre el Teletrabajo de 16 de julio de 2002. Este acuerdo voluntario tiene como objeto establecer un marco general a nivel europeo, conforme a los procedimientos y prácticas específicas a los interlocutores sociales en los Estados miembros. La puesta en marcha de este acuerdo no constituye una razón válida para reducir el nivel de protección acordado para los trabajadores incluidos en el ámbito del acuerdo.

[1295] STJUE de 3 de abril de 2008, asunto C-346/06 Rüffert, en relación con la eventual aplicación de la Directiva 96/71/CE en el marco de la ejecución de un contrato de obra para una Administración Pública. Concretamente la cuestión controvertida que motivó la presentación de la cuestión prejudicial resuelta en la referida sentencia aludía a la situación generada por una empresa adjudicataria de un contrato de obra para edificar un centro penitenciario que recurrió a una contratista polaca para que participase en la ejecución del contrato. El Tribunal afirma la desproporcionalidad de la medida por cuanto que los trabajadores de la subcontratista tenían garantizado un salario mínimo adecuado de acuerdo con la legislación del Estado miembro, entendiendo que ello va más allá del objetivo de protección de los trabajadores. *Vid*. MARTÍNEZ FONS, D.: Las restricciones a las clausulas sociales en las contratación

sobre la posible vulneración del art. 267 del TFUE, en relación con el teletrabajo. Los hechos son los siguientes: para la realización de un contrato público de digitalización de documentos y de conversión de datos en materia de urbanismo se abrió un concurso por la *Stadt Dortmund* en Alemania, en cuyas condiciones se establecía que los licitadores debían comprometerse a abonar un salario mínimo de 8,62 euros la hora y a exigir a los subcontratistas igual compromiso. Un licitador polaco consideró que dicha cláusula no era ajustada al derecho comunitario dado que tal salario mínimo no estaba previsto en Polonia y además no se correspondía con las condiciones de vida de dicho país, por lo que no podía imponerse a un subcontratista de otro estado miembro y cuyos trabajadores intervendrían exclusivamente desde dicho país.

Ampliando la estela de la doctrina *Rüffert*[12961297], el Tribunal de Justicia considera que el salario mínimo no podría imponerse fuera del territorio alemán y que su extensión

---

pública impuestas por la libre prestación de servicios. Cometario a la STJUE de 18 de septiembre de 2014. Asunto C-549/13, *Iuslabor* núm. 3, 2014, págs. 6-7.

[1296] STDH de 18 septiembre 2014. Caso *Bundesdruckerei GmbH* contra *Stadt Dortmund* (TJCE 2014\221) . El Tribunal de Justicia no atiende a una posible huida hacia países con costes sociales más bajos y ni siquiera contempla este argumento, sino que simplemente arguye que de necesitar ayudas sociales los trabajadores polacos por disponer de un salario inadecuado, las consecuencias no recaerían sobre la seguridad social alemana, sino sobre la polaca. No es intrascendente el señalar que el Tribunal de Justicia considera que ello no puede ampararse en razones imperiosas de interés general relacionadas con la protección de trabajadores. Y ello se hace sobre la base de considerar que la cuantía por hora correspondiente a dicho salario mínimo sería para numerosos estados miembros claramente superior a la necesaria para garantizar una remuneración adecuada a la luz del coste de vida en esos países. También se desestima la argumentación de que la limitación podría ampararse en un perjuicio grave para el equilibrio financiero del sistema de seguridad social alemán.

[1297] STDH de 18 septiembre 2014. Caso *Bundesdruckerei GmbH* contra *Stadt Dortmund* (TJCE 2014\221) . El Tribunal de Justicia no atiende a una posible huida hacia países con costes sociales más bajos y ni siquiera contempla este argumento, sino que simplemente arguye que de necesitar ayudas sociales los trabajadores polacos por disponer de un salario inadecuado, las consecuencias no recaerían sobre la seguridad social alemana, sino sobre la polaca. No es intrascendente el señalar que el Tribunal de Justicia considera que ello no puede ampararse en razones imperiosas de interés general relacionadas con la protección de trabajadores. Y ello se hace sobre la base de considerar que la cuantía por hora correspondiente a dicho salario mínimo sería para numerosos estados miembros claramente superior a la necesaria para garantizar una remuneración adecuada a la luz del coste de vida en esos países. También se

para la ejecución de dicho contrato público constituiría una restricción de la libre prestación de servicios y- lo que no deja de resultar llamativo: ello "privaría … a los subcontratistas establecidos en este último Estado miembro de obtener una ventaja competitiva de las diferencias existentes entre las cuantía s de los salarios respectivos" (ap. 34 de la sentencia). La discriminación de los licitadores de otros Estados miembros contrasta con el hecho de que en ningún caso el Tribunal de Justicia tome en cuenta la situación de los empresarios del estado miembro donde se abrió la licitación que sí que quedarían obligados a pagar dicho salario mínimo y verían su posición competitiva claramente mermada[1298].

E) Estatuto de los Trabajadores

Con la aprobación del RD 3/2012, de 10 de febrero, de Medidas urgentes para la Reforma del Mercado Laboral posteriormente mantenida inalterada en la L 3/2012, de 6 de julio, se lleva a cabo una importante reforma laboral, que cambia, entre otros aspectos las modalidades de contratación, la Exposición de Motivos de esta ley, expresa la necesidad de nuevas formas de desarrollo de la actividad laboral, y entre ellas el teletrabajo, concretamente el artículo 13 ET, inalterado en su redacción desde 1980. El actual artículo 13.1 ET establece lo siguiente "*Tendrá la consideración de trabajo a distancia aquel en que la prestación de la relación laboral se realice de manera predominantemente en el domicilio del trabajador o en el lugar libremente elegido por este, de modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa*".

a) Omisiones

El precepto parte de una proclamación genérica de la igualdad de derechos de los trabajadores a distancia con los trabajadores internos, pero sus disposiciones son excesivamente escuetas e imprecisas[1299]. Se prescinde en la nueva regulación de toda

desestima la argumentación de que la limitación podría ampararse en un perjuicio grave para el equilibrio financiero del sistema de seguridad social alemán.

[1298] ESTEVE SEGARRA, A.: «Un balance de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de libertad de prestación de servicios y dumping social», *Revista de Información Laboral*, núm. 6, 2015 (BIB 2015\2560)

[1299] GARCÍA ROMERO, B.: El teletrabajo, *op.cit.* Pág.26.

referencia a la utilización de las tecnologías de la información como seña distintiva del teletrabajo, en el ámbito del Acuerdo Marco Europeo sobre teletrabajo de 2002[1300]; no obstante, el denominador común de los diferentes tipos de teletrabajo, es la existencia de un trabajo realizado a distancia y con uso de las nuevas tecnologías de la información y de la comunicación "*con una especial intensidad*"[1301].

Con anterioridad a la reforma en el ET se intitulaba el art. 13 "*Contrato de trabajo a domicilio*", modificándose el título por el de "*Trabajo a distancia*"; se ha eliminado también la previsión de que este trabajo se realice con vigilancia del empresario, lo que supone un refrendo adicional a la naturaleza laboral del teletrabajo, que puede interpretarse en el sentido de que el trabajo a distancia no impide el control empresarial en línea con la actividad laboral general[1302].

b) Objeto

El contrato de trabajo a distancia tiene un objeto más amplio que el teletrabajo y abarca no solo aquéllos supuestos en que se utilicen TIC, sino otros distintos, siempre que se puedan realizar sobre todo, en el domicilio u otro lugar distinto elegido por el trabajador, lo que incluye, tareas tales como montaje, confección, costura, etc. De este modo, el teletrabajo es solo una parte del género que constituye el trabajo a distancia[1303].

Con esta regulación expresa el legislador tan solo "*ha tocado uno de los fenómenos de externalización ligado a las nuevas tecnologías de la información*"[1304], no todos los tipos de teletrabajo existentes, sino solo una modalidad. Por lo que debido a la

---

[1300] Art. 2 AMETT: " El teletrabajo es una forma de organización y/o de realización del trabajo, utilizando las tecnologías de la información en el marco de un contrato o de una relación de trabajo, en la cual un trabajo que podría ser realizado igualmente en los locales de la empresa se efectúa fuera de estos locales de forma regular*".*

[1301] ESCUDERO RODRÍGUEZ, R.: «Descentralización productiva y nuevas formas organizativas del trabajo», *op. cit*. Pág. 771.

[1302] AA.VV. FUNDACÍON MASFAMILIA (Coor). El libro blanco del teletrabajo en España. Del trabajo a domicilio a los e-workers. Un recorrido por la flexibilidad espacial la movilidad y el trabajo en remoto. *op.cit*., págs.- 58-59 y 63.

[1303] PURCALLA BONILLA, M.A. y DE PRECIADO DOMENECHQ, C.H.: «Trabajo a distancia vs. teletrabajo: estado de la cuestión a propósito de la reforma laboral de 2012» *Actualidad Laboral*, núm. 2013 (LALEY286/2013).

[1304] SEMPERE NAVARRO, A.V. y KAHALE CARRILLO, D.T.: *Teletrabajo, op. cit*., pág.83.

inexistencia de una regulación legal de toda la tipología del teletrabajo, es preciso analizar la jurisprudencia que va emanando de los tribunales en esta materia.

c) Inclusiones y exclusiones

Por otro lado, y respecto a la anterior regulación, se ha prescindido del documento de control de la actividad laboral a disposición de los trabajadores, que por parte de la doctrina se considera como algo obsoleto[1305]. La nueva regulación sigue manteniendo como determinante la libre elección del lugar de prestación de trabajo. En el anterior artículo parecía presuponerse que la totalidad de la actividad laboral debía desarrollarse fuera de la empresa, el nuevo articulado alude expresamente a que la prestación se desarrolle de manera predominante de una forma externalizada.

Quedan fuera de la categoría de teletrabajo las actividades intrínsecamente externas, ya sean de carácter fijo o se desarrollen de manera itinerante. Igualmente deben quedar excluidas en la noción de teletrabajo aquellas actividades que aun sirviéndose de la tecnología de la información, no se prestan fuera de la empresa o del centro de, a saber: *contact center* antes *telemarketing*, la teletienda, los trabajadores " *mediante llamada"*[1306].

F) Acuerdo Interconfederal

El III Acuerdo para el Empleo y la Negociación Colectiva 2015/2017 (BOE 15 junio 2015), reconociendo el teletrabajo como un medio de modernizar la organización del trabajo para hacer compatible la flexibilidad para las empresas y la seguridad para los trabajadores, establecer algunos criterios que pueden ser utilizados por las empresas y por los trabajadores y sus representantes:

- El carácter voluntario y reversible del teletrabajo, tanto para el trabajador como para la empresa.
- La igualdad de derechos, legales y convencionales, de los teletrabajadores respecto a los trabajadores comparables que trabajan en las instalaciones de la empresa.
- La conveniencia de que se regulen aspectos como la privacidad, la confidencialidad, la prevención de riesgos, las instalaciones, la formación, etc.

[1305] SEMPERE NAVARRO, A.V. y KAHALE CARRILLO, D.T.: *Teletrabajo*. Claves Prácticas, *op. cit.*, pág. 13.
[1306] GARCÍA ROMERO, B.: El teletrabajo, *op. cit.*, pág. 45.

- Las pautas del Acuerdo Marco Europeo sobre Teletrabajo, suscrito por los interlocutores sociales europeos en julio de 2002, y revisado en 2009, en el que se recogen pautas relativas al desarrollo del teletrabajo.

K) Control empresarial

Esta cuestión constituye una de las cuestiones más polémicas, por la limitación que supone al derecho a la privacidad de los trabajadores; pues la dirección y control se incorporan al propio instrumento de trabajo o bien a los resultados del mismo.

a) Dificultad

Para evitar la invasión de la vida privada del teletrabajador, el Acuerdo Marco Europeo exige que el método de vigilancia utilizado por el empresario sea proporcional al objetivo perseguido; que exista un equilibrio entre los medios de vigilancia y el objetivo perseguido por el control. La principal dificultad en el teletrabajo es determinar el grado de transparencia laboral que al empresario le es lícito exigir y dónde se debe colocar la barrera de la opacidad que al trabajador le corresponde como persona. El empleador desea comprobar la efectiva realización de la prestación de trabajo y para ello el empleado tiene que perder parte de su libertad individual, y resulta preciso equilibrar ambos intereses contradictorios[1307].

El poder de control del empresario varía su intensidad según los distintos tipos de relaciones de teletrabajo, en base a la conexión telemática y/o el grado de autonomía del trabajador en la organización del trabajo[1308] y está sometido a límites; uno de ellos es la finalidad misma del control, que consistente en verificar únicamente el cumplimiento de las obligaciones y deberes laborales por el trabajador, otro ya analizado en la parte general que son los derechos fundamentales en relación a la consideración debida a la dignidad del trabajador.

Es posible diferenciar entre aquellos poderes que se ejercen directamente sobre la actividad del trabajador, lo que en principio es legítimo; de aquellos otros realizados mediante técnicas de elaboración de datos que permiten la formulación de un juicio de la

[1307] THIBAULT ARANDA, J.: *El teletrabajo. Análisis jurídico laboral*, *op. cit*., pág. 122.

[1308] SIERRA BENITEZ, E.M.: El contenido de la relación laboral en el teletrabajo, *op. cit*., págs. 300-301.

actividad del trabajador, exclusivamente válido cuando existan razones objetivas productivas o de seguridad en el trabajo. Estos controles pueden ir dirigidos tanto a la persona del trabajador como al control sobre las comunicaciones de la empresa[1309].

b) Requisitos

Los presupuestos para que sea considerado lícito y la legitimo el poder de control del empresario, se basan en la normativa de protección de datos, por entender que es la más adecuada para garantizar la privacidad[1310] y son los siguientes:

- Presencia de un fin legítimo, que justifique la restricción de los derechos fundamentales de los teletrabajadores (art.4.1 LOPD)
- Proporcionalidad en la adopción y en la realización de las actividades de vigilancia empresarial.
- Información previa a los trabajadores (arts.5, 15 y 16 LOPD)
- Compatibilidad con la finalidad inicial; que consiste en la prohibición de tratar datos con fines distintos de aquellos para los que fueron recabados.

