Escuela Internacional de Doctorado

Programa de Doctorado en Ciencias Jurídicas

ANÁLISIS JURISPRUDENCIAL DEL CONTROL EMPRESARIAL A TRAVÉS DE LAS TIC Y SU INCIDENCIA EN LOS DERECHOS FUNDAMENTALES DE LOS TRABAJADORES

Tesis que presenta D. Jesús Enrique Pascual López para optar al grado de doctor, realizada bajo la dirección de la Dra. Dª. Laura Sanz Martín y tutorizada por la Dra. Dª. Laura Sanz Martín.

Madrid, septiembre de 2023

Escuela Internacional de Doctorado

Programa de Doctorado en Ciencias Jurídicas

ANÁLISIS JURISPRUDENCIAL DEL CONTROL EMPRESARIAL A TRAVÉS DE LAS TIC Y SU INCIDENCIA EN LOS DERECHOS FUNDAMENTALES DE LOS TRABAJADORES

Autor: Jesús Enrique Pascual López

Directora de Tesis: Profesora Dra. Laura Sanz Martín

Tutora: Profesora Dra. Laura Sanz Martín

Madrid, septiembre de 2023

"Todos somos muy ignorantes.

Lo que ocurre es que no todos ignoramos las mismas cosas".

Albert Einstein, científico.

A Mónica, por darme todo.

A Diego y Nora, por ser mi motor.

A mi madre, por mirarme con tan buenos ojos.

Este trabajo de investigación se ha llevado a cabo en el programa de Doctorado en Ciencias Jurídicas de la Universidad Camilo José Cela bajo la excelente dirección de la Dra. Laura Sanz Martín, sin la cual esta tesis no hubiera sido posible. Por ello, quiero agradecer públicamente su confianza, su insistencia, sus sugerencias y sus críticas.

También quiero agradecer este trabajo al Profesor Juan Ramón Cuadrado Roura, el cual me advirtió, hace ya algún tiempo, de la dificultad, dedicación y tiempo necesario para realizar este trabajo.

INDICE

ABREVIATURAS UTILIZADAS

AEPD	Agencia Española de Protección de Datos
Art.	Artículo
ATD	Acuerdo de trabajo a distancia
BOE	Boletín Oficial del Estado
CC	Código Civil
CCOO	Comisiones Obreras
CE	Constitución Española
CNT	Confederación Nacional del Trabajo
ET	Estatuto de los Trabajadores
ETT(s)	Empresa(s) de Trabajo Temporal
FJ	Fundamento Jurídico
FFJJ	Fundamentos Jurídicos
IVA	Impuesto sobre el Valor Añadido
LISOS	Ley de Infracciones y Sanciones del Orden Social
LOLS	Ley Orgánica de Libertad Sindical
LOPD	Ley Orgánica de Protección de Datos
LRJS	Ley Reguladora de la Jurisdicción Social
Núm.	Número
OIT	Organización Internacional de los Trabajadores
Pág.	Página
PP.	Páginas
RA	Recurso de Apelación
Rec.	Recurso
RD	Real Decreto
RDL	Real Decreto-Ley
RD Leg.	Real Decreto Legislativo
RGPD	Reglamento General de Protección de Datos
RTC	Repertorio del Tribunal Constitucional
SAN	Sentencia de la Audiencia Nacional
STC	Sentencia del Tribunal Constitucional
SSTC	Sentencias del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo

STSJ	Sentencia del Tribunal Superior de Justicia
TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de la Información y Comunicación
UGT	Unión General de los Trabajadores

1. Introducción.

La evolución constante de las relaciones laborales a través del uso de la tecnología y el manejo de esta en la prestación de servicios y en el control empresarial, junto con la irrupción de diferentes redes sociales que inciden directa o indirectamente en la relación laboral, hacen necesaria una adecuación del ordenamiento jurídico, y en particular, del Derecho del Trabajo. En este sentido, resultará necesaria una conciliación entre los intereses de las empresas y la evolución de las nuevas herramientas de que disponen sus empleados.

La adecuación del ordenamiento jurídico dependerá tanto del legislador, que va a introducir novedades como la Ley Orgánica de Protección de Datos 3/2018, de 5 de diciembre, como de la interpretación que hagan los jueces y tribunales, que regulará y limitará los medios utilizados por el empresario para el control de sus empleados.

La presente tesis estudia y analiza la incidencia del control empresarial realizado a través de las tecnologías de la información y comunicación en los derechos fundamentales de los trabajadores.

La investigación se divide en 10 capítulos. Tras una breve introducción histórica de la evolución del derecho laboral en general se estudian los derechos fundamentales que pueden verse vulnerados por el control empresarial a través de las TIC, deteniéndose en la dignidad, base de todos los derechos fundamentales. Después, se realiza un análisis conceptual de las tecnologías de información y comunicación y se relacionan con el control laboral ejercido por el empresario en el desarrollo de su actividad, estudiando su régimen jurídico (desarrollo y límites) y la jurisprudencia más notable.

Más tarde, se enumeran y desarrollan los derechos fundamentales más sensibles al control empresarial a través de las nuevas tecnologías de la información y comunicación, como son el derecho a la intimidad, el derecho a la protección de datos, y el derecho al secreto de las comunicaciones. En este sentido, se mostrará la evolución histórica del derecho fundamental, su régimen jurídico y la jurisprudencia y doctrina judicial relevante a nivel nacional y comunitaria. Por lo tanto, se tratará de un estudio "del poder de dirección

versus los derechos fundamentales", partiendo de dos premisas, que el poder del empresario tiene límites y que los derechos fundamentales de los trabajadores no son absolutos.

Aunque el trabajador acepte formar parte de una organización y de una dirección, el poder de dirección que tiene el empresario no es un derecho incondicional, sino que está sometido a una serie de limitaciones de las que son fundamentales las que se derivan de la obligación del empresario de respetar la intimidad y la consideración debida a la dignidad de los trabajadores.

Asimismo, como se adelantaba, los derechos fundamentales tampoco son absolutos, y deberá ponderarse, en cada caso, su ejercicio atendiendo a las diferentes circunstancias, principalmente si entran en conflicto con otros derechos.

En este sentido, el Tribunal Constitucional ha establecido la modulación de estos derechos del trabajador cuando se incorpora a una organización empresarial en la medida estrictamente imprescindible para que la actividad productiva se lleve a cabo correcta y ordenadamente[1].

De igual forma, si tales derechos colisionasen, corresponde apreciar los intereses en juego, mediante una adecuada ponderación de las circunstancias concurrentes en cada caso (STC 99/1994, 6/1995, 106/1996, 136/1996, 204/1997, 98/2000, 186/2000).

En relación con los límites del poder de dirección, el Tribunal Constitucional ha establecido las directrices para validar el control empresarial y que no se entienda vulnerador de un derecho fundamental, como son:

1. que la medida sea idónea, capaz de alcanzar el objetivo propuesto por la empresa de controlar el trabajo y/o incumplimientos del trabajador;

[1] LLUCH CORELL, F. J. "El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador, El Derecho, 2017 (disponible en http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronicotrabajador_11_1045180003.html; última consulta 25/03/18).

2. necesaria, que no se halle otra medida más prudente para conseguir el mismo propósito con la misma eficacia;
3. equilibrada o proporcional, velando por los intereses generales y con poco o nulo perjuicio sobre otro bien o valor en conflicto; y
4. que sea justificada, con razones objetivas y motivadas que legitimen la decisión de control empresarial.

En el epicentro de la tesis se realiza un estudio de la evolución de la Jurisprudencia y Doctrina Judicial en España y en Europa[2] en cuanto al control laboral a través de diferentes tecnologías de la información y comunicación y su incidencia en los derechos fundamentales de los trabajadores valorando, además, la posible invalidez o ineficacia de la prueba obtenida a través de dicho control empresarial.

Se presta especial atención a los conflictos que se suscitan entre el correo electrónico y el derecho a la intimidad y el secreto de las comunicaciones, la navegación por Internet y el derecho a la intimidad, las cámaras de videovigilancia y el derecho a la intimidad y protección de datos, así como el GPS y el derecho a la intimidad.

Por último, se plantean soluciones prácticas, como la implantación de un código de conducta telemático en la empresa, para que el control de la actividad productiva por el empresario se realice sin vulnerar los derechos fundamentales de los trabajadores, siempre bajo la premisa de dar una correcta información previa a los trabajadores y a sus representantes legales. En él se podrán incluir Protocolos de teletrabajo y desconexión digital, cuyos modelos o ejemplos se acogerán en los diferentes anexos.

Las empresas al establecer las reglas de uso de los medios informáticos, telemáticos y de otra índole a través de un código de conducta de este tipo e informar a los trabajadores de que va a existir un control, impiden que se produzca una tolerancia con el uso personal de dichos medios y/o un desconocimiento del control establecido, lo cual justificaría una expectativa razonable de confidencialidad o una vulneración a la intimidad u otro derecho fundamental de los trabajadores.

[2] Tribunal Europeo de Derechos Humanos.

En relación con la metodología de la investigación efectuada, se ha realizado una investigación dentro del ámbito jurídico o de las ciencias jurídicas de forma cualitativa, aunque también se ha hecho una contrastación empírica de lo publicado por diferentes juristas, la normativa, la jurisprudencia y la doctrina judicial.

Desde el punto de vista cronológico, se ha realizado una introductoria investigación histórica de la evolución del derecho laboral, de los derechos fundamentales y de los diferentes medios utilizados para realizar el control empresarial, pero también, una investigación descriptiva, pues se estudia la jurisprudencia con el fin de plasmar una interpretación correcta, es decir, qué forma de control empresarial a través de las nuevas tecnologías de la información y comunicación es conforme a derecho y como se debe realizar para no vulnerar los derechos fundamentales. Por tanto, también se ha tratado de una investigación aplicada, pues existe interés de aplicarla, utilizarla y aprender de los resultados prácticos del conocimiento científico producido.

Asimismo, se ha realizado una investigación documental, analizando libros, revistas, artículos, manuales, etc.) y experimental, pues se han analizado casos y sentencias en las que he participado como letrado.

2. Los Derechos Fundamentales en el marco de la relación laboral.

2.1. Introducción.

La Constitución Española establece una serie de derechos de los trabajadores que van a estar íntimamente relacionados a su condición laboral, como son el derecho a una remuneración suficiente para satisfacer sus necesidades y las de su familia (art.35), el derecho a la negociación colectiva (art.37), el derecho a sindicarse libremente (art.28.1) y el derecho a la huelga (art.28.2).

Asimismo, los trabajadores, como ciudadanos, también tienen los mismos derechos que se reconocen a todas las personas y que se recogen en el capítulo II del Título I de nuestra Constitución. Ello ha sido una constante en nuestra doctrina constitucional, por la cual,

se ha entendido que celebrar un contrato de trabajo no conlleva para los trabajadores la privación de los derechos que la Constitución les confiere en su condición de ciudadanos.

La jurisprudencia del Tribunal Supremo, del Tribunal Constitucional y de los tribunales europeos ha ido definiendo y, concretando el poder de dirección y el control del empresario que se dispone en el "Estatuto de los Trabajadores" (Art. 20), instaurando su contenido y sus límites. Como límite principal se encuentra el respeto de los derechos fundamentales de quienes trabajan, como la dignidad, la intimidad, el honor o el del secreto de las comunicaciones.

Además, en lo que respecta al control empresarial, teniendo en cuenta que están involucrados otros derechos fundamentales y sus posibles limitaciones, debe prevalecer el principio del equilibrio de derechos constitucionales, el cual, precisa de una ineludible información previa al trabajador de que va a ser sometido a ese control, además, de la superación del "juicio de proporcionalidad" (SSTC 14/2003, 89/2006 y 96/2012)[3] al ejercer dicho control. Más adelante se verá la evolución jurisprudencial de estas exigencias.

A lo largo de la tesis se planteará cómo debe realizarse dicha información para que esta sea eficaz y lícita (sin vulnerar derechos fundamentales), tanto para que el trabajador conozca sus derechos y los del empresario, como para que dicha información sirva de base para una posible sanción, rompiendo así la expectativa de privacidad o intimidad del trabajador.

Según la jurisprudencia mencionada con antelación que recoge los criterios establecidos por el Tribunal de Justicia de la Unión Europea para realizar el test de proporcionalidad, será necesario que se cumplan determinadas condiciones para considerar si el sistema de vigilancia utilizado por el empresario para efectuar el control de sus trabajadores es adecuado para la satisfacción de los objetivos e intereses empresariales antes mencionados. Así se deberá analizar;

[3] SSTC 14/2003, de 28 de enero, 89/2006, de 27 de marzo y 96/2012, de 7 de mayo.

1. que la medida resulte idónea, capaz de alcanzar el objetivo propuesto por la empresa de controlar el trabajo o su incumplimiento por parte del trabajador;
2. que sea necesaria, esto es, que no se halle otra medida más prudente para velar por el mismo propósito con la misma eficacia;
3. que sea equilibrada o proporcional, velando por los intereses generales y con poco o nulo perjuicio sobre otro bien o valor en conflicto; y
4. que sea justificada, con razones objetivas y motivadas que legitimen la decisión de control empresarial.

Estas condiciones se establecen por el no absolutismo de los derechos fundamentales y la ponderación de su ejercicio.

Según algunos autores, como Fernández Avilés o Rodríguez-Rico Roldán[4], este test de proporcionalidad aplicado en el ámbito laboral por la doctrina constitucional desde la STC 99/1994, de 11 de abril, "implica que la doctrina constitucional no concede el mismo valor a los intereses de los trabajadores y a los de la empresa, de forma que el equilibrio entre derechos fundamentales del trabajador y poder de dirección del empresario no se halla en el punto medio entre ambos, pues uno y otro no coinciden en el mismo plano de relevancia constitucional". Solo en el momento que se supere este test de proporcionalidad se podrán limitar los derechos de los trabajadores.

De igual modo, defienden estos autores que el juicio de proporcionalidad surge "como una herramienta indispensable que se convierte en parámetro de determinación de la validez de las posibles acciones restrictivas de derechos, verificando su adecuación en función de una finalidad que ha de resultar legítima y proporcionada". Se tratará, por tanto, de valorar la idoneidad, necesidad y proporcionalidad de la medida para conseguir un fin legítimo. En el juego de las obligaciones recíprocas de empresario y trabajador se admiten, por tanto, ciertos condicionamientos o limitaciones al ejercicio del derecho fundamental a la intimidad, siempre que se respecte el principio de proporcionalidad. En todo caso, no es suficiente alegar la mera conveniencia de introducir una determinada restricción a los derechos pues se deben invocar motivos objetivos. En este sentido se

[4] AVILÉS, J.A.F y ROLDÁN, V.R.R. (2016) Nuevas tecnologías y control empresarial de la actividad laboral en España, Revista Labour & Law Issues, Vol. 2, nº 1, Págs. 55-56.

pronunció el Tribunal Constitucional en sentencias 99/1994, de 11 de abril y 106/1996, de 12 de junio, las cuales establecieron que la posibilidad de limitación de derechos fundamentales por parte del empresario solo puede derivar del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho, o por una acreditada necesidad empresarial, sin que sea suficiente la simple invocación del poder de dirección para limitarlo. De acuerdo con esta doctrina y jurisprudencia, será necesario garantizar el equilibrio entre las obligaciones provenientes del contrato de trabajo para el trabajador y los derechos fundamentales, limitándose en la medida estrictamente imprescindible para el correcto y ordenado respeto de los derechos fundamentales del trabajador y, muy especialmente, del derecho a la intimidad personal que protege el art. 18.1 CE.

Una vez asentada la base de la interpretación jurisprudencial, es oportuno recordar cómo se regulan estos derechos fundamentales en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

En el artículo 4 se recogen los derechos básicos de los trabajadores, estableciendo el contenido y alcance para cada uno de los mismos disponga su específica normativa, destacando el genérico derecho al trabajo y a la libre elección de profesión u oficio, la libre sindicación, el derecho a la negociación colectiva y a la adopción de medidas de conflicto colectivo, los derechos de huelga y reunión, y por último, el derecho de información, consulta y participación en la empresa" (art. 4.1).

En la segunda parte del artículo 4 se recoge los derechos:

> "(a) A la ocupación efectiva; (b) A la promoción y formación profesional en el trabajo (…); (c) A no ser discriminados directa o indirectamente para el empleo, o una vez empleados (…); (d) A su integridad física y a una adecuada política de prevención de riesgos laborales; (e) Al respeto de su intimidad y a la consideración debida a su dignidad (…); (f) A la percepción puntual de la remuneración pactada o legalmente establecida; (g) Al ejercicio individual de las acciones derivadas de su contrato de trabajo…" (art. 4.2).

De otro lado, en el artículo 20 ET se recoge lo relativo al poder de control y dirección del empresario, estableciendo en su primer apartado que el trabajador estará obligado a realizar el trabajo pactado bajo la dirección del empresario o persona en quien este delegue.

En el tercer apartado del artículo 20 ET se tratan las medidas que puede adoptar el empresario para realizar esa labor de control y dirección, pudiendo optar a las medidas que considere oportunas respetando la consideración debida a la dignidad de los trabajadores, y teniendo en cuenta, en su caso, la capacidad real de los que tienen discapacidad.

Por tanto, parecen ser dos los límites que este último artículo impone en la facultad de control del empresario, es decir, la consideración debida a la dignidad de los trabajadores y la capacidad de los trabajadores con discapacidad, "de modo que no cabría entender que, en su ejecución, este dispusiese de absoluta libertad"[5].

2.2. Evolución histórica del derecho laboral y de los derechos fundamentales.

En el análisis de la evolución histórica tanto del derecho laboral como del control del empresario, partimos de que el propio derecho va cambiando y evolucionando con el paso del tiempo en sintonía con la manera en la que evoluciona la sociedad.

El derecho laboral no es una excepción por lo que a medida que la sociedad se desarrolla, la economía crece y las relaciones laborales van evolucionando, el derecho laboral deberá adecuarse a las nuevas formas productivas y a las nuevas formas de relacionarse entre el empresario y el trabajador.

Partimos desde la antigua Roma, donde el Derecho Laboral no era prioritario y por ello no se centrarían en su desarrollo. El motivo principal de esta falta de desarrollo era porque

[5] LÓPEZ AHUMADA, J. E. (2007) "La tutela del derecho a la intimidad del trabajador y el control audiovisual de su actividad laboral", RGDTSS, núm. 14, pág. 9. En el mismo sentido, CHACARTEGUI JÁVEGA, C. (2013) "Dignidad de los trabajadores y derechos humanos del trabajo según la jurisprudencia del Tribunal Europeo de Derechos Humanos", Albacete, España: Bomarzo, pág. 91.

entendían que el trabajo no era precisamente una virtud, y lo consideraban como indigno de los hombres libres, reservándose principalmente para los esclavos o extranjeros, que eran quienes trabajaban la agricultura y otros oficios. Ante esta concepción del trabajo y que el Derecho civil era el que caracterizó el mundo jurídico de la Roma Clásica, las relaciones empresario trabajador se regulaban desde un ámbito civil, entendiéndose al trabajo como un arrendamiento de servicios. De esta manera, se contrataban los servicios de limpieza, de jardinería, arreglos de ropa o actuaciones en fiestas y celebraciones. El contrato de trabajo romano se denominó *locatio conductio operarum* y los trabajadores no gozaban de gran protección ni derechos, tratándose como un arrendamiento de servicios en el que el *conductor* pagaba una remuneración a cambio de un servicio prestado por el *locator* respondiendo hasta el límite de culpa levis[6]. La *locatio operarum* se extinguía cuando se finalizaban los trabajos pactados o moría el *locator*, sin embargo, no se extinguía por la muerte del *conductor*, pues este tipo de contratos tenían la característica de transmitirse a los herederos.

"Los romanos agruparon bajo un único contrato la *locatio conductio*"[7], que consistía en plasmar las relaciones jurídicas con dos fines económicos distintos: "la cesión remunerada del uso temporal de un bien [y] (…) la realización, también remunerada, de una serie de actividades, trabajos o servicios"[8].

La *locatio conductio* fue uno de los cuatro contratos consensuales, junto con la compraventa, el mandato y la sociedad [9]. En este sentido se pronunció Gayo en su obra Instituciones donde entendió que las obligaciones se contraían mediante el acuerdo en las compraventas, los arrendamientos o locaciones, en las sociedades y en los mandatos"[10].

Tras la caída del Imperio Romano, la concepción indigna para el ser humano del trabajo dio paso una concepción del trabajo como un bien social, como casi la única forma para sustentarse, muy similar a lo que sucede en nuestros días.

---

[6] Falta de atención ordinaria.

[7] SEVERÍN FUSTER, G., (2015) "Sobre el modelo de contratación de servicios remunerados en el derecho romano. Algunos aspectos relevantes de la *locatio conductio*". Revista de Derecho Universidad Católica del Norte vol.22 no.2, Coquimbo. Pág. 384.

[8] SEVERÍN FUSTER, G., (2015) "Sobre el modelo de contratación…" ob. cit Pág. 384.

[9] SEVERÍN FUSTER, G., (2015) "Sobre el modelo de contratación…" ob. cit Pág. 358.

[10] GAYO (2009) Instituciones, Madrid, España: CIVITAS.

Durante los siglos centrales de la Edad Media el feudalismo era el sistema político más utilizado en Europa. Se caracterizaba por la descentralización del poder político y por las relaciones de producción y dependencia entre el campesinado y los señores, en un momento en el que la agricultura predominaba como fuente de riqueza. Los campesinos ofrecían sus servicios en días de trabajo (corveas) y pagaban un impuesto o tributo al señor feudal a cambio de protección en los castillos durante las invasiones. En esta época comenzarían a aparecer las actividades artesanales, desarrolladas por unos trabajadores autónomos que se situarían de forma intermedia entre los señores feudales y los campesinos o vasallos, lo que dificultaba la instauración de un Derecho laboral.[11]

Al final de la Edad Media, gracias a la Revolución Industrial, surgiría una nueva ideología que no concebía la riqueza solamente en la tenencia de propiedades de tierra o pertenecer a la nobleza. En esta época nacería la idea de la oportunidad de crecimiento y enriquecimiento independientemente de la clase social a la que se perteneciera. Surgirían los gremios o asociaciones formadas por maestros, oficiales y aprendices de un mismo oficio. La finalidad de estos gremios era principalmente económica, pues intentaban controlar los precios y la oferta de los productos que trataban, pero también social, pues velaban por los intereses de sus asociados. Estos gremios crearon sus propias ordenanzas para regular su actividad laboral, la formación y el aprendizaje de sus asociados, instaurando una estricta jerarquía entre ellos (maestros en lo más alto, después oficiales y por último los aprendices). Asimismo, se establecieron sistemas de protección social para los casos de orfandad, viudedad o incapacidad. Podemos concluir que estas asociaciones gremiales fueron el antecedente más inmediato de los sindicatos e incluso de la Seguridad Social.

A lo largo del siglo XVIII los gremios fueron desapareciendo sustituyéndose por la libertad de industria y comercio, primero con las denominadas “Domestic System”, una especie de industria casera principalmente textil que producía mercancías fuera de las ordenanzas gremiales, y después con el propio capitalismo, dando paso a una nueva edad, la Edad Moderna.

[11] LE GOFF J. (2007). “La Edad Media explicada a los jóvenes”. Barcelona, España: Paidos, pág. 86.

En la Edad Moderna surgirían nuevas maquinarias que dieron lugar a grandes fábricas, lo que conllevaría unos nuevos sistemas de producción y nuevas necesidades sociales. Nació la gran competencia derivada del consumo y los grandes mercados de abastos. En esta época sucedieron diferentes acontecimientos históricos, como el descubrimiento de América (1492), que inicia esta Edad Moderna o la Revolución Francesa (1789-1799), que cierra la misma. Otros acontecimientos como la fiebre del oro (1848) en Estados Unidos, llegarían al poco tiempo.

En relación con el derecho laboral, aparecería en esta época el "Edicto Turgot" (1776) mediante el cual se proclamaba la posibilidad de que el hombre se dedicará a realizar cualquier oficio, si bien prohibía la agremiación y suprimía las corporaciones de oficios, estatutos y privilegios.

Tras la Revolución Francesa (1789-1799) se aplicaría el principio de libertad contractual y en 1791 surgiría el "Decreto de Allard", el cual reconocía la libertad de industria y de comercio. Asimismo, se desarrollaría la Ley de Libre Concurrencia donde se fijaría el derecho a un salario, aunque se mantendría la prohibición del derecho de organización. Ese mismo año, en Francia, surgiría la "Ley Chapelier", que concedía a los trabajadores el derecho a asociarse y a formar corporaciones sin riesgo a ser encarcelados. También reconocería la libertad de elección de un trabajo, profesión u oficio, y sostenía que era facultad del individuo fijar la jornada de trabajo.

En 1804, nacería el Código Civil de Francia (o de Napoleón Bonaparte), donde figuraría una reglamentación de las relaciones laborales fundada en los principios de libertad del trabajo, autonomía de la voluntad e igualdad de las partes celebrantes en un contrato. Sin embargo, a pesar de ser una normativa laboral se impondrían condiciones laborales inhumanas.

En 1847 la Liga Comunista, una organización obrera internacional secreta, encargó a Marx y Engels la redacción de un programa teórico y práctico destinado a la publicidad de la organización, y que, además, se pudiese utilizar como programa del partido. De esta

forma nacería el Manifiesto Comunista, que podemos calificarlo como el antecedente oficial del Derecho Laboral moderno.

En 1884 la "Ley Waldeck-Rousseau" recogió el derecho al sindicalismo y, por tanto, la libertad de organización sindical. Esta ley derogó la "Ley Chapelier" de 14 de junio de 1791. Con la "Ley Waldeck-Rousseau" se generó un potente avance en la libertad sindical al elevar la libertad de asociación de la anterior "Ley Chapelier" a una creación libre de sindicatos y la gestión de sindicatos profesionales. Sin embargo, por otra parte, se limitaba este derecho a la libertad sindical, pues había una estricta supervisión en relación con la creación y desarrollo de los sindicatos implicando un cumplimiento estricto de la ley con imposición de sanciones para los incumplidores. La filosofía de esta ley era la integración de la clase trabajadora en la nación tras la "Comuna de París"[12], e intentaba mostrar a los trabajadores que la Republica podría hacerles un hueco.

Por lo que respecta a España, la primera norma que iba a reconocer alguna forma de asociación obrera fue la "Circular del 28 de febrero de 1839". Sin embargo, esta Circular solo permitía la asociación de las denominadas Sociedades de Socorros Mutuos, no siendo posible en otras sociedades mucho más vinculadas a la lucha obrera. Por su parte y como ejemplo de represión al derecho de asociación, el Código Penal de 1848 iba a establecer sanciones contra las asociaciones ilegales o contra aquellos que se alzasen en pro de la lucha obrera.

La denominada Revolución Gloriosa de 1868 sería clave para que se reconociese el derecho de asociación en nuestro país, primero con la publicación del Decreto de 20 de noviembre de 1868 y después con su incorporación en la Constitución de 1869, que disponía que "ningún español podía ser privado del derecho de asociarse para todos los fines de la vida humana que no sean contrarios a la moral pública" (art. 17). En dicha

[12] Tras la derrota y derrumbe del gobierno imperial de Napoleón en la guerra franco-prusiana (1870-1871), París fue sometida durante más de cuatro meses, que culminó con el triunfo de los prusianos y la proclamación imperial de Guillermo I de Alemania en el Palacio de Versalles. Como París no aceptaba rendirse, la nueva Asamblea Nacional y el gobierno provisional de la República, se instalaron en Versalles dejando un vacío de poder en París que provocó que la milicia ciudadana, la Guardia Nacional de París, se hiciera de forma efectiva con el poder a fin de asegurar la continuidad del funcionamiento de la administración de la ciudad. Se beneficiaron del apoyo y de la participación de la población obrera descontenta, del radicalismo político muy extendido en la capital que exigía una república democrática, lo que conformaría la Comuna de París. Ante esta rebelión y tras el asesinato de dos generales del ejército francés, se iniciaría una lucha calle por calle, la llamada "Semana Sangrienta" (del 21 al 28 de mayo), generando unos 20 000 muertos, el destrozo e incendio de más de 200 edificios y monumentos históricos, y el sometimiento de París a la Ley Marcial durante cinco años.

Constitución también se reconocerían otros derechos, como "la libertad de expresión, reunión y petición" (CN, 1869). Junto con su publicación, el Código Penal también sería modificado, estableciendo como "ilícitas las asociaciones contrarias a la moral pública o que tuvieran como objetivo cometer delitos" (CP, 1870).

La Constitución Federal de 1873, a pesar de que nunca entraría en vigor, reconocía un el "derecho de asociación" en su artículo 3.

Los cambios propiciados por la Revolución Industrial en España hacían necesaria la regulación de las relaciones entre empresarios y trabajadores, por lo que nacería la primera ley al efecto, la Ley Benot de 1873[13], oficialmente denominada Ley sobre el trabajo en los talleres y la instrucción en las escuelas de los niños obreros, cuyo objeto fundamental era proteger a los menores de las condiciones abusivas que sufrían en las fábricas y talleres, y poder darles una educación.

En 1874, tras el golpe de Pavía se suspendería el derecho de asociación, aunque un año después, a través de un Decreto, se restablecería este derecho, solo que se restringiría a las asociaciones que fuesen partidarias de la monarquía.

Por su parte, la Constitución de 1876, calificada por los constitucionalistas como una norma elástica al permitir desarrollos legislativos posteriores en diferentes materias, iba a reconocer el "derecho de asociación" (art. 16). Sin embargo, este derecho de asociación evidentemente no fue desarrollado por los conservadores, que priorizaban el orden antes que las libertades. No sería hasta 1881, a través de la Circular del Ministerio de la Gobernación de 17 de febrero, que el asociacionismo obrero dejaría de ser clandestino.

La primera Ley de Asociaciones de España nacería en 1887, e iba a reconocer diferentes formas de asociación como asociaciones políticas, religiosas, patronales y de trabajadores. La primera asociación de personas trabajadores sería la Unión General de Trabajadores (UGT) que nacería al amparo de esta Ley de 1887.

[13] MARTINEZ PEÑA, L. (2011) "Los inicios de la legislación laboral española: La Ley Benot". Revista Aequitas, Volumen 1 Págs. 25-70

En 1900 se aprobaría en España la Ley de Accidentes de Trabajo, y unos años más tarde la Ley del descanso dominical.

En 1906 se aprobaría la Ley de Sindicatos Agrícolas, una ley de marcado signo católico, donde se establecían diferentes formas de asociación además de los sindicatos, como asociaciones, sociedades, comunidades y las denominadas "cámaras agrícolas", pero solo para el gremio agrícola, no de otra índole.

En el año 1912 se promulgó la conocida como Ley de la Silla, que obligaba al empresario a facilitar una silla a las trabajadoras en los establecimientos no industriales. Recogía la obligación para el empresario de tener un asiento exclusivo por cada empleada en centro de trabajo (sin contar con los asientos de espera para clientes) con la finalidad de proteger a las mujeres que trabajaban de pie en comercios o almacenes debido a la incidencia negativa de la bipedestación prolongada en su salud, como era la congestión en los ovarios, deformidades en los pies y en la pelvis y que según los médicos de la época podría ser causa de distócicos advertidos en multitud de mujeres que realizaban su trabajo en bipedestación y sin disponer de un asiento[14].

Esta ley fue muy criticada por ser excesivamente paternalista y discriminatoria al aplicarse solo a las mujeres, por lo que en 1918 se dictó un Real Decreto por el que se protegía también a los hombres. Esta ley sigue vigente en nuestros días al no haber sido derogada.

En 1919, después de la Huelga de La Canadiense[15] de Barcelona, tras 44 días de huelga y más de 100.000 participantes que paralizaron la economía, el gobierno español de la época aceptó las demandas de los trabajadores que incluían una jornada de ocho horas, el reconocimiento de los sindicatos y el reintegro de los trabajadores despedidos.

[14] TUSET DEL PINO, P. (1 de mayo de 2021) "Tome Vd. Asiento. Acerca de la ley de la Silla" https://www.economistjurist.es/premium/la-firma/tome-vd-asiento-acerca-de-la-ley-de-la-silla/

[15] Fue un movimiento de reivindicación laboral dirigido en 1919 por la Confederación Nacional del Trabajo (CNT) que incluyó huelgas, boicots e insumisión civil iniciada en la empresa eléctrica Riegos y Fuerza del Ebro, perteneciente a Barcelona Traction, Light and Power Company, Limited, conocida como La Canadiense.

Los años que duraría la dictadura militar de Primo de Rivera (1923-1930) serían los años de mayor represión para las organizaciones comunistas y anarquistas y, se prohibirían, además, las actividades de partidos políticos y sindicatos.

La Constitución de 1931 iba a reconocer el derecho a la libre asociación y sindicación y, un año después, aprobaría la "Ley de Asociaciones profesionales de patronos y obreros" (1932), la cual se basaba en la de 1887, aunque buscaba la creación de un nuevo régimen para las relaciones laborales en el que se aumentarían las responsabilidades sindicales. Se crearía un registro público para que los sindicatos y las asociaciones se inscribieran y se ordenaría que se disolviera toda orden religiosa que tuviera votos especiales de obediencia a una autoridad que no fuese el Estado. Consecuentemente, se suprime la Compañía de Jesús y se aprueba la "Ley de Congregaciones Religiosas" (1933)[16].