Como norma específica, el trabajador tendrá derecho a conocer la información extraída por el empresario; y también el uso dado por este conocimiento que tendrá que estar relacionado con la valoración de la cantidad y de la calidad del trabajo[1311].

c) Jornada y horario

Llegados a este punto, creemos merece destacarse la STSJ Castilla y León de 3 de febrero de 2016[1312], porque ha sido pionera en clarificar las bases del control empresarial, incluido en lo relativo a la jornada de trabajo, en relación con el teletrabajo. Como cuestión previa hay que tener en cuenta que el art.13 ET al regular la figura del trabajo a distancia lo define como el que "se realice de manera preponderante en el domicilio del trabajador o en el lugar libremente elegido por este, de modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa", indicándose que "los trabajadores a distancia tendrán los mismos derechos que los que prestan sus servicios en el centro de trabajo de la empresa" así como "derecho a una adecuada protección en materia de

[1309] *Ibídem*, pág. 303.
[1310] *Ibídem*, pág. 378
[1311] GARCÍA ROMERO, B.: *El teletrabajo*, *op. cit.*, pág.119.
[1312] STSJ de Castilla y León de 3 febrero 2016 (AS 2016\99).

seguridad y salud" mientras que por su lado el empresario debe establecer las pautas de control precisas[1313].

La referida sentencia expresamente ratifica la condena a la empresa al pago de horas extraordinarias sobre la base de la inexistencia de control alguno sobre la jornada a pesar de tratarse de teletrabajo. No se admite los argumentos de la empresa contra la reclamación de horas extraordinarias, alegando que al tratarse de una prestación de servicios con conexión remota y desde el domicilio del trabajador no se implementó control ni registro alguno para no interferir sobre el derecho fundamental a la intimidad e inviolabilidad del domicilio del empleado. Bien al contrario, ha de ser la propia empresa la que debe establecer las reglas de juego del control sobre el trabajador, sea un trabajador presencial o un teletrabajador, de modo que la ausencia de estos controles, y específicamente los de jornada, actúan en perjuicio claro de la empresa. Tampoco tienen acogida favorable por el tribunal los argumentos empresariales que se decantan por la plena libertad de organización y autonomía del trabajador desde su domicilio y hacen imposible la generación de horas extraordinarias, pues la estimación de esta argumentación haría imposible determinar a la autoridad laboral y al propio trabajador cual es efectivamente su jornada de trabajo, y en consecuencia el límite de ésta.

Sin duda, los argumentos recopilados en la referida sentencia, deben hacer reflexionar a las empresas sobre la necesidad de dotarse de políticas concretas de teletrabajo que regulen los procedimientos de conexión, los medios de control y los registros de jornada, para evitar que precisamente la falta de sistemas de control puedan hacer proliferar reclamaciones por parte de los trabajadores no sólo en relación al exceso de jornada sino incluso por vulneración de sus derechos vinculados a la seguridad y salud laboral, especialmente por exceso de conexión y estrés[1314].

[1313] MIRÓ MORROS, D.: «El control de la jornada y el teletrabajo», *Actualidad Jurídica Aranzadi* núm. 920, 2016 (BIB 2016\3966).

[1314] *Ibídem*, pág. 139.

d) Modalidades

En la regulación del control por parte del empresario el empleador se encuentra obligado a informar en todo caso al teletrabajador de las modalidades, instrumentos y dispositivos para efectuar el control a distancia[1315]. El seguimiento por el empresario de los hábitos de navegación de los teletrabajadores, permite incluso elaborar un perfil, en función del tipo de páginas que se visiten. Es necesario en un primer momento distinguir, en función de si se han regulado o no las condiciones de uso y acceso a Internet.

En un primer supuesto en el que se haya regulado de manera expresa una política de empresa al efecto sobre el uso de las nuevas tecnologías, cabe la posibilidad de que se prohíba el uso particular, por lo que la monotorización al empleado se realizaría para comprobar el correcto o incorrecto uso de un trabajador, en concreto, del que se han encontrado irregularidades o bien realizando una selección aleatoria de trabajadores a controlar, habiendo advertido previamente de la realización de tales controles.

Si pensamos en un segundo supuesto, en el que se haya regulado de manera expresa una tolerancia de un uso mixto, la solución podría estar en el uso de determinados *software* discriminadores que dependiendo de la naturaleza del mensaje, almacenan el mensaje en una zona u otra del equipo informático[1316]. A saber; carpeta de mensajes profesionales y carpeta de mensajes personales, los profesionales podrían ser fiscalizados y los personales, no.

Con respecto al uso de la videovigilancia en el ámbito del teletrabajo, la doctrina especializada no la encuentra justificada, puesto que esta ofrece una panorámica que comprende todos los actos del empleado, incluidos los pertenecientes a su intimidad, por lo cual los medios informáticos y telemáticos son siempre más idóneos y precisos para alcanzar el mismo resultado sin menoscabar de una manera tan manifiesta la dignidad del trabajador[1317]. En relación a un posible control de los trabajadores a través de la grabación de las llamadas telefónicas, hay que distinguir entre las privadas y las comunicaciones profesionales y en los supuestos en los que el empresario haya autorizado el uso privado del teléfono de manera tácita o expresa el control ha se considerarse vedado, sin más matizaciones[1318].

[1315] THIBAULT ARANDA, J.: *El teletrabajo*. *Análisis jurídico laboral, op. cit.*, pág. 288.
[1316] *Ibídem*, pág. 139.
[1317] *Ibídem*, págs. 125-126.
[1318] *Ibídem*, pág. 130.

Escucha de llamadas.- En el control de las llamadas de trabajo, debe diferenciarse la escucha y el control de destino de las llamadas. Con respecto a la escucha de las llamadas, sin vetos ni restricciones, solo sería jurídicamente posible en aquellos supuestos en los que el empleado queda obligado como consecuencia de la suscripción de un contrato de trabajo[1319], que precisamente consista en la comunicación en sí misma[1320].

La grabación de una conversación suele ser una mayor invasión de la intimidad que la filmación de imágenes, porque puede revelar pensamientos o sentimientos internos que el otro medio no proporciona, ya hemos analizado anteriormente en la doctrina de la STC 98/2000[1321], que realizó la ponderación, inclinando la balanza hacia la intimidad. No se puede extraer la conclusión de que todo el sistema de grabaciones es ilícito, lógicamente, por lo que el interés de la empresa ha de residir en que la forma de control de las escuchas, se ajuste a controles aleatorios, y con la finalidad de la calidad del servicio. Por el contrario, cuando la llamada de trabajo sea residual o secundaria en el teletrabajo un control tan penetrante, en principio no sería de recibo.

Control de destino.- Con respecto al control de destino de las llamadas, el empresario verifica los destinatarios de las llamadas realizadas con el propósito de comprobar que el teléfono de la empresa no se usa con fines particulares; o en su caso, cuando la empresa emplea esta política, había de facturar al trabajador las llamadas privadas. Es un control que pretende salvaguardar el patrimonio empresarial, pero la comprobación de la identidad de los destinatarios puede lesionar la intimidad si no son números notorios a terceros.

[1319] En este sentido, y a título de ejemplo, la STSJ de Galicia de fecha 21 de diciembre de 2009 (EDJ 2009/3457679) resuelve de manera estimatoria, el recurso de suplicación planteado por la empleadora que lo vio desestimado en la instancia, el primer día de trabajo el actor "*firmó un contrato que contenía una clausula expresa en la que consentía que cualquier llamada suya pudiera ser escuchada o grabada con carácter valorativo o formacional*". La empresa asimismo, tenía un control de escuchas aleatorio, le advirtió previamente al recurrido que las conversaciones con los compañeros no podían exceder de 0,45 s, en base al protocolo establecido, y tras esta amonestación, el trabajador hace caso omiso, y en un mes realiza unas cuarenta llamadas de media siete minutos en las que incluso se dedicaba a cantar, la Sala estima el recurso por desobediencia grave y culpable, la gerencia en la intimidad es mínima, el control de la empresa se limita a verificar el tiempo de la conversación.

[1320] THIBAULT ARANDA, J.: El teletrabajo. *Análisis jurídico laboral*, *op.cit.*, pág. 130-131.

[1321] STC 98/2000, de 10 de abril (RTC 2000\98).

e) En el trabajo a domicilio

En la modalidad de teletrabajo a domicilio, encontramos sobre todo a profesionales relacionados con el manejo de datos. Las TIC son un instrumento que se muestra como un medio de control a los empleados; que en este caso aumenta las posibilidades de invasión de la vida privada. En concreto, el empresario no podrá presentarse sin que el trabajador haya autorizado su visita, ni tampoco ningún otro tipo de cargos o personas relacionadas con la empresa. Por lo cual, a falta de regulación específica, será necesario que la empresa consensúe con el trabajador y se especifiquen los días, la hora, la frecuencia la duración y la zona de la visita[1322]; también puede pactarse el tipo de control telemático más adecuado.

Los preceptos relacionados son la inviolabilidad del domicilio están mencionados art. 18 CE, el art. 7 de la Carta Europea de Derecho Fundamentales y la cláusula octava del Acuerdo Marco Europeo, que establece que solo por razones de seguridad y salud laboral podrían los representantes de trabajadores y las autoridades competentes en esta materia solicitar el acceso al domicilio del trabajador.

f) Telecentros

En los telecentros el poder de dirección se muestra igual que en los centros de trabajo tradicionales cuando el telecentro depende directamente de la empresa, porque en el resto de los casos, el poder se ejerce sobre el espacio de trabajo virtual.

L) El teletrabajo fronterizo

El teletrabajo fronterizo es también conocido como "*off- shore*" define la situación de un teletrabajador que reside y trabaja de forma permanente en un país para una empresa situada en otro. La primera cuestión que se nos plantea es qué legislación es la aplicable. Según la doctrina se ha de estar a la *lex locis laboris*, la ley del país en la que el trabajador en ejecución de su contrato de trabajo ejecuta su prestación o su trabajo.

[1322] GARCÍA ROMERO, B.: El teletrabajo, *op. cit.*, págs. 120-121.

Cuando el trabajo se ejecuta en varios países; por ejemplo, el teletrabajo móvil, se somete a la ley del establecimiento que lo ha contratado, a menos que se demuestre que tiene lazos más estrechos con otro país, en cuyo caso será aplicable la legislación de este[1323]. Cuestión distinta es la de un teletrabajador que se encuentre temporalmente por cuenta y dirección de su empresa a otro país[1324]. La ley aplicable será no la del lugar en la que se encuentra físicamente el trabajador, sino la del territorio en el que se recibe la prestación[1325].

El teletrabajo comporta numerosas luces en el sentido de beneficios para los países receptores de teletrabajadores, pero también abundantes sombras, como el dumping social, que lleva a una jornada maratoniana con innumerables horas, a la falta de afiliación al organismo homólogo del sistema de seguridad social, a la inexistencia prevención de riesgos laborales en el puesto de trabajo, etc. Por eso la doctrina recomienda la adopción de medidas voluntarias como los códigos de buena conducta, que no pasan de ser meras declaraciones de intenciones cuyo incumplimiento no desencadena sanción distinta a la puramente moral[1326]. Desde luego, en un terreno tan movedizo como el de las relaciones laborales internacionales cualquier auxilio, por elemental que sea, debe ser bienvenido[1327]. También se apunta al posible uso del "*etiquetado social*"[1328] que atestigua las condiciones de fabricación del artículo.

[1323] Art. 4 del Convenio de Roma.

[1324] Aplicable para el caso de trabajadores en misión.

[1325] THIBAULT ARANDA, J. *El teletrabajo*, *op. cit.*, pág. 264-267.

[1326] Ibídem, pág. 270-271.

[1327] MONTOYA MELGAR, A.: «Empresas multinacionales y relaciones de trabajo», *Revista española de Derecho del Trabajo*, núm. 16, 1983 , págs. 485-502.

[1328] La OIT entiende por "*etiquetado social*" cualquier medio por el que se facilita información mediante una etiqueta física sobre las condiciones laborales que rodean a la producción de un producto o a la prestación de un servicio. Las etiquetas sociales pueden colocarse a los productos o a sus embalajes o pueden exponerse en los escaparates de los lugares de venta al por menor. Otras etiquetas se asignan a empresas, normalmente a productores o a fabricantes y se destinan a los consumidores y/o a los posibles socios comerciales.

J) Reflexiones conclusivas

Se podría afirmar que el "*control*" del teletrabajo dependiente siempre se aleja de las características del control empresarial clásico; pues ni es personal ni inmediato (puesto que no se puede apoyar en la presencia física simultánea de trabajador y empresario en el mismo lugar de trabajo), sino que siempre es informático o tecnológico, y por ello, mediático o instrumental[1329].

Si la empresa ha establecido pautas claras sobre tiempo de trabajo respetuosas con la regulación legal y convencional sobre jornada y descansos, y si además establece, de acuerdo con el trabajador, instrumentos de declaración y control del tiempo de trabajo a distancia o en el domicilio, sería posible admitir que una conducta del trabajador en el interior de su domicilio en vulneración de dichas pautas y omitiendo los instrumentos de control empresarial, pudiera dar lugar a exceptuar el pago de las correspondientes horas y su cómputo como tiempo de trabajo.

Pero en ausencia de esas pautas y criterios y de unos mínimos instrumentos de control, no puede admitirse tal exceptuación, que sería equivalente a crear un espacio de total impunidad y alegalidad en el trabajo a distancia y en el domicilio.

[1329] SELMA PENARANDA, A. «Propuestas y reconsideraciones sobre el teletrabajo» *Anales de Derecho.* Universidad de Murcia, núm. 18, 2010, págs.20-45.

2. El telemarketing

A) Delimitación

El *telemarketing*, trabajo en *contact-center* o telemercadotecnia es una forma de trabajo, en la que un trabajador que actúa de asesor utiliza el teléfono o cualquier otro medio de comunicación para contactar con clientes potenciales y comercializar los productos y servicios. Las encuestas de opinión se realizan de una manera similar.

B) Problemas jurídicos

Este tipo de trabajo lleva implícito que se graben las conversaciones, como nos anuncia la operadora, "*para un mejor control de la calidad del servicio su llamada puede ser grabada",* desde el punto de vista del trabajador, la grabación de la conversación puede ser mucho más sensible, que otro tipo de seguimientos por parte del empresario. La grabación de una conversación suele suponer una mayor invasión de la intimidad que una imagen, porque puede relevar pensamientos o sentimientos internos que el otro medio no proporciona, ya hemos analizado la STC 98/ 2000 de 10 de abril[1330], que realizó la un juicio de ponderación, inclinando la balanza hacia la intimidad, de ello no se puede extraer la conclusión de que todo el sistema del telemarketing es ilícito, lógicamente, por lo que el interés de la empresa ha de residir en que la forma de control de las escuchas; que se ajuste a controles aleatorios, y con la finalidad de la calidad del servicio.

El hecho cierto es que si las conversaciones no pudieran ser grabadas, y en su caso controladas, la prestación tampoco podría ser dirigida y vigilada, por el empresario, por lo que el control de las conversaciones es indispensable por la propia lógica del contrato, se ha de realizar en unas condiciones que minimicen la eventual lesión de la esfera de la intimidad, a través de los ya mencionados controles aleatorios.

La existencia de teléfonos adicionales para uso personal por los teleoperadores suele ser en este tipo de trabajo algo habitual. Comportaría un acceso ilimitado del

[1330] STC 98/2000, de 10 de abril (RTC 2000\98).

empresario a la utilización que se haga de los teléfonos profesionales si bien, por supuesto, en el hipotético caso de que algún empleado insistiera en usar aquéllos para fines personales, el empresario debería limitarse a verificar esta situación y no avanzar sobre datos de la intimidad de este último[1331].

C) La STS 5 diciembre 2003 como punto de inflexión

La STS de 5 de diciembre de 2003[1332] marca un hito en esta materia. En ella el Tribunal Supremo no encontró ningún inconveniente para no permitir al empleador intervenir el contenido de las conversaciones telefónicas mantenidas por los trabajadores cuando existía una finalidad legítima que justificara la intromisión, como lo era, en un supuesto de telemarketing, analizar las técnicas comerciales de los trabajadores para impartir las oportunas instrucciones para mejorarlas[1333]. Se desestimó que existiera una lesión del derecho a la intimidad, por la grabación de conversaciones entre los trabajadores (asesores comerciales de Telefónica) y sus clientes, aplicando el principio de ponderación, pues la medida es idónea para la finalidad pretendida, necesaria y equilibrada: "*En efecto, si el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de telemarketing y a la vez disponen de otro teléfono para sus conversaciones particulares, si, como se ha apreciado, los trabajadores conocen que ese teléfono lo tienen sólo para trabajar y conocen igualmente que puede ser intervenido por la empresa, si además la empresa sólo controla las llamadas que recibe el trabajador y no las que hace, si ello lo realiza de forma aleatoria –un 0,5%–, y con la finalidad exclusiva de controlar la buena realización del servicio para su posible mejora, la única conclusión razonable a la que se puede llegar es a la de que se trata de un control proporcionado a la finalidad que con el mismo se pretende, en el sentido antes indicado"* (FJ 3º).

Aceptada esa metodología de la sentencia, la conclusión de que estamos ante "*un control proporcionado"* hay que compartirla pues se cumplen las exigencias reiteradamente marcadas por la doctrina constitucional. Ese control "*no puede ser considerado contrario a los derechos invocados desde el punto de vista del derecho colectivo, puesto que*

[1331] SEMPERE NAVARRO, A.V. y SAN MARTIN MAZZUCONI, C.: «Escuchas telefónicas a teleoperadoras», Repertorio de Jurisprudencia núm. 4, 2004 (BIB 2004\322).

[1332] STS de 5 de diciembre de 2003 (RJ 2004\313).

[1333] TASCÓN LÓPEZ, R.: «El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica» *op. cit.*

la práctica empresarial se ha acreditado que va dirigida exclusivamente a controlar el trabajo de sus empleados con una finalidad meramente laboral y con medios ponderados y por lo tanto acomodados a las exigencias garantistas de la normativa denunciada como infringida".

D) El Convenio Colectivo sectorial

El Convenio colectivo aplicable era estatal y fue suscrito con fecha 23 de mayo de 2012[1334], de una parte, por la asociación empresarial Asociación de *Contact Center* Española (ACE), en representación de las empresas del sector, y de otra, por los sindicatos, en representación de los trabajadores, CCOO y UGT. En su art. 2, definía el ámbito funcional: *"Quedan encuadradas en la prestación de servicios de Contact Center todas aquellas actividades que tengan como objetivo contactar o ser contactados con terceros ya fuera por vía telefónica, por medios telemáticos, por aplicación de tecnología digital o por cualquier otro medio electrónico, para la prestación, entre otros, de los siguientes servicios que se enumeran a título enunciativo: contactos con terceros en entornos multimedia, servicios de soporte técnico a terceros, gestión de cobros y pagos, gestión mecanizada de procesos administrativos y de back office, información, promoción, difusión y venta de todo tipo de productos o servicios, realización o emisión de entrevistas personalizadas, recepción y clasificación de llamadas, etc, así como cuantos otros servicios de atención a terceros se desarrollen a través de los entornos antes citados".*

El Convenio, define la figura de teleoperador en su artículo 38 de la manera siguiente: *"Los teleoperadores son aquellos trabajadores que realizan tareas de Contact Center habituales y normales con una formación previa. Atienden o emiten contactos siguiendo métodos de trabajo con actuaciones protocolizadas, y recepcionan llamadas para la prestación o atención de cualesquiera servicios".* En consecuencia, este tipo de trabajo, podíamos afirmar que el control telefónico de las grabaciones de los teleoperadores, como regla general, viene siendo admitido, eso sí la agresión es potencialmente alta porque afecta a la comunicación, pero si las conversaciones no pudieran ser controladas, la prestación de trabajo tampoco podría ser dirigida y vigilada, con lo que probablemente no hubiera, ni tan siquiera contrato de trabajo[1335].

[1334] BOE 27 julio 2012, núm. 179.

[1335] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.B.: Control informático, videovigilancia y protección de datos en el trabajo, *op.cit.*, pág 29.

E) Tipología judicial sobre novación contractual

a) MSCT (STS 17 enero 2007)

Cabe destacar en esta materia que se ha declarado que constituye una modificación sustancial el hecho de que la empresa, tras dos infructuosas reuniones con el Comité, confeccione unilateralmente un calendario laboral con jornada de 7 horas y 52 minutos, en 22 días al año, en lugar de ocho horas al día y cuatro más de descanso, STS de 17 de enero de 2007[1336].

b) Novación contractual (STS 17 enero 2007)

No es renuncia prohibida el pacto por el que se incluye en el contrato temporal por obra o servicio una cláusula novatoria en un anexo cambiando la obra o servicio a que se estaba asignado en el sector del telemarketing (STS de 17 de enero de 2007[1337]).

G) Tipología judicial sobre bajo rendimiento

a) Disminución del rendimiento involuntaria (STSJ Cataluña 13 noviembre 2008)

Es una de las mayores causas de despido alegadas en este sector. El sistema de control de productividad y los porcentajes que se suelen imputar a los trabajadores para proceder a sus despidos, suelen considerarse por los Tribunales "*poco objetivos, muy poco fiables y totalmente faltos de garantías*" [1338], impuestos por las empresas teleoperadoras de modo unilateral sin control alguno y sin participación del trabajador o de sus representantes. Lo cierto es que en los despidos con causa en una disminución continuada y voluntaria en el rendimiento del trabajo, debe tratarse del trabajo normal o pactado, y en muchas ocasiones no consta que se pactase con la empresa la realización de determinados objetivos.

También debe atenderse, a falta de otros medios, a elementos de comparación del rendimiento actual con el anterior; habiéndose utilizado, por parte de la jurisprudencia,

---

[1336] STS de 17 de enero de 2007 (EDJ 2007/4160).
[1337] STS de 12 de mayo de 2009 (EDJ 2009/134887).
[1338] STSJ de Galicia de 17 de noviembre de 2011 (JUR 2011\422711).

diversos sistemas: la costumbre, el rendimiento del trabajador medio, el rendimiento de otros compañeros, o el rendimiento anterior del propio trabajador, pero en el caso enjuiciado, la orfandad probatoria sobre otros elementos comparativos es total y absoluta. Desde la más antigua doctrina sentada por el TCT (sentencia de 17 de enero de 1989[1339]) se señala que es preciso que existan datos fiables que acrediten el rendimiento exigido, y para que proceda el despido es preciso que el trabajador no alcance un rendimiento determinado, el normal, es decir, el alcanzable por cualquier trabajador capaz en rendimiento ordinario; exigiéndose que la disminución de rendimiento sea de forma continua, voluntaria y culpable. En tal sentido cabe citar la STSJ de Cataluña de 13 de noviembre de 2008[1340], conforme a la cual el concurso de este último requisito, no concurre, cuando no consta ningún motivo ajeno al trabajador; y aunque los diversos Tribunales no exigen un dilatado período de bajo rendimiento, sí se hace precisa la exigencia de la necesaria proporcionalidad entre la conducta y la sanción impuesta.

b) Objetivación del rendimiento (STSJ Galicia 14 marzo 2014)

La STSJ Galicia de 14 de marzo de 2014[1341] señala la falta de objetividad en la valoración de la disminución del rendimiento realizada por la empresa en la carta de despido. Los hechos declarados como probados son los siguientes: la recurrente trabajaba para una empresa que a su vez prestaba servicios para la conocida compañía ORANGE MOVILES. El citado servicio tenía como objetivo contactar telefónicamente con usuarios de móvil de otras operadoras para suscitar su interés por el producto ofertado y de este modo acepten contratar el servicio y portar su línea de móvil a Orange. La aceptación por parte del cliente era lo que reputaba como positivo para la trabajadora. Se procede a su despido disciplinario, porque se le imputó que sus objetivos estaban claramente por debajo de los exigidos por la operadora telefónica ORANGE y por debajo del resto de sus compañeros, a pesar de las numerosas monitorizaciones de sus llamadas que después fueron analizadas con ella para poder corregir los errores detectados.

[1339] Sentencia Tribunal Central de Trabajo de 17 enero de 1989 (RTCT1989\610).

[1340] STSJ de Cataluña de 17 de noviembre de 2008 (JUR 2009\74967).

[1341] STSJ de Galicia de 14 de marzo de 2014 (JUR 2014\209825).

En la Instancia se declara el despido como improcedente y en suplicación recurre la empresa, y la cuestión litigiosa se circunscribe a determinar si, conforme a los hechos declarados probados, concurre la causa de despido disciplinario consistente en la disminución continuada y voluntaria en el rendimiento de trabajo normal o pactado.

La Sala analiza, en primer lugar, el concepto usado en la carta de despido denominado "*objetivo*" y considera que, en realidad, no es un término de comparación calificable en su sentido literal porque es realmente un criterio subjetivo. La Sala de Galicia razonó que dados los amplios términos que caben en este concepto y que pueden amparar situaciones de abuso de derecho cuando la empresa vaya más allá de lo acorde con un ejercicio racional de sus facultades directivas. En segundo lugar, con respecto al término "*media del servicio*", interpretó que también era utilizado por la empresa en la carta de despido disciplinario para intentar justificar un despido improcedente; tampoco se asemeja a un concepto totalmente objetivo al no resultar acreditada la homogeneidad entre las personas incluidas en la comparación, pues, mientras con relación a la trabajadora demandante constaba el disfrute de vacaciones y no se proporcionaba el dato de si el restante personal integrante del servicio disfrutó vacaciones.

Por estos dos argumentos esgrimidos con carácter principal impiden determinar si el rendimiento de la recurrida suponía una disminución del rendimiento que se pudiera calificar de continuada y voluntaria, por falta de objetividad.

c) Fijación unilateral de rendimiento (STSJ Galicia 19 junio 2013)

La STSJ de Galicia de 19 de junio de 2013[1342] confirma la improcedencia del despido disciplinario. Los hechos declarados probados son los siguientes: se le imputaba a la recurrida la disminución del rendimiento laboral, por descenso en el nivel de ventas. La actora estaba adscrita a la campaña de las "*páginas amarillas*" YELL-TPI, que su empresa desarrolla en virtud de contrato mercantil, cuyo objeto era la venta de espacios publicitarios en los productos de YELL, pactándose expresamente en dicho contrato que el servicio se prestará por Campañas de venta determinadas, cuya duración y vigencia podrá variar en función de las especificaciones concretas.

[1342] STSJ de Galicia de 19 de junio de 2013 (AS 2013\2021).

La Sala declara que ante la ausencia de datos comparativos homogéneos y objetivos, así como por la inexistencia de un rendimiento pactado entre las partes, el despido es improcedente ya que las condiciones son de un marcado carácter unilateral: "*Las acordó unilateralmente el cliente y las trasladó a la empresa demandada, y ésta se los impuso también unilateralmente a la trabajadora, fijando unos porcentajes de cumplimiento, cuya falta de impugnación por la demandante no basta para deducir el compromiso de la misma de asumirlos, desconociéndose también si otros trabajadores cumplieron o no esos porcentajes de trabajo*" (FJ 3º).