En la época franquista (1936-1975), se mantendría vigente la normativa laboral previa a la República, dictándose nuevas leyes que pretendían limitar el acceso de la mujer al trabajo, más si esta estaba casada, "liberándola del taller y de la fábrica", para dejar al hombre como la fuente de ingresos principal, y ello con la idea de aumentar el desarrollo demográfico. Por otra parte, y con este mismo fin, se potenciarían diferentes subsidios y ayudas por nacimientos (Fuero del Trabajo de 9 de marzo de 1938, y Ley de Bases de 18 de julio de 1938). En relación con las asociaciones, el franquismo prohibió cualquier tipo de asociaciones fuera del Movimiento Nacional, con la excepción de las asociaciones de la Iglesia Católica.

En materia de derechos fundamentales, había una clara discriminación por razón de sexo, llegando a la prohibición de contratar a mujeres casadas. Esta legislación también impedía el acceso a la mujer a profesiones liberales como la abogacía del Estado, la Inspección de Trabajo, la Judicatura, etc. dejando solamente acceder a la mujer a la enseñanza como la única profesión.

[16] Historia del derecho de asociación en España (www.losojosdehipatia.com.es)

Ruiz Resa señala que el Fuero de Trabajo no solo incidió sobre la forma de trabajar y de entender el trabajo, sino también en la configuración de la vida familiar y social, como por otra parte se pretendió[17]. Además, añade a este punto que:

> "La justificación de estos derechos no fue solo el amor, la caridad o la justicia social, sino que, se tratará del cumplimiento de los deberes que el orden del universo impone a los seres humanos en relación con su lugar dentro de las comunidades en que nace (familia, corporación laboral o profesional, Patria) sin olvidar las finalidades específicas (armonía social o protección de la familia) a las que respondieron muchos de estos derechos"[18].

En 1950, con la revisión de la política económica a través del Plan de Estabilización (1959) y el Plan de Desarrollo (1961), habida cuenta del pleno empleo de la mano de obra masculina se levantó la mano con la prohibición del trabajo de la mujer casada. En este año se proclamaría la Ley de derechos políticos profesionales y de trabajo de la mujer donde se recogía la prohibición de discriminación por sexo ni por estado civil en el ejercicio de los derechos políticos y de trabajo, llegando a establecer el derecho a cobrar lo mismo que los hombres por el mismo trabajo.

En relación con la evolución historia del derecho laboral y del control del empresario en nuestro país resulta difícil realizar una profundización, toda vez que existe un vacío importante en nuestra historiografía del Derecho en relación con las obras dedicadas al estudio de los derechos de los trabajadores en la época franquista.

Durante el régimen franquista la sociedad española era una sociedad ordenada y prácticamente redimida a través del trabajo[19], donde se daba un especial protagonismo a las corporaciones sociales que estructuraban la sociedad en estamentos (como la familia o la iglesia). Para Ruiz Resa la ideología de la época que sustentaba la unidad en el Régimen pasaba por "inocular en la regulación laboral la ideología del nacionalsindicalismo y del nacionalcatolicismo, así como la superación del

[17] RUIZ RESA, J.D. (2015) "Los Derechos de los Trabajadores en el franquismo, Madrid, España: Dykinson, Pág. 407
[18] RUIZ RESA, J.D. (2015) "Los Derechos de los Trabajadores en el franquismo…" ob. cit Pág. 407
[19] RUIZ RESA, J.D. (2015) "Los Derechos de los Trabajadores en el franquismo…" ob. cit Pág. 295

individualismo a favor del organicismo"[20]. Con ello se consiguió unos derechos de los trabajadores inspirados, por una parte, en los valores cristianos tradicionales de justicia social armónica y restauradora, la dignidad de la persona y la protección de la familia tradicional católica; y por otra, en la necesidad que tenía el Régimen de garantizar la paz social por necesidad de supervivencia[21].

Para Ruiz Resa, el fascismo débil y el tradicionalismo religioso condujeron al modelo teórico de los derechos calificado como "cartismo social autoritario", generando un holismo de tipo corporativista, organicista y armonicista que rechaza la consideración del sujeto titular de los derechos como individuo opuesto a la sociedad y el Estado[22], sin embargo, no creo que fuera consecuencia del fascismo débil, pues el cartismo es propio de los Estados autocráticos, y aunque se debilitara, no sería hasta la llegada de la democracia cuando se pasará del organicismo a una concepción más individual de los derechos de los trabajadores.

Tras el franquismo, con la llegada de la Constitución, nacería la normativa básica actual en Derecho laboral, como el Estatuto de los Trabajadores, la Ley de Procedimiento Laboral, la Ley de infracciones y sanciones en el orden social, la Ley General de la Seguridad Social o la Ley de Prevención de Riesgos Laborales entre otras.

En la actualidad, era de la tecnología, de Internet y de las redes sociales, las relaciones laborales y la forma de controlar las mismas ha evolucionado notablemente, y lo seguirá haciendo aún más rápido, motivo por el cual, legislación y jurisprudencia deben evolucionar y modificarse, con el fin, no único, pero si principal de proteger los derechos fundamentales de los trabajadores.

En este sentido y tras un largo periodo de desatención o de desregularización de las nuevas tecnologías en el ámbito laboral, la "Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales" (LO 3/2018), basada en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo sobre la "protección de las personas físicas en lo

[20] RUIZ RESA, J.D. (2015) "Los Derechos de los Trabajadores en el franquismo…" ob. cit Pág. 295
[21] RUIZ RESA, J.D. (2015) "Los Derechos de los Trabajadores en el franquismo…" ob. cit Pág. 295
[22] RUIZ RESA, J.D. (2015) "Los Derechos de los Trabajadores en el franquismo…" ob. cit Pág. 406

que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos" (2016), sí que recoge, al menos sucintamente, el régimen jurídico del control empresarial a través de las TICs, así como los derechos digitales.

2.3 Especial referencia al derecho fundamental a la Dignidad de la persona.

La Constitución española reconoce la dignidad de la persona como base fundamental de todos los demás derechos fundamentales. A modo de preámbulo se fija entre el Título I y el Capítulo I que "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social" (CE, Preámbulo).

Además, se recoge que "…las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España" (CE, Preámbulo).

Por tanto, como avanzábamos, la dignidad es un derecho fundamental central originario de los demás, o lo que es lo mismo, el resto de derechos fundamentales lo son porque giran en torno a la dignidad del individuo y al desarrollo de su personalidad.

Según reiterada doctrina del Tribunal Constitucional, como la que deriva de su sentencia 170/2013, de 7 de octubre el derecho a la intimidad es una derivación de la dignidad de la persona (art. 10.1 CE). Según esta doctrina, el derecho a la intimidad personal, al derivar de la dignidad de la persona generará la existencia de un espacio de privacidad reservado frente a las intrusiones de terceros, necesario para mantener una calidad mínima de la vida humana.

El Tribunal Constitucional, a través de su doctrina, ha venido constatando lo establecido en artículo 10 de la CE[23].

[23] CE, Artículo 10.
1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

Esto constituye, consecuentemente, un mínimo invulnerable. De igual forma se va a entender que los derechos fundamentales son derechos subjetivos, del individuo, siendo esenciales en la sociedad al configurarse esta como marco de la convivencia humana justa y pacífica que se desarrolla en nuestro estado de derecho.

Por otra parte, va a entender la Constitución que la dignidad de las personas, sin perjuicio de sus derechos inherentes, está intrínsecamente emparentada con la libre personalidad, y así lo hace constar el propio artículo 10 CE, pero también en los siguientes artículos, como el 16.1 CE, donde se garantiza la libertad ideológica, religiosa y de culto…" y el artículo 18.1 CE donde se garantiza "…el derecho al honor, a la intimidad personal y familiar y a la propia imagen", derechos que devienen de la libre personalidad.

De igual forma, la dignidad de la persona aparece en el artículo 14 CE cuando dice "Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social", en lo que dispone el artículo 15 CE, relativo a "la integridad física y moral", en el art. 20.1. a) CE, en "…expresar y difundir libremente los pensamientos, ideas y opiniones…", en el art. 21.1 CE, cuando habla del "…derecho de reunión…" y en el art. 24.1 "…obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos…".

2.3.1 La Dignidad en el ámbito laboral.

Conforme hemos avanzado, la dignidad de las personas conforma la médula espinal de los demás derechos fundamentales, y de la misma forma, lo será de los derechos fundamentales de los trabajadores, considerando la libertad sindical o la huelga, igual que ocurre con aquellos que son propios del ciudadano, como su intimidad o la libertad de expresarse.

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

Desde un punto de vista laboral, la regulación o el régimen jurídico de la dignidad del trabajador viene establecido en el Estatuto de los Trabajadores donde aparecen varias menciones expresas a la dignidad:

- En el artículo 4.2 e) se recoge como expresamente como condición general, que el trabajador tiene derecho a la consideración debida a su dignidad (art. 4.2 e) ET).

- En el artículo 18, bajo el título "Inviolabilidad de la persona del trabajador", se establece que solo será posible realizar registros en 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, condicionando esos registros al respeto máximo a la dignidad y a la intimidad del trabajador, además de a realizarse dentro del centro de trabajo y en horas de trabajo.

  Según la doctrina constitucional, lo que garantiza el art. 18.1 CE es el secreto sobre nuestro espacio de vida personal, excluyendo que sean los terceros, particulares o poderes públicos, los que delimiten los contornos de nuestra vida privada (STC 159/2009, de 29 de junio, FJ 3; o SSTC 185/2002, de 14 de octubre, FJ 3; y 93/2013, de 23 de abril, FJ 8).

- En el artículo 20 se establece la forma de realizar el control empresarial, pudiendo adoptarse las medidas de vigilancia y control que el empresario estime oportunas, pero respetando la consideración debida a la dignidad de los trabajadores y, además, se deberá tener en cuenta la capacidad real de los trabajadores con discapacidad.

  Sin embargo, para que esas directrices y exigencias se ubiquen en un marco lícito, es preciso que respeten, en todo momento, los límites de la dignidad personal del trabajador, prescindiendo de cualquier acto que pueda considerarse desproporcionado, ofensivo o degradante. Como ejemplo, se admite la vigilancia de temas estrictamente laborales y las grabaciones de vídeo en el lugar de trabajo, pero bajo ningún concepto se permiten estas actuaciones en cuestiones que atañan a la vida privada de las personas.

- En el artículo 39, se recoge lo relativo a la "movilidad funcional", donde se destaca que la misma ha de realizarse sin menoscabo de la dignidad del trabajador.

- Asimismo, se contempla la posibilidad de que el trabajador extinga el contrato unilateralmente *ex.* artículo 50.1 a) si se modifican sustancialmente las condiciones pautadas por el empresario al punto de menoscabar su dignidad, o bien, *ex.* artículo 49.1 j) fundamentada en un incumplimiento contractual grave del empresario.

  Para el punto a) del artículo 50.1 ET, la jurisprudencia ofrece indicaciones a considerar en la determinación de lo que fuese una "modificación sustancial". Entre otras cosas, las modificaciones pueden ser: incumplir el proceso establecido en el artículo 41; realizar perjuicio tangible sobre el trabajador; el abuso de poder, malintencionado o no, cuando redunde en la dignidad de los trabajadores.

Así, la dignidad es un derecho indiscutible de los trabajadores con graves sanciones a los empresarios en caso de ser vulnerada.

2.3.2 La dignidad y el contrato de trabajo.

En el espacio organizativo de la empresa, la relación laboral surge de la interacción de dos partes donde una realiza el trabajo (empleado) permitiendo que la otra (empleador) le dé órdenes o directrices acerca de cómo hacerlo. Así, los empleadores o empresarios organizan el trabajo, mientras que los empleados o trabajadores se subordinan a dicha organización.

Ahora bien, aunque el trabajador acepte formar parte de una organización el poder de dirección de un empresario no constituye un derecho absoluto, sino que se somete a unas limitaciones, principalmente, las derivadas de la obligación del empleador de respetar la intimidad y la dignidad de las personas trabajadoras. En este sentido, la doctrina constitucional ha establecido que el trabajador no pierde sus derechos constitucionales

como ciudadano por el hecho de realizar un trabajo, y conservará estos derechos también en el ámbito de la relación laboral.

Este entorno de sumisión también se ha generado a través de la aceptación del propio contrato por parte del trabajador. Por tanto, a estos efectos se debe tener en cuenta la finalidad del contrato y de qué manera podría limitar los derechos fundamentales en busca de satisfacer los intereses de los firmantes. Y ello porque según la doctrina constitucional van a existir una serie de actividades que generan una restricción de derechos (como el derecho a la imagen de los trabajadores actividades en contacto con el público). Cuando ello suceda, el trabajador que aceptó cumplir esas tareas y formalizó el contrato, no puede después invocar el derecho fundamental a la intimidad, u otro, para eximirse de su realización, si la restricción en ese derecho impuesta por el contrato de trabajo no resulta agravada por lesionar valores elementales de su dignidad o intimidad[24].

El empresario podrá establecer las medidas que considere de vigilancia y control para comprobar el cumplimiento de la prestación de servicios por parte de los trabajadores, aunque para ello deberá respetar la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores con discapacidad (art. 20.3 ET).

Sin embargo, el poder de control y dirección del empleador no va a ser absoluto ni ilimitado, siendo nuestra jurisprudencia la que ha establecido los limites:

1. En primer lugar, ha de ejercitarse respetando los límites establecidos en la Constitución, las leyes, los convenios colectivos y los contratos de trabajo" (STS, 5 de febrero de 2008), es decir, que su ejercicio sea conforme a Derecho, excluyendo la ilegalidad, la vulneración de derechos fundamentales de los trabajadores y la actuación torticera por parte del empresario, contraria a su deber de buena fe[25].
2. La dignidad del trabajador va a ser el límite principal de este poder de dirección del empresario, aunque también lo serán el resto de los derechos fundamentales

[24] SSTC 99/1994, de 11 de abril.

[25] MOLERO, C. (2003). Manual de Derecho del Trabajo. 3ª. Ed. Madrid, España: Editorial Civitas. Pág. 257

de los trabajadores, y el deber de la buena fe contractual (STSJ Cataluña, 18 de septiembre de 2001).

En relación con la posible colisión de los intereses del empresario y los derechos de las personas trabajadores, el Tribunal Constitucional ha insistido en que sean los propios tribunales quienes preserven el necesario equilibrio entre las obligaciones y deberes del empleado, y sus derechos y libertades constitucionales. Es decir, "dada la posición preeminente de éstos en el ordenamiento jurídico, en cuanto proyecciones de los núcleos esenciales de la dignidad de la persona (art. 10.1 CE) y fundamentos del propio Estado Democrático (art. 1 CE), la modulación que el contrato de trabajo puede producir en su ejercicio ha de ser la estrictamente imprescindible para el logro de los legítimos intereses empresariales, y proporcional y adecuada a la consecución de tal fin" (STC 213/2002, de 11 de noviembre, FJ 7 o SSTC 20/2002, de 28 de enero, FJ 3 y 151/2004, de 20 de septiembre, FJ 7).

La libertad sexual va a erigirse como una manifestación trascendental de la dignidad de las personas trabajadoras, conllevando una especial protección frente al acoso sexual en nuestro ordenamiento jurídico. Al respecto, el ET congrega en la noción de respeto a la intimidad y dignidad, el resguardo de ofensas verbales o físicas de connotación sexual, incluyéndose de forma explícita el acoso sexual como infracción muy grave en el entorno de poder del director/empresario.

Asimismo, como ya se ha adelantado, ante cualquier abuso por parte del empleador que perjudique la dignidad del empleado, podrá este reclamar ante los Tribunales que se extinga el contrato de trabajo. Procedimiento practico (ex. Artículo 50 ET) y ágil, sobre todo a raíz de la sentencia dictada por el Tribunal Supremo en fecha 20/7/2012 (RCUD. 1601/2011), seguida por las de 28-10-2015 (RCUD. 2621/14), 3-2-2016 (RCUD. 3198/14), y 23-02-2016 (RCUD 2654/2014), que elimina la necesidad del mantenimiento de la relación laboral hasta que se dicte sentencia y, por tanto, admite la acción de reclamación y la salida del empleado de la organización con anterioridad al dictado de la sentencia.

En concreto, dicha jurisprudencia establece que "no cabe la exigencia del mantenimiento de la relación laboral hasta que recaiga sentencia en supuestos en que el trabajador puede tener un grave perjuicio patrimonial, sin que la posibilidad establecida en el art. 79.7 de la Ley Reguladora de la Jurisdicción Social (LRJS) de que solicite las medidas cautelares contempladas en el art. 180.4 de la propia norma constituya una obligación del trabajador" (RCUD 2654/2014).

En el procedimiento penal también se ha establecido proteger la dignidad del trabajador, existiendo un tipo penal expreso donde se encuadran conductas relacionadas con las actuaciones del empresario.

Así, se recoge expresamente en los delitos de agresión y abuso sexual la circunstancia agravante si el agresor abusa de su "situación de superioridad sobre su víctima" (CP, art. 180.1)[26]. Asimismo, se recoge más intensamente la participación del empresario, cuando se dice que comete un delito "de acoso sexual aquella persona que, en el ámbito de una relación laboral continuada, docente o de prestación de servicios habitual, solicita de otros favores de naturaleza sexual para él mismo o para un tercero" (CP, art. 184.2).[27]

3. Análisis conceptual de las tecnologías de la Información y de la Comunicación (TIC).

Es evidente que hoy en día nos encontramos ante una nueva revolución tecnológica o, posiblemente, en una revolución de las tecnologías de manera constante, que, sin duda, se revela como un "proceso de carácter estructural en nuestra sociedad", tal como entiende Eusebi Colàs en su publicación "Derechos fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia". Constituye la tercera gran transformación social en la historia de la humanidad tras la revolución industrial, considerando que se trata de la "revolución cultural más importante desde el invento de

[26] CODIGO PENAL Art. 180.1. 4.ª *"Cuando, para la ejecución del delito, el responsable se haya prevalido de una relación de superioridad o parentesco, por ser ascendiente, descendiente o hermano, por naturaleza o adopción, o afines, con la víctima".*

[27] *CODIGO* PENAL, Art. 184 2. *"Si el culpable de acoso sexual hubiera cometido el hecho prevaliéndose de una situación de superioridad laboral, docente o jerárquica, o con el anuncio expreso o tácito de causar a la víctima un mal relacionado con las legítimas expectativas que aquélla pueda tener en el ámbito de la indicada relación, la pena será de prisión de cinco a siete meses o multa de 10 a 14 meses".*

la imprenta"[28]. En este sentido Colàs afirma que el estado presente de las tecnologías de la información y comunicación está a la altura de la máquina de vapor en la revolución industrial de 1820, la cual era en aquel contexto lo que hoy son los ordenadores.

En cualquier caso, hay una serie de distinciones entre la presente revolución tecnológica y otras que han ocurrido con anterioridad:

- La primera distinción se puede encontrar en que esta última revolución está fundamentada en las tecnologías de la información y comunicación (TIC), que se centran en el tratamiento, procesamiento y gestión de la información, así como su transmisión, es decir, la propia comunicación. La clave la encontramos en la digitalización (a través del lenguaje binario, es posible la convergencia de diferentes formatos de información) que es el fundamento de estas nuevas tecnologías.

- Como segundo hecho diferenciador, las transformaciones que generan las TIC tienen como consecuencia "una mutación de las bases materiales de la sociedad"[29], y lo que distingue a las relaciones sociales actuales son la gran cantidad de información producida que circula constantemente de forma sistematizada.

La influencia de las nuevas tecnologías sobre las relaciones laborales va a conllevar dos cuestiones que suscitaran controversia y pronunciamientos judiciales:

- Los límites a los usos extralaborales de los medios informáticos puestos a disposición de los empleados;
- La facultad de la empresa para vigilar y controlar tales usos.

Ahora bien, estas cuestiones no son nuevas y el aumento en el uso de las nuevas tecnologías de la información y la comunicación (TIC) no ha generado conflictos

[28] COLÁS NEILA, E. (2012) "Derechos fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia". (1ª. ed). Albacete: Bomarzo. Pág 126
[29] CASTELLS, M. (2000). "La sociedad red: Una visión global" (2ª. ed) Madrid, España: Alianza. Pág 75

diferentes a los ya planteados relativos al uso privativo de herramientas facilitadas por la empresa y el derecho de los empresarios de controlar tal utilización, sin embargo, las nuevas TIC han permitido aumentar exponencialmente las posibilidades de efectuar el control empresarial y, la inspección y control de la prestación de servicios. Con estas nuevas tecnologías se va a poder monitorizar los ordenadores, el correo electrónico y la navegación por Internet, lo que permitirá realizar controles más directos y con menor esfuerzo por parte del empresario. Esos controles, aun siendo realizados con respeto a la legislación vigente, pueden llegar a poner en riesgo diferentes derechos fundamentales que asisten a los trabajadores.

En este apartado se va a estudiar la evolución de las diferentes tecnologías de la información y la comunicación, incluyendo diferentes nociones básicas y definiciones que ayudarán a contextualizar el posterior análisis de la jurisprudencia y de la doctrina.

Si se habla de tecnologías de la información y la comunicación se debe distinguir, por tanto, entre información y comunicación. La información conlleva la libre difusión de todo tipo o forma de datos, y la comunicación es la que busca relacionar a las personas y poder transmitirse entre ellas mensajes y opiniones de diversa índole. Por tanto, la información se realizaría en un entorno abierto mientras que la comunicación se realizaría en un círculo más cerrado. Sin embargo, diferentes autores no efectúan una distinción y subrayan que el aspecto más curioso de las nuevas TIC es la correlación entre las diferentes tecnologías de las telecomunicaciones, la informática y la radiodifusión, de modo que "(…) en el futuro inmediato ya no tendrá sentido entender el teléfono como algo diferente de la televisión y esta como algo muy distinto de un periódico"[30]. Resultará cada vez más complejo separar información y comunicación, conceptos que tenderán a converger[31].

3.1. La evolución de las tecnologías de la información y la comunicación. Antecedentes.

[30] FERNÁNDEZ ESTEBAN, M.L. (1998). *Nuevas tecnologías, Internet y Derechos Fundamentales*. Madrid, España: McGraw Hill.
[31] GARCÍA MEXÍA, P. (2005). El Derecho de Internet, Valencia, España: Tirant lo Blanch, Pág. 121 y ss.

Es evidente que la evolución de las tecnologías de la información es rapidísima y además constante en el tiempo, pues los progresos tecnológicos y las innovaciones que transcurren se van retroalimentando.

Podemos entender que la era de la información se inicia con Samuel Morse, que en 1837 creó el primer emisor y receptor de señales eléctricas, el telégrafo, el cual se empezó a comercializar en el año 1844. El telégrafo es considerado como el aparato que transformó las comunicaciones. Se trataba de un dispositivo que empleaba señales eléctricas para transmitir mensajes codificados de texto (como el código Morse), por medio de comunicaciones de radio o líneas alámbricas. En relación con los cableados de largas distancias, en 1866 se trazó el primer cable de comunicaciones instalado bajo el mar, y en 1956 se realizó el trazado del primer cable transatlántico.

En 1876 Graham Bell patentaría el teléfono, entendido como un aparato que transmitía sonidos a través de señales eléctricas. Por su parte la radio aparecería en 1920 teniendo su esplendor en la década de los 40, siendo en la siguiente década, la de los 50, cuando nacería la televisión.

En lo que respecta a los ordenadores, se iniciaron en los años 40, con el ENIAC (Electrical Numerical Integrator and Computer), un ordenador rápido y flexible para la época, que fue desarrollado para calcular tablas balísticas. En 1976 empezaría a comercializarse el primer ordenador de la marca Apple, el denominado Apple I, pero no fue hasta 1982, cuando apareció el IBM PC, que empezó a extenderse por oficinas, industrias y hogares.

3.2. Las revoluciones tecnológicas.

Actualmente se está produciendo una revolución tecnológica que esta cambiado el mundo laboral y en referencia al control de la actividad laboral por el empresario están surgiendo nuevos equipos (hardware y software) que hacen más fácil y preciso este control. Sin embargo, hasta los últimos años, con el registro de fichajes a través de tarjetas (primero de cartón y luego de plástico) e incluso a través de análisis de huella dactilar, el control del empresario a través de las tecnologías ha sido bastante limitado.

Cada una de las revoluciones tecnológicas sucedidas a lo largo de la historia han estado ligadas a una materia prima o a una energía, como el carbón, el vapor, el hierro, el acero, o el petróleo. En lo que respecta a la revolución tecnológica en la que nos encontramos en la actualidad podemos relacionarla con el plástico, pues de dicho material se conforman la mayoría de los dispositivos informáticos. Asimismo, el litio tendrá especial relevancia pues es el componente principal en las baterías de todo dispositivo informático inalámbrico.

La primera revolución tecnológica se produce en la Primera Revolución Industrial (1760-1840), originándose en uno de los países con más materias primas, Inglaterra. Esta revolución tecnológica utilizó la energía hidráulica en canales y vías fluviales y se centró en el desarrollo de la maquinaria y la mecanización de la industria del algodón.

La segunda revolución tecnológica se produce con el uso del vapor y el desarrollo del ferrocarril también en Inglaterra, a lo largo del año 1829, expandiéndose con posterioridad a Europa y Estados Unidos. Las máquinas a vapor y las maquinarias de hierro se van a desarrollar en este periodo, así como las nuevas infraestructuras como las redes de ferrocarriles. En esta revolución se construyeron los grandes puertos que sirvieron de base a la navegación mundial.

La tercera revolución tecnológica utilizará el acero como materia prima principal, generando la denominada industria básica o pesada, la cual se encargaría de la extracción y transformación de las materias primas. En esta época se comenzaría a utilizar la energía eléctrica como fuente de energía principal cobrando especial relevancia en la presente revolución tecnológica, utilizándose por primera vez en las industrias y apareciendo en las ciudades. El comienzo de la Acería Bessemer de Carnegie en Pensilvania en 1875 sería uno de los hitos más importantes de esta revolución, pues permitía producir acero de bajo coste en una época donde el transporte marítimo era la principal forma de transporte. Además, gracias al uso del acero se mejorarían las redes transnacionales de ferrocarril, y junto con la aparición de la energía eléctrica se mejorarían las ciudades y se iniciaba la era de las construcciones de enormes obras civiles. Por otra parte, en esta época se desarrolló el teléfono y el telégrafo.

La cuarta revolución tecnológica, podría relacionarse con el año 1908, y viene de la mano de la era del automóvil, y por supuesto, del petróleo. Liderando esta revolución se encontraban los Estados Unidos y Alemania, dos potencias de la fabricación de automóviles. Este periodo se caracteriza por el "Fordismo", el modelo de producción en cadena que llevó a la práctica Henry Ford, fabricante de automóviles. En esta época, gracias al petróleo se desarrolló el motor de combustión, lo cual fue esencial para el transporte, con autobuses y aviones, y también para la agricultura, con los tractores, e incluso para la guerra, con la creación de los tanques. En esta era se mejoró la cobertura eléctrica tanto a nivel industrial como doméstico y se construyeron múltiples autopistas, aeropuertos y puertos, que mejoraban la comunicación y el comercio.

La quinta revolución tecnológica podemos decir que comienza en 1971, con el anuncio del microprocesador Intel en California, pero no es hasta los años 90 e incluso 2000 con la aparición de Internet, cuando cobra especial relevancia en el mundo laboral. A nivel tecnológico es la época del desarrollo de las telecomunicaciones, de la informática, y de la revolución de la información. Se crean a nivel mundial nuevas infraestructuras de telecomunicación digital, como Internet y en lo que al transporte físico se refiere, es el momento de la alta velocidad ferroviaria.

Por lo tanto, no será hasta esta última revolución tecnológica, con la llegada de la informática y su desarrollo, cuando la tecnología se utilice para el control empresarial.

3.3. Definiciones.

Las TIC pueden ser definidas como tecnologías de la información y de la comunicación utilizadas en la prestación de servicio y para el control de esta. Es habitual separar las tecnologías de la información y comunicaciones en tres tipos de tecnologías: la microelectrónica, la informática y las telecomunicaciones. Con el paso de los años estas tres tecnologías se harán interdependientes, de tal manera que cualquier avance en una de estas tecnologías necesariamente afectará a las demás.

3.3.1. La microelectrónica.

Se entiende la microelectrónica como la aplicación de la ciencia electrónica a componentes y circuitos sobre una pastilla de un semiconductor, formando un circuito integrado de dimensiones muy pequeñas para después producir dispositivos y equipos electrónicos.

En el año 1959 los científicos estadounidenses R. Noyce y J. Kilby crearon el circuito integrado o chip, colocando unos transistores y otros componentes en un mismo bloque semiconductor e interconectándolos[32].

A partir de aquí se pudo crear en 1971 el microprocesador, lo que permitiría la fabricación de ordenadores de un tamaño razonable para el uso doméstico y laboral.

Se trata de una de las tecnologías más importantes de nuestro tiempo, pues a través de ella, permite que los instrumentos de medida, además de realizar mediciones, las analicen. Además, ha permitido también un control totalmente automático de los procesos, de la maquinaria industrial, del transporte y la movilidad inteligente, de las comunicaciones, de los electrodomésticos, y de los ordenadores[33].

3.3.2. La informática.

La informática[34] se trata de la ciencia que administra métodos, procesos y técnicas, para el almacenamiento, procesamiento y transmisión de datos o información en formato digital. Implica un procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales, de ahí que también sea llamada computación. Los sistemas informáticos deben cumplir cuatro funciones básicas que en su conjunto se conocen como algoritmo, y son;

- entrada o captación de información,
- procesamiento,
- almacenamiento de la información, y

[32] https://polaridad.es/historia-del-circuito-integrado-quien-lo-invento/
[33] https://www.secpho.org/microelectronica
[34] https://es.wikipedia.org/wiki/Inform%C3%A1tica

- salida o trasmisión de resultados.

La informática se desarrolla de una manera espectacular desde mediados del siglo XX con el surgimiento de tecnologías como los circuitos integrados, Internet y los smartphones. La misma se puede entender como la parte de la tecnología que se ocupa de un tratamiento automático de la información.

3.3.3. Las telecomunicaciones.

Las telecomunicaciones son consideradas como "las transmisiones y recepciones de señales de cualquier naturaleza, normalmente electromagnéticas, que contienen signos, sonidos y/o imágenes. Las telecomunicaciones son, por tanto, cualquier transferencia de información"[35].

Igualmente se denomina así, a la disciplina que estudia, diseña, desarrolla y explora aquellos sistemas que permiten dichas comunicaciones.

El telégrafo, el teléfono y la radio fueron los tres grandes hitos de la historia de las telecomunicaciones. En la actualidad, la fibra óptica, la transmisión vía satélite y la telefonía móvil han desbancado a las anteriores en materia de telecomunicaciones.

Los avances de la microelectrónica y la informática han posibilitado una mejora en la calidad de los servicios de las telecomunicaciones. Lo que se ha mejorado es la incorporación de técnicas digitales a los equipos de telecomunicaciones, las cuales permiten descomponer cualquier tipo de señal analógica en una señal digital y, por tanto, en una sucesión de códigos que permiten que toda información pueda ser manipulada por un ordenador.

3.4. Sistemas que conforman las TIC en el ámbito de las relaciones laborales.

[35] https://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n

Diferente normativa, como el artículo 20.3 ET o el artículo 22 de la Ley 10/2021 van a recoger las facultades de control del empresario, y va a permitir a este que adopte las medidas de vigilancia que estime más oportunas para verificar el cumplimiento por los trabajadores de sus obligaciones y deberes laborales, incluida la utilización de dispositivos o medios telemáticos.

Por su parte, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, va a recoger de manera expresa los derechos que pueden verse afectados por el uso de dispositivos en el entorno laboral

A continuación, se relaciona una serie de dispositivos o sistemas que conforman las nuevas tecnologías en el entorno laboral y que son susceptibles de generar conflictos entre los derechos del empresario y de los trabajadores.

3.4.1. Ordenadores.

La primera generación de ordenadores nacería con la creación del ordenador ENIAC, desarrollado en 1946. Se trataba de un ordenador de gran tamaño y excesivo consumo de energía.

En la actualidad, gracias al circuito integrado estos ordenadores son de un tamaño fácilmente manejable y transportable, siendo vital su utilización en la mayoría de los sectores y puestos de trabajo.

Con la utilización de las tecnologías de la información y comunicación para el control laboral se multiplican las facultades de control empresarial y la capacidad de inspección de la ejecución de la prestación laboral.

Este instrumento de la empresa, al ser susceptible de monitorizar y de realizar controles sobre la navegación en Internet y el correo electrónico, generará una serie de problemas relacionados con la vulneración de diferentes derechos fundamentales como el derecho a la intimidad o al secreto en las comunicaciones, toda vez que permite realizar controles más rigurosos y con un menor esfuerzo por parte del empresario. Aunque este control se

realice con respeto a la legalidad, pueden surgir conflictos con respecto a la intimidad de los trabajadores[36].

Por ello, relacionaremos el ordenador directamente con la utilización del correo electrónico y la navegación por Internet.

3.4.2. Correo electrónico.

Hoy por hoy todo el mundo conoce que es el correo electrónico, pero, aun así, no está demás hacer una descripción formal del mismo, que nos ayudará a entender el tipo de vulneración en la que es posible incurrir si se indaga en el mismo sin el adecuado consentimiento.

El correo electrónico (en inglés, electronic mail, comúnmente abreviado como e-mail o email) es un servicio de red o de Internet que posibilita que los usuarios envíen y reciban mensajes a través de redes electrónicas de comunicación.

Correo electrónico se usa de manera genérica para denominar al sistema que ofrece este servicio vía Internet mediante el protocolo SMTP (Simple Mail Transfer Protocol). Los mensajes de correo electrónico permiten el envío de textos y de cualquier tipo de documento digital (imágenes, videos, audios, etc.).