H) Tipología judicial sobre operaciones falsas

Estamos ante supuestos de actuación fraudulenta que constituyen, en el supuesto de ser probados, actos de venta ilegítima mediante engaño con perjuicio a terceros, por tanto como muy graves y culpables, constitutivos y relevantes a los efectos de despido procedente, al amparo del artículo 54, apartado d) del Estatuto de Trabajadores por trasgresión de la buena fe contractual y abuso de confianza.

a) Pólizas de seguro (STSJ Madrid 30 noviembre 2015)

La STSJ de Madrid de 30 de noviembre de 2015[1343] desestima el recurso de suplicación de una trabajadora, confirmando el fallo de la instancia. Los hechos transcurren del siguiente modo: una empresa de telemarketing que a su vez trabaja para una compañía de seguros, recibió una reclamación de un cliente por cobro de servicios de manera indebida al no haber contratado servicio o producto alguno con la citada compañía. La empresa procedió a la escucha de la grabación de la recurrente con la reclamante, en ella, por parte de la teleoperadora, se trataba de que la reclamante suscribiera una póliza de accidentes pero esta manifestó que ya poseía un seguro y la teleoperadora le comunicó, que a pesar de ello, le enviaba la documentación sin compromiso. Para la formalización del contrato de seguro por teléfono, era requerido según el procedimiento de la empresa, primero la aceptación clara del cliente, y con posterioridad informar de los textos legales y de la política de protección de datos correspondiente. Como se constató en la transcripción literal de la conversación grabada,

[1343] STSJ de Madrid de 30 noviembre de 2015 (JUR 2016\13634).

la recurrente no realizó dichos procedimientos y optó de manera unilateral y por activar la póliza y notificar a la empresa como venta válida y conforme a procedimiento.

En el recurso se alega infracción del art. 24 CE, y revisión de los hechos declarados probados, motivos que se desestiman. El último motivo alega infracción del art 53.4 ET, aduce en esencia que la causa de despido no ha sido acreditada, al no haber quedado probado la identidad de la persona que participaba en la conversación aportada por la empresa; y que ésta no practicó prueba alguna a fin de probar la identidad de las personas que intervinieron en la grabación y en consecuencia la participación de la trabajadora en la misma; finalizó diciendo que la falta de probanza de la causa determina la declaración de improcedencia del despido operado.

La Sala no comparte las alegaciones vertidas en el recurso, pues del ya firme relato de hechos se afirma que queda constancia de que la actora finalizó la venta y que ésta quedó validada por la verificadora (persona que escucha simultáneamente la conversación); que en la conversación la actora no siguió el manual de procedimiento, no avisando al cliente de que la conversación iba a ser grabada, engañando a la misma sobre el compromiso que adquiría, cerrando la venta sin su consentimiento; todo se extrajo de las pruebas practicadas en el acto de juicio, y además, no constaba que la de grabación, fuese impugnada en debida forma, pues la mera alegación de la trabajadora en el acto de juicio de que no "recuerda la conversación, porque son muchas las que se realizan" , no era suficiente a juicio de la Sala como para poder colegir que la prueba fue impugnada o que no se reconoció su autenticidad; es más de la grabación del acto de juicio se constataba que al inicio de la grabación aportada como prueba la interlocutora se identifica con su nombre coincidente con el de la hoy actora; lo que permite extraer las conclusiones en orden a ultimar en la concurrencia de la causa que dio lugar al despido.

En consecuencia, si en acto de juicio, no se impugnó la validez de la grabación de la conversación, no se puede en vía de recurso tratar de que prospere, por no ser ya en suplicación, el momento procesal adecuado.

b) Altas telefónicas fraudulentas

En el caso de la STSJ de Asturias de 13 de noviembre de 2015[1344] la empresa de telefonía ORANGE procede a despedir a la trabajadora de manera disciplinaria, por haber gestionado de manera improcedente el alta de 179 líneas de teléfono de clientes. Los hechos transcurren del siguiente modo: la empleada, teleoperadora, trabajaba en el departamento de portabilidad, atendiendo llamadas de clientes, y averiguando por qué quieren los usuarios cambiar de compañía telefónica, e intentaba retenerlos ofreciendo promociones y ofertas por parte de la empresa; realizando una gestión comercial. En su trabajo manejaba datos confidenciales, que según el protocolo de la empresa no se podían usar en beneficio propio, lo que suponía no cobrar incentivos, sin perjuicio de otras medidas disciplinarias consta que se le entregó un manual llamado Política Antifraude de ORANGE, y que además realizó un curso sobre ello. La recurrente desoyó esta prohibición y usó las bases de datos simulando acciones comerciales exitosas que no realizaba, buscaba líneas canceladas y tras ver que no había interacción, abría solicitud con su usuario para que se le imputase la acción de retención sobre dicho cliente. Todos los meses la ratio que sacaba respecto a sus compañeros de trabajo, era por encima de la media, lo que le suponía unos incentivos salariales. Se creó dentro de la empresa un departamento denominado de prevención del fraude que detectó como irregular la conducta de la teleoperadora, por lo que se abre una investigación (se supone que se le monitoriza el ordenador, pero esto no consta como hecho probado), que concluye que la trabajadora en cuestión no está realizando una labor de retención real de sus clientes[1345].

No consta la fiscalización de los medios tecnológicos que se le hicieron a la trabajadora, se presupone que se escucharían las conversaciones telefónicas que mantuvo con los clientes, que se accedería a su ordenador, cuanto más datos tenga en su poder el juzgador a la hora de enjuiciar mejor, pues así se podría haber planteado un posible conflicto de derechos fundamentales, para tratar de que prosperara la acción.

[1344] STSJ de Asturias de 13 noviembre de 2015 (JUR 2015\294245).

[1345] Buscar manualmente en la aplicación SGP líneas de clientes que ya están canceladas y, sin que haya previo contacto telefónico con ellos, comprueba que no tienen solicitud de cancelación abierta y posteriormente abre solicitud con su usurario asignado para que dicha retención se le impute a ella. La finalidad es aumentar sus ratios comerciales y alcanzar un tanto por ciento de pago variable.

c) Ventas simuladas

La STSJ de Galicia de nueve de mayo de 2013[1346] resuelve el recurso de la teleoperadora a la se le que imputaba haber realizado unas supuestas ventas engañosas, con el fin de aumentar sus ratios, y que presuntamente provocó posteriores revocaciones, se procedió a la grabación de tales conversaciones y a la transcripción de las mismas en la carta de despido, lo que se declara no probado en la Instancia y el despido como improcedente.

La Sala de Galicia confirma la improcedencia del despido declarado en la Instancia, por la falta de acreditación de los hechos, pero no la nulidad, como postulaba la recurrente, por no existir lesión del derecho fundamental a la intimidad, con respecto a la grabación de la conversación en telemarketing.

I) Tipología judicial sobre aplicación indebida de ventajas

Igual que en el supuesto anterior de ventas engañosas, estamos ante supuestos de actuación fraudulenta que constituyen, en el supuesto de ser probados, actos realizados mediante engaño con perjuicio a terceros, por tanto, graves y culpables, constitutivos y relevantes a los efectos de despido procedente, al amparo del artículo 54 d) ET por trasgresión de la buena fe contractual.

a) Asignación de puntos promocionales (STSJ Castilla-La Mancha 27 febrero 2015)

La STSJ de Castilla la Mancha de 27 de febrero de 2015[1347] estima el recurso de suplicación de la empresa y declara procedente el despido de la trabajadora que fue despedida de manera disciplinaria porque procedió a realizar de manera fraudulenta y con el usuario correspondiente a su compañera de trabajo, una inyección de puntos por atención comercial a un familiar suyo. Los hechos son los siguientes: la parte recurrida en acto de juicio reconoció que se sirvió del conocimiento que por razón del trabajo realizado tenía de la clave de acceso como usuario del programa de otra compañera para

[1346] STSJ de Galicia de 9 de mayo de 2013 (JUR 2013\204373).
[1347] STSJ Castilla-La Mancha de 27 de febrero de 2015 (EDJ 2015/23754).

asignar unos puntos promocionales a su hermano, cliente de la compañía telefónica a la que la demandada presta servicios de teleoperadores. Dichos puntos promocionales servían para obtener descuentos en gasolineras, establecimientos comerciales, etc.

Los trabajadores de la plataforma que trabajan como teleoperadores tienen asignada una clave propia que sus compañeros pueden conocer, porque aunque se cambia regularmente a veces se sustituyen entre ellos y otras, para aumentar la productividad, utilizan más de una. Sobre el uso restringido por cada usuario de la asignada y la prohibición de utilizarla en cuestiones ajenas al trabajo, o en beneficio propio, así como su confidencialidad, los trabajadores firman un compromiso.

Con este relato de hechos, el Juzgador en la Instancia le aplica la teoría gradualista y entiende que la conducta no reviste de la máxima gravedad para ser constitutiva de despido, pero la Sala discrepa, y considera que el órgano judicial no puede modular la sanción si ésta está prevista entre las posibles para la falta cometida, y la misma se encuentra correctamente calificada. Si el Juez no se mantiene dentro de tales límites y, ante una sanción adecuada a la gravedad de la falta, declara que ha de imponerse un correctivo distinto, está realizando un juicio de valor que descalifica, más que el acto del empresario, el cuadro normativo sancionador, pues está expresando que algunas de las diversas sanciones prevista para un nivel de gravedad son excesivas y no pueden ser utilizadas por el empresario, lo que sobrepasa la potestad revisora que las leyes conceden al Magistrado: "*Si el Juez no se mantiene dentro de tales límites y, ante una sanción adecuada a la gravedad de la falta, declara que ha de imponerse un correctivo distinto, está realizando un juicio de valor que descalifica, más que el acto del empresario, el cuadro normativo sancionador, pues está expresando que algunas de las diversas sanciones previstas para un nivel de gravedad son excesivas y no pueden ser utilizadas por el empresario, y esto sobrepasa la potestad revisora que las leyes conceden al Juez*".

b) Descuento en factura (STSJ Madrid 4 diciembre 2013)

La STSJ de Madrid de 4 de diciembre de 2013[1348] confirma la procedencia del despido disciplinario de la recurrente. Los hechos transcurren del siguiente modo: la empleadora de la trabajadora, Trascom, prestaba a su vez servicios para la mercantil

[1348] STSJ de Madrid de 4 de diciembre de 2013 (JUR 2014\7824).

Orange, gestionando a través de un *outsourcing*[1349] de servicios la fidelización y retención de clientes a través de sistemas informáticos, aplicativos y procedimientos propios de Orange.

Debido a los controles y auditorías habituales que realizaba Orange, se detectó que se habían aplicado descuentos irregulares no autorizados sobre facturas de clientes telefonía móvil de Orange. Éstos hechos se produjeron al aplicar en las facturas de determinados clientes unos descuentos destinados a la retención y fidelización, sin que tales descuentos correspondiesen a los referidos clientes, no siendo éstos público objetivo de dicha campaña.

En la denuncia interpuesta por Orange se comunicó que los descuentos indebidos mencionados en el párrafo anterior se han realizado facturas de trabajadores Transcom y de personas con nexo de unión a dichos trabajadores, siendo éstos familiares directos de ellos o bien personas que, por la prueba que se adjuntaba en la denuncia penal Orange, tienen vinculo confirmado por su parte con el tráfico de llamadas habituales. A la trabajadora se la despide disciplinariamente, porque que se encontraba en la lista irregularidades de la auditoría mencionada, y se le imputó, que en la campaña de retención- fidelización, había tenido acceso a un aplicativo informático con el que trabajaba diariamente pero que interactuó directamente en el mismo de forma fraudulenta, unos descuentos sobre su propia línea y sobre determinadas líneas de terceros, creándose un beneficio económico importante (aproximadamente 2650 Euros) sobre sus líneas y a su favor, que en ningún caso correspondía, y por importe de más de 4.000 euros a líneas de familiares y amigos, según se detalla el documento uno que se adjunta. El descuento que se aplicó, correspondía a una campaña que Orange ofreció como medida de retención a clientes provenientes de la Operadora Euskaltel y no siendo en ningún caso de aplicación.

[1349] Proceso económico empresarial en el que una sociedad mercantil delega los recursos orientados a cumplir ciertas tareas a una sociedad externa, empresa de gestión o subcontrata, dedicada a la prestación de diferentes servicios especializados, por medio de un contrato. el proceso económico empresarial en el que una sociedad mercantil delega los recursos orientados a cumplir ciertas tareas a una sociedad externa, empresa de gestión o subcontrata, dedicada a la prestación de diferentes servicios especializados, por medio de un contrato.

Se solicita la revisión del derecho aplicado pues la recurrente alegó que antes de iniciar su trabajo con los potenciales clientes de la empresa su empleadora no le detalló con exactitud y concreción cuáles eran los términos de lo que debía ofertarles, la Sala contesta: "*Los Términos y ofertas que por ser de diferente entidad según las cosas está dentro de lo normal y creíble que se las proporcionaron por escrito pues de otro modo lo normal es que no se hubieran acordado de las mismas la trabajador"*(FJ 4º). Para concluir que si los hechos están acreditados y probados y su calificación o tipificación es la adecuada a las mismo que lo serían porque las infracciones muy graves de sus obligaciones laborales por parte de la trabajadora conllevan la posibilidad legal por parte de la empresa perjudicada por tales incumplimientos de proceder al despido disciplinario de aquélla conforme a lo dispuesto en los artículos 54.1 y 2, y 53 ET.

J) Valoración conclusiva

Es una medida adecuada y razonable controlar el teléfono puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de telemarketing que a la vez disponen de otro teléfono para sus conversaciones particulares. Teniendo en cuenta que los trabajadores conocen que ese teléfono lo tienen a su disposición sólo para trabajar y conocen asimismo que puede ser intervenido por la empleadora en cualquier momento , y además la empresa sólo controla las llamadas que recibe el trabajador y no las que hace, y lo hace de forma aleatoria , con la finalidad exclusiva de controlar la buena realización del servicio para su posible mejora, que ello sea así como medida genérica.

No obstante lo anterior, todo ello no significa que la empresa no pueda por esa vía atentar al derecho de intimidad de cualquier trabajador por cuanto, a pesar de todo, en esas conversaciones con los clientes pueden surgir comentarios que afecten a derechos fundamentales del trabajador incluidos dentro de la esfera de su intimidad en cuanto espacio excluido de cualquier posible intervención ajena, que, en cuanto fueran utilizados por el empleador podrían conducir a una declaración de nulidad en un proceso particular adecuado al caso.

CONCLUSIONES

Al hilo de la mayoría de Capítulos o apartados se ha ido sentando unas valoraciones, a modo de corolario parcial que dejara constancia de lo que suele entenderse como "conclusiones". En buena lógica, podría ahora recuperarse el elenco de tales apartados y ofrecerlo a modo de compendio. Sin embargo, lo cierto es que eso comportaría reiteraciones estériles y dejaría con poco sentido este apartado penúltimo. Así, se ha optado por realizar una reflexión global, más que un resumen; unas propuestas libres, más que una valoración.

Primera.- Regulación conveniente

Parece conveniente una regulación estatal sobre el uso de las nuevas tecnologías en el trabajo, estableciendo unas pautas mínimas de las que partir con respecto a cada uno de los mecanismos de control en particular. Una previsión legal, sería idónea para prevenir posibles abusos por parte de empleadores y de trabajadores, pues al fin y al cabo ante la falta de normativa, hemos de estar, en muchas ocasiones, a lo arbitrado de manera unilateral por el empresario, que solo va a ser fiscalizado si se somete a control por parte de los tribunales, por lo que no se puede permitir que este vacío normativo desemboque en mayor poder para la parte fuerte de la relación laboral.

Segunda.- Conveniencia de la política empresarial admonitiva y preventiva

En práctica ausencia de regulación, resulta muy conveniente que las empresas, siempre que ello sea posible, posean unas reglas claras, comprensibles para sus destinatarios y comunicadas previamente acerca de todas las cuestiones relacionadas con las TICs.

Se trata de deslizar la actuación patronal hacia la admonición y clarificación, evitando que el poder disciplinario asuma el protagonismo de cara a conseguir los objetivos de eficiencia y productividad; de que la prevención de conductas abusivas prevalezca sobre la detección de infracciones.

Tercera.- Confluencia de derechos fundamentales

Por más que se adopten diversos enfoques para abordar la materia expuesta, al final acaba teniendo que acudirse a la doctrina constitucional sobre interacción de derechos.

La delimitación de los derechos fundamentales es una operación absolutamente imprescindible que delimita el campo de actuación; no existirá ponderación cuando el método delimitador revele que no existe conflicto de derechos fundamentales. Estaríamos ante falsos conflictos entre derechos fundamentales, no encontrándose verdaderamente afectado ninguno de estos. La prohibición de uso para fines particulares, supone una delimitación y excluye la vulneración de derechos fundamentales, como se desprende de las SSTC 241/2012 y la STC 29/2013.

Cuarta.- Relevancia de los pronunciamientos constitucionales

Las SSTC 98/2000 y 186/2000, fueron las primeras que abordaron directamente el trasfondo constitucional de la adopción de medidas de control y vigilancia por parte del empresario. En ellas se afirma que el control empresarial, no puede ejercerse sin límites objetivos, ni de forma incondicionada, sino que debe someterse a una doble limitación; mediante el establecimiento por parte de la empresa de unas condiciones de uso que deben ser conocidas por los trabajadores y a través de mecanismos de control arbitrados para verificar la corrección de dicho uso. Todo ello bajo la observancia del canon de proporcionalidad; juicio que pondera y constata si la medida arbitrada cumple con los criterios de idoneidad, necesidad y proporcionalidad en sentido estricto.

La falta de previsión específica en esta materia, nos lleva a estar ante un derecho de creación jurisprudencial inminentemente constitucional, que modula los derechos fundamentales del trabajador en conflicto con los del empleador, lo que, en ocasiones, implica una relativización del planteamiento, pues desemboca a veces que en una aplicación del principio de proporcionalidad, meramente pro forma, sometiendo la medida de control tecnológico a un juicio de razonabilidad que queda dentro del ámbito de la subjetividad. Por lo que, algunas veces, se aprecia que la aplicación del mencionado principio de proporcionalidad, puede ensombrecer otros posibles parámetros de enjuiciamiento, y lleva a validar con enorme laxitud cualquier tipo actuación empresarial de control. No obstante, dando por hecho que el principio de proporcionalidad no constituye un procedimiento objetivo para la determinación del contenido de los derechos fundamentales, sí cumple en la mayor medida de lo posible y en comparación con otros criterios alternativos, las exigencias de racionalidad.

La relevancia de las sentencias constitucionales se aprecia de manera inmejorable a raíz del caso Bershka. La STC 39/2016 ha propiciado todo un cambio de enfoque en los pronunciamientos de los órganos judiciales, comenzando por el Tribunal Supremo.

Quinta.- La expectativa razonable de intimidad

El criterio general de la doctrina de la expectativa razonable de intimidad aparece consagrado en diversas sentencias de los grandes tribunales (por ejemplo, en las SSTS de 26 de septiembre de 2007, de 8 de marzo de 2011 y de 6 de octubre de 2011) y constituye una piedra de toque útil para abordar cuestiones muy problemáticas.

Así, cuando no hay reglas sobre el manejo de los medios tecnológicos de la empresa, existe una situación de tolerancia con una expectativa razonable de intimidad y un desconocimiento de una prohibición absoluta expectativa que ha de ser protegida a nivel constitucional. El trabajador actúa creyendo que la utilización que está haciendo es adecuada y confía en el carácter íntimo y secreto del contenido del medio, si se fiscalizase vulneraría sus derechos constitucionales. La existencia de un hábito social generalizado de tolerancia, con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores, crea una expectativa en esos usos y a la hora de enjuiciarlos, procede aplicar la teoría gradualista.

Ese parámetro también es útil en la situación contraria, cuando la empresa ha proscrito el uso de las TICs para cualquier finalidad ajena a la prestación laboral. Cuando el trabajador desoye una prohibición expresa del empresario, porque existen unas reglas de uso y manejo de los equipos de la empresa y el empleado puede fácilmente prever una posible fiscalización, no existe una situación de tolerancia ni una expectativa razonable de intimidad, por lo que no se vulneraría derecho constitucional alguno.

Sexta.- La expectativa razonable de confidencialidad

La ampliación hacia la expectativa razonable de confidencialidad se aborda en la STC 241/2012 de 17 de diciembre, que acuña este término por primera vez, aplicado a enervar la eficacia de la inmunidad de la protección formal del art. 18.3 CE; en la medida que se haga permeable una determinada comunicación al conocimiento ajeno, dejará de amparar la protección formal del secreto de las comunicaciones. La expectativa de confidencialidad no es absoluta, está sometida a las reglas de la buena fe, se ha de informar al trabajador de las reglas de uso de las nuevas tecnologías, de los posibles controles.

Este criterio, pese a lo que generalmente se afirma, no se ve alterado por la STC 170/2013. De manera indirecta, la resolución lo convalida cuando expone que una vez

establecidas las reglas de uso, su incumplimiento por parte del trabajador justifica una auditoría sin conocimiento del mismo y es ilícita la prueba obtenida tras una auditoría de los ordenadores, sin haber establecido esas reglas. La novedad de la sentencia es basase en una prohibición establecida en convenio colectivo y no en una orden del empresario (ya sea en código de conducta, anexo al contrato de trabajo, etc.).

Sí que parece claro que de esta construcción se desprende una doble conclusión: a) El hecho de que un convenio colectivo tipifique una conducta como sancionable equivale a prohibirla, aunque no lo anuncie expresamente. b) Un Convenio Colectivo podrá limitar decisivamente el ejercicio de derechos fundamentales.

Séptima.- Afianzamiento de la videovigilancia

La repercusión de la STC 29/2013 (caso Universidad de Sevilla), es mucho mayor en la jurisprudencia que la de STC 170/2013 (prohibición albergada en convenio sectorial), aunque ésta tuvo mayor impacto en los medios y fue archiconocida para los profanos del Derecho. A través de la STC 29/2013 se marcó la senda constitucional de la doctrina respecto al principio de la autotutela informativa en las relaciones laborales y se aplicó en videovigilancia permanente y por analogía en control por GPS.

Para la videovigilancia oculta se aplicaban los criterios de la STC 186/2000, de 10 de julio: instalación ocasional y temporal de una cámara de grabación tras acreditadas sospechas razonables de incumplimientos contractuales.

Lo que sucede es que esa doctrina se ha modificado muy sustancialmente por la STC 39/2016, de 3 de marzo (caso Bershka), reformulando lo que se entiende por derecho fundamental a la autodeterminación informativa , con un significativo descenso en el grado de protección del art. 18.4 CE. En esta resolución se aplica el principio de proporcionalidad. Consideramos que al intentar someter la técnica del triple test al 18.4 CE el Alto tribunal se equivoca, confundiendo los términos del debate porque es una cuestión de delimitación previa. Desde la STC 39/2016, de 3 de marzo, para entender satisfecha la obligación empresarial, es suficiente con el distintivo informativo general de "*zona videovigilada*" al que alude la Instrucción núm.1/2006, de 8 de noviembre, sin necesidad de comunicar a los trabajadores los ámbitos concretos de control de la prestación laboral a que pueden destinarse las grabaciones de las cámaras. Si no llegara a ofrecerse esa información general, se deriva que, en tal caso, la instalación de videovigilancia por parte de la empresa no determinaría automáticamente la vulneración

del art. 18.4 CE, sino que, por el contrario, la legitimidad constitucional de la medida empresarial vendría determinada por la superación o no del principio de proporcionalidad.

Ahora parece que ya no hay distinción conceptual entre cámaras fijas para videovigilancia permanente y móviles para videovigilancia oculta; se establece una doctrina común, con la información previa con el distintivo conforme a la Instrucción 1/2006 de la Agencia Española de Protección de Datos es suficiente.

Octava.- El control del ordenador y del correo electrónico

El control empresarial del ordenador se funda en el art. 20.3 ET y no en el art. 18 ET, es un medio de trabajo y el titular es el empresario. No es necesario que la fiscalización empresarial se practique en el centro y en horario de trabajo ni ante la presencia del trabajador afectado. Si consta acreditado el conocimiento del trabajador de la prohibición de uso particular del ordenador, nos hallamos ante un caso claro transgresión de la buena fe contractual caracterizada por la necesaria lealtad y confianza que ha de observarse en la relación laboral, no cabe argüir una quiebra de una expectativa razonable de intimidad porque la prohibición la anula. La falta de autorización para un uso privado no implica prohibición, sino tolerancia, y protección constitucional de los derechos del trabajador.

La existencia de una prohibición de uso del correo electrónico con fines particulares supone que la empresa fiscalice el contenido de los correos electrónicos enviados y recibidos por el trabajador, sin advertencia previa de la posibilidad de realización de posibles controles y enervar la expectativa razonable de confidencialidad, razón por la cual no se consideran vulnerados el derecho constitucional al secreto de las comunicaciones y a la intimidad. Por el contrario la tolerancia o ausencia de regulación despliega los derechos fundamentales del y trabajador.

Novena.- Recurso a detectives equipados tecnológicamente

El empleo de detectives es un último recurso, una excepción al funcionamiento ordinario de control empresarial por otro tipo de medios, porque con indicios de actividad irregular y con los otros diferentes mecanismos de control existentes no es posible llegar a los resultados de esta prueba. La doctrina judicial suele ser declara lícita la prueba del detective cuando el trabajador no presta servicios en dependencias de la empresa y el control se realiza en espacios públicos y durante el desarrollo de la jornada laboral, sin

invadir espacios privados y con una previa sospecha de posibles irregularidades cometidas.

Respecto al control del crédito de las horas sindicales, los cánones son muy restrictivos y sobre su uso existe una presunción de probidad, que admite la prueba en contrario, siempre y cuando no se someta al representante a una vigilancia singular y la medida supere el juicio de proporcionalidad. Salvo casos muy flagrantes, esta prueba suele conllevar a la nulidad de la sanción del representante de los trabajadores.

Décima.- Control de redes sociales y mensajería instantánea

La transcripción de los mensajes de whatsapp es una cuestión no controvertida, pues suele admitirse su práctica como documental en el acto de juicio. Se admite que uno de los comunicantes sea el que aporte tal información a la empresa pues en este caso no se vulnera el secreto de las telecomunicaciones ya uno de los interlocutores ha intervenido en el proceso de la comunicación, se vulneraría el derecho a la intimidad del trabajador denunciado ante la empresa pero el infractor es el interlocutor no la propia empresa.

La redes sociales son medios probatorios cuya proposición y práctica en el proceso social es claramente admisible y admitida; los Tribunales consideran lícita la conducta del empleador de utilizar la información y opiniones del trabajador manifestadas en redes sociales para adoptar medidas disciplinarias contra ellos.

Undécima.- Control biométrico

Las aplicaciones biométricas más idóneas para usar por parte del empleador, son las que no requieran almacenar la biometría en una base de datos centralizada, si no en un soporte a disposición exclusiva del usuario, por cuanto ello permite al trabajador ejercer un mejor control sobre los datos personales que le afectan. Ya que el mayor problema que se plantea al respecto es el correcto control y tratamiento de los datos biométricos por parte de la empresa, por posibles infracciones de la LOPD.