El correo electrónico funciona de forma similar al correo postal, pues ambos permiten enviar y recibir mensajes sin la necesidad de que ambos se encuentren conectados simultáneamente, como si sucede con el teléfono o con las videollamadas. Para que esto suceda, a modo de buzón existen los servidores, que actuando como intermediarios o carteros guardan temporalmente los mensajes hasta que el destinatario los lea.

Existen multitud de servidores en Internet y estos se nombran tras el “arroba” (@). El estadounidense Ray Tomlison fue quien añadió “@” a los correos electrónicos con la idea

[36]CARDONA, M. B. (2003) “Las relaciones laborales y el uso de las tecnologías informáticas”. Revista de Relaciones Laborales. Nº Extra-1, pp. 157-173.

de separar el nombre del usuario y el servidor. En ingles se pronuncia “at” y significa “en” por lo que indica el servidor donde tiene alojado el correo el usuario[37].

En la empresa el correo electrónico es un instrumento más de trabajo, y un medio de comunicación. En próximos apartados veremos cómo se realiza el control por parte del empresario y si supone o no una intromisión en la intimidad o vulneración del secreto en las comunicaciones. De igual forma, se valorará la incidencia de su uso extralaboral.

3.4.3. Navegación por Internet.

Otro ejemplo de nuevas tecnologías es la navegación por Internet en la empresa. En este aspecto se plantean las mismas cuestiones que en el correo electrónico, es decir, la posibilidad de realizar un uso del mismo no estrictamente laboral por parte del trabajador, y la facultad del empresario de controlar dicha utilización, de manera que este control sea respetuoso con la intimidad del trabajador.

Antes de ahondar en el control empresarial efectuado en la navegación por Internet, para mejor comprensión y practicidad, se realiza un análisis conceptual de diferentes términos que conforman y se encuentran en la navegación por Internet.

- Internet es una red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación[38]. La línea de protocolos TCP/IP “garantiza que las redes físicas heterogéneas que la componen formen una red lógica única de alcance mundial”[39].

Dentro de Internet existen diferentes servicios y protocolos:

- World Wide Web (WWW): Es un sistema que funciona a través de Internet por el cual se pueden transmitir diversos tipos de datos a través del Protocolo de

[37] PÉREZ PORTO, J., MERINO, M. (2008). *“Correo electrónico - Qué es, definición, cómo funciona y estructura”.* Definicion.de. Última actualización el 7 de mayo de 2021. Recuperado el 19 de mayo de 2023 de https://definicion.de/correo-electronico/
[38] Definición R.A.E.
[39] https://es.wikipedia.org/wiki/Internet

Transferencia de Hipertextos o HTTP, que son los enlaces de la página web" (Wikipedia)[40].

- El protocolo para transferencia simple de correo (en inglés: Simple Mail Transfer Protocol o SMTP) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, impresoras, etcétera)[41].

- El Protocolo de transferencia de archivos (en inglés File Transfer Protocol o FTP) es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo[42].

Otros servicios de Internet son las conversaciones en línea (IRC), la mensajería instantánea, mediante aplicaciones como WhatsApp o Skype, la comunicación en multimedios y transmisión de contenidos, la telefonía (VoIP), la televisión (IPTV), los protocolos de transferencia de noticias (NNTP), los juegos online y el acceso remoto de un dispositivo a otro (SSH y Telnet).

3.4.4. Smartphone.

La increíble capacidad de estos ordenadores de bolsillo donde podemos encontrar infinitas aplicaciones como un teléfono, navegación por Internet, correo electrónico, cámaras, grabadoras de audio, mensajería, aplicaciones para geolocalizar, etc. permitiría la elaboración de una tesis individualizada.

Al tratarse prácticamente de un ordenador, trataremos a los mismos no como una tecnología en sí misma, sino como las aplicaciones en él recogidas.

---

[40] https://es.wikipedia.org/wiki/World_Wide_Web
[41] https://es.wikipedia.org/wiki/Protocolo_para_transferencia_simple_de_correo
[42] https://es.wikipedia.org/wiki/Protocolo_de_transferencia_de_archivos

3.4.5. Cámaras de videovigilancia.

Diferente doctrina, como la de Calonge Crespo[43], define la videovigilancia como un proceso automático en el que por medio de cámaras se obtienen imágenes de personas y objetos, cuya finalidad será la observación y el control de esas personas y objetos para la evitación de la producción de daños o de situaciones de peligro, y que posteriormente se almacenarán en un dispositivo de almacenamiento.

Las imágenes recogidas por las videocámaras fueron consideradas como datos de carácter personal en la LOPD de 1999 al contener información respecto de personas físicas identificadas o identificables, y su grabación era considerada como tratamiento de datos. La vigente Ley Orgánica de Protección de Datos, 3/2018, recoge los tratamientos de datos con fines de videovigilancia, y permite la videovigilancia de las empresas "con fines de seguridad en las personas y en los bienes, incluyendo las propias instalaciones" (art. 22). En cuanto a las imágenes que se captan en la vía pública, se permite para el mismo fin y en la medida imprescindible.

A la hora de valorar las posibles intromisiones del empresario por el uso de este tipo de cámaras para realizar el control laboral, debemos estar al tipo de cámara (visible u oculta) y a la finalidad de la cámara instalada. Es decir, si la cámara se utilizó como medio de vigilancia del control laboral o, por el contrario, era un medio en principio utilizado por cuestiones de seguridad. A lo largo de esta tesis se podrá ver la evolución de la jurisprudencia sobre la vulneración del derecho fundamental a la intimidad y el derecho a la protección de datos de carácter personal por la utilización para el control empresarial de todo tipo de cámaras de videovigilancia.

[43] CALONGE CRESPO, I. (2011) "Videovigilancia y seguridad pública. [Videovigilancia: ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales]". Coor. ETXEBARRIA GURIDI, J.F. y IXUSCO ORDEÑANA, G. País Vasco, España: Tirant lo Blanch. Pág. 81.

3.4.6. Monitorización empresarial.[44]

La monitorización empresarial se puede definir como la mera labor de control y seguimiento efectuada por el empresario para con sus trabajadores. La monitorización no deja de ser un control en las diferentes áreas y en los medios de trabajo facilitados por el empresario y, en relación con la asistencia al trabajo, es posible llevarla a cabo con los medios de trabajo o con el propio contenido del trabajo.

El Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo se centró en controlar la asistencia y el registro horario, con el fin de evitar las horas extraordinarias o excesos de jornada no remunerados.

Dado que resulta complejo un sistema de fichaje cuando los trabajadores realizan sus jornadas en diferentes lugares o centros de trabajo, los smartphones y sus aplicaciones han permitido un modo de reportar el ingreso y la salida del puesto de trabajo. Estos sistemas utilizan geolocalización para controlar aquello a lo que apunta el RDL 8/2019.

Sin embargo, emergen algunos interrogantes con respecto a utilizar con fines laborales el dispositivo que es propiedad del trabajador o no hacerse cargo del abono del servicio mensual de telefonía (conocido en USA como BYOD, siglas de “bring your own device”, donde los empleadores no sufragan los dispositivos ni su mantenimiento), además de poner en tela de juicio hasta qué punto se respetan los derechos a la intimidad o de qué manera se protegen los datos.

La cuestión de hacer uso del dispositivo particular del empleado aún no se ha legislado en España. No obstante, existe jurisprudencia en la que se han declarado nulas cláusulas contractuales donde se condicionaba la relación laboral a que el trabajador aportara su teléfono móvil, aunque la misma hace foco, principalmente, en los derechos a la privacidad [45].

[44] PASCUAL LOPEZ, J.E. (5 de julio de 2019) La monitorización empresarial https://www.dpglegal.es/es/noticia/la-monitorizacion-empresarial/

[45] PASCUAL LOPEZ, J.E. (5 de julio de 2019) La monitorización empresarial https://www.dpglegal.es/es/noticia/la-monitorizacion-empresarial/

Es evidente que estas problemáticas germinan de una sociedad hiperconectada y rica en medios (España es uno de los países con más Smartphones por habitantes). Por esta razón, apelando a lo que el sentido común indica, los trabajadores deben tener derecho a desconectarse, descansar y proteger sus datos personales.

3.4.7. RFID.[46]

Las etiquetas RFID (identificación por radiofrecuencia), aluden a sistemas para el almacenamiento y la recuperación de data remota, por medio de dispositivos conocidos como transpondedores RFID, etiquetas o tarjetas. Estas mejoran y amplían las posibilidades de control empresarial de la actividad laboral de cada trabajador. Permiten, por ejemplo, localizarlo en todo momento durante su jornada de trabajo. La localización podría completarse con la tecnología GPS.

A pesar de la facultad de control reconocida al empresario, el control permanente en el trabajo y en los desplazamientos dentro de la compañía, vulneran el derecho a la intimidad del trabajador, así como el derecho a proteger sus datos de carácter personal, pues se pueden obtener datos como, las veces que acude a la máquina de café, la entrada y salida del parking, etc.

De esta manera, la medida de control debe ser razonable. Los límites a la utilización de las RFID para el control de la actividad laboral, los establece la Comisión Europea a través del principio de seguridad e intimidad según el Reglamento del Parlamento Europeo y del Consejo 679/2016, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos (UE, 679/2016).

[46] Radio Frequency Identification.

3.4.8. GPS.[47]

El GPS es un sistema de radionavegación estadounidense basado en el espacio que proporciona servicios de posicionamiento, navegación, y cronometría gratuita e ininterrumpidamente a usuarios civiles en todo el mundo[48].

Toda persona que tenga un receptor del GPS, el sistema le proporcionará su localización y la hora exacta en cualquier lugar del mundo, en cualquier condición atmosférica, de día o de noche y sin límite al número de usuarios simultáneos.

El GPS se compone de tres elementos: los satélites en órbita alrededor de la Tierra, las estaciones terrestres de seguimiento y control, y los receptores del GPS propiedad de los usuarios. Desde el espacio, los satélites del GPS transmiten señales que reciben e identifican los receptores del GPS; ellos, a su vez, proporcionan por separado sus coordenadas tridimensionales de latitud, longitud y altitud, así como la hora local precisa.[49]

La tecnología GPS utiliza treinta y un satélites que giran en seis órbitas diferentes alrededor de la Tierra, donde cada satélite transmite una señal radioeléctrica extraordinariamente precisa. Un receptor, como un smartphone actual, podrá determinar su ubicación cuando la antena del GPS reciba al menos cuatro de dichas señales.

El GPS se comenzó a utilizar como dispositivo de seguimiento y localización por espías durante la Guerra Fría. En la actualidad, estos sistemas se instalan en vehículos o en teléfonos móviles y fueron utilizados para proporcionar una mejor conducción, pues el GPS permite conocer la ubicación actual del vehículo y, por tanto, "guiar" al mismo. Esta capacidad de localización permite en un ámbito general el control del trabajo y el uso que se le está dando al vehículo fuera del centro de trabajo[50].

---

[47] Global Positioning System.

[48] https://www.gps.gov/spanish.php

[49] https://www.gps.gov/spanish.php

[50] FERNÁNDEZ GARCIA, A. (2010) "Sistemas de geolocalización como medio de control del trabajo: un análisis jurisprudencial". Revista Doctrinal Aranzadi Social. Nº 17/2010.

En lo que respecta a las personas, el GPS se utiliza también contra la delincuencia en general y contra la violencia de género en particular, implantando el GPS en una pulsera al agresor o preso en libertad vigilada, para conocer su paradero y con un sistema de aviso para el momento en el que este entra en el radio de seguridad establecido en torno a la víctima[51].

El GPS es uno de los sistemas más utilizados para el control laboral pues permite la localización exacta del empleado durante su jornada laboral, sobre todo en puestos de trabajo desarrollados fuera del centro de trabajo, como es el caso de conductores, comerciales o vigilantes de seguridad. No obstante, con el auge del teletrabajo esta forma de control se ha extendido a otros sectores.

Con la utilización de este sistema, el empresario puede conocer la ubicación con total exactitud de sus trabajadores y, de este modo, controlar la prestación de los trabajos.

La Unión Europea en colaboración con la Agencia Espacial Europea (ESA) creó en 2016 un sistema de navegación propio, GALILEO, independiente del GPS estadounidense, que funciona de manera similar. En la actualidad cuenta con 22 satélites operativos y a diferencia del GPS, es de creación, gestión y uso civil[52]. Este sistema funciona conjuntamente con el GPS, es decir, que el receptor utiliza indistintamente los satélites de uno u otro sistema.

4. El control del empresario.

El control del empresario se sustenta en el poder de dirección, el poder disciplinario y el poder sancionador. El poder de dirección puede definirse como la posibilidad que tiene el empresario de alterar los límites de la prestación laboral sin que supongan una

[51] Los tratamientos de datos por las fuerzas y cuerpos de seguridad para la investigación y prevención de delitos se rigen por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

[52] 881/11/ES. WP 185. Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes.

modificación sustancial de las condiciones de trabajo[53]. Por su parte, el poder disciplinario y sancionador van a permitir al empresario poder sancionar las conductas reprochables de sus empleados.

4.1. Empresa y control laboral.

Diferentes autores han tratado el control empresarial partiendo de la llamada "Teoría de la agencia y de la Teoría del servidor"[54], de forma que la empresa, como verdadera caja de contratos, con clientes, proveedores, administraciones públicas, inversores y trabajadores, entre otros, aúna los esfuerzos de todos los que contratan en su seno para conseguir objetivos tanto a nivel general de empresa como individualmente cada uno de los que conforma la otra parte de los contratos. En función de ciertos factores situacionales y sus características personales el directivo elige comportarse como agente o como servidor. Si elige comportarse como agente, el directivo se caracteriza por una aproximación al gobierno de la organización desde un punto de vista económico, comportándose de modo individualista, oportunista y centrado en sus propios intereses. De esta manera, dejará de lado los objetivos de la empresa para centrarse en los suyos propios, sus motivaciones y sus estructuras se identificarán por estar orientadas al seguimiento y a la supervisión, su actitud será de aversión al riesgo y la relación se basará en el control.

Cuando toma el rol del "servidor" el directivo dirigirá su organización desde un punto de vista sociológico y psicológico, y por ello, seguirá un modelo de persona basado en un comportamiento de trabajo colectivo, pro-organizacional y de confianza. En este caso, sus objetivos, intereses y motivaciones coincidirán con los de la empresa, y sus estructuras

---

[53] Art. 41.1 ET *"(…) Tendrán la consideración de modificaciones sustanciales de las condiciones de trabajo, entre otras, las que afecten a las siguientes materias:*

- *a) Jornada de trabajo.*
- *b) Horario y distribución del tiempo de trabajo.*
- *c) Régimen de trabajo a turnos.*
- *d) Sistema de remuneración y cuantía salarial.*
- *e) Sistema de trabajo y rendimiento.*
- *f) Funciones, cuando excedan de los límites que para la movilidad funcional prevé el artículo 39 (…)".*

[54] MARTÍNEZ LÓPEZ, F. J.; LUNA HUERTAS, P.; MORO INFANTE, A. y MARTÍNEZ LÓPEZ, L. (2003). Los sistemas de control de la actividad laboral mediante las nuevas tecnologías de la información y las comunicaciones. Relaciones Laborales Nº 1. págs. 1415.

se centrarán de forma facultativa y delegada de poder, por lo que su actitud será de propensión al riesgo y relaciones de confianza.

Consecuentemente, cuando el directivo asume el rol de "agente", con el comportamiento individualista, oportunista y que solo sirve a sus propios intereses, le servirá para justificar algunas medidas de control.

El método más habitual de vigilancia y control en el trabajo serán las tecnologías diseñadas para la seguridad y el control. Estas medidas de seguridad y control sirven en muchos casos para justificar la introducción de tecnologías de vigilancia como son las cámaras de video y las tarjetas de identidad magnéticas. Es decir, la prevención de posibles incidentes en la empresa, permite la instalación de medidas de control, las cuales se instaurarán tanto en la empresa física como de forma virtual a través de programas informáticos[55].

Juristas como Paula Luna Huerta o Luis Martínez López entienden que los sistemas empresariales de información basados en las TIC extienden la vigilancia y el control al monitorizar el desempeño de los trabajadores y la acción de este, por lo que se van a extralimitar[56]. Sin embargo, entendemos que no siempre existirá la extralimitación, habrá que valorar si esa vigilancia y control se ha realizado conforme al test de proporcionalidad.

La irrupción de las nuevas tecnologías en el ámbito laboral ha generado una evolución positiva en el rendimiento de los trabajadores y en la productividad de las empresas, sin embargo, también genera una preocupación en el empresario, sobre el uso ajeno al trabajo de esas nuevas tecnologías en su horario laboral. Desde el punto de vista del trabajador, es cierto que, a lo largo de la historia, las evoluciones tecnológicas no han sido bien asumidas por estos, toda vez que, en muchos casos, la evolución tecnológica es sinónimo

[55] MARTÍNEZ LÓPEZ, F. J.; LUNA HUERTAS, P.; MORO INFANTE, A. y MARTÍNEZ LÓPEZ, L. (2003). "Los sistemas de control de la actividad laboral mediante las nuevas tecnologías de la información y las comunicaciones". *Relaciones Laborales*. Nº 1. Pág. 1416

[56] MARTÍNEZ LÓPEZ, F. J.; LUNA HUERTAS, P.; MORO INFANTE, A. y MARTÍNEZ LÓPEZ, L. (2003). Los sistemas de control de la actividad laboral …" ob. cit Pág. 1416

de amortización de puestos de trabajo. Ahora, con la inclusión de las TIC, es evidente que el empresario puede realizar un mayor control en la actividad laboral del trabajador.

Sin embargo, el control del empresario a través de las TIC puede generar la violación de diferentes derechos fundamentales del trabajador, lo cual es el objeto principal de esta tesis.

4.2. Régimen jurídico.

Tanto la Constitución Española como el Estatuto de los Trabajadores recogen diferentes preceptos de los que deriva el poder de dirección del empresario. Partimos de un reconocimiento esencial como es la libertad de empresa (art. 38 CE), para después entender que los trabajadores prestan sus servicios dentro del ámbito de organización y dirección de un empresario (art. 1.1 ET) cumpliendo sus órdenes e instrucciones estando obligado a realizar el trabajo pactado bajo su dirección (art. 20 ET).

Por lo tanto, de tal normativa podemos extraer que:

- Los trabajadores prestan sus servicios en una empresa, y por tanto, dentro del ámbito de organización y dirección de un empresario. (ET, Art. 1.1).
- Entre los deberes básicos de las personas trabajadoras destaca el deber de cumplir las órdenes e instrucciones del empresario o la persona en quien delegue en el ejercicio regular de sus funciones de dirección. (ET, Art. 5 c).
- La obligación de realizar el trabajo pactado bajo la dirección del empresario. (ET, Art. 20.1).
- Se reconoce la libertad de empresa en el marco de la libre economía de mercado. Los poderes públicos van a garantizar y proteger el ejercicio de la libertad de empresa y la defensa de la productividad, de acuerdo con los requerimientos de la economía general. (CE, art. 38).

4.3. Doctrina y Jurisprudencia.

La sentencia del Tribunal Superior de Justicia de Cataluña de 22/10/2001 definió la relación laboral como la relación que surge entre empresario y trabajador, en la que, como consecuencia de la obligación de trabajar emanada del contrato, el trabajador debe prestar su servicio con la diligencia y la colaboración que marquen las leyes, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres.

Al mismo tiempo, un contrato laboral deriva la buena fe de las partes. Sin embargo, el concepto de buena fe es algo impreciso, pues las legislaciones actuales no la han definido, aunque sí que se recoge su infracción como causa de despido en el Estatuto de los Trabajadores (art. 54.2 d)). De igual forma, el art. 5 a) ET establece que el trabajador tiene el deber de cumplir con las obligaciones inherentes a su concreto puesto de trabajo, conforme con las reglas de la buena fe y la diligencia debida. Ante la falta de definición específica en nuestra normativa, el concepto de buena fe contractual se ha ido perfilando por la jurisprudencia, como por ejemplo, en la sentencia del Tribunal Supremo de 15/06/2009 (Rec 2660/2004)[57] que recoge la evolución del concepto de la buena fe que se ha ido erigiendo por el propio Tribunal Supremo en base a lo establecido en el artículo 1258 CC, como cumplimiento efectivo del contrato en orden a la realización del fin propuesto, para puntualizar que la misma como criterio objetivo, viene a estar formada por una serie de pautas coherentes con el comportamiento humano que en relación con los contratos funciona como norma general de la voluntad reflejada en el consentimiento

[57] *"Según ha señalado este Tribunal al precisar el alcance del art.* 1258 Código Civil *(STS 12/02/2009, y las que en ella se citan), si bien es doctrina de esta Sala la de que la buena fe, en su sentido objetivo consiste en dar al contrato cumplida efectividad en orden a la realización del fin propuesto, por lo que deben estimarse comprendidas en las estipulaciones contractuales aquellas obligaciones que constituyen su lógico y necesario cumplimiento, también se ha sentado por la misma que el carácter genérico del art.* 1258 Código Civil *ha de armonizarse con los más específicos que para cada contrato y en cada supuesto contiene el* Código Civil *y que la posibilidad de ampliar o modificar, a su amparo, lo estrictamente convenido, ha de admitirse con gran cautela y notoria justificación, es decir, que la expansión de los deberes al amparo del art. 1258 Código Civil, debe ser lo más restringida posible, porque no puede escindirse este artículo del contenido del art. 1283* Código Civil*, según el cual en los términos de un contrato no deberán entenderse comprendidos cosas distintas ni casos diferentes de aquellos sobre los que los interesados se propusieron contratar ", añadiendo que "La buena fe es un criterio objetivo, constituido por una serie de pautas coherentes con el comportamiento en las relaciones humanas y negociales, que en materia contractual no solo funciona como un canon hermenéutico de la voluntad reflejada en el consentimiento, sino también como una fuente de integración del contenido normativo del contrato, que actúa por vía dispositiva, a falta de pacto y abstracción hecha de la intención o de la voluntad de las partes, de tal forma que estas consecuencias que complementan el contrato hayan su fundamento vinculante no solo en el mismo, en sus indicaciones explicitas o implícitas, sino en la norma o principio general de la buena fe".*

y como fuente de integración del contenido normativo del contrato que actúa ante la falta de pacto o concreción, complementando el mismo.

Desde otro punto de vista, la jurisprudencia en consonancia con el art. 5 y 20 ET ha establecido que la transgresión de la buena fe constituye una actuación contraria a los deberes básicos del trabajador conforme al contrato de trabajo (STS 26/1/1987 o 19/12/1990), y puntualiza que la misma es esencial en el contrato de trabajo, pues genera derechos y deberes recíprocos, constituyendo un principio general de derecho que impone un comportamiento arreglado a valoraciones éticas, como la lealtad, la honorabilidad, la probidad y la confianza (Sentencia del Tribunal Supremo de 21 enero 1986, FJ 2); La esencia del incumplimiento no estará en el daño causado o al lucro personal, sino en la propia transgresión de la buena fe depositada y de la lealtad debida, al configurarse la falta por la ausencia de valores éticos (SSTS 8 febrero 1991, FJ 3); Asimismo, no será necesario una acción dolosa, bastando la acción culposa cuando la negligencia sea grave e inexcusable (Sentencias del Tribunal Supremo de, 4 febrero 1991, FJ 5 o 19 enero 1987, FJ 4); La buena fe se sustenta en la confianza depositada en el trabajador por lo que a los efectos de valorar la gravedad y culpabilidad de la infracción se tendrá en cuenta la categoría profesional, la responsabilidad y la confianza depositada en el trabajador (Sentencias del Tribunal Supremo 19 diciembre 1989, FJ 3), aunque no debe establecerse graduación alguna (STS 29 noviembre 1985, FJ 4).

Desde otra perspectiva, se ha entendido la buena fe como un deber de fidelidad entre empresario y trabajador, traduciéndose en una exigencia de comportamiento ético jurídicamente protegido y exigible en el ámbito contractual, y concibiéndose como un modelo de tipicidad de conducta exigible.

Sin embargo, no toda transgresión de la buena fe contractual justifica el despido sino solo aquella que por ser grave y culpable imponga la violación trascendente de un deber de conducta del trabajador (Sentencias Tribunal Supremo 13 de marzo de 1996 y 4 de junio de 1999).

Por su parte, el abuso de confianza se entiende como una modalidad cualificada de la buena fe contractual, consistente en un mal uso o un uso desviado por parte del trabajador

de la responsabilidad y confianza otorgadas (Sentencia de la Sala de 27 de enero de 1999 y 26 de septiembre de 1984 o 9 de diciembre de 1986).

En consonancia con lo ya tratado, de acuerdo con el ET, el empresario podrá establecer las medidas que considere de vigilancia y control para comprobar el cumplimiento de la prestación de servicios por parte de los trabajadores, respetando la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores con discapacidad (art. 20.3 ET).

Sin embargo, también se ha mencionado que el poder de dirección del empleador no es absoluto ni ilimitado. Por esta razón, nuestra doctrina jurisprudencial ha establecido ciertos requisitos para poder realizarlo sin vulnerar los derechos fundamentales de quienes trabajan.

3. En primer lugar, ha de ejercitarse respetando los límites establecidos en la Constitución, las leyes, los convenios colectivos y los contratos de trabajo" (STS, 5 de febrero de 2008), es decir, que su ejercicio sea conforme a Derecho, excluyendo la ilegalidad, la vulneración de derechos fundamentales de los trabajadores y la actuación torticera por parte del empresario, contraria a su deber de buena fe[58].
4. La dignidad del trabajador va a ser el límite principal de este poder de dirección del empresario, aunque también lo serán el resto de los derechos fundamentales de los trabajadores, y el deber de la buena fe contractual (STSJ Cataluña, 18 de septiembre de 2001).

En cuanto a los límites del poder de dirección, el Tribunal Constitucional[59], tal y como se advirtiese al inicio de esta tesis, instauró ciertas pautas para atender a la validez de las medidas emanadas del poder de dirección del empleador.

[58] MOLERO, C. (2003). Manual de Derecho del Trabajo. 3ª. Ed. Madrid: Editorial Civitas. Pág. 257

[59] Las sentencias del Tribunal Constitucional 98/2000 y 186/2000 marcan la jurisprudencia del juicio de proporcionalidad en sentido estricto.

El Tribunal Constitucional defiende que, dada la prevalencia de los derechos fundamentales de quienes trabajan, su limitación por parte del empresario "solo puede derivar del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho" (SSTC 99/1994, de 11 de abril, FJ 7 y 6/1995, de 10 de enero, FJ 3). Según esta doctrina, la relación laboral, como conlleva una sumisión del trabajador a los poderes empresariales, o al menos en algunos aspectos de su actividad humana, es necesario que esta sumisión se tenga en cuenta en el momento de equilibrar los intereses de los empleadores, así como si ocurriesen colisiones entre ellos.

Este entorno de sumisión también se ha generado a través de la aceptación del propio contrato por parte del trabajador. Por tanto, a estos efectos se debe tener en cuenta la finalidad del contrato y de qué manera podría limitar los derechos fundamentales en busca de satisfacer los intereses de los firmantes. Y ello porque según esta doctrina van a existir una serie de actividades que generan una restricción del derecho a la imagen de los trabajadores que deban realizar ese tipo de tareas, y ello por una relación de conexión necesaria, impulsada por la propia naturaleza de estas, como lo son, por ejemplo, todas las actividades en contacto con el público. Cuando ello suceda, el trabajador que aceptó cumplir esas tareas y formalizó el contrato, no puede después invocar el derecho fundamental a la intimidad, u otro, para eximirse de su realización, si la restricción en ese derecho impuesta por el contrato de trabajo no resulta agravada por lesionar valores elementales de su dignidad o intimidad[60].

Igualmente, la jurisprudencia constitucional ha mantenido que el ejercicio de las facultades empresariales en materia organizativa y disciplinaria no pueden conllevar en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador. (SSTC 94/1984, de 16 de octubre, FJ 3; 171/1989, de 19 de octubre, FJ 3; 123/1992, de 28 de septiembre, FJ 5; y 173/1994, de 7 de junio, FJ 5), además de que el uso de un derecho constitucional nunca podrá ser sancionable (STC 11/1981, de 8 de abril, FJ 22).

[60] SSTC 99/1994, de 11 de abril.

A partir de este momento y con las sentencias STC 66/1995, de 8 de mayo, FJ 4 Y 5; 55/1996, de 28 de marzo, FJ 7, 207/1996, de 16 de diciembre, FJ 4, y 37/1998, de 17 de febrero, FJ 8, se asentará la doctrina del principio de proporcionalidad, por la cual, la constitucionalidad de cualquier medida que implique la restricción de derechos fundamentales vendrá determinada por la rigurosa observancia del principio de proporcionalidad.

Para confirmar si la medida restrictiva de derechos cumple con este principio, se debe valorar si cumple tres requisitos: el juicio de idoneidad, el juicio de necesidad y el juicio de proporcionalidad. En el juicio de idoneidad se valora si la misma puede lograr su propósito. Con el juicio de necesidad se valora la necesidad de la medida, es decir, la no existencia de otra más conveniente e igualmente eficaz para ese fin. Por último, en el juicio de proporcionalidad se valora si la medida es ecuánime, evaluando si de ella se derivan más ventajas que desventajas para el interés general.

Por tanto, como se ha adelantado, el Tribunal Constitucional[61] se va a centrar en mantener el equilibrio entre el poder de dirección desarrollado a través del control empresarial y la posible vulneración en los derechos fundamentales de las personas trabajadoras, o dicho de otra forma, mantener el necesario equilibro entre las obligaciones establecidas en el contrato de trabajo y el ámbito de la libertad constitucional de los trabajadores, que viene modulada en el contrato pero que solo debe producirse en la medida estrictamente imprescindible para el correcto y ordenado respeto de los derechos fundamentales del trabajador y, muy especialmente, del derecho a la intimidad personal que protege el art. 18.1 CE, respectando además el principio de proporcionalidad en caso de limitación.

5. Derechos fundamentales que se pueden ver comprometidos en la relación laboral por la utilización de las nuevas tecnologías.

5.1. Introducción.

[61] STC 6/1998, de 13 de enero.

En primer lugar, es conveniente indicar que nuestra Constitución no recoge expresamente una protección de los derechos fundamentales frente a la intromisión efectuada a través de las nuevas tecnologías de la información y comunicación, y que la misma carece de mecanismo o cláusula que permita la creación de nuevos derechos fundamentales. Por lo tanto, la protección de los derechos fundamentales se realizará desde una perspectiva jurisprudencial y legislativa.

El reconocimiento por parte del Tribunal Constitucional del derecho a la protección de datos personales automatizados fue una buena ocasión para plantear esa posibilidad, sin embargo, la jurisprudencia constitucional (ya consolidada), no es más que a criterio de algunos juristas[62] una posición provisional, la cual se ha ido adaptando a la jurisprudencia de los Tribunales Europeos.

Por el Tribunal Constitucional se acabó reconociendo un derecho autónomo a lo que primero se denominó "libertad informática" y que pasó luego a ser un derecho a la protección de datos automatizados.[63]

Es prudente considerar que la CE considera como garantías constitucionales el "derecho al honor, a la intimidad personal y familiar y a la propia imagen" (Art. 18.1), tanto como el "derecho a la protección de datos de carácter personal" (Art. 18.4), donde "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" (Art. 18.4). Por tanto, como adelantábamos, será la ley la que limitará el uso de las nuevas tecnologías y protegerá los derechos fundamentales.

El Tribunal Constitucional en su sentencia 292/2000, de 30 de noviembre, entendió que las imágenes grabadas en un soporte físico constituyen, en sí mismas, un dato de carácter personal que queda integrado en la cobertura del art. 18.4 CE, ya que se trata de datos que permiten la identificación o individualización de la persona y puedan servir para la

[62] ROIG, A. (2010) "Derechos fundamentales y tecnologías de la información y de las comunicaciones (TICs)", Barcelona, España: BOSCH, Pág. 11.

[63] ROIG, A. (2010) "Derechos fundamentales y tecnologías de la información…" ob, cit Pág. 14.

confección de su perfil (ideológico, racial, sexual, económico o de cualquier otra índole) o para cualquier otra utilidad que podría constituir una amenaza para las personas (FJ 6).

A lo anterior se añaden, además, los soportes “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" (STC 29/2013).

Por tanto, nos encontraríamos en el punto neurálgico del derecho fundamental del artículo 18.4 CE, actualizado de forma más acentuada en el ámbito de la videovigilancia, la cual permite una multiplicidad de tratamientos de los datos, y que, por tanto, debe asegurarse que toda acción establecida por el empresario encaminada a la vigilancia o a la seguridad no contravenga el derecho a la protección de datos, el cual va a tener un especial protagonismo en cuanto a captar y grabar imágenes personales para identificar sujetos, siendo más importante y delicado dentro de la relación laboral y el contrato de trabajo.

En la doctrina constitucional se diferencia y coordina lo contemplado en el art. 18.1 y 18.4 de la Constitución evocando que "se vulnera el derecho a la intimidad personal cuando la actuación sobre su ámbito propio y reservado no sea acorde con la ley y no sea consentida, o cuando, aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida" (STC 196/2004, de 15 de noviembre) y, distinguiéndolo, porque "la función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (…)” (STC 292/2000, de 30 de noviembre).

En este sentido, la sentencia del Tribunal Constitucional 98/2000, establece que la libertad de empresa (art. 38 CE) o la celebración de un contrato de trabajo no puede implicar la limitación o perdida de derechos fundamentales y libertades públicas para los trabajadores.