Duodécima.- Planteamiento de los casos en suplicación

A la hora de establecer una tipología judicial de los tribunales menores se ha observado que una gran parte de los recursos de suplicación en esta materia están mal planteados pues ni tan siquiera plantean una revisión del Derecho aplicado en la sentencia

de Instancia por vulneración de los derechos fundamentales del trabajador a la hora de obtener la prueba en la que se ha fundado su despido, si no que inciden en la tan infructuosa tarea de intentar una revisión de los hechos declarados probados o en la revisión del Derecho tratando de aplicar la teoría gradualista al despido efectuado. Todo ello hace que el debate no adquiera la calidad deseada en la tipología judicial de cada uno de las tecnologías analizadas.

BIBLIOGRAFÍA

ADSUAR PRIETO, Y.: «Incremento del uso y el abuso en la videovigilancia», *Actualidad Jurídica Aranzadi*, núm. 851, 2012.

AGUSTINA SANLLEGHÍ, J. R.: «¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa? Estudio interdisciplinar sobre políticas de uso de las TIC, prevención y gestión de "conflictos" en una muestra de empresas españolas», *IDP: revista de Internet, derecho y política*, núm. 16, 2013.

AGUT GARCÍA, C.: «Las facultades empresariales de vigilancia y control sobre útiles y herramientas de trabajo y otros efectos de la empresa» en AA. VV. VICENTE PACHÉS, F. (Coor.): *El control empresarial en el ámbito laboral*, ed. CISSPRAXIS, 2005.

ALEMÁN PAEZ, F.: «Bases teóricas, fácticas y contra-fácticas del acoso moral e institucional», *Revista Doctrinal Aranzadi Social*, núm. 11, 2014.

ALEXY, R.: *Teoría de los derechos fundamentales*, ed. Centro de Estudios Constitucionales, 1993.

ALFONSO MELLADO, C. L.: «Despido, prohibición de discriminación y derechos fundamentales» en AA. VV. SALA FRANCO (Coor.), *Libro Homenaje a Abdón Pedrajas Moreno*, ed. Tirant Lo Blanch, 2012.

ALONSO OLEA, M.: *Las fuentes del derecho, en especial del Derecho del Trabajo según la Constitución*, ed. RAJL, 1981.

ALONSO OLEA, M. y MONTOYA MELGAR, M.: *Jurisprudencia Constitucional Sobre Trabajo y Seguridad Social, Tomo XVIII, 2000*, ed. Civitas, 2000.

ÁLVAREZ ALONSO, D.: «Medios audiovisuales de vigilancia empresarial y derechos fundamentales del trabajador», comunicación a la ponencia temática: El Derecho del Trabajo y las Relaciones Laborales ante los cambios económicos y sociales del X Congreso de Derecho del Trabajo y de la Seguridad Social, 2011.

- «Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: sentencia TC 98/2000 de 10 de abril» en AA. VV., GARCÍA MURCIA, J. (Coor.) *Derechos del Trabajador y Libertad de Empresa*, ed. Aranzadi, 2013.

- «Modulación laboral de los derechos fundamentales. Ponderación y principio de proporcionalidad. ¿Un paradigma en retroceso?», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

APARICIO ALDANA, R. K.: «Derecho a la propia imagen en las relaciones laborales», *Revista Doctrinal Aranzadi Social,* núm. 27, 2013.

-«Nuevas tecnologías y derecho a la libertad de expresión e información de los trabajadores en la empresa», *Anuario jurídico y económico escurialiense*, núm. 50, 2017.

ARETIO BERTOLIN, J. y ARETIO BERTOLIN, M. T.: «Análisis en torno a la tecnología biométrica para los sistemas electrónicos de identificación y autenticación», *Revista española de electrónica,* núm. 630, 2007.

ARIAS DOMINGUEZ, A.: «Detectives privados, jurisdicción social y proyecto de ley de seguridad privada», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

ARMENTIA MORILLAS, P.: «La importancia de un "Código de uso" de las redes sociales», *Actualidad Jurídica Aranzadi* núm. 888, 2014.

ASQUERINO LAMPARERO, M. J.: «El derecho de resistencia frente al poder de dirección», *Revista Doctrinal Aranzadi Social* núm. 8, 2012.

BALLESTER PASTOR, I.: «Facultades de control empresarial sobre el aspecto exterior del trabajador: Límites a la expresión del derecho a su propia imagen en el desarrollo de la prestación laboral», *Tribuna Social: Revista de seguridad social y laboral*, núm. 169, 2005.

BECK, U.: *La sociedad del riesgo. Hacia una nueva modernidad*, ed. Paidós, 1998.

BEL ANTAKI, J.: «Redes sociales y su incidencia jurídico laboral en los derechos fundamentales del trabajador», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

BERNAL PULIDO, C.: *El Principio de proporcionalidad y los derechos fundamentales*, ed. Centro de Estudios Políticos y Constitucionales, 2007.

BOU FRANCH, V. y CASTILLO DAUDÍ, M.: *Curso de Derecho Internacional de los Derechos Humanos,* ed. Tirant Lo Blanch, 2008.

CABELLOS ESPIERREZ, M. A.: «El derecho a ser informado como elemento esencial del derecho a la protección de datos. Una visión crítica de la jurisprudencia del Tribunal Constitucional y de

su cambio de doctrina en la STC 39/2016», *Revista Vasca de Administración Pública, Herri-Arduralaritzako Euskal Aldizkaria,* núm. 106, 2016.

CALVO GALLEGO, F. J.: «TIC y poder de control empresarial: reglas internas de utilización y otras cuestiones relativas al uso de Facebook y redes sociales», *Revista Doctrinal Aranzadi Social,* núm. 71, 2012.

CARDONA RUBERT, M. B.: *Informática y contrato de trabajo (aplicación de la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*), ed. Tirant lo Blanch, 1999.

CARRASCO DURÁN, M.: «El Tribunal Constitucional y el uso del correo electrónico y los programas de mensajería en la empresa» *Revista Aranzadi Doctrinal,* núm. 9, 2014.

CASTAÑO MARTÍNEZ, M. S.: «*La política cultural y los nuevos canales de acceso a la cultura*», *Economía industrial* núm. 389, 2013.

CASTELO GARCÍA, M.: «Aproximación a la apropiación comercial de la imagen», *Base de Datos de Bibliografía El Derecho*, núm. 9, 2006.

CAVAS MARTÍNEZ, F.: «Globalización y Relaciones Laborales», *Revista de sociales y de jurídicas,* núm. 3, 2008.

-«Las prestaciones de servicios a través de las plataformas informáticas de comercio colaborativo», *Estudios financieros, Revista de trabajo y seguridad social,* núm. 406, 2017.

CONTRERAS NAVIDAD, S.: «La responsabilidad por comentarios ofensivos en Internet. Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos de 10 de octubre de 2013. Asunto Delfi As contra Estonia», *Revista Aranzadi Doctrinal* núm. 11, 2014.

CÓRDOBA CASTROVERDE, D.: «Las cámaras de videovigilancia en la jurisprudencia. Respuesta de los tribunales», *Revista de Inmobiliario El Derecho*, núm. 2, 2015.

CORTÉS, S. y PEDRAJAS QUILES, A.: «Pactos de no competencia desleal para después de extinguido el contrato de trabajo», *TOGAS,* núm. 25, 2003.

CORTES OSORIO, J. A., MEDINA AGUIRRE, F. A. y MURIEL ESCOBAR, J. A.: «Sistemas de seguridad basados en Biometría» *Scientia et Technica* , núm. 46, 2010.

CUADROS GARRIDO, M. E.: «El uso del WhatsApp en las Relaciones Laborales», *Nueva Revista Española de Derecho del Trabajo,* núm. 171, 2014.

DÁVILA MURO, J.: «Confines BYOD: Hic sunt Dracones, *Revista SIC ciberseguridad, seguridad de la información y privacidad*», núm. 104, 2013.

- «Cuando el malware se viste de ciberarma», *Revista SIC ciberseguridad, seguridad de la información y privacidad*, núm. 108, 2014.

DÁVARA RODRÍGUEZ, M. A.: *Manual de Derecho Informático*, ed. Aranzadi, 2015.

DE MIGUEL ASENSIO, P. A.: «Servicios de la Sociedad de la Información», *Estudios y Comentarios Legislativos Civitas. Derecho Privado de Internet*, núm. 1, 2015.

-«Caracterización y organización de internet: perspectiva jurídica», *Revista de Derecho Privado de Internet. Estudios y Comentarios Legislativos*, núm.7, 2015.

-«Derechos de propiedad industrial», *Revista de Derecho Privado de Internet. Estudios y Comentarios Legislativos*, núm. 12, 2015.

DE LA QUADRA-SALCEDO JANINI, J. y SUÁREZ CORUJO, B.:«¿Trabajadores incomunicados?: La deriva de doctrina constitucional en torno a los márgenes de actuación empresarial en el control de las comunicaciones», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

DE LIMA PINEL, M. F.: «Asimetría geográfica en la deslocalización: señal verde para las empresas y roja para los trabajadores», *Revista Universitaria de Ciencias del Trabajo*, núm. 11, 2010.

DEL VALLE VILAR, J. M.: «El derecho a la intimidad del trabajador durante la relación de trabajo en el ordenamiento laboral español» en AA. VV. *Estudios sobre el derecho a la intimidad*, ed. Tecnos, 1992.

DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, ed. Lex Nova, 2012.

DÍEZ PICAZO, L. M.: *Sistema de Derechos Fundamentales. Serie Derechos Fundamentales y Libertades Públi*cas, ed. Aranzadi, 2008.

ESTEVE SEGARRA, A.: «Un balance de la jurisprudencia del Tribunal de Justicia de la Unión Europea en materia de libertad de prestación de servicios y dumping social», *Revista de Información Laboral*, núm. 6, 2015.

ELIZALDE MEDRANO, A. , ROJAS RAMÍREZ, J. A. y TEJEIDA PADILLA, R.: «Medición Sistémica del Desempeño en el Transporte de Carga con GPS», *Revista Científica ConCiencia Tecnológica*, núm. 45, 2013.

ESCUDERO RODRIGUEZ, R.: «Descentralización productiva y nuevas formas organizativas del trabajo», comunicación al X Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2000.

FERRANDEZ AGULLÓ, F.: Tesis doctoral: Sistemas criptográficos de curva elíptica basados en matrices, Universidad de Alicante, 2005.

FERNÁNDEZ GARCÍA, A.: «Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial» *Revista Doctrinal Aranzadi Social*, núm. 17, 2010.

FERNÁNDEZ SEGADO, F.: «Los overruling de la jurisprudencia constitucional», *Foro Nueva Época*, núm. 3, 2006.

FERNÁNDEZ LÓPEZ, M. F.: «La intimidad del trabajador y su tutela en el contrato de trabajo» en AA. VV. CASAS BAAMONDE, E., CRUZ VILLALÓN, J. y DURÁN LÓPEZ, F. (Coords.): *Las transformaciones del derecho del trabajo en el marco de la Constitución española: estudios en homenaje al profesor Miguel Rodríguez-Piñero y Bravo-Ferrer*, ed. Wolters Kluwer, 2006.

FERNANDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, Thomson- Aranzadi, 2003.

- « 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.

FERRANDO GARCÍA, F.: «Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías», *Estudios financieros. Revista de trabajo y seguridad social* ,núm. 399, 2016.

FOLGUERA CRESPO, J. A.: «¿Puede el empresario controlar los ordenadores y correos electrónicos de sus empleados? (STC 170/2013, as."ALCALIBER")», *Revista Otrosí* ,núm. 3, 2013.

FORMETÍN ZAYAS, Y.: «La unificación de criterios sobre la utilización de la firma digital en los contratos electrónicos», *Base de Datos de Bibliografía*, núm.30, 2007.

FUNDACÍON MASFAMILIA (Coor).: *El libro blanco del teletrabajo en España. Del trabajo a domicilio a los e-workers. Un recorrido por la flexibilidad espacial la movilidad y el trabajo en remoto*, 2012.

GAETA, L.: «Trabajo y derecho: la experiencia italiana», *Documentación Laboral*, núm. 49, 1996.

GALVEZ MUÑOZ, L.: «La ineficacia de la prueba obtenida con violación de derechos fundamentales. Normas y Jurisprudencia (TEDH,TC,TS,TSJ y AP) en los Ámbitos Penal, Civil, Contencioso- Administrativo y Social», *Cuadernos Aranzadi de Derecho Constitucional*, núm. 10, 2003.

GALLARDO MOYA, R.: *El viejo y el nuevo trabajo a domicilio: de la máquina de hilar al ordenador*, ed. *Ibídem*, 1998.

GARATE CASTRO, J.: «Efectos de la vulneración de los derechos fundamentales o libertades públicas en el empleo de las nuevas tecnologías con objeto de obtener datos cuya reproducción pretende aportarse como prueba», *Cuadernos Digitales de Formación,* núm. 3, 2009.

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», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

GARCÍA GARRIGOS. J. J.: Proyecto Fin De Carrera. «Sistema de Autenticación Biométrica de Huella Dactilar asistido por Interfaz de Voz para el Control de Accesos», Escuela Técnica Superior de Ingeniería de la Universidad de Valencia, 2006.

GARCÍA DE SOLA y VERA, J. M: «Hackers cómo pueden destruir tu vida», *Revista One Magazine Seguridad nacional,* núm. 9, 2014.

GARCÍA MURCIA, J.: «Presentación» en AA. VV. GARCÍA MURCIA, J. (Dir.): *Derechos del Trabajador y Libertad de Empresa*, ed. Aranzadi, 2013.

GARCÍA NINET, J. I. y VICENTE PACHÉ, F.: «El derecho valor a la dignidad humana y el derecho a la protección de datos personales en la Constitución Europea», *Revista del Ministerio de Trabajo e Inmigración,* núm. 57, 2005.

GARCÍA ORTIZ, S. y SALAS DARROCHA, J. T.: «STC 170/2013 y nueva doctrina sobre el derecho a la intimidad del trabajador» *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 30, 2014.

GARCÍA PERROTE- ESCARTIN, I. y MERCADER, U.: «El registro del correo electrónico de un trabajador en el ámbito penal requiere autorización judicial: los matices de una inquietante doctrina» *Revista de Información Laboral*, núm. 8, 2014.

GÓNZALEZ BEILFUSS, M.: «El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional», núm. 11, 2003.

GOÑI SEIN, J. L.: *El respeto a la esfera privada del trabajador*, ed. Civitas,1988.

- «Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y de archivo de datos» en AA.VV. ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA, R. (coords.): *Nuevas tecnologías de la información y de la Comunicación y Derecho del Trabajo*, ed. Bomarzo, 2004.

- «Los criterios básicos de enjuiciamiento constitucional de la actividad de control empresarial: debilidad y fisuras del principio de proporcionalidad», *Revista de derecho social,* núm. 3, 2005.

- «La videovigilancia empresarial y la protección de datos personales», ed. Aranzadi, S.A. 2007.

-«Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos», *Justicia Laboral*, núm. 39, 2009.

- «Los Derechos Fundamentales Inespecíficos en la Relación Laboral Individual: ¿Necesidad de Reformulación?» en AA. VV. (AEDTSS): *Los Derechos Fundamentales Inespecíficos en la Relación Laboral y en Materia de Protección Social*, XXIV Congreso Nacional Del Trabajo y de la Seguridad Social , ed. Cinca, 2014.

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

GRANDE ESTURO, C. y GORDILLO, C.: «El uso de las redes sociales en la jurisprudencia social» *Actualidad Jurídica Aranzadi*, núm. 855, 2013.

GUDÍN RODRÍGUEZ- MAGARIÑOS, F.: «La lucha contra el ciberblanqueo como vía para acabar con el phising», *Revista Aranzadi Doctrinal*, núm. 9, 2014.

GUERRERO PERALTA, O. J.: «La expectativa razonable de intimidad y el derecho fundamental a la intimidad en el proceso penal», *Revista de Derecho Penal y Criminología*, núm. 92, 2011.

GUITIERREZ PÉREZ, M.: «Prohibición expresa del uso privado del ordenador de la empresa como fundamento para su control. STSJ Andalucía 14 noviembre 2013», *Revista Española de Derecho del Trabajo*, núm. 165, 2014.

HERRERO-TEJEDOR ALGAR, F.: «La protección del honor y de la intimidad en el ámbito de las telecomunicaciones» en AA.VV. PÉREZ-UGENA COROMINA, M. (Coor.): *Régimen de las telecomunicaciones*, ed. Tecnos, 1998.

HOLGADO GÓNZALEZ, M.: «La protección constitucional de la intimidad de los trabajadores frente a el uso de las nuevas tecnologías de la comunicación» en AA.VV., GALÁN MUÑOZ, A. (Coord.): *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación*, ed. Tirant Lo Blanch, 2014.

INDA ERREA, M.: «Despedido por atender un negocio particular en horas sindicales», *Revista Aranzadi Doctrinal*, núm. 4, 2012.

JIMENEZ CAMPO, J.: «La garantía constitucional del secreto de las comunicaciones», *Revista española de Derecho Constitucional*, núm. 20, 1987.

JOSSERAND, L.: «El espíritu de los Derechos y su relatividad» , MONEREO LÓPEZ (Trad.), Estudio Preliminar *Teoría del abuso de Derecho: El abuso de los Derechos Fundamentales*, ed. Comares, 2012.

LAITA, C., MARÍN SANUI. D., ÑUNEZ, S. y BECKER, C.: «Bring Your Own Device (BYOD)», *Bit* núm. 23, 2013.

LAS HERAS, J.: «"United we stand, divided we fall": poder de clase, cadenas globales de valor y estrategias sindicales en el parque de proveedores de Mercedes-Benz Vitoria-Gasteiz», *Lan harremanak: Revista de relaciones laborales*, núm. 35, 2017.

LINDOSO MUÑOZ, A.: Tesis Doctoral. «Contribución al reconocimiento de huellas dactilares mediante técnicas de correlación y arquitecturas hardware para el aumento de prestaciones», Universidad Carlos III de Madrid, 2009.

LÓPEZ ANTUÑA, J.: «Pulsar "Me gusta" en Facebook: Despido Nulo y Riesgos del uso de WhatsApp en la comunicación abogado cliente», *Revista del Consejo General de Graduados Sociales*, núm. 29, 2014.

LÓPEZ RIVERO, A. J.: «Tratamiento estadístico de Big Data: un cambio de paradigma tecnológico en la utilización de la información», *Cuadernos salmantinos de filosofía*, núm. 42, 2015.

LOZANO GAGO, M. L.: «Los derechos al honor, intimidad e imagen en la Constitución Española y en las de EEUU y Francia», *Diario La Ley*, núm. 8593, 2015.

LUCENA CID, I. V.: «El concepto de intimidad en los nuevos contextos tecnológicos» en AA. VV. GALÁN MUÑOZ, A. (Dir.): *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación* 2014, ed. Tirant Lo Blanch.

LUCH CORRELL, F. J.: «El acceso a internet para fines particulares en la empresa como causa de despido disciplinario. Respuesta de los tribunales», *Revista de Jurisprudencia El Derecho*, núm. 1, 2006.

LLANO SÁNCHEZ, M.: «Derecho a la propia imagen y apariencia externa del trabajador: sentencia TC 170/1987, de 30 de octubre» en AA. VV. GARCÍA MURCIA, J.(Dir.): *Derechos del Trabajador y Libertad de Empresa*, ed. Aranzadi, 2013.

LLORENS ESPADA, J.: «El uso de Facebook en los procesos de selección de personal y la protección de los derechos de los candidatos», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

LLUCH, CORELL, F. J.: «Las ofensas verbales como causa de despido disciplinario. Respuesta de los tribunales», *Revista de Jurisprudencia El Derecho*, núm. 3, 2005.

MAGRO SERVET, V.: «Panorama legal sobre la videovigilancia. Viabilidad legal de su utilización en la seguridad pública y privada», *Revista de Jurisprudencia El Derecho*, núm. 4, 2008.

MARÍN ALONSO, I.: «La utilización del correo electrónico por los sindicatos o sus secciones sindicales para transmitir noticias de interés sindical a sus afiliados o trabajadores en general», *Revista Doctrinal Aranzadi Social* núm. 1, 2001.

-«El uso por los trabajadores de las comunicaciones electrónicas en la empresa. ¿Se encuentran protegidas por el secreto de las comunicaciones», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

MARIN ALONSO, I. y GUTIERREZ PÉREZ, M.: «La práctica de la prueba en materia de derechos fundamentales tras la ley de jurisdicción social», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 21, 2012.

MARTÍN JIMENEZ, R. «El derecho a la intimidad del trabajador y las cámaras de vigilancia», *Diario de las Audiencias y TSJ*, núm. 291, 2002.

MARTÍNEZ FONS, D.: «El poder de control ejercido a través de medios audiovisuales en la relación de trabajo. A propósito de las SSTC 98/2000 , de 10 de abril y 186/2000, de 10 de julio», *Relaciones Laborales: revista crítica de teoría y práctica*, núm.1, 2002.

MARTÍNEZ FONS, D.: «Las restricciones a las clausulas sociales en las contratación pública impuestas por la libre prestación de servicios. Cometario a la STJUE de 18 de septiembre de 2014. Asunto C-549/13», *Iuslabor*, núm. 3, 2014.

MARTÍNEZ MARTINEZ, R.: «¿Controlar a los trabajadores?», *Actualidad Jurídica Aranzadi*, núm. 864, 2013.

- «¿Controlar las redes sociales?», *Actualidad Jurídica Aranzadi*, núm. 886, 2014.

MARTÍN MORALES, R.: «El derecho a la intimidad: Grabaciones con Videocámaras y microfonía oculta», *La Ley Revista jurídica española de doctrina, jurisprudencia y bibliografía*, núm. 4, 2004.

MIRÓ LLINARES, F.: «Estudios y Comentarios Legislativos La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing», *Revista electrónica de ciencia penal y criminología*, núm.15, 2013.

MIRÓ MORROS, D.: «El uso del correo electrónico en la empresa: protocolos internos», *Actualidad Jurídica Aranzadi*, núm.874, 2013.

MERCADER UGINA, J. R.: *Derecho del Trabajo. Nuevas tecnologías y sociedad de la información*, ed. Lex Nova, 2002.

- «Límites del control empresarial sobre el uso del trabajador del ordenador facilitado por la empresa como instrumento de trabajo: TS 26/9/07 como "*leading case*"» en AA.VV. GIL SUÁREZ.L y SARGADOY DE SIMÓN, I. (Coors.): *Jurisprudencia y grandes cuestiones laborales*, ed. Francis Lefebvre, 2010.

- *El futuro del trabajo en la era de la digitalización robótica*, ed. Tirant Lo Blanch, 2017.

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» en AA.VV. VICENTE PACHÉS. (Coor.): *El control empresarial en el ámbito laboral*, ed. CISS PRAXIS, 2005.

MOLINA NAVARRETE, C.: «Expectativa razonable de privacidad" y poder de vigilancia empresarial: ¿*Quo vadis* Justicia Laboral?», Estudios financieros, Revista de trabajo y seguridad social núm. 399, 2016.

MONEREO PÉREZ, J. L: «Artículo 64» en AA. VV. MONEREO PÉREZ, J.L. y ALARCÓN CARACUEL, M. R. (Coors.): *Comentario al Estatuto de los Trabajadores*, ed. Comares,1998.

MONEREO PÉREZ, J. L. y LÓPEZ INSUA, B. M.: «El control empresarial del correo electrónico tras las STC 170/2013», *Revista Doctrinal Aranzadi Social* núm. 11, 2014.

MONTOYA MELGAR, A.: «Empresas multinacionales y relaciones de trabajo», *Nueva revista española de Derecho del Trabajo*, núm. 16, 1983.

- «Nuevas dimensiones jurídicas de la organización del trabajo en la empresa», *Revista del Ministerio de Trabajo y Asuntos Sociales*, núm. 23, 2000.

- *La buena fe en el derecho del trabajo*, ed. Tecnos, 2001.

- «Nuevas tecnologías y buena fe contractual (buenos y malos usos del ordenador en la empresa)», *Relaciones laborales: revista crítica de teoría y práctica*, núm. 1, 2009.

- *Derecho del Trabajo*, ed. Tecnos, 2016.

MORALES DE LABRA, E.: «Crédito horario sindical. Un derecho limitado», *Revista Doctrinal Aranzadi Social* núm. 58, 2011.

MORENO GARCÍA, J. A.: «Informes de los detectives privados y prueba en el proceso», *Revista de Jurisprudencia El Derecho*, núm. 1, 2007.

MORÓN LERMA, E.: *El secreto de empresa: protección penal y retos que plantea ante las nuevas tecnologías*, Aranzadi, 2002.

MUÑOZ RUIZ, A. B.: «Convergencia y Divergencia entre los Tribunales del Orden Social y la Agencia Española de Protección de Datos en materia de control informático de la prestación de trabajo, (Comentario a las SSTS de 8 de marzo y 6 de octubre)», *Revista Española de Derecho del Trabajo*, núm. 156, 2012.

NIETO ROJAS, P.: «El correo electrónico como medio de transmisión de información sindical y el papel de la negociación colectiva en la fijación de su alcance», *Nueva revista española de derecho del trabajo*, núm. 172, 2015.

NORES TORRES, E.: «La utilización de las redes sociales como medio de prueba en el proceso laboral», núm. 1, *Revista de Jurisprudencia El Derecho*, núm.1, 2013.

OJEDA AVILÉS, A.: «Equilibrio de intereses y bloque de constitucionalidad personal en la empresa», *Revista de derecho social*, núm. 35, 2006.

OJEDA AVILÉS, A. e IGARTUA MIRÓ, M. T.: «La dignidad del trabajador en la doctrina del Tribunal Constitucional. Algunos apuntes», *Revista del Ministerio de Trabajo e Inmigración*, núm. 73, 2008.

ORENES RUIZ, J. C.: «La responsabilidad de los medios digitales. A propósito de la sentencia Delfi contra Estonia», *Actualidad Jurídica Aranzadi*, núm. 877, 2014.

ORIHUELA COLLIVA, J. L.: «Internet: la hora de las redes sociales», *Nueva Revista de Política Cultura y Arte*, núm. 119, 2008.

ORTEGA ORTAS, M.: Tesis doctoral «Automatic system for personal authentication using the retinal vessel tree as biometric pattern», Universidad de la Coruña, 2009.

ORTIZ LÓPEZ, P.: «Redes sociales: funcionamiento y tratamiento de información personal», *Revista Derecho y Redes sociales*, 2013.

PACHECO ZERGA, L.: *La dignidad humana en el Derecho del Trabajo*, ed. Thomson-Civitas, 2007.

PALOMEQUE LÓPEZ, M. C.: *Los derechos laborales en la Constitución Española*, ed. Centro de Estudios Constitucionales (CEC), 1991.

PASCUAL GASPAR, J. M.: Tesis doctoral «Uso de la firma manuscrita dinámica para el reconocimiento biométrico de personas en escenarios prácticos», Universidad de Valladolid, 2010.

PASTOR FRANCO, J. y SARASA LÓPEZ, M. A.: *Criptografía digital: fundamentos y aplicaciones*, ed. Universidad de Zaragoza, 1998.

PEDRAJAS QUILES, A.: «Derechos fundamentales de la persona, del trabajador y autonomía privada» en AA.VV. SALA FRANCO, T. (Coor.). : *Libro Homenaje a Abdón Pedrajas Moreno*, ed. Tirant Lo Blanch, 2012.

PÉREZ DE LOS COBOS ORIHUEL, F.: *Nuevas tecnologías y relación de trabajo*, ed. Tirant Lo Blanch, 1980.

- «La subordinación jurídica frente a la innovación tecnológica», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 1, 2005.