En los sucesivos apartados de esta sección de la tesis se establecerá una evolución histórica y se plasmarán los regímenes jurídicos de cada derecho fundamental, que podrán verse comprometidos en la relación de trabajo por el control empresarial realizado con las TIC. En el siguiente punto se estudiará el compromiso que genera utilizar una tecnología en concreto en uno o varios derechos fundamentales, indicando la evolución jurídica tanto nacional como comunitaria.

5.2. Derecho a la intimidad.

5.2.1. Evolución histórica.

La idea de derecho a la intimidad o "privacy", como se le denomina en el sistema anglosajón, aparece por el siglo XIX. Será en 1890, cuando los juristas norteamericanos Warren y Brandeis elaboren las bases técnico-jurídicas de este derecho en su monografía «The Right to Privacy». En esta monografía, que tuvo la pretensión de poner de manifiesto la necesidad del reconocimiento del derecho a la intimidad fundamentándolo en el principio de la inviolabilidad de la persona, ambos juristas intentaron impedir las continuas intromisiones de la prensa en la vida privada de las personas estableciendo una serie de límites jurídicos. Así, concluyeron: “el principio que protege los escritos personales y cualquier otra producción del intelecto o las emociones es el derecho a la privacidad”.

A pesar de que esta fue la génesis jurídica a nivel conceptual, la noción de privacidad es anterior, empezándose a ver, posiblemente, desde que se disolviera la sociedad feudal, y llegándose a considerar en la sociedad liberal como un privilegio de minorías selectas que hacen valer ante el grupo su facultad de aislarse y de evitar toda interferencia en su vida privada y la posibilidad consecuente de disponer de ella.

Este concepto se transforma en la segunda mitad del siglo XIX, considerando al derecho a la intimidad como el derecho que todo individuo tiene a ser protegido y libre de intrusiones. En la sociedad moderna renacería la necesidad de protección al individuo, pero no de una forma aislada, sino como ser social.

5.2.2. Régimen jurídico.

El derecho a la intimidad viene regulado en el artículo 18.1 de nuestra Constitución, garantizando el mismo junto al derecho al honor y a la propia imagen.

Asimismo, eleva la intimidad al domicilio, el cual entiende inviolable, acuñando que no se podrá realizar ninguna entrada o registro en él sin consentimiento del titular, o resolución judicial, salvo caso delito flagrante (art. 18.2). Indicando, además, que "la Ley limitará el uso de la informática para garantizar la intimidad personal y familiar, así como el derecho al pleno ejercicio de sus derechos" (art. 18.2).

Por su parte, el Estatuto de los Trabajadores recoge en su artículo 4.2 que los trabajadores tendrán derecho a que se respete su intimidad en la relación de trabajo y a la consideración debida a su dignidad. Se concibe como "un derecho que acompaña a la persona en todo momento, y que no abandona al trabajador en las puertas del centro de trabajo"[64].

Algunos autores han definido la intimidad como el derecho a aislarse, a que los demás no sepan ni indaguen lo que somos, creemos, pensamos o hacemos, a ser desconocidos[65], concretando su contenido en "la facultad de excluir del conocimiento ajeno cualquier hecho comprendido dentro del propio ámbito que reserve el ciudadano para sí mismo, y para su familia"[66].

Por su parte, el Tribunal Constitucional definió la intimidad como "un ámbito reducto en el que se veda que otros penetren, de ahí la protección constitucional que se le otorga a fin de evitar las injerencias arbitrarias en las vidas privadas" (STC 73/1982 de 2 de diciembre). Asimismo, entendió que conforma un patrimonio personal que "hace necesario relacionar la cuestión con lo que constituye el espacio vital de cada uno, y que se proyecta sobre el concepto impreciso de lo que constituye el círculo reservado e íntimo, compuesto por datos y actividades que conforman la particular vida existencial de cada

[64] GOÑI SEIN, J.L. (1988). "El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder central empresarial". Madrid, España: Editorial Cívitas. Págs. 147-148.
[65] ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F. (2006). "El Derecho de los Trabajadores a la Intimidad". Navarra: Aranzadi, S.A., Págs. 45-46.
[66] ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F. (2006). "El Derecho…ob, cit, Págs. 45-46.

persona y autoriza a preservarla de las injerencias extrañas" (STC de 112/2004 de 12 de julio).

En la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, va a ser la primera vez donde se recojan de manera expresa (artículos 87 al 91) los derechos relacionados al uso de dispositivos en el entorno laboral como son, entre otros, el derecho a la intimidad, a la protección de datos de carácter personal y el derecho a la desconexión digital. Asimismo, esta ley también va a recoger la jurisprudencia nacional y comunitaria relacionada con los derechos digitales y el uso de dispositivos en el ámbito laboral.

El artículo 87 recoge lo relativo al Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, estableciéndose que los trabajadores tendrán derecho a proteger su intimidad en el uso de los dispositivos digitales de la empresa. Además, se recoge la posibilidad de que el empleador pueda acceder a los concretos contenidos que se generen por el uso de los medios digitales facilitados a los trabajadores, pero siempre con la única finalidad de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de los propios dispositivos. Por último, se va a recoger la obligación empresarial de establecer protocolos o criterios de utilización de los dispositivos digitales, los cuales, deberán respetar los estándares mínimos de protección de la intimidad de los trabajadores de acuerdo con los usos sociales y los derechos que la Constitución y las leyes les reconocen.

Si en un momento dado, el empleador admitiera un uso con fines privados de los dispositivos y, después pretendiera acceder al contenido de estos, deberá de modo preciso indicar los usos autorizados y establecer garantías para preservar la intimidad de los trabajadores, como, por ejemplo, indicando las prohibiciones expresas a determinados contenidos o estableciendo los periodos de tiempo en que los dispositivos podrán utilizarse para fines privados, resaltando la necesaria información a los trabajadores de los criterios de utilización.

En el artículo 89 se recoge el Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, permitiéndose el control empresarial *ex* artículo 20.3 ET a través de sistemas de cámaras o videocámaras,

imponiendo la obligación de información previa, expresa, clara y concisa a los trabajadores y, en su caso, a sus representantes, de la colocación de la medida de control. En relación con el requisito de información previa, se establece la salvedad para los casos de comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos, y se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica, es decir, el cartel genérico. Asimismo, se establece la salvedad de instalación de sistemas de grabación de sonidos o de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores, tales como vestuarios, aseos, comedores y análogos. Por último, en relación con los dispositivos para la grabación de sonidos en el lugar de trabajo se establece la limitación a su instalación, únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad y el de intervención mínima. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley[67].

En el artículo 90 es donde se va a recoger todo lo concerniente al Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Aquí, al igual que en lo relativo a los sistemas de videovigilancia, se establece la posibilidad de control empresarial ex artículo 20.3 ET a través de sistemas de geolocalización. Igualmente, se recoge la necesidad de información previa, expresa, clara e inequívoca a los trabajadores y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. De la misma forma se deberá informar a los trabajadores sobre el ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Por último, en el artículo 91 se va a recoger lo relativo a los Derechos digitales en la negociación colectiva, donde se va a indicar posibilidad de que los convenios colectivos establezcan mejoras o garantías adicionales de los derechos y libertades relacionados con

[67] Art. 22. Tratamientos con fines de videovigilancia, 3. *"Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación".*

el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

5.3. Derecho al secreto de las comunicaciones, 18.3 CE.

5.3.1. Evolución histórica.

El derecho al secreto de las comunicaciones se reconocerá por primera vez en la "Declaración Universal de Derechos Humanos" (1948), en su artículo 12. Más tarde también se recogería en otros tratados internacionales ratificados por España, como el "Convenio de Roma para la protección de los Derechos Humanos y de las Libertades Fundamentales" (1950), o el "Pacto Internacional de Derechos Civiles y Políticos" (1966). Lo cierto es que estas declaraciones hacían referencia a la correspondencia, comunicación principal efectuada en aquella época, término que evidentemente es equiparable a la comunicación (correspondencia=comunicación).

5.3.2. Régimen Jurídico.

En nuestra Constitución se va a garantizar "el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial" (art. 18.3).

Evidentemente, como comunicaciones se entienden los correos electrónicos, los cuales, en relación con el derecho al secreto de las comunicaciones, serán objeto de estudio más adelante.

Asimismo, el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea afirma, en términos similares, que "…toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones" (2000/C 364/01).

A fin de lograr un mayor entendimiento acerca de este derecho resulta interesante relacionarlo con los otros derechos recogidos en el artículo 18 de nuestra Constitución. Todos ellos están basados en la protección de la vida privada o privacidad de la persona en su ámbito estrictamente personal. En este sentido, resulta llamativa la vinculación entre

el secreto de las comunicaciones y la intimidad personal y familiar, que se reconoce en el artículo 18.1, y ello porque lo que va a proteger el secreto de las comunicaciones va a ser la comunicación entre personas en la distancia, garantizando que sea una comunicación privada.

De esta forma, se estableció la misma conclusión en la sentencia del Tribunal Constitucional 123/2002, de 20 de mayo, FJ 5, cuando se justificó la individualización de este derecho fundamental en la especial vulnerabilidad de la confidencialidad de estas comunicaciones en la medida en que son habilitadas por la intermediación técnica de un tercero ajeno a la comunicación.

Para diferentes autores, como Díaz Revorio[68], la relación entre el derecho a la intimidad y el secreto a las comunicaciones no impide una necesaria delimitación entre el contenido y sentido constitucional de los mismos, pues su constitucionalidad resulta de la configuración del derecho al secreto de las comunicaciones como garantía formal (independiente del contenido), y por la necesidad de limitar este derecho mediante una resolución judicial, que sin embargo no se dan en el derecho a la intimidad.

En cuanto a las comunicaciones, la Ley Orgánica de Protección de Datos (3/2018), exige que el deber de información previa conforme al artículo 12 del Reglamento (UE) 2016/679 se realice mediante la colocación de un dispositivo informativo en lugar suficientemente visible donde figure, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del mencionado Reglamento (art. 22.4 LOPD).

Por tanto, en materia de protección de datos de carácter personal será suficiente realizar una información genérica y no específica para realizar un control empresarial de la actividad laboral.

5.4. Protección de datos de carácter personal, 18.4 CE.

[68] DIAZ REVORIO, F. J. (2006). "El derecho fundamental al secreto de las comunicaciones". Revista de la Facultad de Derecho, ISSN 0251-3420, ISSN-e 2305-2546, Nº 59, págs. 159-175

5.4.1. Evolución histórica.

Al igual que el derecho a la intimidad, el origen más evidente en la dimensión de la protección de datos lo encontramos en Estados Unidos, en "The Right to Privacy" ensayo escrito por los autores Samuel Warren y Louis Brandeis en 1890, considerado como la primera publicación en defender el derecho a la privacidad. En él la privacidad se entiende como el derecho a la soledad, en inglés, "the right to be let alone". Por ello, se puede observar que la privacidad se fundamenta en el anonimato, el secreto, teniendo como pilares la autonomía, individualidad el desarrollo de la personalidad, y la inviolabilidad de la dignidad personal[69].

Sin embargo, tiempo atrás, en 1763, nos encontrábamos con la cita del clásico aforismo inglés "a man's house as his castle"[70] de William Pitten. Se trata de uno de los principios básicos del Derecho inglés, por medio del cual se entiende al hogar de los ciudadanos como el lugar de mayor protección a nivel personal. La reivindicación de William Pitten fue la de la "protección personal del individuo frente al poder del Monarca en cualquier lugar, incluso en la más humilde morada".

Como se ha indicado con anterioridad, el Tratado de Derecho Constitucional, "A Treatise on the Constitutional Limitations which Rest upon the Legislative Power of the States of the American Union" (1868), dictado por el juez Thomas M. Cooley, sentaría las primeras referencias legales de la protección de la privacidad, puesto que indicaba que las garantías de la 3ª, 4ª y 5ª Enmienda de la Constitución de los Estados Unidos constituían un vehículo de protección de la privacidad de los individuos. Este jurista entendió que la expresión de Willian Pitten "a man's house as his castle" es la expresión jurídica garantista de que, encontrándose en su domicilio, la ciudadanía es inmune a las acciones gubernamentales y, por extensión de la protección en "su persona, propiedad y documentación personal"[71], incluso frente a un procedimiento judicial.

---

[69] GONZÁLEZ PORRAS, A. (2015). "Privacidad en Internet: Los derechos fundamentales de privacidad e intimidad en internet y su regulación jurídica. La vigilancia masiva". Universidad de Castilla-La Mancha.

[70] La casa de cada uno es su castillo.

[71] NISA ÁVILA, J.A. "Origen jurídico histórico de la protección de datos: evolución de las diferentes teorías jurídicas que la han protegido", Artículo publicado el 8/10/2020 en la web www.elderecho.com.

Por todo ello, el Tribunal Supremo de los Estados Unidos, a lo largo de su jurisprudencia, ha considerado la existencia del derecho a la privacidad implícito en la libertad de asociación que ampara la Primera Enmienda. Esta Enmienda preserva a los ciudadanos ante cualquier intromisión de los poderes públicos a tener que revelar la pertenencia a una organización. Asimismo, también en la Cuarta Enmienda se preserva el derecho a la privacidad, al impedir intromisiones ilegitimas de los poderes públicos a través de registros y requisas en las personas, domicilios, documentos y efectos personales. También en la Quinta Enmienda en lo que se refiere al derecho a no declarar contra sí mismo ni a revelar datos personales.

Sin embargo, iba a ser en 1905 cuando se aplicaría el concepto de protección de datos y privacidad desde un punto de vista jurídico, y lo haría la Corte Suprema de Georgia en el caso Pavesich contra New England Life Insurance Company (Sentencia de 3 de marzo de 1905). El dictado de esta sentencia supuso un reconocimiento definitivo para la tesis de Warren y Brandéis, al reconocer en dicho supuesto, tanto el derecho a la propia imagen como el derecho a la intimidad, en los siguientes términos "...hasta ahora no se ha recogido en ninguna sentencia la apelación a un derecho a la intimidad, independiente del derecho a la propiedad (...) El derecho a la intimidad tiene sus raíces en los instintos de la naturaleza (...) La libertad personal abarca el derecho a la vida pública tanto como el derecho correlativo a la intimidad"[72]. En este caso la compañía aseguradora utilizó la imagen de Paolo Pavesich en un anuncio el cual considero que violaba su privacidad y era difamatoria.

No sería hasta casi un siglo después, cuando se empezaría a legislar en Europa en esta materia. Primero, con referencias de carácter filosófico, como John Locke[73] y Benjamín Constant De Rebecque[74], y después, con la "Declaración Universal de Derechos

---

72 HERRERO-TEJEDOR, F. (1990) "Honor, Intimidad y Propia Imagen", Colex, Madrid. Pág. 34

73 *"La libertad del hombre dada por la Ley de la Naturaleza era restringida por las leyes de la sociedad para que esta última exista y subsista"*, vid. LOCKE, J., (1969) "Ensayo sobre el gobierno civil", Madrid, España: Aguilar, págs... 63-65, trad. LÁZARO ROS, A.

74 *"La libertad es el derecho de no estar sometido sino a las leyes, no poder ser detenido, ni preso, ni muerto, ni maltratado de manera alguna por el efecto de la voluntad arbitraria de uno o de muchos individuos: es el derecho de decir su opinión, de escoger su industria, de ejercerla, y de disponer de su propiedad, y aún de abusar si se quiere, de ir y venir a cualquier parte sin necesidad de obtener permiso, ni de dar cuenta a nadie de sus motivos o sus pasos: es el derecho de reunirse con otros individuos, sea para deliberar sobre sus intereses, sea para llenar los días o las horas de la manera más conforme a sus inclinaciones y caprichos: es, en fin, para todos el derecho de influir o en la administración del gobierno, o en el nombramiento de algunos o de todos los funcionarios, sea por representaciones, por peticiones o por consultas, que la autoridad está más o menos obligada a tomar en consideración"*, vid. DE REBECQUE, B. C. (1819) "La libertad de los modernos" Madrid, España: Alianza Editorial. Trad. RIVERO RODRIGUEZ, A.

Humanos" (1948), que señalaba en su artículo 12 que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Resolución 217 A III, art. 12)[75].

Dos años después, el "Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales del Consejo de Europa" (Roma, 1950) establecía que toda persona tenía derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia[76].

En 1961 Lord Mancroft presentaría en Reino Unido un proyecto de ley cuyo objetivo era la regulación y protección de la privacidad. El proyecto Lord Mancroft[77] entendía que se debía de proteger el derecho a la no invasión de la privacidad y el mantenimiento de la dignidad humana. Más adelante surgirían otros proyectos fracasados pero destacados como el de Alexander Lyon (1967), de Brian Walden (1969), de Kenneth Baker (1969), de Leslie Huckfield, "Control of personal information" (1971).

Un año más tarde se elaboraría en Inglaterra el informe de Kenneth Younger, conocido "Younger Report" (1972); donde un Comité, "Younger Committee", constataba que "la opinión pública de los países desarrollados sitúa el respeto de la vida privada en el lugar prioritario de sus aspiraciones de protección de los derechos humanos"78 disintiendo de la definición dada hasta ahora de la privacidad como el derecho a ser dejado solo, "right to be let alone".

En 1979 el "White Paper"[79] de Roy Jenkins sobre las relaciones entre la privacy y la informática estudió la privacidad no desde un punto de vista genérico sino especifico en

---

75 La Declaración fue proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su (Resolución 217 A (III)

76 Art. 8 Convenio Roma: 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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

77 https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido.

78 REBOLLO DELGADO, L. (2005), "El Derecho Fundamental a la intimidad", Madrid, España: Editorial Dykinson, 2ª edición, Pág. 128.

79 Informe titulado "Computers and Privacy".

relación con la informática y las bases de datos. Se trataba de una serie de propuestas planteadas al gobierno a fin de elaborar una ley sobre datos personales.

En 1975, Norman Lindop publicó un informe complementario al "White Paper", el Reporte Lindop, que culminaría con la promulgación de la ley sobre protección de datos de carácter personal "Data Protection Act" (1984)[80].

Con posterioridad, la Comunidad Europea aprobaría en 1981 el "Convenio 108 del Consejo de Europa para la Protección de las Personas al Tratamiento Automatizado de Datos de Carácter Personal", donde se garantizaba "… a cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona" (art. 1).

En España, la "Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal" (5/1992) o LORTAD, desarrollaba lo recogido en la CE (1978) y establecía, por primera vez, "la limitación del uso de la informática para garantizar la intimidad personal" (art. 18).

Posteriormente, la "Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos" (CE, 1995), determina el marco jurídico en el que se desarrolla la actual legislación española en Protección de Datos de Carácter Personal.

La LORTAD tardó siete años en disponer de su desarrollo reglamentario, que llegó con el denominado "Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal" (Real Decreto 994/1999).

A los pocos meses de su aprobación, se publicó la "Ley Orgánica de Protección de Datos de Carácter Personal" (LOPD, 15/1999), donde se adecua la legislación española a la

[80] "Data Protection Act" vigente y aprobada por el Parlamento en el año de 1998. El texto completo en inglés puede consultarse íntegramente en la web http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1›

Directiva europea, desarrollando la protección de datos más allá de los datos informatizados, incluyendo dentro de su ámbito de aplicación los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento automatizado o no, y toda modalidad de uso de los mismos.

A la postre, la LOPD, habiendo convivido durante ocho años con el "Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal" (1999), vio plasmarse su evolución reglamentaria en el "Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal" (Real Decreto 1720/2007).

El pasado 6 de diciembre de 2018 entró en vigor la nueva "Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales" (LOPDGDD, 3/2018), que sustituye y deroga en su totalidad a la anterior LOPD 15/1999.

La LOPDGDD de 2018 recoge diez títulos en los que se establecen noventa y siete artículos, veintidós disposiciones adicionales, seis disposiciones transitorias, dieciséis disposiciones finales, y una disposición derogatoria.

El antes mencionado Real Decreto, por el que se aprueba el Reglamento de desarrollo de la anterior Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RD 1720/2007), se mantiene en tanto no se oponga o resulte incompatible con el Reglamento 679/2016 de la UE o con la actual LOPDGDD.

5.4.2. Régimen Jurídico.

La CE establece 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" (art. 18.4).

La imagen personal se va a considerar como un dato de índole privada a partir de la antigua Ley Orgánica, 15/1999, de protección de datos de carácter personal, que define como dato de carácter personal "cualquier información concerniente a personas físicas

identificadas o identificables" (art. 3). Asimismo, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, considera como dato de carácter personal la información gráfica o fotográfica (art. 5.1 f).

Por obra del Tribunal Constitucional se reconoció un derecho autónomo denominado primeramente como "libertad informática", siendo luego considerado un "derecho a la protección de datos automatizados"[81].

En la STC 254/1993, de 20 de julio, se describe el derecho a la libertad informática, vinculándose al derecho a la intimidad, toda vez que "en la sociedad moderna, gran parte de las decisiones que afectan a los individuos descansan en datos registrados en ficheros informatizados". Se define la "libertad informática", reconocida por el art. 18.4 CE[82], como "la libertad de controlar el uso de los datos privados insertos en un programa informático: lo que se conoce con el nombre de habeas data". Conforme con la CE, el respeto al honor y a la intimidad conforman los límites del uso de la informática, sin embargo, "la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España" (STC 1993). De esta forma, la protección de la intimidad que recoge nuestra Constitución lo hace en forma de derecho de control sobre los datos relativos a la propia persona.

Desde la STC 292/2000, el artículo 18.4 CE se interpreta como un derecho a la protección de datos personales y no como un aspecto especial o vertiente positiva del derecho a la intimidad[83]. Considerando su función, su objeto y su contenido, el Tribunal Constitucional diferencia estos derechos. De un lado, entiende al derecho a la intimidad como el derecho que protege frente a invasiones en la esfera personal y familiar, y de otro lado, el derecho a la protección de datos personales garantiza al ciudadano un poder de control o de disposición sobre el uso y el destino de sus datos personales (STC 2000). En cuanto al objeto, como se adelantaba, también difieren, pues "los datos personales no son

[81] ROIG, A. (2010) "Derechos fundamentales y tecnologías de la información…" ob, cit Pág 14.

[82] Art. 18. 4. CE, "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".

[83] ROIG, A. (2010) "Derechos fundamentales y tecnologías de la información…" ob, cit Pág 14.

únicamente los datos íntimos de la persona sino también todos aquellos que la identifiquen, como la dirección IP[84] de nuestro ordenador"[85].

Según el RGPD[86] dato personal es toda información relativa a una persona física identificada o identificable. Por su parte, una persona identificable es aquella a la que es posible identificar, directa o indirectamente, a través de datos como nombre, DNI, ubicación, identificador "on line" u otros aspectos como rasgos físicos, fisiológicos, genéticos, culturales, económicos o sociales (RGPD, art. 4). Por lo tanto, la dirección IP será considerada como dato personal, pues indirectamente, a través del proveedor de internet que posee los datos necesarios para asociar esa IP a una persona concreta, se puede identificar a la persona.

En cuanto al contenido, el derecho a la protección de datos exige el consentimiento[87] previo para la recogida de datos de carácter personal, el derecho a ser informado sobre el destino y uso de los datos, y el derecho de acceder, rectificar y cancelar dichos datos. Sin embargo, el derecho a la intimidad para poder ser limitado, solo podrá hacerse en materia de control laboral y va a imponer la obligación de información previa, expresa, clara y concisa a los trabajadores y, en su caso, a sus representantes, de la colocación de la medida de control, con la excepción para los casos de comisión flagrante de un delito por los trabajadores.

En relación con el consentimiento y la protección de datos de carácter personal, el Reglamento europeo reivindica fervientemente el derecho a la privacidad y a que cada persona decida libremente los datos de su vida que permite que puedan ser conocidos por terceros, incluido el propio empresario dentro del ámbito laboral[88]. Con esta finalidad convierte el "consentimiento" de la persona afectada en un valor fundamental para el tratamiento legal

---

84 Internet Protocol (Protocolo de Internet) es una marca numérica atribuida a cada uno de los dispositivos conectados a una red informática que usa el Protocolo de Internet. https://dpej.rae.es/lema/direccion-ip

85 ROIG, A. (2010) "Derechos fundamentales y tecnologías de la información…" ob, cit Pág 14.

86 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

87 RGPD, art. 4.11. *"Consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen".*

88 SERRANO GARCIA, J. Mª (2021) *"La Protección de datos y la regulación de los derechos digitales en la negociación colectiva y en la jurisprudencia*". Publicada en la Revista de derecho social nº 94, págs. 6-7

de datos, estableciéndose en su art. 6.1.a) como debe realizarse, es decir, a través de una manifestación de la voluntad libre, específica, informada e inequívoca por la que este acepta el tratamiento de sus datos personales[89]. Sin embargo, en materia laboral se admite el tratamiento de datos sin consentimiento cuando sea necesario para la ejecución del contrato de trabajo, aunque no se exime de la obligación de información por parte del empresario, que debe ser expreso y claro en relación con el tratamiento de datos, su finalidad, los destinatarios y la identidad del responsable del tratamiento. (art. 11 LOPD)

Si bien este planteamiento se presenta con una identidad legítima, la realidad es que la posterior Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, si establece una regulación y un régimen jurídico tanto para los derechos digitales como para la captación de imágenes con cámaras de videovigilancia.

La finalidad que tiene esta ley, siempre según su preámbulo, es adecuar el ordenamiento jurídico español al Reglamento del Parlamento Europeo y el Consejo, de 27 de abril de 2016, sobre la protección de las personas físicas (UE, 2016/679), prestando especial atención al tratamiento de sus datos personales y a su libre circulación, garantizando los derechos de los ciudadanos conforme a lo establecido en el artículo 18.4 de la Constitución.

Por tanto, "el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el mencionado Reglamento (UE) 2016/679 y en esta ley orgánica" (LO 3/2018).

La Ley Orgánica de Protección de Datos, 3/2018, recoge en su artículo 22 los tratamientos de datos con fines de videovigilancia, y permite la videovigilancia de las empresas con fines de seguridad en las personas y en los bienes, incluyendo las propias instalaciones. En relación con las imágenes captadas en la vía pública se permite para la misma finalidad y en la medida imprescindible.

[89] SERRANO GARCIA, J. Mª (2021) *"La Protección de datos y la regulación de los derechos digitales en la negociación colectiva y en la jurisprudencia*". Publicada en la Revista de derecho social nº 94, pág. 7

En relación con la información y comunicación, se entenderá cumplido el requisito de información previa establecido en el artículo 12[90] del Reglamento General de Protección de Datos (UE 2016/679) mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD[91].

El título "Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo" (art. 89), recoge lo relativo al poder de dirección del empresario y los sistemas de cámaras o videocámaras para el control laboral. En dicho artículo se concluye la posibilidad de que los empresarios puedan tratar las imágenes obtenidas a través de las cámaras de videovigilancia con el fin de control laboral que le legitima el artículo 20.3 ET, sin embargo, deberán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida controladora" (art. 89). No obstante lo anterior, en el caso de haber captado la comisión flagrante de un acto ilícito por los trabajadores se entenderá cumplido el deber de informar cuando existiese al menos el cartel al que se refiere el artículo 22.492 de esta ley orgánica" (art. 89).

---

[90] RGPD, art. 12, *"Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado 1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios. 4.5.2016 ES Diario Oficial de la Unión Europea L 119/39 2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado. 3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo(…)".*

[91] LOPD 13/2018, art. 22.4 *"4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento."*

[92] Art. 22.4 LOPD *"(…) el deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679".*

El límite se encuentra en la grabación de sonidos o imágenes en lugares destinados al descanso o entretenimiento de los trabajadores, tales como vestuarios, comedores o similares (art. 89). Ello se debe principalmente a la expectativa de privacidad que un empleado puede esperar en un lugar de trabajo, el cual se graduará por la jurisprudencia, estableciendo un grado elevado en baños y vestuarios, donde no es posible realizar una vigilancia, un grado importante en los despachos y un grado mínimo en lugares visibles o accesibles a los compañeros de trabajo o al público en general.

En esta ley se dará más importancia a las escuchas que a lo visionado y, por tanto, a la imagen propiamente dicha. La voz, al igual que la imagen, se considera un dato de carácter personal, toda vez que permite identificar o singularizar a una persona. Como decíamos, se le da más importancia a la voz que a la imagen, pues la utilización de dispositivos para la grabación de sonidos en el lugar de trabajo solo será posible cuando la seguridad de las instalaciones, bienes y personas este en entredicho, y siempre respetando el principio de proporcionalidad y de intervención mínima (art. 89).

6. Control del empresario vs derechos fundamentales del trabajador.

Como se ha adelantado, el creciente uso de las nuevas tecnologías en la relación laboral y el nacimiento de otras, hacen indispensable la adecuación del ordenamiento jurídico, pues es evidente que el control del empresario sobre sus trabajadores puede limitar diferentes derechos fundamentales de los trabajadores.

En este apartado se va a realizar un análisis de la afectación de las nuevas tecnologías a las relaciones laborales en el contexto del control que ejerce el empleador sobre la actividad laboral, así como las situaciones conflictivas que surgen entre empresario y trabajadores. De la misma manera, se realizará un análisis jurisprudencial de estas nuevas tecnologías o herramientas de control empresarial valorando a su vez, el método que utilizan los tribunales con el cometido de resolver si los medios de control son lícitos o no, aplicando el juicio de proporcionalidad.

6.1. Sistemas de control de la actividad laboral.

La implantación generalizada de las TIC en el ámbito de las relaciones laborales viene generando diferentes conflictos, tanto jurídicos como sociales. De un lado, los límites del uso privativo de los dispositivos informáticos por las personas trabajadoras y, por otro lado, el poder de control y vigilancia del empresario sobre dicho uso y la confrontación entre los derechos fundamentales del trabajador y los poderes empresariales en esa labor de control.

A esto, se debe añadir que hay una ausencia de regulación específica en España que ayude a solventar los conflictos laborales derivados del uso de los dispositivos informáticos. Tampoco las normas generales de derecho existentes ayudan a resolver estos conflictos, como si existe en otros ordenamientos e incluso, en la propia legislación comunitaria[93]. Se contaba con la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos

[93] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección a la intimidad en el sector de las telecomunicaciones; Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (Directiva sobre la privacidad y las comunicaciones electrónicas).

de Carácter Personal (LORTAD, 5/1992), que nació con el fin de proteger "el honor y la intimidad de los ciudadanos" (1992) del uso de la informática, en cumplimiento del mandato constitucional establecido en el artículo 18.4 CE. Con posterioridad, se dictaría la Ley Orgánica de Protección de Datos de Carácter Personal (15/1999), que adaptaba la norma a la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. La Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (3/2018), que nace con motivo de la aplicación del Reglamento sobre Protección de Datos 2016/679 del Parlamento Europeo y del Consejo (UE, 2016).

Es importante mencionar, aunque lo haremos en todo el recorrido de la tesis, la inclusión de un nuevo artículo 20 bis en el ET[94], introducido por la disposición final decimotercera de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (3/2018), que dispone para quienes trabajan el derecho a la intimidad en el uso de los dispositivos digitales facilitados por la empresa, el derecho a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

Sin embargo, son normas demasiado generales, por lo que su aplicación no ha sido fácil ni clara, generando diferentes conflictos en el ámbito laboral resueltos por los tribunales. Asimismo, en materias diferentes a la Protección de Datos, pero relacionada con el uso de nuevas tecnologías se encuentra la Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la Información y del Comercio Electrónico.

En relación con la utilización extralaboral de las tecnologías puestas a disposición por el empresario, el artículo 20.2 ET exige al trabajador que cumpla con sus obligaciones laborales de conformidad con las reglas de la buena fe; Sin embargo, ante un posible incumplimiento y sanción, se debe estar a la "Teoría Gradualista". En este sentido, entendemos que el uso de la tecnología puesta a disposición del empresario, si se realiza

[94] Artículo 20 bis ET. *"Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión". Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.*

de forma prudencial, en momentos de descanso y con buena fe, no debería de generar ningún problema al trabajador, pues no realizaría ningún incumplimiento contractual.

Por otra parte, el artículo 20.3 ET establece el derecho del empresario a la adopción de medidas que considere oportunas para vigilar y controlar el trabajo. Eso sí, debe adoptarlas y aplicarlas considerando debidamente su dignidad. Y es aquí donde encontramos una laguna a nivel normativo, sin que la legislación actual avance al mismo ritmo en que avanza la sociedad de la información. Por ello, deben ser los tribunales quienes den una solución individualizada a cada conflicto planteado, pues como se analizará más adelante, los convenios colectivos o no regulan esta materia o lo hacen de tal forma que rápidamente quedan obsoletos[95].

Debe entenderse que las nuevas tecnologías son también la expresión del poder de vigilancia y control del empresario sobre la prestación del trabajo establecido en el art.20.3 ET y no solo unas formas novedosas de organización en el trabajo y de su actividad productiva. La normativa mencionada no manifiesta específicamente los límites para que su adopción por parte del empresario respete la consideración debida de la dignidad del trabajador, límites que encontraremos en los derechos fundamentales que asisten al trabajador y en la jurisprudencia que los desarrolla.

Desde luego, y en relación con lo manifestado en el párrafo anterior, las medidas de vigilancia y control tienen la finalidad de salvaguardar los intereses mercantiles y empresariales del empresario y el derecho de la propiedad establecido en el artículo 33 de la Constitución Española, ahora bien, debemos recalcar una vez más, que ese derecho, como casi todos los que asisten al empresario, tienen unos límites. Esos límites no son otros que los derechos fundamentales propios de los trabajadores, como son, principalmente, el derecho a la intimidad del art.18.1 CE y el secreto de las comunicaciones, establecido en el art.18.3 CE.