- «Prólogo» en THIBAULT ARANDA, J. *El teletrabajo. Análisis jurídico laboral*, ed. CES, 2001.

PEYTIBI CARBONEL, F. X.: «La segmentación electoral, cuando la información es poder», *Revista Más poder local*, núm. 13, 2012.

PORTAL MANRUBIA, J.: «La huella genética en la jurisdicción de menores», *Revista Aranzadi Doctrinal* núm. 9, 2010.

PUENTE ESCOBAR, A.: «Legitimación para el tratamiento» en AA. VV. MARTÍNEZ MARTÍNEZ, R. (coord.) *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD*, ed. Tirant lo Blanch Tratados, 2009.

PURCALLA BONILLA, M. A. y DE PRECIADO DOMENECHQ, C. H.: «Trabajo a distancia vs. teletrabajo: estado de la cuestión a propósito de la reforma laboral de 2012», *Actualidad Laboral*, núm. 2, 2013.

QUINTANILLA NAVARRO, Y. R.: «El Teletrabajo: Delimitación, Negociación colectiva y conflictos» en AA.VV. SAN MARTÍN MAZZUCONI, C. (DIR). *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, ed. Eolas, 2014

RIVERO LAMAS, J.: «La descentralización productiva y las nuevas formas organizativas del trabajo», en AA. VV. *Descentralización productiva y nuevas formas de organizar la producción*, X Congreso Nacional de Derecho del Trabajo, MTSS, 2000.

RODRIGUEZ CARDO, I. A.: «Dignidad, honor e intimidad en el trabajo», *Revista del Ministerio de Empleo y Seguridad Social*, núm. 108, 2014.

-«Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador», comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

RODRIGUEZ COPÉ, M. L.: «Facultades de control empresarial y circuito cerrado de televisión STC 29/2013 de 11 de febrero», *Temas Laborales*: *Revista andaluza de trabajo y bienestar social*, núm. 121, 2013.

RODRÍGUEZ ESCANCIANO, S.: «El control empresarial de la mensajería electrónica como prueba de la transgresión de la buena fe contractual. A propósito de la STC de 7 de octubre de 2013», *Diario La Ley*, núm. 8195, 2013.

- *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, ed. Tirant Lo Blanch, 2015.
- «Internet en el trabajo», *Diario la Ley* núm. 8926, 2017.

RODRIGUEZ LAINZ, J. L.: «El principio de la expectativa razonable de confidencialidad en la STC 241/2012, de 17 de diciembre», *Diario La Ley*, núm. 8122, 2013.

-«Reflexiones sobre los nuevos contornos del secreto de las comunicaciones (Comentario a la STC 170/2013 de 7 de octubre)», *Diario La Ley*, núm. 8271, 2014.

RODRIGUEZ MAGARIÑOS, F. G.: «Réquiem por el derecho a la intimidad en los smartphones: análisis de la última Jurisprudencia del TC contrastada con la del TEDH», *Revista Aranzadi Doctrinal*, núm. 9, 2014.

RODRIGUEZ PIÑERO y BRAVO-FERRER, M.: «Intimidad del trabajador y contrato de trabajo», *Revista Relaciones Laborales: revista crítica de teoría y práctica*, núm. 8, 2004.

- «Derecho a la Intimidad y Relaciones laborales», ponencia en la Universidad de Huelva en el Seminario sobre Tendencias de la Protección Jurídica de la Intimidad "Privacidad y Relaciones Laborales", 2006.

RODOTÁ, S.: «Democracia y protección de datos», *http:// www. agdp.es*

ROQUETA BUJ, R.: *Uso y control de los medios tecnológicos de información y comunicación en la empresa*, ed. Tirant lo Blanch, 2005.

SALAS PORRAS, M.: «Ponderación y modulación del ejercicio del derecho a la libertad religiosa en el contexto obligacional laboral: una mirada a la jurisprudencia española», *Revista Crítica de la Historia de las Relaciones Laborales y de la Política Social*, núm. 9, 2014.

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 libertade*s públicas, ed. La Ley, 1999.

SÁNCHEZ TRIGUEROS, M. C.: «Tiempo de trabajo y permisos del trabajador por motivos personales y sindicales», de Carolina Blasco Jover, *Revista Doctrinal Aranzadi Social*, núm. 9, 2014.

SÁNCHEZ MIGALLÓN, R. D.: «La vigilancia de la actividad del trabajador mediante videocámaras y circuitos cerrados de televisión», *Revista Iuslabor*, núm. 3, 2014.

SAN JUAN DELGADO, I. D.: «La página web», *Boletín de Legislación El Derecho*, núm. 262, 2003.

SAN MARTIN MAZZUCONI, C.: «El uso y el control empresarial de las nuevas tecnologías en el ámbito laboral. Algunas pautas recurrentes en la doctrina judicial para tener en cuenta», *Aranzadi Social*, núm. 26, 2007.

- «El derecho a la protección de datos personales de los trabajadores. Criterios de la Agencia Española de protección de Datos» en AA. VV. SAN MARTIN MAZZUCONI, C. (Dir.): *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, ed. Eolas Ediciones, 2014.

SAN MARTIN, D.: «TIC y riesgos en materia de espionaje industrial: hacia un nuevo escenario de amenazas», *Togas Biz*, núm.71, 2007.

SANTANA BELTRÁN, S.: «A vueltas sobre el impacto en las relaciones laborales de la última doctrina constitucional acerca del derecho a la protección de datos ex. art. 18.4 CE STSJ País Vasco 18 de Junio 2013», *Nueva Revista Española de Derecho del Trabajo*, núm. 171, 2014.

SEGOVIANO ASTABURUAGA, M. L.: «El difícil equilibrio entre el poder de dirección del empresario y los derechos fundamentales de los trabajadores», *Revista jurídica de Castilla y León*, núm. 2004.

SEGURA VAZQUEZ, A.: «El pastor, el doctor y el Big Data». *Teknokultura: Revista de Cultura Digital y Movimientos Sociales*, núm. 2, 2014.

SELMA PENALVA, A.: «El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores», *Revista Doctrinal Aranzadi Social* núm. 9, 2010.

- «Propuestas y reconsideraciones sobre el teletrabajo», *Anales de Derecho*, núm.18, 2010.

- «Los límites de la tolerancia en la utilización del ordenador de la empresa para fines personales», *Revista Doctrinal Aranzadi Social*, núm. 83, 2012.

SEMPERE NAVARRO, A. V.: «Modulación laboral de los derechos cívicos: STC 99/1994, de 11 de abril», *Persona y derecho*. *Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos*, núm. 54, 2006.

-«La Constitución y la doctrina constitucional», *Revista Actualidad Jurídica Aranzadi*, núm. 737, 2007.

-«Tras el pronunciamiento del Tribunal Supremo, ¿cabe controlar el ordenador de los trabajadores?» , *Actualidad Jurídica Aranzadi*, núm. 741, 2007.

-«Apuntes sobre la libertad de conciencia en el ámbito laboral», *Revista Aranzadi Doctrinal*, núm. 10, 2015.

SEMPERE NAVARRO, A. V. y ARIAS DOMÍNGUEZ, A.: *Detectives en las relaciones laborales, Impacto de la Ley de Seguridad Privada (L5/2014),* ed. Francis Lefebvre, 2014.

SEMPERE NAVARRO, A. V. y KAHALE CARRILLO, D.T.: *Teletrabajo. Claves Prácticas*, ed. Francis Lefebvre, 2014.

SEMPERE NAVARRO, A. V. y MATEOS y DE CABO, O. I.: « Uso y control de herramientas informáticas en el trabajo(Marco legal, pautas judiciales convencionales) Tolerancia» en AA. VV. SAN MARTIN MAZZUCONI, C.: (Dir.) *Tecnologías de la información y de la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, 2014.

SEMPERE NAVARRO, A. V. y SAN MARTIN MAZZUCONI, C.: «Escuchas telefónicas a teleoperadoras», *Repertorio de Jurisprudencia*, núm. 4, 2004.

-«El uso sindical del correo electrónico a la luz de la STC 281/2005, de 7 noviembre», *Doctrinal Aranzadi Social*, núm. 17, 2005.

-«¿Puede la empresa controlar el ordenador usado por su trabajador?», *Repertorio de Jurisprudencia* núm. 21, 2007.

-«Derechos fundamentales inespecíficos y negociación colectiva», *Cuadernos Aranzadi Social*, núm. 40, 2011.

- «Sobre el control empresarial de los ordenadores», *Revista Doctrinal Aranzadi Social, núm*. 3, 2012.

-*Las TIC's en el ámbito laboral*, ed. Francis Lefebvre, 2015.

SERRANO -COBOS, J.: «Big data y analítica web: estudiar las corrientes y pescar en un océano de datos», *Revista científica el profesional de la información*, núm. 6, 2014.

SEVILLANO PÉREZ, F.: «Big data», *Revista Economía Industrial*, núm. 395, 2015.

SIERRA BENITEZ, E. M.: *El contenido de la relación laboral en el teletrabajo*, ed. Junta de Andalucía, Consejo Económico y Social, 2011.

SIERRA FERNÁNDEZ, J.: «Bases de datos policiales sobre identificadores obtenidos a partir del ADN, la nueva normativa aplicable», *Revista de Jurisprudencia El Derecho*, núm. 4, 2008.

TALENS VISCONTI, E. E.: «La expectativa razonable de confidencialidad como presupuesto de la vulneración de derechos fundamentales en la fiscalización informática llevada a cabo por el empresario», *Revista doctrinal Aranzadi,* núm. 51, 2013.

-«La libertad de expresión de los representantes de los trabajadores y sus nuevas tecnologías. Su alcance en las redes sociales» Comunicación a la ponencia temática: Los Derechos fundamentales inespecíficos en el proceso laboral del XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, 2014.

TASCÓN LÓPEZ, R.: «La protección de datos personales de los trabajadores», Ejemplar dedicado a Protección de datos de carácter personal, *Revista Jurídica de Castilla y León*, núm. 16, 2008.

-«El trabajo humano (y su derecho) ante el imparable fenómeno de las redes sociales en Internet», *Revista de Trabajo y Seguridad Social Centro de Estudios Financieros*, núm. 340, 2011.

- «El tratamiento por la empresa de datos personales de los trabajadores. ¿Un problema resuelto o caído en el olvido?», *Revista Aranzadi Social*, núm. 5, 2005.

-«El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica», *Revista Doctrinal Aranzadi Social*, núm. 17, 2007.

TASCÓN, M.: «Introducción: Big Data. Pasado, presente y futuro», *Telos: cuadernos de información e innovación*, núm. 95, 2013.

THIBAULT ARANDA, J.: «La incidencia de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en el ámbito de las relaciones laborales», *Revista de Relaciones Laborales, revista crítica de teoría y práctica*, núm. 2, 2000.

-*El teletrabajo. Análisis jurídico laboral*, ed. CES, 2001.

-*Control Multimedia de la Actividad Laboral*, ed. Tirant Lo Blach, 2006.

- «La vigilancia del uso de Internet en la empresa y la protección de datos personales», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 10960, 2009.

THOMPSON, J. B.: «Los límites cambiantes de la vida pública y privada», *Revista Nueva Época*, núm. 15, 2011.

TOSCANI JIMENEZ, D. y CALVO MORALES, D.: «El uso de Internet y el correo electrónico en la empresa: límites y garantías», *Revista Española de Derecho del Trabajo*, núm.165, 2014.

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

TORRES DEL MORAL, A.: *Principios de Derecho Constitucional Español*. *Tomo I. Sistemas de Fuentes. Sistemas de los Derechos*, ed. Facultad de Derecho de la Universidad Complutense, 2004.

TORRES VARGAS, G. A. y ARIAS DURÁ, R.: « El cómputo ubicuo y su importancia para el cómputo del Internet de las cosas y el big data», *Revista General de Información y Documentación*, núm. 2, 2014.

TULLINI, P.: «Medios de comunicación electrónica y control empresarial», *Relaciones Laborales revista crítica de teoría y práctica*, núm. 5-6, 2009.

URBANO CASTRILLO, E.: *El Derecho al secreto de las comunicaciones*, ed. La Ley, 2011.

- «Los delitos informáticos tras la reforma del CP de 2010», *Revista Aranzadi Doctrinal*, núm. 9, 2011.

USHAKOVA , T.: «El teletrabajo en el Derecho de la OIT», *Revista de Información Laboral*, núm. 9, 2015.

VALDÉS DAL-RÉ, F.: «Contrato de trabajo, derechos fundamentales de la persona del trabajador y poderes empresariales, una difícil convivencia», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 2, 2003.

- «Derechos fundamentales de la persona del trabajador: un ensayo de noción lógico- formal», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 18, 2003.

- «Presentación del Seminario Internacional sobre medios de comunicación y control empresarial», *Relaciones Laborales revista crítica de teoría y práctica*, núm. 30, 2009.

VELASCO NUÑEZ, E.: *Delitos cometidos a través de Internet. Cuestiones procesales*, ed. La Ley, 2010.

- «Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías», *Revista de Jurisprudencia El Derecho*, núm. 4, 2011.

- «Investigación procesal de redes, terminales, dispositivos informáticos, imágenes, GPS, balizas, etc.: la prueba electrónica», núm. 8, 2013.

VICEDO CAÑADA, L. y VIDAL VIDAL, J.: «Límites a los Derechos Fundamentales del Trabajador: intimidad y dignidad», *Revista Doctrinal Aranzadi Social*, núm. 55, 2012.

VIDAL LÓPEZ, P.: «La utilización de las cámaras de videovigilancia para fines disciplinarios y de control del trabajo», *Actualidad Jurídica Aranzadi*, núm. 888, 2014.

VIGNEAU, C.: «El control judicial de la utilización del correo electrónico y del acceso a internet en las empresas en Francia», *Relaciones Laborales: revista crítica de teoría y práctica*, núm. 5-6, 2009.