[95] SAN MARTÍN MAZZUCCONI, C. (2007) "El uso y el control empresarial de las nuevas tecnologías en el ámbito laboral". Revista Doctrinal Aranzadi. Nº 7/2007 - 8/2007.

El articulado anteriormente mencionado viene a proteger la privacidad del trabajador de aquellos ataques intrusivos y desproporcionados en su esfera privada, pero sin vaciar de contenido el control empresarial establecido en el artículo 20.3 ET. En concreto, el artículo 20.3 ET establece las facultades del empresario, pero a su vez, establece los límites, condicionados por los propios límites del contrato de trabajo. El primero de los límites estaría en la finalidad de control propiamente dicha, ciñéndose ese control a la verificación del cumplimiento por el trabajador de sus obligaciones y deberes laborales. El segundo de los límites no es otro que la dignidad de las personas trabajadoras, puesto que como se ha avanzado al principio de esta tesis, la dignidad[96] se halla presente en todos los derechos fundamentales y, por supuesto, en el derecho a la intimidad recogido en los arts. 18 de la Constitución Española y 4.2 ET.

Ahora bien, tampoco podrá el trabajador en su relación laboral mantener el derecho a la intimidad de una forma incondicional. La formalización de un contrato de trabajo y el ingreso en la unidad productiva de la empresa comporta una pequeña pérdida o al menos una reducción de la intimidad de las personas trabajadoras, "comportando cierta compresión de los derechos de los que el individuo es titular"[97], sin que con ello se permita justificar medidas incompatibles con la dignidad de los trabajadores. La normativa establecida interviene para evitar todo control que se ejerza o efectúe sobre la esfera de la vida privada del trabajador y que no tenga relación con la organización de la empresa, además de evitar toda vigilancia que elimine el espacio de libertad de la persona que está en la propia esencia del derecho a la intimidad[98].

De esta forma se pronunció el Tribunal Constitucional en la sentencia 88/1985, de 19 de julio, FJ 2, la cual entendió que la celebración de un contrato de trabajo no iba a conllevar la pérdida para los trabajadores de los derechos fundamentales reconocidos en la Constitución como ciudadano, pues las empresas no forman un mundo separado y estanco del resto de la sociedad, ni la libertad de empresa va a permitir que los trabajadores soporten limitaciones injustificadas de sus derechos fundamentales y libertades públicas, los cuales, tienen un valor central y nuclear en el sistema jurídico constitucional.

---

[96] Art. 10.1 CE.

[97] FERNÁNDEZ LÓPEZ, M.F. (1985) "Libertad ideológica y prestación de servicios", en Relaciones Laborales, nº 7, pág. 189.

[98] GOÑI SEIN, J.L. (1988). "El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder central empresarial". Madrid: Editorial Civitas, Madrid, págs. 116 y 117

6.2. Las nuevas tecnologías ante la relación laboral

El uso de las nuevas tecnologías de la información y la comunicación en el entorno laboral va a multiplicar las facultades de control del empresario y, por tanto, mejorar la fiscalización de la prestación del servicio. Sin embargo, va a generar conflictos diferentes a los existentes en relación con el uso de herramientas de trabajo para fines privados y el derecho del empresario de controlarlo.

Con la incursión de las nuevas tecnologías en el ámbito laboral resulta más sencillo y con mayor precisión realizar el control empresarial, por ejemplo, sobre la navegación por Internet o sobre el correo electrónico corporativo. Sin embargo, esta nueva forma de control empresarial puede conllevar la intromisión en el secreto a las comunicaciones y el derecho a la intimidad de los trabajadores, incluso, aunque se realice con respecto a la normativa establecida.

Algunos autores, como Alejandra Selma en su estudio "Las peculiaridades prácticas del control en la empresa" (2009), han entendido que la dependencia laboral se mantendrá, no experimentará cambios en relación con el grado de intensidad, pero si lo hará en su forma de manifestarse[99]. Esto va a ocurrir en el momento en el que las nuevas tecnologías se utilicen como herramientas de trabajo, pasando esos instrumentos a nueva forma control empresarial.

Según la autora, el control pasará a ser informático, dejando de ser personal, directa e inmediata como venía siendo, no siendo necesaria la presencia física del empresario en el lugar de trabajo para realizar la supervisión. Estos modelos servían principalmente en relación con mano de obra poco cualificada, la cual se podía controlar con una simple comprobación o "vistazo".

Asimismo, Alejandra Selma, entiende que el control empresarial que se realizaba hasta la irrupción de las nuevas tecnologías en el entorno laboral era una control directo e

[99] SELMA PENALVA, A. (2009). "Las peculiaridades prácticas del control en la empresa. Actualidad Laboral". Nº 14. Pág. 93.

inmediato, que se realizaba de forma constante durante la prestación del servicio, toda vez que tanto el trabajador y como empresario se encontraban simultáneamente en el mismo lugar y tiempo de trabajo, lo que permitía realizar un control inmediato y constante de la prestación de servicios. En esta tipología de control clásico y directo no van a existir elementos materiales, soportes o herramientas de control entre empleador y empleado.

Sin embargo, la forma de control productivo actual se va a caracterizar por la introducción constante de nuevas tecnologías y herramientas en el trabajo produciéndose una transformación en las formas clásicas e inmediatas de ejercer control en las empresas. Seguirá cabiendo, no hay duda alguna, la característica subordinación del trabajador, mientras que las facultades para organizar, dirigir, controlar y sancionar el trabajo no se van a manifestar siguiendo las líneas del control empresarial que se consideraban típicos, como ya se ha indicado anteriormente, pasando del control presencial al control que podemos denominar, tecnológico. Ese control tecnológico no necesariamente implica la flexibilidad para la subordinación. Inversamente, se da en la actualidad que se han intensificado los controles en la prestación de puntuales servicios, rigor que aflora del constante avance de la tecnología y que abre puertas a mayor intensidad de control, que ya se comenzó a nombrar "control informático".

Desde luego que, con el mencionado control informático o tecnológico, cambian radicalmente las peculiaridades de las prestaciones laborales. Esto puede notarse en la flexibilización de la relación laboral de dependencia que ostentaba la clásica empresa, donde las nuevas tecnologías se emplean en el trabajo en busca de incrementar las libertades, aunque también se desvela en la intensificación del control que las mismas tecnologías ponen a disposición del empresario, en el camino hacia la mejora en la eficiencia de los procesos productivos.

Como hemos avanzado en apartados anteriores, este cambio tecnológico de los procesos productivos tiene proyección en las herramientas de trabajo, mejorando el rendimiento de los trabajadores, facilitando su labor, reduciendo los tiempos de presencialidad en la compañía, etc. Aun así, el mismo cambio que conlleva beneficios con un potencial jamás imaginado en el ámbito de trabajo, repercutirá no solo en la forma de desarrollar la prestación laboral, en la flexibilidad horaria, en el lugar de trabajo (teletrabajo), sino

también en modos tan precisos de supervisar el trabajo que podrían atentar contra la intimidad del trabajador u otros de sus derechos fundamentales, como veremos a continuación.

Por lo tanto, al evolucionar el contenido de la prestación laboral clásica y de las propias herramientas que van modernizándose, también evolucionará y se cambiará la forma de ejercer el control empresarial.

Alejandra Selma destaca, en este contexto, dos grandes funcionalidades de tales nuevas herramientas, pues por un lado son novedosas y facilitan el desarrollo de la actividad laboral, y por otro, permiten la deslocalización del trabajo[100].

Sin embargo, estas nuevas herramientas también actúan como novedosos e intensos instrumentos de control de la prestación laboral, facilitando al empresario el ejercicio de las facultades de organización, dirección y control de trabajo que le confiere el ordenamiento laboral[101].

En relación con las nuevas herramientas o aparatos técnicos, López Ahumada en su estudio "La tutela del derecho a la intimidad del trabajador y el control audiovisual de su actividad laboral" (2006) indica que, a diferencia de otros países, en nuestra legislación laboral no figuran normas que restrinjan la facultad de control del empresario en relación con la instalación y utilización de nuevas tecnologías, únicamente se contempla un límite general relativo a su utilización. Por tanto, se permite el control empresarial a distancia a través de nuevas tecnologías, pero solo podrá realizarse para la supervisión del trabajo y respectando la dignidad de los trabajadores[102].

6.3. Correo electrónico vs Derecho a la intimidad y Secreto de las comunicaciones.

[100] SELMA PENALVA, A. (2009). "Las peculiaridades prácticas del control en la empresa. Actualidad Laboral". Nº 14. Pág. 37.
[101] SELMA PENALVA, A. (2009) "Las peculiaridades prácticas…" ob. cit Págs. 2-37.
[102] LÓPEZ AHUMADA, J. E.: "La tutela del derecho a la intimidad del trabajador y el control audiovisual de su actividad laboral", Cuadernos electrónicos de Derechos Humanos y Democracia, núm. 3, enero-julio, 2006, pág. 213

Actualmente, el correo electrónico es un medio de comunicación habitual e incluso esencial para la mayoría de las empresas y trabajadores. La consolidación del correo electrónico como una de las herramientas más utilizadas en las empresas ha generado múltiples ventajas, como la eficiencia de las comunicaciones, aunque también ha creado nuevos conflictos derivados del uso por parte de los trabajadores y su fiscalización por parte de las empresas, por lo que resultará de interés conocer los derechos y los límites, tanto desde la perspectiva del empleador como desde la del empleado.

La forma de trabajar en las empresas ha cambiado con la utilización del correo electrónico. Gracias a él todas las comunicaciones que se realicen por este medio van a quedar registradas en los servidores, por lo que, dichas comunicaciones podrán ser fácilmente controladas y supervisadas por los empresarios. Sin embargo, este control y supervisión del empresario puede acarrear una intromisión ilegítima en los derechos fundamentales de los trabajadores.

En concreto, el uso del correo electrónico en la empresa genera una tensión entre el derecho a la intimidad personal (CE, art. 18.1), la inviolabilidad de las comunicaciones (CE, art. 18.3) y la facultad del empresario de cuidar de su medio organizativo, y de administrar, controlar y supervisar las actividades laborales que se desarrollen en su empresa.

6.3.1. Jurisprudencia Española.

La utilización abusiva realizada por un trabajador de un instrumento de trabajo con fines personales plantea, desde el punto de vista del empresario, diferentes perjuicios. En primer lugar, aunque pueda ser difícil calcular o no ser muy notable, hay un perjuicio económico, en una doble vertiente, el gasto propio de la herramienta, el servicio de Internet, coste de la llamada, deterioro del ordenador y sus componentes, y el lucro cesante, es decir, el tiempo que el trabajador no dedica a la prestación efectiva del trabajo sino a tareas personales que no solo repercuten en la disminución de su rendimiento, sino también en el de los otros compañeros a los que pudiera enviar mensajes o correos electrónicos.

Asimismo, ese uso irregular del correo electrónico y de otras herramientas puede comprometer la seguridad de la empresa, su imagen o la capacidad o funcionamiento del sistema informático para transmitir información. Además, puede ser un medio para realizar prácticas de acoso laboral o sexual a otros compañeros de trabajo.

Por lo tanto, resulta patente que "el interés del empresario puede verse comprometido por el uso irregular y abusivo del correo electrónico, conllevando una transgresión de la buena fe contractual y un abuso de la confianza depositada en el trabajador, frente al cual se le reconoce al empresario capacidad de reacción, con medidas disciplinarias al uso (art. 54 ET) pero también, la facultad de prevenir dichas conductas, mediante el ejercicio del poder de control de la actividad productiva (art. 21 ET)"[103].

Los conflictos vienen cuando el control sobre la prestación del trabajo y el uso de las herramientas por parte del empleador no es proporcional, no está justificado o es abusivo, pudiendo lesionar los derechos fundamentales a la intimidad o al secreto en las comunicaciones de los empleados, recogidos en los artículos 18 CE. Por su parte, el artículo 4.2.e) ET, relevante en materia laboral, recoge el derecho a la intimidad y a la consideración debida a su dignidad, incluida la protección frente a ofensas verbales o físicas de naturaleza sexual.

Además, el Estatuto de los Trabajadores recoge en su artículo 20.3 el poder de dirección del empleador, reconociéndole y delimitando una serie de facultades de control y vigilancia en la ejecución de los trabajos, al indicar 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" (ET, art. 20.3).

Asimismo, los artículos 18 y 20.4 ET recogen otras facultades más concretas del empleador para ejercitar el control laboral en cuanto al registro sobre la persona y bienes

[103] Sobre los criterios de la doctrina judicial para la apreciación de estas conductas como transgresoras de la buena fe contractual, vid. la clasificación realizada por SEMPERE NAVARRO, A.V., SAN MARTIN MAZZUCCONI, C., Nuevas Tecnologías y Relaciones Laborales. Aranzadi, Cizur Menor, 2002, págs. 75-77.

del trabajador y de comprobación de su estado de salud, único límite a las facultades potestativas del empresario, donde el respeto a la dignidad se mantiene como único límite.

Esta normativa, pretende defender la privacidad del trabajador ante todo ataque intrusivo y desproporcionado en su espacio privado que pueda cometerse por el empleador por medio del control empresarial, pero sin impedir el mismo. Concretamente, el ET establece los límites condicionados por los propios límites del contrato de trabajo (art. 20.3). El primer límite, estaría en la finalidad de control propiamente dicha, ciñéndose ese control a la verificación del cumplimiento por el trabajador de sus obligaciones y deberes laborales. El segundo límite, no es otro que la dignidad de las personas trabajadoras, puesto que como se ha avanzado al principio de esta tesis, la dignidad (CE, art 10.1) se halla presente en todos los derechos fundamentales y, por supuesto, en el derecho a la intimidad recogido en el art. 18 de la Constitución Española y 4.2 ET.

Ahora bien, tampoco podrá el trabajador en su relación laboral mantener el derecho a la intimidad de una forma incondicional. La formalización de un contrato de trabajo y el ingreso en la unidad productiva de la empresa comporta una pequeña pérdida o al menos una reducción de la intimidad de las personas trabajadoras, soportando cierta compresión de los derechos de los que el individuo es titular[104], sin que con ello se permita justificar medidas incompatibles con la dignidad de los trabajadores. La normativa establecida interviene para evitar todo control que se ejerza o efectúe sobre la esfera vida privada del trabajador y que no tenga relación con la organización de la empresa, además de evitar toda vigilancia que elimine el espacio de libertad de la persona que está en la propia esencia del derecho a la intimidad[105].

Tal y como se ha indicado con anterioridad, al plantearse un conflicto laboral se tratará de encontrar el difícil equilibrio entre los derechos de las personas trabajadores y, los intereses del empresario. Con la utilización de las nuevas tecnologías en el entorno laboral y tras la firma del contrato de trabajo es patente que el trabajador ve reducido su derecho a la intimidad, pero, en cualquier caso, son ambas partes las que deben ceder. Por un lado,

[104] FERNÁNDEZ LÓPEZ, M.F. (1985). Libertad ideológica y prestación de servicios, en Relaciones Laborales, nº 7, pág. 65.

[105] GOÑI SEIN, J.L. (1988). El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder central empresarial. Madrid: Editorial Cívitas. págs. 116 y 117.

el empresario debe ejecutar sus facultades de control y vigilancia del empresario de forma racional, proporcional y equilibrada y, además, si lo hace a través de nuevas tecnologías, estas deben tener en cuenta tanto las exigencias del empresario como las de los trabajadores. Por tanto, el equilibrio conlleva una solución donde se recojan los intereses del empresario y de las personas trabajadores, aunque como se ha adelantado, ambas partes deben ceder, resultando imposible preservar la intimidad del trabajador de modo absoluto. Sin embargo, la solución debe ir encaminada a preservar el mayor grado de intimidad posible.

En relación con el derecho al secreto de las comunicaciones, la jurisprudencia del Tribunal Constitucional puede resumirse en los siguientes puntos:

1) Se protege implícitamente la libertad de comunicaciones y, expresamente, su secreto, prohibiendo la interceptación o el conocimiento de las comunicaciones ajenas. El bien jurídico protegido es la libertad de las comunicaciones, pudiendo quebrantarse tanto por la interceptación en sentido estricto (interpretación del soporte físico del mensaje), siendo independiente que se haya conocido el contenido del mensaje, como por el simple conocimiento ilícito de lo comunicado.
2) No cubre solo el contenido de la comunicación, sino también, la identidad de los interlocutores o de los corresponsales (STC 117/1984, de 29 de noviembre, FJ 7).
3) Se garantiza el secreto de la comunicación frente a terceros (públicos o privados) ajenos a la comunicación misma (STC 114/1984, de 29 de noviembre, FJ 7)
4) El concepto de lo secreto tiene carácter formal, lo importante es el comunicado en sí, no lo que se comunica. Es indiferente que lo comunicado pertenezca al ámbito de lo personal, íntimo o reservado (SSTC 114/1984, de 29 de noviembre, FJ 7; 34/1996, de 11 de marzo, FJ 4).

En idéntica línea, el Tribunal Constitucional actualizará el derecho al secreto de las comunicaciones en la sentencia 70/2002 y en la sentencia 123/2002, entendiendo que el mismo protege frente a las interferencias en todo tipo de comunicación, independientemente de la técnica de transmisión utilizada y con independencia del contenido del mensaje (conversaciones, imágenes, informaciones, datos, votos, etc.

En esta materia debemos diferenciar entre los correos electrónicos personales y los corporativos, cuyo acceso podrá generar una intromisión ilegítima en el derecho a la intimidad personal de los trabajadores, y a su vez, una violación del derecho al secreto de las comunicaciones.

Es conveniente invocar la doctrina constitucional sobre la materia, destacando la sentencia del Tribunal Constitucional 170/2013, de 7 de octubre, que resolvía la controversia entre la necesaria delimitación de bienes e intereses de relevancia constitucional en el marco de las relaciones laborales, como son los derechos del trabajador a la intimidad (CE, art. 18.1) y al secreto de las comunicaciones (CE art. 18.3) y el poder de dirección del empresario, expresamente reconocido en el artículo 20.3 ET, reflejo de los derechos establecidos en los artículos 33 y 38 CE, concretándose en la facultad del empresario de tomar las medidas de vigilancia y control que estime más oportunas a fin de comprobar el cumplimiento laboral de sus empleados, con el debido respeto a su dignidad (SSTC 98/2000, de 10 de abril, FJ 5, 186/2000, de 10 de julio, FJ 5, y 241/2012, de 17 de diciembre, FJ 4).

Asimismo, recordaba que el contrato de trabajo no podía ser considerado "un título legitimador de recortes" en la ejecución de los derechos fundamentales que incumbían al empleado en su carácter de ciudadano, pues este no perdía su citada naturaleza por incorporarse una empresa (STC 88/1985, de 19 de julio, FJ 2).

A mayor abundamiento, la inclusión del trabajador en la empresa acortará sus derechos en la medida estrictamente necesaria para el correcto y ordenado funcionamiento de la empresa "reflejo, a su vez, de derechos consagrados en nuestra Constitución" (STC 99/1994, de 11 de abril, FJ 4 y artículos 38 y 33). En vistas de aplicar esta imprescindible adaptación de los derechos del empleado a las fundadas imposiciones de la empresa en que trabaja, se interpretó que "manifestaciones del ejercicio de aquéllos que en otro contexto serían legítimas, no lo son cuando su ejercicio se valora en el marco de la relación laboral" (STC 126/2003, FJ 7) y que "la relación laboral, en cuanto tiene como efecto típico la sumisión de ciertos aspectos de la actividad humana a los poderes empresariales, es un marco que ha de tomarse en forzosa 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 colisionar con él" (STC 99/1994, FJ 7).

En relación con la posible colisión de los intereses del empresario y los derechos de las personas trabajadores, el Tribunal Constitucional ha insistido en que sean los propios tribunales quienes preserven el necesario equilibrio entre las obligaciones y deberes del empleado, y sus derechos y libertades constitucionales. Es decir, dada la posición preeminente de éstos en el ordenamiento jurídico, en cuanto proyecciones de los núcleos esenciales de la dignidad de la persona (art. 10.1 CE) y fundamentos del propio Estado Democrático (art. 1 CE), las limitaciones que pueda producir el contrato de trabajo ha de ser la mínima para conseguir los intereses legítimos de la empresa, proporcional y adecuada al fin propuesto" (STC 213/2002, de 11 de noviembre, FJ 7 o SSTC 20/2002, de 28 de enero, FJ 3 y 151/2004, de 20 de septiembre, FJ 7).

Como oportunamente se adelantaba, el derecho al secreto de las comunicaciones en el entorno de las TIC está íntimamente relacionado con el correo electrónico. Cuando entra en juego el correo electrónico El Tribunal Constitucional va a garantizar el secreto de las comunicaciones, pero quizás, en menor medida que el derecho a la intimidad[106.]. En su sentencia 70/2002, de 3 de abril, el Tribunal Constitucional afirmaba que el artículo 18.3 suponía una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizarlas, entendiendo que los avances tecnológicos desarrollados en los últimos años se han producido en el ámbito de las telecomunicaciones, especialmente en el uso de la informática, por lo que se hacía necesario entender las nuevas formas de comunicación y el objeto de protección del derecho fundamental a la intimidad, que extienda la protección a esos nuevos espacios (STC 70/2002, FJ 9).

En lo que respecta puntualmente al derecho al secreto de las comunicaciones, el Tribunal Constitucional comprende en sus distintas resoluciones que la noción de "intimidad constitucionalmente protegida es un concepto de carácter 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" (STC 10/2002, de 17 de enero), un "ámbito reservado

[106] MARIN ALONSO, A. (2004) "El poder del control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones", Valencia, España: Tirant Lo Blanch, , Págs. 140-141 y 155-158.

de la vida de las personas excluido del conocimiento de terceros en contra de su voluntad" (STC 127/2003, de 30 de junio y 189/2004, de 2 de noviembre).

Sin embargo, también sostiene asiduamente que "el secreto de las comunicaciones que la Constitución garantiza salvo resolución judicial es un concepto rigurosamente formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido" (SSTC 114/1984, de 28 de noviembre y 34/1996, de 11 de marzo). Por ello, no se concede la protección del secreto en virtud del contenido de la comunicación, ni se garantiza el secreto porque lo comunicado sea íntimo o personal, sino que lo que se protege es el hecho en sí de la comunicación, la vulnerabilidad de las comunicaciones realizadas en canal cerrado a través de la intermediación técnica de un tercero, pretendiendo que todas las comunicaciones, "incluidas las electrónicas" (STC 142/2012), puedan realizarse en total libertad (SSTC 123/2002 y 281/2006, de 9 de octubre).

Por esta razón, es el proceso de comunicación en libertad y no el cuerpo del mensaje que se transmite (contenido que podría considerarse superfluo tanto como de relevante interés general) el objeto que protege el art. 18.3 CE. Lo que garantiza la Constitución es la no intromisión por parte de terceros, vedando el conocimiento antijurídico o la interceptación "de las comunicaciones ajenas" (SSTC 114/1984, 175/2000, de 26 de junio, y 56/2003, de 24 de marzo).

Asimismo, como hemos puntualizado, el Tribunal protege con el secreto de la comunicación no solo el contenido, sino también la identidad de los interlocutores (SSTC 230/2007). Por tanto, "este derecho queda pues afectado tanto por la entrega de los listados de llamadas telefónicas por las compañías telefónicas como también por el acceso al registro de llamadas entrantes y salientes grabadas en un teléfono móvil" (SSTC 230/2007, de 5 de noviembre, 142/2012, de 2 de julio , 241/2012, de 17 de diciembre, y 115/2013, de 9 de mayo). Sin embargo, el Tribunal Constitucional no protege todas las comunicaciones, solo irá a proteger las que se realicen por determinados medios o canales cerrados. Consecuentemente, "no gozan de la protección constitucional del artículo 18 CE aquellos objetos que, pudiendo contener correspondencia, sin embargo, la regulación legal prohíbe su inclusión en ellos, pues la utilización del servicio comporta la aceptación de las condiciones de este" (SSTC 115/2013). De esta manera, "quedan

fuera de la protección constitucional aquellas formas de envío de la correspondencia que se configuran legalmente como comunicación abierta y, por tanto, no secreta" (SSTC 115/2013).

La sentencia STC 241/2012, en relación a las comunicaciones electrónicas en el entorno laboral, indica que, a cuenta de las idoneidades de organización, dirección y control del empresario, es aceptable que este ordene y regule el uso de las herramientas y medios informáticos de su titularidad, y también será aceptable y admisible la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas al uso de dichas herramientas, siempre mediando el pleno respeto a los derechos fundamentales de sus trabajadores.

En referencia a la limitación relativa al respeto a los derechos fundamentales, ha de considerarse que "los grados de intensidad o rigidez con que deben ser valoradas las medidas empresariales de vigilancia y control son variables en función de la propia configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin" (STC 241/2012, FJ 5).

En el caso que resuelve la STC 241/2012, la empresa despidió a una trabajadora por la utilización privativa de los medios de la empresa incumpliéndose, además, la prohibición expresa de la empresa de instalar programas en el ordenador. En el caso que se juzgada en esta sentencia la empresa accedió a una serie de ficheros informáticos donde se habían quedado registradas unas conversaciones mantenidas por dos trabajadoras a través de una aplicación informática que habían instalado las trabajadoras en un ordenador de uso común a todos los empleados sin clave de acceso. Esta sentencia determinó que no existía una situación de tolerancia empresarial al uso personal del ordenador y que, en consecuencia, no existía una expectativa razonable de confidencialidad en la utilización del programa instalado.

En lo que respecta a la intimidad personal, es doctrina constitucional afianzada su posible extensión a los correos electrónicos, lo que implicará que exista un ámbito personal y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas

de nuestra cultura, para mantener una calidad mínima de la vida humana, toda vez que según reiterada doctrina del Tribunal Constitucional el derecho a la intimidad es una derivación de la dignidad de la persona. Por lo que, para defender ese ámbito reservado, el derecho a la intimidad conllevará la imposibilidad de que terceros se entrometan en la esfera privada y la prohibición de hacer uso de lo así conocido (STC 10/2002, de 17 de enero, 127/2003, de 30 de junio o 189/2004, de 2 de noviembre). En este punto lo fundamental, es la expectativa de confidencialidad o intimidad que pueda tener el empleado a la hora de utilizar los medios tecnológicos para enviar o recibir información y mantener comunicaciones en el desarrollo de su trabajo, como es el caso del correo corporativo.

En consonancia, distintas sentencias comprenden que lo que viene a garantizar el art. 18.1 CE es el "secreto sobre nuestra propia esfera de vida personal, excluyendo que sean los terceros, ya sean particulares o poderes públicos, los que delimiten los contornos de nuestra vida privada" (SSTC 185/2002, de 14 de octubre, 159/2009, de 29 de junio, y 93/2013, de 23 de abril).

Vinculado a los límites a este ámbito reservado, la esfera de la intimidad personal estará fuertemente relacionada con los límites que establezca el propio titular del derecho, habiendo reiterado el Tribunal Constitucional que cada persona puede reservarse un espacio protegido de la "curiosidad ajena", y por tanto, corresponderá a cada persona delimitar el ámbito de intimidad personal y familiar que reserva a la curiosidad o conocimiento ajeno, por lo que, solo el consentimiento eficaz de la persona permitirá la intromisión en su derecho a la intimidad (SSTC 241/2012, de 17 de diciembre, FJ 3, 173/2011, de 7 de noviembre, FJ 2).

En este orden de cosas, el Tribunal Constitucional también ha entendido que "la intimidad protegida por el artículo 18.1 CE no se reduce a la que se desarrolla en un ámbito doméstico o privado, sino también en otros ámbitos, como el relacionado con el trabajo o la profesión, en el que se generan relaciones interpersonales, vínculos o actuaciones que pueden constituir manifestación de la vida privada" (STC 12/2012, de 24 de febrero, FJ 5).

Por este motivo, el derecho a la intimidad puede aplicarse al ámbito de las relaciones laborales, y así se comprende en las STC 98/2000, de abril y 186/2000, de 10 de julio.

En lo que respecta al contenido de los mensajes electrónicos, la STC 173/2011, de 7 de noviembre, comprende que también va a formar parte del ámbito de la intimidad constitucionalmente protegido, toda la información, ya sea privada o profesional, que se almacena en un ordenador personal (STC 173/2011, FJ 5).

La doctrina constitucional también ha defendido que el ordenador es funcional para emitir o recibir correos electrónicos, con lo que existe la posibilidad de que quede perjudicado el derecho a la intimidad de las personas, siendo que los escritos o ya leídos quedarían en el almacenamiento interno del ordenador utilizado. Esta consideración la hace también el Tribunal Europeo de Derechos Humanos, en concreto, en el "caso Copland contra Reino Unido" (STEDH de 3 de abril de 2007), que trata, entre otras cosas, sobre la vulneración del derecho a la intimidad y el secreto en las comunicaciones de los correos electrónicos enviados desde el lugar del trabajo. Entiende que los mismos se incluyen en la esfera de protección del art. 8 del "Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales" (1953), porque pueden contener datos sensibles que afecten a la intimidad y al respeto a la vida privada. No obstante, nuestro Tribunal Constitucional ha establecido, por ejemplo, en su sentencia 12/2012, ciertos matices en cuanto al alcance de la protección del derecho a la intimidad (art. 18.1. CE), y como en otros derechos fundamentales, el alcance vendrá determinado por que existiera una expectativa razonable de privacidad o confidencialidad.

Pero como siempre se establece en relación con los límites de los derechos fundamentales, el derecho a la intimidad no es absoluto, por tanto, podrá ceder este derecho frente a otros derechos o intereses constitucionalmente relevantes, pero esa cesión no puede vaciar de contenido el derecho a la intimidad, por lo que cualquier límite que sufra este derecho fundamental debe ser proporcionado y el estrictamente necesario para lograr un fin constitucionalmente legítimo. En este sentido se pronunciaron las sentencias STC 115/2013, de 9 de mayo, 143/1994, de 9 de mayo y 70/2002, de 3 de abril. Dichas sentencias, han entendido que el uso del correo electrónico por los trabajadores en el ámbito laboral va a incluirse dentro del ámbito de protección del derecho a la intimidad,

aunque serán las circunstancias de cada caso las que finalmente determinen si su monitorización por la empresa ha generado o no la vulneración de dicho derecho fundamental (SSTC 115/2013, 143/1994 y 70/2002).

Por tanto, para el Tribunal Constitucional el uso del correo electrónico por los trabajadores en la empresa queda dentro del ámbito de protección del derecho a la intimidad (STC 115/2013, FJ 5), aunque habrá que estudiar en cada caso si la fiscalización efectuada por el empresario conlleva la vulneración del derecho a la intimidad.

En lo que respecta a las garantías aplicables al control empresarial de los diversos instrumentos informáticos puestos a disposición de sus empleados, el Tribunal Supremo en su sentencia de la Sala Cuarta de 26 de septiembre de 2007 precisa como la empresa debe realizar el control a fin de no vulnerar los derechos fundamentales de las personas trabajadores, estableciendo que debe actuar conforme a las exigencias de buena fe. Para ello, deberá establecer previamente las reglas de uso de esos medios (indicando las prohibiciones absolutas o parciales, en su caso), informar a los trabajadores de que va a existir control y de los medios que van a utilizarse para realizarlo y, en su caso, dar acceso a la información generada, emitida o consultada por los empleados con los medios facilitados por el empresario (SSTS 26 de septiembre 2007 y 6 de octubre de 2011).

Al realizar el control empresarial de esta manera desaparece toda expectativa razonable de intimidad, pues, si el medio facilitado por la empresa se utiliza por los trabajadores para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, podrá ser sancionado sin existencia de vulneración alguna por parte de la empresa.

Sin embargo, la falta de esta información previa sobre las normas de uso o la posibilidad de control sobre los medios informáticos, como el correo corporativo, que van a utilizar los empleados para el desarrollo de su trabajo genera la mencionada expectativa de confidencialidad o intimidad sobre el contenido de las comunicaciones o archivos que se utilicen a través de estos medios informáticos. Si bien esta es la norma general, el Tribunal Constitucional en su sentencia 170/2013, de 7 de octubre de 2013, ha admitido la

inexistencia de expectativa de intimidad de un trabajador a pesar de no haber recibido información previa por parte de la empresa, pues la prohibición del uso privado de las herramientas informáticas propiedad de la empresa si venía expresamente regulada en el convenio colectivo aplicable a la empresa.

En esta materia, es destacable la sentencia dictada por el Tribunal Superior de Justicia de Madrid, de 13 de mayo de 2016, nº 407/2016, rec. 282/2016, en la cual, tuve la suerte de participar como parte demandante (recurrente) y de obtener una sentencia estimatoria. Dicha sentencia realiza un repaso jurisprudencial en esta materia y estudia el despido de un trabajador al que fue sometido tras entender competencia desleal a raíz de encontrar diversos correos electrónicos cruzados por el trabajador desde su cuenta personal, y si la pericial informática practicada se admitía como medio de prueba dadas las circunstancias en que la empresa llegó a su conocimiento o, si tal información se obtuvo ilícitamente, lo que, en caso afirmativo, le privaría radicalmente de cualquier validez probatoria.

A pesar de que entiende que el procedimiento de investigación consistente en la intervención, sellado, depósito y obtención de una copia del disco duro se realizó correctamente, garantizando la cadena de custodia de la información constante en el ordenador propiedad de la empresa que esta había facilitado al actor como herramienta de trabajo. El problema fue que lo que se buscaba con el análisis del disco duro fue, no la utilización de ese ordenador para fines ajenos al trabajo, para lo que habría podido estar facultada la empresa, sino el análisis de correos electrónicos obtenidos "a través de una cuenta de correo electrónico localizada merced a un archivo temporal que pudo recuperarse parcialmente, pero que era personal del recurrente (no corporativa), por mucho que pudiera haberse creado y utilizado en alguna ocasión desde el ordenador de la demandada, de igual modo que todas las cuentas abiertas en un servidor de mensajería electrónica pueden serlo desde cualquier equipo o dispositivo informático con conexión a Internet, incluidos los teléfonos móviles" (STSJ, 2016).

Era una dirección de correo de "hotmail.com", lo que significa que era una dirección personal de correo electrónico de un servidor que podía usarse no solo desde el ordenador propiedad de la demandada, sino también desde cualquier otro equipo informático conectado a Internet mediante la introducción del correspondiente usuario y contraseña

con la razonable expectativa de que los textos enviados y recibidos y demás información adjunta permaneciesen en el ámbito de su esfera privada y protegidos, en suma, por el secreto de las comunicaciones.

En concreto, se encontró en el ordenador propiedad de la empresa que usaba el trabajador un fichero temporal que, según explica el tribunal tras el estudio de las pruebas periciales, logró restaurarse en parte, y que correspondía con una cuenta personal de correo electrónico (Hotmail.com), que, como tal, el trabajador podía utilizar con solo conectarse a Internet desde cualquier dispositivo informático. A pesar de su carácter personal y privado, la empresa abrió mediante un navegador útil para ello y encontró (no puede determinar el Tribunal con qué sistema o herramienta informática), una serie de referencias parciales, probablemente metadatos, de los que se obtuvieron los textos de los correos electrónicos que, una vez adaptados, se reproducían en la carta de despido disciplinario (STSJ, 2016). Concluyó, ineludiblemente, el Tribunal que la acción de la empresa constituía un flagrante quebrantamiento de los derechos fundamentales.

Es importante añadir que no constaba ninguna previsión o protocolo empresarial tendente al procedimiento de utilización de los ordenadores u otros equipos informáticos de su titularidad por parte de sus empleados para fines diferentes del profesional. De todos modos, los hechos que se imputan al trabajador no guardan relación con el uso dado a una herramienta de trabajo (el ordenador), sino con el contenido de unos correos electrónicos restaurados parcialmente por medios ciertamente sofisticados desde un fichero temporal encontrado en el disco duro de la unidad que condujo a la cuenta privada que tenía abierta en un servidor de mensajería, comunicaciones que el actor únicamente pudo llevar a cabo conectándose a Internet y en canal cerrado.

En el supuesto enjuiciado no se trataba de fiscalizar por la empresa el uso que el actor hubiese hecho del ordenador que le facilitó como Gerente comercial, sino de investigar si había participado en alguna medida en los hechos en que se ampara la demanda dirigida contra su empleador en materia de derechos de propiedad intelectual promovida por otra empresa.

En conclusión, no siendo una investigación acerca del uso del ordenador por parte de la persona trabajadora, sino que la empresa contrato a una empresa especializada para el examen de su disco duro y restaurase en parte un archivo temporal hallado, el cual condujo a una cuenta privada de correo electrónico del trabajador, lo que permitió identificar algunos fragmentos de textos y referencia, el Tribunal entendió que no hubo duda que con esta forma de actuar la demandada vulneró los derechos fundamentales a la intimidad personal y al secreto de las comunicaciones.

Esta forma de aplicar garantías puede ser objeto de mayor debate en el caso que nos ocupa, siendo que no se remite a comunicaciones propiamente dichas (aunque fueron causantes del despido), ni de documentos personales, sino de los archivos temporales, copias de los sitios que se visitan en la web y son automáticamente guardados en el disco duro. Por tanto, es un rastro o huella de la navegación en la web y no de informaciones ni comunicaciones personales de índole reservada. Como destaca la sentencia, para el Tribunal Europeo de Derechos Humanos estos archivos temporales también se incluyen, primeramente, en la esfera de protección de la intimidad. En este sentido, se estableció la inclusión en la protección del artículo 8 del Convenio Europeo de derechos humanos la información derivada del seguimiento del uso personal de Internet, y ello porque esos archivos pueden contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladoras sobre determinados aspectos de la vida privada, como aficiones personales, ideología, orientación sexual, etc. (STEDH de 3 de abril de 2007).

Para finalizar, se establece por parte del Tribunal una pequeña valoración sobre la falta de clave de acceso del ordenador que alegó la empresa para justificar su proceder, concluyendo que no era importante esta falta de clave de acceso en el ordenador, como tampoco lo será la localización del ordenador en un despacho sin llave, pues en ningún caso, podrá suponer una aceptación por parte del trabajador de un acceso abierto a la información contenida en su ordenador.

Por todo ello, el Tribunal Superior de Justicia consideró que el examen realizado por la empresa de un disco duro y la restauración de un archivo temporal que conducía a una cuenta privada de correo electrónico de un trabajador vulneraba los derechos

fundamentales a la intimidad personal y al secreto de las comunicaciones, y, por tanto, el despido al que fue sometido el trabajador, basándose únicamente en esta prueba, se declaró nulo.

Según aclaró con posterioridad el propio Tribunal, "no significa que los empresarios no puedan, en ninguna circunstancia, monitorizar las comunicaciones de los empleados o que no puedan despedir a sus empleados por el uso de los recursos de la empresa para temas personales, sino que para poder establecer medidas de monitorización de las comunicaciones de los empleados debe tomar medidas adecuadas y suficientes para salvaguardar no solo sus derechos como empleador, sino también los derechos del empleado" (Sentencia de 3 de abril de 2007). En resumen, para el mencionado Tribunal, una monitorización es aceptable y legal si se cumplen una serie de medidas previas que permitan impedir los abusos del empresario hacía el empleado y, sobre todo, la violación de derechos humanos.

Las sentencias del Tribunal Constitucional nº 39/2016 de 3 de marzo y la dictada por el Tribunal Supremo nº 119/2018, de 8 de febrero de 2018 (Inditex), han entendido que la monitorización es válida siempre y cuando la empresa tome medidas para evitar abusos y vulneraciones en los derechos de los trabajadores, como la información previa, concreta y adecuada a los trabajadores.

6.3.2. Jurisprudencia TEDH.

La sentencia del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 en el caso Halford vs Reino Unido es la primera sentencia que vincula la vulneración del artículo 8 del Convenio con la vigilancia en el centro de trabajo. Esta sentencia no estudiaba la intrusión en el correo electrónico, sino la interceptación de llamadas telefónicas. El caso trataba sobre una mujer policía que pretendía su promoción interna y alegaba que la policía británica había "interceptado sus llamadas efectuadas en el trabajo y en su casa para negarle el ascenso" (1997). El Tribunal concluyó que hubo vulneración en el artículo 8 pues las conversaciones que había mantenido la interesada se incluían dentro de los conceptos vida privada y correspondencia.

Diez años después, el 3/4/2007, el Tribunal Europeo de Derechos Humanos se vuelve a pronunciar sobre la vulneración del artículo 8 del Convenio. Esta vez en el caso Copland vs Reino unido, donde se trataba la queja de la secretaria del rector de un centro de educación superior público que, en el curso de una investigación al propio rector, sufrió la fiscalización de su teléfono, su correo electrónico y su ordenador. Basándose en la doctrina del caso Halford vs Reino Unido entendió que se había producido la vulneración del artículo 8 del Convenio, pues tanto las llamadas efectuadas desde el centro de trabajo como los correos electrónicos remitidos desde el ordenador del trabajo se incluían en los conceptos de vida privada y de correspondencia.

Asimismo, se puntualiza que la trabajadora no había sido advertida ni informada de que sus llamadas y sus mensajes podrían ser objetivo de control, generándose, por tanto, una expectativa razonable de privacidad en relación con las llamadas y mensajes realizados en el trabajo, así como sobre su uso de Internet. La empresa se defendió alegando que los datos los obtuvo legítimamente por medio de unas facturas telefónicas y que no se revelaron a terceras personas, ni tampoco utilizados en otros procedimientos disciplinarios contra la trabajadora. Sin embargo, el Tribunal entendió que la trabajadora había sufrido una intromisión en su vida privada y, por tanto, una violación del artículo 8 del Convenio, pues la empresa obtuvo y almacenó datos relativos al uso del teléfono, correo electrónico e Internet de una trabajadora sin su conocimiento.

En los casos indicados, los primeros en esta materia, el Tribunal no se pronuncia acerca del equilibrio de la vida privada con otros derechos, ni valora el juicio de proporcionalidad, clave de la jurisprudencia que dictará más adelante, pero sí que va a apuntalar tres puntos o principios que serán determinantes en sus futuras sentencias, como son, la generación de expectativa razonable de privacidad ante la falta de información, el hecho de que el centro de trabajo también está protegido dentro del concepto de vida privada y la protección que el propio artículo 8 del Convenio otorga frente al control empresarial de las nuevas tecnologías puestas a disposición de los trabajadores.

Con posterioridad llegó la sentencia del Tribunal de Derechos Humanos de 12 de enero de 2016, (Caso Barbulescu vs Rumanía), conocida como Barbulescu I, en la cual se estudia el caso de un trabajador, ingeniero encargado de compras, que a solicitud de sus

jefes creó una cuenta en Yahoo Messenger para hablar con sus clientes, sin embargo, al cabo de un tiempo la empresa le informó de que su cuenta había sido monitorizada y le mostraron las evidencias y pruebas del uso de dicha cuenta para asuntos personales, y en consecuencia, le despidieron.

Allí, existía un reglamento interno en la compañía que prohibía de manera expresa la utilización privada de los ordenadores que se habían puesto a disposición de los trabajadores, pero no hacía referencia alguna a que se pudieran comprobar las comunicaciones. Los trabajadores fueron informados del reglamento, firmaron una copia del mismo y, además, la dirección de la empresa remitió una comunicación en la que informaba sobre el despido de una trabajadora por haber utilizado para fines privados Internet, el teléfono y la fotocopiadora.

Pocos días después, la compañía inició la revisión en tiempo real de los mensajes que enviaba y recibía el Sr. Barbulescu, lo que se prolongaría durante 8 días. Tras la fiscalización, la empresa procedió a informar al trabajador sobre la revisión de su cuenta de mensajería y sobre la existencia de pruebas del uso personal de la misma (figuraban mensajes con su hermano y novia), incumpliendo el reglamento de empresa, por lo que fue despedido.

Entiende esta sentencia que no hubo vulneración pues la empresa accedió a la cuenta de Yahoo Messenger creyendo que contenía mensajes profesionales, ya que el trabajador les había afirmado inicialmente que la utilizaba para asesorar a los clientes. De ello se desprende que el empleador actuó dentro de sus facultades disciplinarias ya que, como constataron los tribunales nacionales, había accedido a la cuenta de Yahoo Messenger suponiendo que la información en cuestión estaba relacionada con actividades profesionales y que, por tanto, dicho acceso había sido legítimo. Además, puntualiza que "no es irrazonable que un empleador desee verificar que el trabajador está desarrollando su tarea profesional en las horas de trabajo" (2016).

Existe un voto particular, emitido por el magistrado portugués Paulo Pinto, en el que pone el acento en la información a los trabajadores sobre el uso de los sistemas informáticos y

de Internet, es decir, en el apropiado conocimiento por parte de estos de las limitaciones o prohibiciones a su uso, y el impacto de las acciones incumplidoras de los trabajadores.

El reclamante solicitó que se remitiera a la Gran Sala, lo que una vez admitido, dio lugar a la sentencia dictada por la Gran Sala del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017, conocida como Barbulescu II, la cual es una de las más determinantes en lo relativo a la fiscalización del correo electrónico y su incidencia en el derecho a la intimidad y al secreto de las comunicaciones. En dicha sentencia, por once votos frente seis, se concluye que el Estado rumano si violó el artículo 8 del Convenio Europeo de Derechos Humanos[107], revocando así, la anterior sentencia dictada por el TEDH de 12 de enero de 2016.

Esta sentencia concluye que el hecho de vigilar los mensajes enviados por un trabajador mediante el ordenador facilitado por la empresa como herramienta de trabajo y acceder al contenido de los mismos supone una vulneración del derecho a la intimidad y al secreto de las comunicaciones, pues el trabajador no fue previamente informado y, por tanto, no se redujo hasta la nulidad la vida privada del trabajador durante su trabajo.

Esta sentencia entiende necesario que, "con el fin de evaluar si una determinada medida es proporcional al objetivo perseguido y si los trabajadores afectados están protegidos, se deben respetar seis criterios" (TEDH de 12 de enero de 2016)[108]:

- Que el empleado haya sido informado previamente y de forma clara de la posibilidad de que el empresario tome medidas de monitorización de su correspondencia y otras comunicaciones.
- Que la monitorización tenga un alcance limitado (que se realice durante un plazo determinado y que los resultados de la monitorización estén restringidos y solo sean accesibles al empresario.

[107] *Artículo 8. Derecho al respeto a la vida privada*
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 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 de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[108] Conocidos como el *"Test Barbulescu".*

- Que el empresario acredite razones legítimas para justificar la monitorización y el acceso a las comunicaciones.
- Si pudieran haberse utilizado métodos de monitorización menos intrusivos que el acceso directo al contenido de las comunicaciones del trabajador.
- El uso que da la empresa al resultado de la actividad de monitorización y si el mismo se utiliza para alcanzar el objetivo que justificaba la misma.
- La existencia de mecanismos de salvaguarda para el empleado, garantizando que el empresario no acceda al contenido de las comunicaciones sin la previa notificación al trabajador.

De acuerdo con dicha sentencia, los Tribunales rumanos:

- No habían protegido adecuadamente el derecho del trabajador al respeto de su vida privada y su correspondencia.
- No verificaron que el trabajador hubiera recibido de la empresa información previa a que las comunicaciones fueran monitorizadas.
- No probaron las razones que justificarían las medidas de monitorización (existen otras medidas menos intrusivas.

Tal y como aclaró con posterioridad el propio Tribunal con la sentencia "Barbulescu II", no se pretende dejar a los empresarios sin poder efectuar un control del trabajo o monitorizar las comunicaciones de sus trabajadores o que no puedan despedirles por usar de forma privada las herramientas o recursos de la empresa, sino que para poder establecer "medidas de monitorización de las comunicaciones de los empleados debe tomar medidas adecuadas y suficientes para salvaguardar no solo sus derechos como empleador, sino también los derechos del empleado".

En resumen, para el mencionado Tribunal, una monitorización es aceptable y legal si se cumplen una serie de medidas previas que permitan impedir los abusos del empresario hacía el empleado y, sobre todo, la violación de derechos humanos.

6.3.3. Conclusiones.

Como se ha profundizado anteriormente, el Tribunal Constitucional se basa principalmente en la interpretación del artículo 18 de la CE y de los derechos a la intimidad personal, al secreto de las comunicaciones y a la limitación del uso de la informática para preservar el pleno ejercicio de los derechos de los ciudadanos. Sin embargo, el TEDH centra su doctrina en el derecho al respeto de la vida privada y familiar, en base al artículo 8 del Convenio de Roma[109].

El Tribunal Europeo de Derechos Humanos ha resuelto, al confrontar los correos electrónicos y el derecho al secreto de las comunicaciones[110], confirmar la defensa del artículo 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales, por cuanto los correos electrónicos enviados desde la empresa pueden contener datos personales sensibles correspondientes a la intimidad y a la vida privada de los trabajadores.

Para evitar una intromisión en los derechos de los trabajadores el TEDH establece una serie de requisitos. El primero de ellos, que la empresa establezca unas reglas de uso sobre el correo electrónico corporativo, además, que se informe a los trabajadores de que se va a controlar el correo, que se informe como se va a controlar el correo y, por último, que medidas o sanciones se van a tomar en caso de un uso contrario a lo establecido previamente por la empresa. En este sentido, para el TEDH, si tras estas reglas, medidas o protocolos el correo electrónico se usa por los trabajadores para fines personales y, por tanto, incumpliendo lo establecido por la empresa, desde luego no podrá entenderse la vulneración de la intimidad por existir una expectativa razonable de intimidad.

Desde la perspectiva de derechos fundamentales vinculados a las TIC, resulta básico comprobar si el acceso a los contenidos de las herramientas informáticas puestos por la empresa a disposición de los trabajadores vulnera uno o varios derechos fundamentales, y para ello, habrá de estarse a los protocolos preestablecidos en la empresa sobre la puesta a disposición.

---

[109] "*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 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*"

[110] STEDH de 3 de abril de 2007 (caso *Copland* contra Reino Unido)

Tras el estudio doctrinal y jurisprudencial efectuado, se puede concluir, como siempre que se involucren los derechos fundamentales, que es necesario que prevalezca el principio del equilibrio de derechos constitucionales, que viene reivindicado por la ineludible previa información sobre el control al trabajador y, superar el llamado juicio de proporcionalidad en la práctica del control, sellado por el Tribunal Constitucional.

Para superar el test de proporcionalidad se deben cumplir las cuatro condiciones[111], ya mencionadas en esta tesis, para considerar si el sistema de vigilancia utilizado por el empleador para efectuar el control de sus empleados es adecuado y no excesivo para la satisfacción de los objetivos e intereses empresariales.

Y ello se establece porque los derechos fundamentales no son absolutos para ninguna de las partes y porque su ejercicio se debe ponderar con la existencia de otros derechos fundamentales que evidentemente van a merecer una protección del ordenamiento jurídico, por lo que deberá, además, atenderse a las circunstancias que suceden en cada casa y valorar la concurrencia de derechos fundamentales.

Por lo tanto, la limitación en la vigilancia o control del empresario vendrá establecida por la existencia de los derechos fundamentales de los trabajadores, aunque los grados de rigurosidad con que deben valorarse las medidas empresariales impuestas variarán en función de la forma en la que el empresario haya establecido los protocolos o las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones previas que hayan sido dadas por la empresa.

En relación con la doctrina estudiada a lo largo de este artículo surgen una serie de cuestiones prácticas que se resuelven a continuación:

[111] Que la medida sea idónea, es decir, que sea susceptible de conseguir el objetivo propuesto de controlar la actividad laboral y/o incumplimientos del trabajador. Necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. Ponderada o proporcional, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. Y, que sea justificada, esto es, si existen razones objetivas y motivadas que legitimen la decisión de control empresarial.

¿Puede mi empresa mirar mi e-mail?, Si se trata de un trabajo sedentario o de oficina, quizás lo primero que se entregue al trabajador en su primer día es un ordenador y una cuenta de correo corporativa, pero esta se suele personalizar con el nombre y apellido del trabajador, que se hace cargo del correo electrónico para el desempeño de su trabajo, pero que al mismo tiempo pasa a ser un medio de comunicación con terceros, pudiendo utilizarlo en ciertas ocasiones con un fin personal.

El interés del empresario es patente, no solo por una labor de control de la producción, sino por el deber que le es exigido a partir de la última reforma del Código Penal, afectando "la responsabilidad penal de las personas jurídicas, de prevenir de riesgos penales" (CP, 2015), que por medio del requerimiento de controlar las tareas de los empleados, toma un sentido especial, particularmente si se tiene en consideración una viable comisión de delitos que recurra al email o al acceso a Internet como herramientas.

Tras todo el estudio realizado, se puede concluir que las compañías podrían vigilar los correos corporativos de sus trabajadores que se utilizan desde los dispositivos que las mismas facilitan, aunque sin omitir la información previa a los equipos de trabajo acerca de la monitorización. De igual forma, es crucial que el control sea proporcional, limitándose a lo indispensable, con el criterio de invadir lo menos posible al empleado, con una evaluación del equilibrio entre derechos, contemplando los intereses de ambas partes, el propósito organizacional y la privacidad del trabajador en cuestión.

En este sentido se puede realizar una analogía entre el correo electrónico y las taquillas de los centros de trabajo, donde el empresario, conforme al artículo 18 del Estatuto de los Trabajadores, podrá acceder a la misma "cuando sea necesario para la protección del patrimonio empresarial y respetando al máximo la dignidad y la intimidad del trabajador" (ET, art. 18).

De ello, surge la siguiente cuestión, ¿Cómo debe realizarse la información? La empresa debe tener una política, clausulado o protocolo que regule el uso de herramientas informáticas (incluyendo el correo electrónico) que haga disminuir, o incluso eliminar, lo que se ha denominado como expectativa razonable de privacidad/intimidad" (caso Halford, 1997) y "debe informar de los controles de los medios informáticos que van a

existir, respetando siempre los derechos fundamentales y, particularmente, el derecho al secreto de en las comunicaciones, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones" (caso Copland, 2007). A modo de ejemplo, indicamos una cláusula tipo que puede ser anexada al contrato laboral:

"CLAUSULA X.- UTILIZACIÓN DE LOS MEDIOS INFORMÁTICOS

Los medios informáticos, incluido el correo electrónico, son herramientas de trabajo propiedad de la empresa, tanto en relación con el hardware y con el software instalado como en relación con los contenidos, y como tales herramientas deben ser considerados, estando destinados los mismos al uso estrictamente profesional. Si, a pesar de ello, el trabajador utilizase los equipos informáticos para guardar documentos o información de carácter privado, la empresa no se hace responsable de una posible pérdida o deterioro de los mismos.

El trabajador será responsable de sus contraseñas personales, así como de la custodia de todos los documentos existentes en su ordenador, no pudiendo hacer uso de su contenido para fines distintos de los laborales, revelar o difundir su contenido ni obtener copias mediante cualquier procedimiento para utilizarlas fuera del ámbito de la empresa, salvo que tenga autorización expresa de la empresa para ello.

Por ello, y en base al poder de Dirección que asiste al empresario conforme al artículo 20 del ET, este podrá revisar el contenido de los medios informáticos propiedad de la empresa, incluido el correo electrónico, navegación por Internet y el teléfono, a los fines de realizar una labor de control laboral, respetando los principios de idoneidad, necesidad y proporcionalidad.

Cualquier incumplimiento a lo regulado en los apartados anteriores será considerado como falta muy grave a efectos laborales".

En relación con el uso extralaboral del correo electrónico, no entendemos necesaria una tolerancia sobre un cierto uso extralaboral del correo electrónico corporativo, toda vez que en la actualidad resulta extremadamente fácil y es gratuito la creación de una cuenta

de correo electrónico. También es cierto que no habría, a priori, un excesivo perjuicio para la empresa, siempre y cuando su uso para fines ajenos al trabajo no se realice durante la jornada laboral. Sería más razonable cierta tolerancia al uso extralaboral de otros medios, como el teléfono o un ordenador portátil, pero no con el correo electrónico corporativo, cuya utilización particular, aunque no dañina para la empresa en términos económicos, sí resultaría caprichosa.

En este sentido, creo importante la diferenciación entre lo que podemos denominar software y hardware facilitados por la empresa. Entendemos que en un momento dado se utilicen los hardware facilitados por el empresario para alguna tarea extralaboral, como hacer una llamada telefónica particular con un móvil fuera del horario laboral (incluso en el horario laboral en tiempo de descanso), sin embargo, en relación a los programas informáticos, aplicaciones, correo electrónico, etc. (software) facilitados por la empresa para realizar el trabajo, no veo la utilización extralaboral justificada, ni que haya una tolerancia en el mundo empresarial, salvo en el correo electrónico corporativo; aunque como he dicho anteriormente, ese uso extralaboral sería caprichoso por parte del trabajador, y aunque no genere un perjuicio económico, si podría generar otros perjuicios a la empresa, como la vulneración de la Protección de Datos, cuya responsabilidad podría recaer en la empresa ante un uso indebido del correo electrónico.

Conviene finalizar indicando la posible responsabilidad penal del empresario, sin perjuicio de la consideración probatoria que tuviese en la jurisdicción social, si el control empresarial efectuado se entendiera que vulnera el secreto de las comunicaciones de los trabajadores, al no haberse efectuado con las debidas garantías y de acuerdo con los criterios jurisprudenciales expuestos. En ese caso, podría constituir delito conforme a lo establecido en el artículo 197 del Código Penal, el cual condena a penas de prisión de uno a cuatro años a los “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 o 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”.

6.4. Implicaciones del Derecho a la libertad sindical y las TICs en el ámbito de la empresa.

La problemática del derecho a la libertad sindical en relación con las nuevas tecnologías surge con la utilización del correo electrónico propiedad de la empresa para fines de información sindical. Por otra parte, para realizar esa labor de información, los sindicatos deben conocer diferentes datos de los empleados lo que hará que muchas veces colisione con el Derecho a la protección de datos de carácter personal.

6.4.1. Correo electrónico vs Derecho a la libertad sindical.

Como hemos adelantado, el uso del correo electrónico no solo se da dentro del ámbito estrictamente productivo del trabajo, sino también en el ámbito sindical, pues es habitual el uso de los correos electrónicos para comunicarse entre los representantes de los trabajadores y los trabajadores, entre los representantes y la organización sindical, o entre los representantes entre sí o con la empresa.

En este sentido fue muy popular y esclarecedor el conflicto entre el sindicato Comisiones Obreras (CC.OO) y el banco BBVA, donde el banco implantó un sistema de conexión electrónica, vía terminal, que se extendía progresivamente a todos sus empleados, sustituyendo las comunicaciones en papel o por medio del teléfono, por las realizadas a través del correo electrónico.

En esos momentos, la sección sindical del sindicato CC.OO utilizaba el correo electrónico de la empresa para realizar la información sindical.

Los mensajes se enviaban desde el servidor externo del sindicato y a través del servidor interno de la empresa, sin que esta se opusiera. En un determinado momento, el caudal de mensajes comenzó a ser de tal volumen que colapsó el servidor del Banco y este decidió establecer un filtro para rechazar aquellos mensajes que vinieran remitidos desde el servidor sindical.

En este sentido, debemos valorar si los representantes sindicales tienen derecho a servirse de las herramientas informáticas propias de la compañía para las comunicaciones con los empleados, y si aplican limitaciones al uso por parte de la empresa, sin detrimento de la libertad sindical. Al respecto, el Tribunal Supremo se pronunció en sentencia de 26 de noviembre de 2001, tras sentencia dictada por la Audiencia Nacional, siendo la sentencia dictada por el Tribunal Constitucional 281/2005 de fecha 7 de noviembre de 2005 la que resolvería el conflicto. El Tribunal Constitucional dictaminó que la empresa no tenía obligación de "garantizar y disponer para uso sindical el correo electrónico, pero sí de facilitar su utilización sindical"[112].

En concreto, en la sentencia de 7 de noviembre, se juzgaba la posible vulneración del derecho de libertad sindical (art. 28.1 CE) al sindicato CC.OO al habérsele impedido la utilización del correo electrónico corporativo como un instrumento de difusión de la información sindical.

En materia de libertad sindical, la doctrina existente en ese momento venía a establecer que cuando del tenor literal del art. 28.1 CE pudiera deducirse la restricción del contenido de la libertad sindical a una vertiente exclusivamente organizativa o asociativa que la enumeración de derechos, no se realiza con el carácter de numerus clausus, sino que en el contenido de dicho precepto se integra también la vertiente funcional (SSTC 94/1995 de 19 de junio).

Esto es, "el derecho de los sindicatos a ejercer aquellas actividades dirigidas a la defensa, protección y promoción de los intereses de los trabajadores; en suma, a desplegar los medios de acción necesarios para que puedan cumplir las funciones que constitucionalmente les corresponden" (SSTC 308/2000, de 18 de diciembre; 185/2003, de 27 de octubre, y 198/2004, de 15 de noviembre).

En este sentido, la Ley Orgánica de Libertad Sindical dispone que:

[112] SEMPERE NAVARRO, A.V. y SAN MARTÍN MAZZUCCONI, C. (2005). El uso sindical del correo electrónico a la luz de la STC 281/2005, de 7 noviembre. Revista Doctrinal Aranzadi Social Nº 17/2005. Pág. 539.

> "…la libertad sindical no solo comprende el derecho a la actividad sindical, reflejado expresamente en el art. 2.1 d) LOLS, sino que además entiende que en el ejercicio de su libertad sindical las organizaciones sindicales tienen derecho a desarrollar actividades sindicales en la empresa o fuera de ella" (LOLS, art. 2.2 d).

Para el Tribunal Supremo, las expresiones del derecho fundamental tales como "organizativas o asociativas y funcionales o de actividad" son el contenido esencial de la libertad sindical y, por tanto, su elemento mínimo e indispensable, y junto a esto, los sindicatos gozan de derechos adicionales que se añadirán al mencionado núcleo mínimo de la libertad sindical, los cuales serán asignados por normas legales o por convenios colectivos.

Por lo tanto, el derecho fundamental a la libertad sindical protegerá la correcta ejecución tanto del contenido esencial, como del contenido adicional, entendiendo que cualquier injerencia podrá infringir el artículo 28.1 CE, así lo entiende el Tribunal Constitucional en sus sentencias por ejemplo, SSTC 173/1992, de 29 de octubre, 164/1993, de 18 de mayo, 13/1997, de 27 de enero o la 36/2004, de 8 de marzo, que "los actos contrarios a ambos contenidos serán susceptibles de infringir el art. 28.1 CE".

Sin embargo, como estableció la sentencia del Tribunal Constitucional 132/2000, de 16 de mayo o la 269/2000, de 13 de noviembre, el contenido del derecho fundamental a la libertad sindical no se agotará en ese doble plano, esencial y adicional normativo o convencional, pues podrán también existir derechos sindicales que provengan de una concesión unilateral del empresario. En estos casos, el empresario podría disponer de lo concedido y, por tanto, podrá suprimir las mejoras o derechos de esa naturaleza que previamente haya concedido, a diferencia de lo que ocurre con el contenido esencial (convencional), que resulta indisponible para el empresario. Sin embargo, esa supresión unilateral de la empresa a una concesión unilateralmente concedida también puede vulnerar el derecho fundamental a la libertad sindical, pues se mantiene a estas concesiones el control constitucional *ex* artículo 28.1 CE. Esto es:

> "…también la voluntad empresarial se encuentra limitada por el derecho fundamental de libertad sindical, de manera que la posibilidad de invalidación de lo previamente concedido tendrá su límite en que no se verifique la supresión con una motivación antisindical" (STC 269/2000, de 13 de noviembre).

En concreto, se entiende por esta sentencia que las organizaciones sindicales no solo tienen derecho a los derechos sindicales que provengan de un contenido esencial y adicional, sino también de una concesión unilateral del empresario, aunque, "no podrán demandar actos positivos de esa naturaleza si no existe una fuente generadora de tal obligación". Sin embargo, se concluye que a pesar de que los trabajadores no podrán demandar esos actos positivos del empresario no significará que ante la falta de una obligación que grave al empresario fuera de aquellos ámbitos, este pueda adoptar decisiones de carácter que nieguen o impidan el ejercicio del derecho, dirigidas únicamente a dificultar su efectividad.

En relación con la acción sindical propiamente dicha, entendida como el derecho a la transmisión de información sindical a los afiliados y a los no afiliados, esta va a formar parte del contenido esencial del derecho fundamental a la libertad sindical, pues constituye el fundamento de la partición la transmisión de noticias de interés sindical, el flujo de información entre el sindicato y los trabajadores, y permite, por tanto, el ejercicio de esa acción sindical. En definitiva, constituye un "elemento esencial del derecho fundamental a la libertad sindical" (STC 94/1995, de 19 de junio, FJ 3).

La Ley Orgánica de Libertad Sindical (LOLS) en su artículo 8.1, b) y c) recoge el derecho a la acción sindical, velando por la transmisión de la información sindical, y permitiendo, por tanto, que los trabajadores afiliados a un sindicato puedan distribuir información sindical fuera de la jornada de trabajo, celebrar reuniones o recibir información de la empresa sin perturbar la actividad normal de la empresa. Y en esta materia de acción sindical, el Tribunal Constitucional ha entendido que con este artículo se garantiza la libre transmisión de comunicaciones sindicales en la empresa, lo cual constituye un legítimo ejercicio del derecho fundamental, permitiendo, además, que la transmisión de información se pueda realizar de cualquier forma, siempre que se desarrolle fuera de las horas de trabajo y no perturbe la actividad normal de la empresa (STC 94/1995).

En relación con la actividad del legislador, este no solo se limita a establecer los preceptos y articulados relativos a la garantía y tutela legal de la vertiente informativa del contenido esencial de la libertad sindical, anteriormente indicado, sino que, además, recoge las obligaciones de terceros dirigidas a la promoción de ese derecho, de esa comunicación entre el sindicato y los trabajadores. Impone, por tanto, cargas al empresario, como el establecimiento en la empresa de ciertos medios materiales o instrumentales (local, tablón de anuncios) para el mejor desarrollo de la actividad sindical.

Por su parte, la sentencia del Tribunal Constitucional 281/2005, entiende que si no hay acuerdo entre las partes la empresa no está obligada a facilitar su sistema de correo electrónico para que se realice la información sindical, pues no hay obligación legal y, además, desborda la pretensión sindical avanzada al respecto de las previsiones del art. 8 LOLS.

Previamente y en el sentido del contenido adicional al derecho fundamental a la libertad sindical, la sentencia del Tribunal Constitucional 173/1992, de 29 de octubre, estableció que la imposición de cargas a la empresa derivada de la actuación sindical implica la promoción de la actividad del sindicato en la empresa o en el centro de trabajo, lo que será un instrumento adicional que el legislador puede lícitamente establecer, ordenar y delimitar sin incurrir en inconstitucionalidad puesto que no está incluido en el contenido esencial de la libertad sindical.

Añadiendo que “estas ventajas y prerrogativas dirigidas a promocionar la actividad sindical en los lugares de trabajo no integran el contenido esencial de la libertad sindical” (STC 173/1992).

Para el Tribunal Constitucional, el artículo 8.2 LOLS no recoge la obligación del empresario de permitir la comunicación entre el sindicato y los trabajadores mediante la utilización de su sistema interno de correo electrónico, pues dicho expositivo, simplemente recoge el derecho a la existencia de un tablón de anuncios, por lo que realizando una interpretación extensiva del derecho a un tablón de anuncio nos encontraríamos con un tablón virtual, pero no con un uso sindical del sistema de correo

electrónico corporativo. Al tratarse de contenido adicional de este derecho fundamental, para el TC no cabe entender que exista una obligación legal de facilitar la transmisión de información sindical a los trabajadores a través de un sistema de correo electrónico con cargo a la empresa. Por este motivo, entendió que la empresa no estaba obligada "a dotarse de esa infraestructura informática para uso sindical".

De la misma forma se va a entender que si ese servidor de correo electrónico ya preexistía en la empresa, aunque no hubiera ninguna obligación empresarial para establecer un sistema informático para uso sindical, no puede negar su uso sindical, pues vulneraría el derecho fundamental a la libertad sindical o en palabras del Tribunal Constitucional, la existencia de un medio electrónico de información preexistente en la empresa "(…) se inscribe directamente en el ámbito del contenido esencial del derecho, habida cuenta de que los actos meramente negativos tendentes a obstaculizar el contenido esencial (aquí informativo) de la libertad sindical, como se expuso más atrás, son contrarios a esta, salvo que encuentren una justificación ajena a la simple voluntad de entorpecer su efectividad".

Sin embargo, la sentencia del Tribunal Constitucional nº 185/2003 entendió que el derecho a transmitir información sindical forma parte del contenido esencial del derecho del art. 28.1 CE, pues la acción sindical propiamente dicha confiere al sindicato una libertad de actuación, que, entre otras, incluye el derecho a la negociación colectiva, a la huelga y al planteamiento de conflictos individuales y colectivos.[113]

En este sentido, las sentencias del Tribunal Constitucional 229/2002, de 9 de diciembre, y 99/1983, de 16 de noviembre, entendieron que cualquier aproximación a la base constitucional de la libertad sindical y, por tanto, también, de la acción sindical, debe dejar previamente sentado el carácter promocional de los sindicatos como elemento clave de la configuración del Estado social y democrático de Derecho y para la defensa y promoción de los intereses colectivos de los trabajadores.

En este punto, el Tribunal Constitucional entendió literalmente que "debe beneficiar, por tanto, el cumplimiento de la función que en un régimen democrático se atribuye a los

[113] Se reconoce la utilización como instrumento de acción sindical de los derechos a la libertad de expresión y a la libertad de información entre otras, en SSTC 143/1991, de 1 de julio, 1/1998, de 12 de enero, y 213/2002, de 11 de noviembre.

sindicatos en beneficio del interés público y del interés particular de los trabajadores, que reclama unas organizaciones sindicales fuertes y dotadas de medios suficientes de acción" (STC 229/2002).

En lo relativo a las limitaciones del derecho a la información sindical, se va a debatir en esta sentencia si la validez del ejercicio de acciones sindicales mediante el derecho a la información puede realizarse con el empleo de medios empresariales que ya existiesen, aunque no se los exigiese una norma sindical. Desde luego entendemos, del mismo modo que el Tribunal, que se produce una lucha de intereses entre los empresarios y los trabajadores y sindicatos, toda vez que se ha planteado el uso de instrumentos propiedad de la compañía, siendo herramienta para la producción, y dándose que las comunicaciones ocurren en el lugar y horario de trabajo.

Se establecen en esta sentencia tres presupuestos para el estudio de los derechos y de los intereses en conflicto (el derecho a la información sindical, el derecho a la propiedad y la organización del empresario):

Primeramente, se entiende que el flujo de información de los sindicatos se perjudica si el empresario obstruye las herramientas que la favorecen.

Luego, al desarrollarse las actividades sindicales en la propia empresa, entiende que las garantías de los contenidos esenciales del derecho fundamental no son ajenas a los empresarios.

En último lugar, se establece que los empresarios están obligados a no poner obstáculos injustificados o arbitrarios a la práctica del derecho a la información sindical.

Dados los anteriores presupuestos, se concluye en la sentencia comentada que si la empresa niega la puesta a disposición de los instrumentos de transmisión de información ya existentes en la empresa que además, resultasen aptos para la finalidad sindical siendo acorde con la actividad productiva para la que fueron creados, sin que medie una justificación en razones productivas o en la legítima oposición a asumir obligaciones

específicas y gravosas no impuestas al empresario, se vulnerará el derecho fundamental a la libertad sindical.

Se razona que no se podrá argumentar el derecho a la propiedad privada del empresario vinculado a sus medios materiales, pues la propiedad continúa siendo de su pertenencia a pesar del uso de estos instrumentos empresariales por parte de los sindicatos, y sin generar en ellos un desgaste.

En virtud de la propiedad privada de los bienes empresariales, manifestada en que existen distintos tipos de propiedad dotados de multiplicidad de estatutos jurídicos, conforme la naturaleza de los bienes sobre los que aplica cada derecho de propiedad es jurisprudencia consolidada y doctrina que la flexibilidad vigente del dominio.

> "…la Constitución no ha recogido una concepción abstracta del derecho de propiedad como mero ámbito subjetivo de libre disposición o señorío sobre el bien objeto del dominio reservado a su titular, sometido únicamente en su ejercicio a las limitaciones generales que las leyes impongan para salvaguardar los legítimos derechos o intereses de terceros o del interés general" (STC 37/1987, de 26 de marzo).
>
> "Y ello hasta el extremo de que, no solo la utilidad individual, sino también la función social, definen indiscutiblemente el contenido del derecho de propiedad sobre cada categoría o tipo de bienes" (STC 37/1987, de 26 de marzo).

En suma, se concluye que el empleador debe permitir y mantener los medios necesarios para que el sindicato ejerza su acción siempre que esos medios se hallen y que su uso por parte del sindicato no vaya en detrimento del propósito para el que la compañía los hubiere creado, respetando limitaciones y normas para su uso. Asumiendo esto, no será posible negar su ofrecimiento, ni tampoco podrá privarse unilateralmente el empleo a los sindicatos.

A propósito, la Sala de lo Social de la Audiencia Nacional afirmó que el sindicato estaba utilizando el sistema de correo electrónico corporativo pues la empresa así lo había

querido, toda vez que este medio era, a juicio de la empresa, económico y rápido, estimulando este medio de comunicación frente a otros más tradicionales.

De igual forma, sostuvo que la utilización del correo electrónico de la empresa no causo ningún perjuicio a la empresa hasta el momento en el que hubo una remisión de correos masiva que colapsó el servidor. Por todo ello, estimó de manera parcial la demanda y declaró el derecho del sindicato accionante y de sus secciones sindicales en las empresas del grupo BBVA a realizar la acción sindical, transmitiendo noticias de interés sindical a través del correo electrónico con la mesura y normalidad inocua con que lo venía realizando desde el 2 de febrero de 1999 hasta el momento en que se emitió una cantidad masiva de mensajes que colapsó el servidor interno de la empresa.

Y así, se estimó parcialmente el recurso de amparo interpuesto por la Federación de Servicios Financieros y Administrativos de las Comisiones Obreras (COMFIA-CC.OO) y, se declaró vulnerado el derecho de la recurrente a la libertad sindical (art. 28.1 CE).

En relación con el Estatuto de los Trabajadores, se puede entender perfectamente que el correo electrónico se encuentra dentro de los medios tecnológicos puestos a disposición del trabajador, considerándose también como una herramienta de trabajo, por lo que, el empresario podría adoptar las medidas más oportunas para el control y vigilancia de la actividad laboral, entrando en juego no solo el art.18 ET, relativo a la inviolabilidad del trabajador, sino también el art.20.3 ET, como ya se ha indicado en apartados anteriores, lo que genera una vez más, la confrontación entre los límites de la inviolabilidad y la faculta dirección y control del empresario.

En este sentido, el Tribunal Superior de Justicia de la Comunidad Valenciana manifestó en su sentencia 2716/2010 que ante la falta de normativa nacional específica que regulara la instalación y utilización de ciertos mecanismos de control y vigilancia, deben ser los órganos jurisdiccionales los encargados de ponderar la concurrencia de intereses del empresario y los trabajadores y valorar en qué circunstancias puede considerarse legítimo su uso por parte del empresario, atendiendo siempre al respeto de los derechos fundamentales del trabajador, y muy especialmente al derecho a la intimidad personal que protege el art. 18.1CE, teniendo siempre presente el principio de proporcionalidad.

Por su parte, el Tribunal Supremo ha entendido que, efectivamente, se van a producir conflictos que afectan a la intimidad de los trabajadores por el uso de los medios informáticos facilitados por la empresa, como el correo electrónico (donde la implicación se extenderá también al secreto de las comunicaciones), la navegación por internet o el acceso a los archivos personales del ordenador.

Esos conflictos emergerán del uso privativo que los trabajadores hacen de los medios que la compañía les facilita, y dados los inconvenientes prácticos del establecimiento de prohibiciones absolutas al uso privativo del ordenador, y la normalización de cierto nivel de tolerancia a la utilización moderada de dichos medios.

No obstante, la empresa es propietaria de tales herramientas y las pone a disposición del trabajador para que preste un servicio, por lo que ese uso se circunscribe al entorno del poder de vigilancia del empleador, que implica que este "podrá adoptar las medidas que estime más convenientes de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales" (ET, art. 20.3), aunque evidentemente, ese control debe respetar la consideración debida a la dignidad del trabajador.

No obstante, resulta conveniente recordar la tolerancia general existente a un uso personal moderado de los medios informáticos que facilitan las compañías a sus empleados. Esa tolerancia, ante la falta de prohibiciones expresas, genera expectativas también generales acerca de la confidencialidad de tal uso. Pero esa expectativa de privacidad generada por costumbre no debería impedir permanentemente el control empresarial, pues 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 esta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio.

Por lo tanto, una vez más, debemos estar a las instrucciones establecidas y, además, a la acreditación del conocimiento de esta por parte del trabajador. Nos encontramos nuevamente con la necesidad de conocimiento previo del trabajador de los límites a la utilización de las diferentes herramientas facilitadas por la empresa.

En España, los límites de la utilización legítima del correo electrónico en el puesto de trabajo comienzan a debatirse con el despido de un empleado por Deustche Bank, que dio origen a la STSJ de Cataluña de 14 de noviembre de 2000. En este caso se despidió a un trabajador por "la utilización del correo electrónico que la empresa puso a disposición de los empleados, ajena de los objetivos profesionales para los que se habilitó el mismo" (STSJ, 2000). Concretamente, en el caso citado, ocurrió que "el trabajador había enviado unos 140 mensajes, en horario laboral, con el correo electrónico facilitado por la empresa, a otros empleados y a su propia dirección personal de correo (un total de 298 destinatarios), con chistes, fotografías, etc." (STSJ, 2000).

6.4.2. Derecho a la libertad sindical y Derecho a la protección de datos.

El Auto dictado por la Sala Tercera del Tribunal Supremo de 3 de junio de 2020 abordó el conflicto entre ambos derechos exponiendo todo el marco normativo regulador en esta materia.

Este Auto trataba la admisión de "un recurso de casación interpuesto por las delegadas sindicales de O'Mega-Médicos de Galicia Independientes, y del Sindicato de Médicos de Galicia (SIMEGA/CESM GALICIA), contra la Sentencia de 23 de octubre de 2019, dictada por la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Galicia" (Recurso de apelación núm. 158/2019). Al mismo tiempo, había sido incluido contra la Sentencia, de 28 de enero de 2019, del Juzgado de lo Contencioso administrativo núm. 2 de Santiago de Compostela.

El fondo del asunto versaba sobre una solicitud de información y documentación sobre los trabajadores del hospital efectuada por las delegadas sindicales amparándose en el derecho a la información que les asistía como representantes sindicales.

Concretamente, se solicitaba la relación de los contratos de todos los facultativos de cada servicio, especificando nombre, tipo de contrato actual y fecha de inicio del mismo, incluyendo los contratos estructurales, y no estructurales, así como la tarifa del proceso quirúrgico y por facultativo, la tarifa global por proceso quirúrgico y la tarifa por consulta

y servicios, los nombramientos estatutarios de todos los facultativos por servicio. Y esto incluía los nombramientos por acúmulo de tareas, las sustituciones y las plazas no estructurales.

El hospital denegó la documentación solicitada por entender que vulneraba la normativa en materia de protección de datos de carácter personal por lo que las recurrentes se alzaron alegando contravención del derecho fundamental a la libertad sindical (art. 28.1 CE).

En un primer momento, tras el recurso contencioso administrativo de las delegadas sindicales, el Juzgado de lo Contencioso Administrativo consideró que la documentación solicitada por las delegadas era excesivamente concreta y masiva en relación con el número de trabajadores, y que la denegación de la misma por parte del hospital no generaba ninguna vulneración de la libertad sindical, negando, por tanto, la indemnización de daños y perjuicios solicitada.

La sentencia estableció conforme a lo dispuesto por la Agencia Española de Protección de Datos, que la función de vigilancia y protección de las condiciones de trabajo atribuida a las Juntas de Personal era factible de realizarse correctamente sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en el Órgano o Dependencia correspondiente, matizando que "solo en el caso en que el control se refiera a un sujeto concreto, que haya planteado la correspondiente queja ante la Junta de Personal, será posible la cesión del dato específico de dicha persona". Continúa alegando que, en todo lo demás, "la función de control quedará plenamente satisfecha mediante la cesión a la Junta de Personal de información debidamente disociada, según el procedimiento definido en el artículo 3.f) de la Ley Orgánica 15/1999, que permita a aquélla conocer las circunstancias cuya vigilancia le ha sido encomendada sin referenciar la información en un sujeto concreto, esto es, sobre personas identificadas o identificables".

Por su parte, el Auto del Tribunal Supremo tras recurso entendió que: el derecho a recabar información por parte de la representación sindical de una forma tan específica, esto es, a través de listados de los nombramientos estatutarios de todos los facultativos por servicio de una forma tan específica, no podía entenderse comprendido bajo la genérica

facultad que se atribuye a las Juntas de personal en el artículo 9 de la Ley 9/1987, de recibir información sobre la política del personal del Departamento, Organismo o Entidad local. La solicitud de información tampoco podría verse comprendida por la vigilancia del cumplimiento de las normas vigentes en materia de condiciones de trabajo, Seguridad Social y empleo, y ejercer, en su caso, las acciones legales oportunas ante los organismos competentes, pues la información tan específicamente demandada por las representantes de los trabajadores conllevaría una cesión de datos personales, para lo cual era necesario el previo consentimiento de las partes interesadas.

Asimismo, entiende que el derecho fundamental del artículo 18.4 de la CE, surgido ante las "nuevas formas de amenaza" que se derivan de la utilización progresiva de la información referente a la persona, supone el derecho a controlar el uso de los datos insertos en un programa informático, "habeas data".

La confrontación de derechos proviene de la invocación de las recurrentes del derecho fundamental a la libertad sindical previsto en el artículo 28.1 de la CE, en su carácter de delegadas sindicales, y el “derecho fundamental de protección de datos” (CE, art. 18.4), que alega la Administración recurrida.

Para el Tribunal Constitucional, suponen parte del contenido esencial del derecho fundamental a la libertad sindical, las expresiones de las organizativas o asociativas y funcionales o de actividad, pues los sindicatos pueden tener una serie de derechos o facultades adicionales, atribuidos por normas legales o por convenios colectivos, que se añaden a aquel contenido esencial, mínimo e indisponible de la libertad sindical (STC 64/2016). De este modo, “el derecho fundamental se integra, no solo por ese contenido esencial, sino también por el citado contenido adicional y promocional, de modo que los actos contrarios a este último son también susceptibles de infringir el artículo 28.1 CE, cuando se ejercitan fuera del marco previsto por la Ley” (SSTC 64/2016, 11 de abril, FJ 4, 173/1992, de 29 de octubre, FJ 4, 164/1993, de 18 de mayo, FJ3 y 36/2004, de 8 de marzo, FJ 5).

Particularmente, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, cuando regula la comunicación de datos, establece que “los datos

de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero, para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado" (STC 64/2016). Consentimiento necesario con carácter general, que sin embargo no resulta preciso, como excepción, "cuando la cesión está autorizada en una ley"[114].

El Tribunal Supremo realiza un análisis del marco normativo en el que las delegadas han basado su recurso, la Ley Orgánica de Libertad Sindical y el Estatuto Básico del Empleado Público.

Con relación a la LOLS, dentro del Título "De la acción sindical" el Tribunal destaca al artículo 10, que establece la equiparación en garantías y derechos de los delegados sindicales y los miembros de los comités de empresa, o de los órganos de representación que se establezcan en las Administraciones públicas. En base a semejantes prerrogativas, los delegados sindicales podrán acceder a la misma información y documentación que la empresa ponga a disposición del comité de empresa, si bien están obligados a guardar el correspondiente sigilo profesional en aquellas materias en las que legalmente proceda.

Por su parte, el Estatuto Básico del Empleado Público, al disponer las competencias de las Juntas de Personal y de los delegados de personal, establece en su artículo 40.1 que los representantes podrán recibir información sobre la evolución de las retribuciones, sobre traslado de instalaciones y revisión de sistemas de organización y métodos de trabajo, sobre las sanciones muy graves que se hayan impuesto, sobre la jornada laboral y horario de trabajo, además de vigilar el cumplimiento de las condiciones de trabajo y prevención de riesgos laborales y colaborar con la Administración para el cumplimiento de la productividad.

Una vez recordado el marco normativo, para la Sala Tercera, el derecho a la libertad sindical también comprende el derecho de información para acceder a documentación y, por tanto, poder informarse, sin embargo, como todo derecho fundamental, el derecho a la libertad sindical también tiene límites. Para el Tribunal, el límite al derecho

[114] Artículo 11.2.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

fundamental de la libertad sindical, respecto del acceso a documentación e información, se produce por el reconocimiento constitucional del derecho a la protección de datos de carácter personal.

En esta materia, la Ley de Protección de Datos de Carácter Personal (LO 15/1999) vigente en aquel momento, en lo que respecta a la regulación de la comunicación de datos planteaba como exigencia la expresión de consentimiento:

> "solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado" (art. 11 LOPD).

Sin embargo, como se avanzado, el consentimiento no será preciso cuando la cesión está autorizada en una ley (art. 11 LOPD).

En este caso, ni el artículo 40 de la Ley del Estatuto Básico del Empleado Público, ni el 10 de la Ley Orgánica de Libertad Sindical, recogen algún supuesto que exceptúe “el consentimiento de los interesados a los efectos del artículo 11.2.a)” (LOPD 15/1999).

Para el Alto Tribunal, en casos donde sea requerido una voluminosa transferencia de datos, sin mínimas explicaciones sobre el destino e importancia de estos para ejercer la labor sindical cuando la misma se solicita, es fundamental “que medie la debida relación entre los datos personales del personal que se solicitan, con la importante función sindical que se desarrolla”. En resumidas cuentas, concluye que solo cuando estos datos personales sean necesarios para el ejercicio de las labores sindicales, podrían considerarse excepcionados del consentimiento, pero no cuando se encuentran desvinculados o se desconozca su relación, al no haberse puesto de manifiesto su conexión con dichas funciones sindicales. Por tanto, “la mera invocación sin justificación no puede servir de excusa para acceder a todo tipo de documentación”, pues de lo contrario se vaciará el tenor del derecho fundamental a la protección de datos, al desconocer el titular de los derechos el uso que se hace de sus datos, perdiendo su poder de disposición, en supuestos en los que no se justifica la concurrencia de alguna de las excepciones legalmente establecidas.

En relación con la posibilidad de entender como no íntimos los datos solicitados, como se invoca por las representantes recurrentes, "el derecho fundamental a la protección de datos se refiere a cualquier dato[115] de la persona en las esferas en las que se desenvuelve, protegiendo la privacidad, que va más allá que la intimidad" (LOPD 15/1999, art. 3 a)).

Aplicando lo anterior, el Tribunal Supremo entendió, en base a la doctrina del Tribunal Constitucional[116], que los datos relativos al nombre y apellidos, tipo de puesto de trabajo, o el inicio de la prestación no disociados de aquél, son datos que, aunque no sean íntimos, están protegidos por la citada Ley Orgánica de Protección de datos de carácter personal de 1999.

6.4.3. Jurisprudencia TEDH.

Lo cierto es que no hemos encontrado jurisprudencia del Tribunal Europeo de Derechos Humanos en relación con el derecho a la libertad sindical y el uso del correo electrónico, centrándose la misma principalmente en el desarrollo del derecho de asociación y el derecho a la negociación colectiva cuando el Estado es el empleador.

Sin embargo, existen varios pronunciamientos relativos a la llamada cláusula de sistema de tienda cerrada, en inglés, *closed-shop system*. Esta forma de asociación consiste en un acuerdo entre sindicatos y empresarios conforme al cual se exige que los trabajadores pertenecientes a determinadas categorías se afilien a una concreta organización sindical como condición para poder ser contratados en ciertas empresas o para conservar su puesto de trabajo, y que sorprendentemente está admitida en algunos Estados, principalmente en el Reino Unido.

Este modelo sindical no se encuentra en España, al menos oficialmente, pues si que coexisten los denominados "sindicatos amarillos" que no son otra cosa que sindicatos

---

[115] Artículo 3.a) de la Ley 15/1999 Orgánica de Protección de datos de carácter persona, "Dato": *"cualquier información concerniente a personas físicas identificadas o identificables".*

[116] STC 292/2000, de 30 de noviembre, *"la protección de datos no se reduce a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros puede afectar a sus derechos, sean fundamentales o no, porque su objeto no es solo la intimidad individual".*

dirigidos por la empresa, por lo que hay cierta analogía con el sistema de asociación inglés, *closed-shop*.

6.4.4. Conclusiones.

De una parte, tenemos el conflicto que se genera con la utilización del correo electrónico propiedad de la empresa para realizar información sindical y, de otra parte, para realizar esa labor de información, los sindicatos deben conocer diferentes datos de los empleados lo que puede colisionar con el Derecho a la protección de datos de carácter personal.

En relación con la utilización del correo electrónico de la empresa para fines sindicales, nuestros tribunales han entendido que la transmisión de información sindical, que conforma una de las formas de acción sindical, va a formar parte del contenido esencial del derecho fundamental a la libertad sindical.

Se parte del contenido esencial y adicional (normativo o convencional) del derecho a la libertad sindical, pero también se entiende que podrán existir derechos sindicales que provengan de una concesión unilateral del empresario. Las prerrogativas sindicales que provengan de una norma no podrán ser suprimidas, sin embargo, las que provengan de concesiones unilaterales extraordinarias por parte del empresario sí se podrían suprimir, pero sino se hace de forma justificada, sin una motivación antisindical, podría vulnerar el derecho fundamental a la libertad sindical.

En base a ellos, los representantes de los trabajadores no podrán reclamar al empresario actos positivos de esa naturaleza si no existe una fuente generadora de tal obligación (pues desborda el art. 8 LOLS), pero eso no significa que ante la falta de una obligación que grave al empresario fuera de aquellos ámbitos, este pueda adoptar decisiones de carácter que nieguen o impidan el ejercicio del derecho, dirigidas únicamente a dificultar su efectividad.

Por tanto, si ya existe en la empresa un servidor de correo electrónico u otro medio tecnológico apto para la acción sindical, aunque no hubiera ninguna obligación empresarial para establecer un sistema informático para uso sindical, no podrá negarse su

uso sindical, a pesar de ser un instrumento propiedad de la compañía, destinada para la producción, y situándose las comunicaciones en el lugar y horario de trabajo, pues vulneraría el derecho fundamental a la libertad sindical.

Como sucede con todos los derechos, estos no son ilimitados y el derecho de libertad sindical no es una excepción. A continuación, y a modo de conclusión, se exponen los diferentes límites al derecho fundamental a la libertad sindical utilizando medios preexistentes en la compañía;

- En principio, habrá que observar el propio objeto del derecho fundamental, derecho de las asociaciones sindicales para ejercer sus funciones de representación ante la organización, por lo que su uso estará limitado a la transmisión de información exclusivamente laboral/sindical.
- La comunicación no podrá alterar la actividad normal de la empresa. En ese sentido, no perturbará la actividad empresarial la recepción de mensajes en la cuenta de correo del trabajador en horario de trabajo, aunque si pudiera serlo su lectura, por lo que sería recomendable, a efectos perturbadores, leer los mismos al finalizar la jornada o en las pausas existentes.
- En relación con la alteración de la actividad normal de la empresa, tampoco podrá perjudicarse el uso para el que la empresa lo implantó, ni podrá prevalecer el uso sindical al empresarial, debiendo emplearse el instrumento de comunicación facilitado por la empresa, de una forma que armonice el modo de manejarlo del sindicato y el logro de los objetivos empresariales, con prevalencia, si acontecieran conflictos, de la segunda funcionalidad mencionada. A tales efectos, resultará lícito a nivel constitucional que la compañía predetermine las condiciones de uso de las comunicaciones electrónicas para propósitos sindicales, cuidando no excluirlas en absoluto.
- el uso de los instrumentos empresariales no podrá incurrir en costes adicionales que la compañía deba afrontar.

Los empresarios están obligados a no poner obstáculos injustificados o arbitrarios a la práctica del derecho a la información sindical, por lo que si la empresa niega la puesta a disposición de los instrumentos de transmisión de información ya existentes en la empresa

que además, resultasen aptos para la finalidad sindical siendo acorde con la actividad productiva para la que fueron creados, sin que medie una justificación en razones productivas o en la legítima oposición a asumir obligaciones específicas y gravosas no impuestas al empresario, se vulnerará el derecho fundamental a la libertad sindical.

El empleador debe permitir y mantener los medios necesarios para que el sindicato ejerza su acción siempre que esos medios se hallen y que su uso por parte del sindicato no vaya en detrimento del propósito para el que la compañía los hubiere creado, respetando limitaciones y normas para su uso.

Por tanto, si se respetan estas limitaciones y pautas para su uso, recurrir a instrumentos preexistentes en la compañía que demuestren eficiencia en las comunicaciones sindicales, estará amparado por el art. 28.1 CE.

En relación con la confrontación del derecho a la protección de datos y el derecho a la libertad sindical, en su vertiente de acceso a la información y documentación, podemos concluir que, como todo derecho fundamental, el derecho a la libertad sindical también tiene límites, se produce por el reconocimiento constitucional del derecho a la protección de datos de carácter personal.

En este sentido nuestros tribunales han entendido que existirá vulneración del derecho a la protección de datos de carácter personal cuando se solicite por parte de los representantes de los trabajadores una importante cantidad de información, de datos, sin concretar mínimamente el destino pues resulta esencial que medie la debida relación entre los datos personales que se solicitan, con la función sindical que se desarrolla, por lo que, solo cuando estos datos personales sean necesarios para el ejercicio de las labores sindicales, podrían considerarse excepcionados del consentimiento, pero no cuando se encuentran desvinculados o se desconozca su relación, al no haberse puesto de manifiesto su conexión con dichas funciones sindicales.

En relación con la posibilidad de entender como no íntimos los datos solicitados, se entiende que el derecho fundamental a la protección de datos se refiere a cualquier dato de la persona en las esferas en las que se desenvuelve, protegiendo la privacidad, que va

más allá que la intimidad, por lo que, aunque los datos relativos al nombre y apellidos, tipo de puesto de trabajo, o el inicio de la prestación, son datos que, aunque no sean íntimos, están protegidos por la Ley Orgánica de Protección de datos de carácter personal.

6.5. Navegación por Internet vs Derecho a la intimidad.

Como propugna la Ley 3/2018 de Protección de Datos y Garantía de Derechos Digitales:

> "Internet se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad".

La posibilidad de navegar por Internet, como fuente de información, es una herramienta más que pone el empresario a disposición del trabajador para prestar el servicio.

Empezando como se ha terminado en el apartado anterior relativo al correo electrónico, en la navegación por Internet sí que existe una tolerancia de la empresa a visitar web de contenido extralaboral, siempre y cuando sea un uso razonable. Desde nuestro punto de vista, entendemos razonable, la visita de páginas web de contenido extralaboral siempre y cuando se realicen en los periodos de descanso del trabajador, por lo que todo lo que exceda de los periodos de descanso, se podrá entender como un abuso de confianza por parte del trabajador, al margen de seguramente, un bajo rendimiento por parte de este.

Dada cuenta la amplísima fuente de información que es Internet y la asequibilidad de esta, hace poco razonable que se exija a los trabajadores un uso estricto laboral de internet. También lo entienden autores como Sempere Navarro o San Martín Mazzucconi, "no parece lógico considerar que exista una quiebra de la confianza y la buena fe por el hecho de que un trabajador verifique a través de Internet la situación de una calle a la que ha de dirigirse después de terminada su jornada laboral, o consiga el número de teléfono de una

agencia de viajes con la que contratará sus próximas vacaciones".[117] Sin embargo, insistimos en que dichas consultas se deberían realizar fuera de la jornada laboral o en los periodos de descanso, pues de lo contrario, desde nuestro punto de vista, sí que nos encontraríamos con un abuso de confianza por parte del trabajador.

Por tanto, la problemática no lo generará la navegación propiamente dicha, pues el uso entendemos que es tolerado, sino cuando se utiliza, y el contenido visitado. En este sentido, no es lo mismo visitar un mapa tras haber terminado tu jornada laboral, que visitar webs de contenido sexual en horario laboral.

En cuanto al control empresarial de la navegación por Internet, no encontramos una normativa específica al respecto, debiendo acudir al genérico artículo 18 del Estatuto de los Trabajadores, que trata la posibilidad de realizar registros sobre la persona del trabajador, sus taquillas y sus efectos particulares. No obstante, se matiza que los registros solo podrán realizarse cuando sean necesarios para la protección del patrimonio empresarial o de los demás trabajadores de la empresa, en del centro de trabajo y en horas de trabajo. Asimismo, se debe respetar en los registros la dignidad e intimidad del trabajador, por lo que aquí aparece el derecho fundamental que limitará el control empresarial relativo a la navegación por Internet.

Sin embargo, habrá que valorar si el ordenador facilitado por la compañía al trabajador es un efecto particular. En este sentido, la sentencia del TSJ de Cataluña 7431/2014, de 7 noviembre[118], entendió que el ordenador facilitado por la empresa no se trataba de un efecto personal, sino de una herramienta de trabajo propiedad de la empresa, por lo que para realizar un control empresarial de las páginas visitadas en el ordenador profesional

[117] SEMPERE NAVARRO, A.V y SAN MARTÍN MAZZUCCONI, C. (2010). Nuevas Tecnologías y Relaciones Laborales. Revista Doctrinal Aranzadi Social Vol. 11 nº 11, págs. 270.

[118] *"(…) exponiendo, la referida doctrina, una primera conclusión, a saber: el artículo 18 del Estatuto de los Trabajadores no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral, o dicho de otro modo: el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores".*

no sería de aplicación lo establecido en el mencionado artículo 18 del Estatuto de los Trabajadores[119], sino lo dispuesto en el artículo 20.3[120] del mismo texto legal.

Por lo tanto, hay que insistir en la idea de que la finalidad del artículo 18 ET parte de concretar unos límites y pautas de prudencia, ya que lo que está permitiendo es el registro de efectos personales del trabajador y de las taquillas, es decir, información personal de los trabajadores. Sin embargo, de acuerdo con la sentencia indicada, tanto el correo electrónico como el ordenador de la compañía son herramientas de trabajo y su fin no es guardar información personal de los trabajadores. No obstante, cabe la posibilidad de guardar información personal, al menos de forma indirecta, pues las páginas web que visitamos son un reflejo de nuestros gustos y aficiones y, por tanto, de nuestra intimidad. De esta manera, veremos si en el control empresarial en la navegación por Internet se aplica el artículo 18 o 20.3 del Estatuto de los Trabajadores.

En cualquier caso, con el fin de evitar intromisiones en los derechos de los trabajadores, las empresas, ya sea de forma unilateral o a través de los convenios colectivos deberán precisar unas reglas de uso de estos tipos de medios tecnológicos, indicando la existencia de vigilancia y control, y las condiciones en que se desarrollarán los mismos. Si concurren estas reglas de uso será más legítimo y sencillo para la empresa sancionar un uso inadecuado, al menos por desobediencia, salvo que existiera una tolerancia ante dichos usos o no se hayan impuesto sanciones a otros trabajadores por similares actuaciones.

6.5.1. Jurisprudencia española.

Para algunos autores, la falta de normativa específica en relación con el uso de medios informáticos va a hacer que en los pronunciamientos judiciales se aprecie una tendencia a fallar en favor de los trabajadores como consecuencia de un mayor margen de tolerancia

---

[119] Artículo 18. Inviolabilidad de la persona del trabajador. *"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 su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible".*

[120] Art. 20.3 ET. *"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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".*

del uso extralaboral de estas herramientas, ya que contribuyen a generar expectativas de intimidad en el uso de la herramienta[121].

El Tribunal Constitucional ha establecido una doctrina sobre el alcance de los derechos fundamentales en el marco de la relación laboral y la necesaria proporcionalidad de sus restricciones o limitaciones. En este sentido, "los trabajadores no dejan de ser ciudadanos por el hecho de realizar una actividad laboral para un empresario, de lo que se deriva que los derechos fundamentales que la Constitución reconoce a todos los ciudadanos no se ven exceptuados por la existencia de una relación laboral"[122].

Un ejemplo de esta doctrina la encontramos en la sentencia del Tribunal Constitucional 197/1998, de 13 octubre, donde el tribunal entiende que

> "las organizaciones empresariales no forman mundos separados y estancos del resto de la sociedad, ni la libertad de empresa que establece el art.38 de la Constitución legitima que los trabajadores deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central en el sistema jurídico constitucional". (STC 1998)

Sobre esta cuestión también se ha pronunciado el Tribunal Supremo[123], el cual ha entendido en múltiples pronunciamientos que, si no hay derecho a un uso privativo del ordenador, tampoco existirá el derecho a usarlo en condiciones de respeto a la intimidad o al secreto de las comunicaciones, pues si no existe tolerancia en el uso privado, tampoco existirá

---

121 MARTINEZ FONS, D. (2002) "Uso y control de las tecnologías de la información y comunicación en la empresa". Relaciones Laborales Nº 2, pp.1311-1344.

122 SEMPERE NAVARRO, A.V y SAN MARTÍN MAZZUCCONI, C. (2012) "Sobre el control empresarial de los ordenadores". Revista Doctrinal Aranzadi Social. Nº 3/2012. Pág. 12.

123 STS (Sala de lo Social, Sección 1ª) Sentencia de 6 octubre 2011 RJ/2011/7699. (caso Annaligia, S.A.)

"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.

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".

> "una expectativa razonable de intimidad, pues, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo". (STS 2011)

La cuestión no es pacifica, pues si no hay derecho al uso privativo o personal del ordenador, no se podrá garantizar la intimidad o el secreto de las comunicaciones a dicho uso y, por tanto, si el uso privativo es ilícito es contradictorio obligar al empresario que lo padezca, pero que no pueda controlarlo. Al respecto, entendemos que si debe hacerse una diferenciación entre ciudadano y trabajador, pues aunque el trabajador es también un ciudadano, y tiene una serie de derechos, estos no pueden respetarse de manera incondicional ni como ciudadano, pues debe respetar los derechos de los otros ciudadanos, ni como trabajador, pues en la relación contractual no se impide el control o fiscalización del trabajador vinculada de los aspectos técnico-organizativos del trabajo, incluidos los efectos personales como se dispone en el art. 18 ET.

En este sentido, se debe recordar que el derecho a la intimidad y el derecho al secreto de las comunicaciones están íntimamente relacionados, sin embargo, el derecho a la intimidad se vinculará en mayor medida con la navegación por Internet, y, en cambio, el derecho al secreto de las comunicaciones con el correo electrónico.

En cuanto al control de la navegación por parte del empresario, si se realiza en relación con el contenido (páginas web visitadas), salvo casos justificados de indicios de comisión de delitos, vulnerará la intimidad del trabajador.

Para determinada corriente doctrinal[124], a fin de respectar el juicio de proporcionalidad, el control de la navegación se debe realizar de forma muy restringida y de la siguiente manera:

- Preferencia sobre controles indirectos. Es preferible que se realice un control del tiempo de navegación que los contenidos, es decir, las webs visitadas. Desde el punto

[124]ROIG, A. (2010) "Derechos fundamentales y tecnologías de la información…" ob, cit Pág 14.

de vista de estos autores, para respetar el juicio de proporcionalidad es recomendable controlar las horas totales de navegación, la duración de la navegación, la frecuencia de las visitas, el horario de trabajo o la disminución de la producción, antes que las webs visitadas, salvo que se tengan indicios de que el trabajador está realizando una actividad delictiva.

- Debe mediar una justificación relevante.
- No debe haber otra medida menos gravosa para obtener los mismos resultados.
- La duración de este control no puede ser indefinida o incluso alargarse en el tiempo sin justificación.
- El control se debe acotar a una finalidad, de suerte que, si esta última decae o cambia, deberá replantearse también el control a utilizar.

Esta reflexión es bastante razonable, sin embargo, la justificación del control de los contenidos por la comisión de delitos por parte del trabajador resulta, a nuestro juicio, un tanto exagerada. Y ello porque el control del empresario está encaminado a que sus empleados trabajen o produzcan durante el tiempo de trabajo, y no a impedir conductas delictivas. Evidentemente, si al supervisar el contenido de la navegación por Internet o el contenido de un ordenador un empresario descubre la comisión de un delito por parte de sus trabajadores, deberá, al igual que todos los ciudadanos, denunciar el ilícito ante las autoridades correspondientes, además, de poder sancionar disciplinariamente al trabajador. Ahora bien, habrá que ver y valorar si el empresario podrá incardinar el hecho delictivo descubierto en alguno de las infracciones recogidas en el Convenio Colectivo de aplicación o en el Estatuto de los Trabajadores.

Como se ha mencionado con anterioridad, el control del contenido de la navegación debe ser necesario para la supervisión del trabajo, pues si solo se vigila el tiempo de conexión, este puede resultar engañoso, máxime cuando la navegación por Internet es básica en la mayoría de los trabajos en los que se utiliza un ordenador como herramienta de trabajo. De hecho, hoy en día, no se concibe un ordenador sin acceso a navegación por Internet.

Al respecto del derecho a la intimidad, es doctrina consolidada de nuestro Tribunal Constitucional la relativa al "carácter no ilimitado del derecho a la intimidad en su colisión con otros intereses constitucionalmente relevantes" (STC 96/2012), debiendo

recordar que, según esta doctrina, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones:

1. Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad) (STC 96/2012);
2. Si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad) (STC 96/2012);
3. Y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) (STC 96/2012, de 7 de mayo, FJ 10; o SSTC 14/2003, de 28 de enero, FJ 9; y 89/2006, de 27 de marzo, FJ 3).

En este punto, la sentencia del Tribunal Constitucional 170/2013, de 7 de octubre, tiene especial relevancia, pues marcará la doctrina sobre el control por parte del empresario de la navegación por Internet y de los correos electrónicos.

Según esta sentencia, el derecho a la intimidad personal, al derivar de la dignidad de la persona (art. 10.1 CE), conlleva la existencia de un espacio de privacidad reservado frente a las intrusiones de terceros, necesario para mantener una calidad mínima de la vida humana. A fin de proteger la privacidad, el derecho a la intimidad va a otorgar a la persona el poder jurídico para imponer a terceros el deber de abstención a la intromisión en su privacidad y, además, la prohibición de hacer uso de lo conocido.

Para el Tribunal Constitucional;

> "lo que garantiza el art. 18.1 CE es el secreto sobre nuestro espacio de vida personal, excluyendo que sean los terceros, particulares o poderes públicos, los que delimiten los contornos de nuestra vida privada" (STC 159/2009, de 29 de junio, FJ 3; o SSTC 185/2002, de 14 de octubre, FJ 3; y 93/2013, de 23 de abril, FJ 8).

En lo que respecta a los límites de ese espacio de privacidad personal, se precisa que:

> "la esfera de la intimidad personal está en relación con la acotación que de la misma realice su titular, habiendo reiterado este Tribunal que cada persona puede reservarse un espacio resguardado de la curiosidad ajena" (STC 241/2012, de 17 de diciembre, FJ 3);

Consecuentemente, cada persona podría delimitar el ámbito de intimidad personal y familiar que reserva para íntimos y ajenos (STC 241/2012, FJ 3), por lo que solo el consentimiento del sujeto interesado permitirá inmiscuirse en su derecho a la intimidad (STC 173/2011, de 7 de noviembre, FJ 2).

Asimismo, también se ha determinado que el derecho a la intimidad (art. 18.1 CE) no solo se aplica en el ámbito privado, sino también en el ámbito laboral, donde también se generan relaciones, vínculos o actuaciones que pueden constituir expresión de la vida privada (STC 12/2012, de 30 de enero, FJ 5). Por ello, el Tribunal Constitucional ha afirmado expresamente que el derecho a la intimidad también se va a aplicar y defender en las relaciones laborales (SSTC 98/2000, de 10 de abril, FFJJ 6 a 9; y 186/2000, de 10 de julio, FJ 5).

Así y con todo, en relación con el alcance de cobertura del derecho a la intimidad, nuestro Tribunal Constitucional ha establecido que viene determinado por la existencia de una "expectativa razonable de privacidad o confidencialidad" (STC 12/2012, FJ 5).

El Tribunal Constitucional, aplicando la jurisprudencia del TEDH, por ejemplo, en sentencia de 25 de septiembre de 2001, P.G. y J.H. c. Reino Unido, § 57, o de 28 de enero de 2003, Peck c. Reino Unido, § 58, entiende que un criterio para poder valorar si nos estamos ante supuestos susceptibles de entenderse como privados ("manifestaciones de la vida privada", TEDH 2001), y por tanto, susceptible de ser protegida frente a intromisiones ilegítimas, será el de las expectativas razonables de privacidad, definiendo esta como, la que la propia persona pueda tener de "encontrarse al resguardo de la observación o del escrutinio ajeno". Se exponen dos ejemplos esclarecedores, cuando una

persona se encuentra en un paraje inaccesible o en un lugar solitario debido a la hora del día, puede entenderse con naturalidad en la confianza fundada de la ausencia de observadores. Por el contrario, si se participa de forma consciente y voluntaria en actividades populares que pueden ser objeto de registro o información pública, no podrá entenderse la existencia de privacidad ni de expectativas razonables de intimidad.

Asimismo, debemos considerar que, conforme a reiterada doctrina constitucional;

> "el derecho a la intimidad no es absoluto (como no lo es ningún derecho fundamental), pudiendo ceder ante otros intereses constitucionalmente relevantes, siempre que el límite que aquél haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo y sea proporcionado" (STC 115/2013, de 9 de mayo, FJ 5, o SSTC 143/1994, de 9 de mayo, FJ 6, y 70/2002, de 3 de abril, FJ 10).

Por su lado, la Sala Cuarta de nuestro Tribunal Supremo ha establecido en sentencia de 26 de septiembre de 2007 (RECUD 966/2006), al estudiar el despido disciplinario de un trabajador por la utilización incorrecta del ordenador (sin clave de acceso), que en relación con las garantías aplicables al control empresarial de los diversos instrumentos informáticos puestos a disposición de los trabajadores, la empresa debe establecer anticipadamente protocolos o reglas de utilización de esos medios -con aplicación de prohibiciones absolutas o parciales- además de informar a los trabajadores de que va existir control y de los medios que se utilizarán para ello, así como de las medidas que han de adoptarse en su caso para garantizar un uso laboral adecuado, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones, todo ello conforme a las exigencias de la buena fe.

De esta manera, si el instrumento facilitado por la empresa se usa de forma contraria a esos protocolos o para usos privados y con conocimiento de los controles y medidas aplicables, no podrá apreciarse la vulneración de la expectativa razonable de intimidad reflejada en las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) EDJ 1997/15630 y 3 de abril de 2007 (caso Copland) para valorar la

existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos.

A esto se debe que tanto se insista en el necesario aviso de la prohibición para fines privativos de una herramienta puesta a disposición por la empresa, y una advertencia previa de que se pueden realizar controles para verificar su correcta utilización (Protocolo de uso y protocolo de control). Se determina que es posible la prohibición total o parcial, aunque esta sentencia no invalidó la doctrina del Tribunal Constitucional sobre el juicio de proporcionalidad, necesidad, idoneidad, etc.

Por otro lado, entiende el Tribunal Supremo que tanto las comunicaciones telefónicas como las realizadas mediante el correo electrónico estarán incluidas en este ámbito con la protección del secreto de las comunicaciones, y que la garantía de la intimidad también se va a extender a los archivos personales del trabajador que se encuentran en el ordenador (STS de 26 de septiembre de 2007, FJ 5).

Los archivos temporales son copias que se guardan automáticamente en el disco duro de los lugares visitados a través de Internet, por lo que, al no ser comunicaciones, ni archivos personales, para el Tribunal Supremo la aplicación de la garantía de intimidad podría ser más debatible.

Para el Alto Tribunal, los archivos temporales "son rastros o huellas de la navegación en Internet y no de informaciones de carácter personal que se guardan con carácter reservado" (STS de 26 de septiembre de 2007, FJ 4). No obstante, entiende que estos archivos también entran, en principio, dentro de la protección de la intimidad, sin perjuicio de la necesidad o conveniencia de la información previa por parte de la empresa, señalando que están incluidos en la protección del artículo 8 del Convenio Europeo de derechos humanos, la información derivada del seguimiento del uso personal de Internet, y es que esos archivos pueden contener datos sensibles en orden a la intimidad, en la medida que pueden incorporar informaciones reveladores sobre determinados aspectos de la vida privada, tales como la ideología o la orientación sexual (STS de 26 de septiembre de 2007, FJ 4).

Por lo tanto, los archivos temporales de Internet también entran dentro de la esfera de protección del derecho a la intimidad. Todo ello, de conformidad con lo establecido por el Tribunal Supremo (Sala de lo Social, Sección 1ª) en sentencia de 26 de septiembre de 2007 y por el Tribunal Europeo de Derechos Humanos en sentencia de 3 de abril de 2007 (Copland vs Reino Unido).

Por último, y en relación con la clave de acceso o despacho sin llave, va a entender al Alto Tribunal que no va a ser obstáculo para la protección de la intimidad el que "el ordenador no tuviera clave de acceso o que el ordenador estuviera en un despacho sin llave, pues no supone por sí mismo una aceptación por parte del trabajador de un acceso abierto a la información contenida en su ordenador" (STS de 26 de septiembre de 2007, FJ 4), aunque ello pueda generar otros problemas como la dificultad de la atribución de la autoría.

El Tribunal Superior de Justicia de Madrid se ha pronunciado recientemente en su sentencia de 26/4/2023 en relación la navegación por internet y el derecho fundamental a la intimidad. Es este caso se juzgaba el despido de un trabajador al que se le imputaba que durante 4 días y en horario de trabajo había visitado páginas en internet de contenido extralaboral. Por ello, se imputaba las faltas de transgresión de la buena fe contractual y abuso de confianza, al existir no solo una prohibición expresa de utilización extralaboral, sino, además, cada vez que se conectaba a una página web salía un recordatorio de dicha prohibición.

Al existir información previa, el TSJ concluyó que la empresa no había vulnerado los derechos fundamentales del trabajador al realizar la monitorización, sin embargo, entendió que la conducta del trabajador no conllevaba fraude, deslealtad o abuso de confianza, sino tan solo se probaría que en cuatro días concretos ha accedido desde el ordenador de la empresa, cuyo uso está ciertamente limitado a fines profesionales, a páginas web no relacionadas con este uso, durante los tiempos que hemos referido (unos 40 minutos al día) lo cual no generaba la infracción más grave, conllevando por tanto la calificación del despido como improcedente.

Por tanto, en este caso, el TSJ de Madrid ha valorado en primer lugar la información previa realizada por parte de la empresa a fin de valorar la vulneración del derecho a la intimidad, y en segundo lugar, ha valorado tanto el contenido de la navegación como el tiempo de la misma para ponderar la sanción impuesta, llegando a la conclusión de que la sanación del despido por unos pocos minutos al día de navegación extralaboral era desproporcionada al no reflejarse los hechos como muy graves en el Convenio Colectivo de aplicación ni como transgresión de la buena fe contractual o abuso de confianza la conducta del trabajador.

Por su parte, el Tribunal Superior de Justicia de Andalucía (Sevilla), en su sentencia de fecha 905/2019 de 28 de marzo 2019 estudiaba el caso de un despido de un trabajador tras constatar una disminución de forma continuada y voluntaria de su rendimiento de trabajo, acreditándose la realización de tan solo un 10% de su producción. Por este motivo, la empresa realizó una investigación que concluyó con un informe técnico-informático detallado con el historial de navegación, tiempo de visionado de web, etc. que determinaba que había 30.118 accesos a Internet, es decir, unos 130 accesos diarios a páginas web de contenido sexual, apuestas, comercios, etc.

El motivo alegado por la empresa para el despido se fundó en trasgresión de la buena fe contractual, abuso de la confianza en el desempeño de su trabajo y por desobedecer las órdenes del empresario.

Sin embargo, el TSJ considera que la monitorización efectuada en el ordenador que utilizaba el trabajador se hizo con vulneración del derecho a la intimidad, toda vez que no había información previa al trabajador y, por tanto, existía una "expectativa razonable de confidencialidad. Por ello, se declaró la nulidad de la prueba así obtenida.

Por lo tanto, se entiende vulnerado el artículo 18.4 de la Constitución, que consagra el derecho a la protección de datos personales.

El TSJ andaluz, basándose en la doctrina constitucional, jurisprudencia y doctrina judicial del TEDH, argumenta (FJ 1) que el trabajador tenía una expectativa razonable de confi-

dencialidad por la que de forma moderada podía utilizar los dispositivos digitales de trabajo con fines privados, y que esa expectativa razonable de confidencialidad podía puede neutralizarse por el empresario mediante la prohibición expresa del uso para fines privados, mediando información previa de dicha prohibición, entendiéndose cumplida si tal prohibición consta en el convenio colectivo, en el contrato de trabajo o en la normativa sobre las técnicas de información y comunicación de la empresa. Sin embargo, pasa por alto que la expectativa razonable de confidencialidad permite realizar un uso moderado, no un uso desproporcionado, y en el caso de autos, así lo era. A pesar de ello, al no existir información previa, no se excluía la expectativa de intimidad.

Por tanto, en este caso fue determinante la falta de información previa y específica, no pudiendo valorar la prueba que acreditaba, desde luego, unos incumplimientos laborales graves.

6.5.2. Jurisprudencia TEDH.

En materia de navegación por Internet se aplica la doctrina relativa a la confrontación de los correos electrónicos y el derecho al secreto de las comunicaciones[125], confirmando la protección del artículo 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales, por cuanto los correos electrónicos enviados desde la empresa pueden contener datos personales sensibles correspondientes a la intimidad y a la vida privada de los trabajadores, al igual que sucede con la navegación por Internet.

Conforme a la sentencia del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) EDJ 1997/15630 y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos, habrá que confirmar si la utilización privativa de un instrumento facilitado por la empresa en contra de prohibiciones expresas y con conocimiento de los controles y medidas aplicables. En caso de la existencia de prohibiciones expresas y

[125] STEDH de 3 de abril de 2007 (caso *Copland* contra Reino Unido)

conocimiento por parte del trabajador del control aplicado, no podrá entenderse que se ha vulnerado la expectativa razonable de intimidad en los términos que establecen las sentencias

Para evitar una intromisión en los derechos de los trabajadores el TEDH establece una serie de requisitos; que la empresa establezca unas reglas de uso sobre el correo electrónico corporativo y la navegación por Internet, que se informe a los trabajadores de que se va a controlar el correo y la navegación, que se informe como se va a controlar y, por último, que medidas o sanciones se van a tomar en caso de un uso contrario a lo establecido previamente por la empresa. En este sentido, para el TEDH, si tras estas reglas, medidas o protocolos se hace un uso por los trabajadores para fines personales y, por tanto, incumpliendo lo establecido por la empresa, desde luego no podrá entenderse la vulneración de la intimidad por existir una expectativa razonable de intimidad.

6.5.3. Conclusiones.

En primer lugar, debemos distinguir entre dos tipos de controles ejercidos por la empresa en la navegación por Internet. Un control de la navegación en relación con el propio contenido, es decir, las páginas web visitadas y, por otro lado, un control de la duración de la navegación, es decir, el tiempo que se está navegando en la red y no se está trabajando. En relación con la duración de la navegación, dependiendo el puesto de trabajo resultará casi imposible de determinar si ha existido un uso inadecuado por parte del trabajador, toda vez que hoy en día en múltiples trabajos es continúa y necesaria la navegación por Internet.

Para una determinada doctrina el control de los contenidos se debe realizar de forma muy restringida y de la siguiente manera:

- Mediando una justificación relevante.
- No debe haber otra medida menos gravosa para obtener los mismos resultados.
- La duración de este control no puede ser indefinida o incluso alargarse en el tiempo sin justificación.

- El control se debe acotar a una finalidad, y si esta cambia o finaliza, deberá modificarse también el control a utilizar.

Sin embargo, la jurisprudencia tanto nacional como europea, no realiza tal distinción (contenido y tiempo de navegación), analizando principalmente si había información previa a los trabajadores y si supera el juicio de proporcionalidad.

El Tribunal Constitucional mantiene el juicio de proporcionalidad para poder valorar las posibles intromisiones en el derecho a la intimidad de los trabajadores a través del control en la navegación realizado por el empresario. Por lo tanto, se debe valorar si el control de los contenidos es idóneo y consigue el objetivo que se propone (juicio de idoneidad); si no existe otra medida más apropiada para el mismo propósito e igual de eficaz (juicio de necesidad); y, por último, si el control es equilibrado y ponderado al caso concreto, generando más beneficio para el interés público que perjuicio sobre otros intereses en conflicto (en sentido estricto, juicio de proporcionalidad).

Por su parte, el Tribunal Supremo da mucha relevancia a la información previa a la imposición de la medida de control para que este no atente a los derechos fundamentales, estableciendo que antes de realizar el control, la empresa debe haber informado a los trabajadores de que va a existir un control en la navegación por Internet, como se va a controlar y qué consecuencias disciplinarias tendrá un uso incorrecto o inadecuado. En este sentido, si no existe derecho de uso del ordenador con fines personales, tampoco podrá exigirse que en ese uso en concreto se respete la intimidad o el secreto de las comunicaciones, pues ante la ausencia de la tolerancia al uso privativo para los trabajadores, tampoco existirán expectativas razonables de intimidad. Si el uso personal del mismo contraría lo establecido previamente por la empresa, no es posible exigir al empresario que lo sostenga y que no pueda controlarlo.

También se va a definir el concepto de archivos temporales como un rastro o huella de la "navegación" en la web, no entendiéndolo como información privada, aunque si entrarán dentro de la protección de la intimidad, sin perjuicio de la necesidad de la información previa por parte de la empresa.

Asimismo, en relación con la clave de acceso del ordenador, no se va a exigir su existencia para valorar la intromisión, no siendo un impedimento para proteger la intimidad el que el ordenador no contara con clave de acceso o, por analogía, que el ordenador estuviera en una oficina sin llave.

El artículo 18 del Estatuto de los Trabajadores no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral, o dicho de otro modo, el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores.

En este sentido se pronunció la sentencia del TSJ de Cataluña 7431/2014, de 7 noviembre[126], la cual entendió que el ordenador facilitado por la empresa no se trataba de un efecto personal, sino de una herramienta de trabajo propiedad de la empresa, por lo que para realizar un control empresarial de las páginas visitadas en el ordenador profesional no sería de aplicación lo establecido en el mencionado artículo 18 del Estatuto de los Trabajadores, sino lo dispuesto en el artículo 20.3[127] del mismo texto legal.

Por lo tanto, hay que insistir en la idea de que la finalidad del artículo 18 ET parte de concretar unos límites y pautas de prudencia, ya que lo que está permitiendo es el registro de efectos personales del trabajador y de las taquillas, es decir, información personal de los trabajadores. Sin embargo, de acuerdo con la sentencia indicada, tanto el correo electrónico como el ordenador de la compañía son herramientas de trabajo y su fin no es guardar información personal de los trabajadores. No obstante, cabe la posibilidad de guardar información personal, al menos de forma indirecta, pues las páginas web que visitamos son un reflejo de nuestros gustos y aficiones y, por tanto, de nuestra intimidad.

---

126 *"(…) exponiendo, la referida doctrina, una primera conclusión, a saber: el artículo 18 del Estatuto de los Trabajadores no es aplicable al control por el empresario de los medios informáticos que se facilitan a los trabajadores para la ejecución de la prestación laboral, o dicho de otro modo: el control empresarial de un medio de trabajo no necesita, a diferencia de lo que sucede con los supuestos del artículo 18 del Estatuto de los Trabajadores, una justificación específica caso por caso. Por el contrario, su legitimidad deriva directamente del artículo 20.3 del Estatuto de los Trabajadores".*

127 Art. 20.3 ET. *"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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".*

De esta manera, veremos si en el control empresarial en la navegación por Internet se aplica el artículo 18 o 20.3 del Estatuto de los Trabajadores.

Por todo lo anteriormente expuesto, llegamos a la conclusión que para controlar la navegación por internet se debe monitorizar el ordenador puesto a disposición del trabajador de la empresa. Este control empresarial, legitimado por el artículo 20.3 ET, podrá realizarse tanto en el contenido de las páginas webs visitadas, como en el tiempo dedicado a la navegación. Asimismo, para que el control no sea vulnerador de los derechos fundamentales de los trabajadores deberá realizarse cumpliendo el juicio de proporcionalidad y mediando información previa y especifica.

6.6. Cámaras de videovigilancia vs Derecho a la intimidad y a la protección de datos de carácter personal.

Gracias a los avances tecnológicos, el uso de la videovigilancia ha aumentado paulatinamente en todas las esferas de la vida, y en la esfera laboral también. Cada vez son más empresas las que disponen de estos medios, ahora más asequibles, para el control de la actividad laboral. Sin embargo, la tecnología y su correlativo uso social muchas veces tropieza con el respeto de los derechos fundamentales de los trabajadores. Esto puede suceder cuando las cámaras de videovigilancia son utilizadas para el control de los trabajadores o como medio probatorio de un incumplimiento laboral (especialmente utilizadas en sectores como la banca o la hostelería).

En la actualidad, ninguna disposición indica detallada o concretamente cómo y cuándo pueden ser utilizados para el control laboral, por lo que la utilización de estos medios para el control laboral es fuente de conflictos, los cuales serán resueltos por la jurisprudencia.

A pesar de la casi nula regulación, si es pertinente señalar que la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales, recoge los tratamientos de datos con fines de videovigilancia, y se permite la videovigilancia de las empresas “con fines de seguridad en las personas y en los bienes, incluyendo las propias

instalaciones" (art. 22). En cuanto a las imágenes que se captan en la vía pública, se permite para el mismo fin y en la medida imprescindible[128].

Esta captura de imágenes por seguridad tiene una limitación temporal de 30 días desde que son tomadas, por tanto, deberán mantenerse durante ese tiempo. Sin embargo, para los casos en los que se hubiera podido comprobar actos que atenten contra la integridad de personas, bienes o instalaciones, las imágenes deberán ser puestas a disposición de la autoridad en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación (LOPD 3/2018, art. 22).

Por tanto, dada la ausencia de una regulación específica, que no ha llegado hasta la LOPD 3/2018, ha sido la jurisprudencia la que ha establecido los requisitos necesarios para que un sistema de videovigilancia laboral se considere lícito, recurriéndose como limitación al respeto de diferentes derechos fundamentales, como el derecho a la intimidad, el derecho al honor, el derecho a la propia imagen, o el derecho a la protección de datos de carácter personal.

A pesar de la falta de regulación específica, conviene destacar que los tribunales de justicia y la doctrina científica admiten el uso de las nuevas tecnologías con la finalidad de controlar la prestación del trabajo[129], aunque no se ha alcanzado un consenso con respecto a las limitaciones facultativas de los empresarios con respecto al control de las conductas de los trabajadores por medio de sistemas de videovigilancia, y ello probablemente se deba a la escasa regulación legal en esta materia, lo que ha generado una jurisprudencia y doctrina constitucional sumamente cambiante.

---

[128] Artículo 22. Tratamientos con fines de videovigilancia.

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

[129] LÓPEZ AHUMADA, J. E. (2006) "La tutela del derecho a la intimidad del trabajador y el control audio-visual de su actividad laboral", Cuadernos electrónicos de Derechos Humanos y Democracia, Nº 3, enero-julio, Pág. 213

6.6.1. Jurisprudencia española.

El Tribunal Constitucional ha fijado cuáles son los requisitos que dentro del ámbito laboral debe cumplir un sistema de videovigilancia para considerarse como lícito (STC 186/2000)[130], sin embargo, a lo largo de los años ha ido modificando su doctrina.

En materia de control empresarial y videovigilancia hay que valorar dos cuestiones, que medios de prueba pueden utilizarse a la hora de ejercer la facultad de control empresarial y si hay alguna injerencia en el derecho a la intimidad de los trabajadores. Por tanto, se debe valorar el equilibrio entre los medios de vigilancia (medio de prueba) y la injerencia en el derecho a la intimidad.

Se parte de la idea establecida en la sentencia del Tribunal Constitucional 114/1984 de que no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales (STC 114/1984, FJ 3).

Este Tribunal entiende que se debe comprender primero que, ante un conflicto de intereses, los derechos fundamentales de los trabajadores deben prevalecer y, por tanto, cualquier limitación en los mismos procedente del control empresarial solo va a poder "derivar del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho" (SSTC 99/1994, de 11 de abril; 6/1995, de 10 de enero, y 136/1996, de 23 de julio). Según esta doctrina, en la que la relación laboral conlleva la perdida de ciertos parámetros de la actividad humana de los trabajadores, se debe valorar si es preceptivo el equilibrio entre el interés del trabajador y el de la empresa, donde, además, el trabajador ha admitido voluntariamente, a través de su aceptación, el contrato de trabajo. Por tanto, la clave para valorar las posibles intromisiones en los derechos de los trabajadores estará en el propio objeto del contrato de trabajo, y en las limitaciones que podrían derivarse del mismo, teniendo en cuenta la satisfacción del interés que llevó a las partes a formalizar ese contrato de trabajo. Y ello porque según esta doctrina hay actividades o trabajos que llevan implícitas una restricción en el derecho a la imagen de los trabajadores que las realicen, por la propia naturaleza de estas, como son las

[130] STC (Sala Primera) Sentencia núm. 186/2000 de 10 julio.

actividades en contacto con el público. De esta forma, el que en su día aceptará realizar un trabajo de atención al público, no podrá invocar la vulneración de la propia imagen para no realizar el trabajo.

Igualmente, la jurisprudencia constitucional ha mantenido que el control empresarial no puede generar o conllevar resultados vulneradores de los derechos fundamentales de los trabajadores, o resultados inconstitucionales, como lo denomina en diferentes sentencias, entre otras, SSTC 94/1984, de 16 de octubre; 171/1989, de 19 de octubre; 123/1992, de 28 de septiembre; y 173/1994, de 7 de junio, además de que la utilización de un derecho fundamental nunca podrá ser objeto de sanción (STC 11/1981, de 8 de abril).

Desde este momento y con las sentencias STC 66/1995, de 8 de mayo; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8, se asentará la doctrina por la cual la constitucionalidad de cualquier medida que limite o restrinja derechos fundamentales vendrá determinada por el estricto cumplimiento del principio de proporcionalidad. Para confirmar si la medida restrictiva de derechos cumple con este principio, se debe valor si cumple tres requisitos, el juicio de idoneidad, el juicio de necesidad y el juicio de proporcionalidad. En el juicio de idoneidad se valora si la medida puede alcanzar el objetivo que se propone. Con el juicio de necesidad, se valora la necesidad de la medida, es decir, si no existe otra medida con mayor moderación para lograr ese fin con la misma eficacia. Por último, en el juicio de proporcionalidad en sentido estricto, se tendrá en cuenta el equilibrio de la medida, valorando si se obtienen más beneficios para el interés general que perjuicios en otros valores.

Por tanto, como se ha adelantado, el Tribunal Constitucional se va a centrar en preservar el equilibrio entre el control empresarial y la injerencia en los derechos fundamentales de los trabajadores[131].

[131] STC 6/1998, *"...preservar el necesario equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito, pues, dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, esa modulación solo deberá producirse en la medida estrictamente imprescindible para el correcto y ordenado respeto de los derechos fundamentales del trabajador y, muy especialmente, del derecho a la intimidad personal que protege el art. 18.1 CE, teniendo siempre presente el principio de proporcionalidad"*

Las sentencias 98/2000 y 186/2000 marcan la jurisprudencia del juicio de proporcionalidad en sentido estricto, y, además, sirvieron a los tribunales nacionales en el caso López Ribalda para fallar la no existencia de vulneración a la intimidad en el uso de cámaras ocultas en el lugar de trabajo sin previo aviso a los trabajadores.

En concreto, la STC 186/2000, de 10 de julio, enjuiciaba el caso de un cajero del economato de su empresa (ENSIDESA), en la cual, efecto de un importante descuadre en caja y de fundadas sospechas de actuaciones irregulares por parte de los cajeros, la dirección de la empresa procedió a contratar a una empresa de seguridad que instalase un circuito cerrado de videovigilancia con cámaras ocultas, que enfocaban únicamente a las tres cajas registradoras y al mostrador de paso de las mercancías desde el techo.

Del resultado de la vigilancia realizada durante unos pocos días, se adoptaron diferentes medidas disciplinarias frente a los cajeros, uno fue despedido y el resto fueron suspendidos de empleo y sueldo durante dos meses. Con el visionado de las cámaras se reveló que un cajero sustraía diferentes cantidades de dinero de la caja, y los otros distraían diferentes prendas.

El trabajador despedido se alzó en suplicación alegando vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE) siendo que el órgano judicial se basó en "pruebas nulas por haberse obtenido con violación del derecho fundamental a la intimidad" (art. 18.1 CE).

En esta sentencia se estableció que el empresario no realizó una intromisión ilegítima en la intimidad de los trabajadores en el centro de trabajo amparándose en sus facultades de vigilancia y control establecidas en el artículo 20.3 ET. Por otra parte, el tribunal entendió que debía existir un equilibrio de derechos entre las partes intervinientes en el contrato, lo que va a suponer limitaciones en las facultades organizativas de empresario por los derechos fundamentales de los trabajadores, quedando obligado el empresario a respetarlos. Y no solo ello, sino que, además, el ejercicio del poder de dirección no podrá generar resultados inconstitucionales, lesivos de los derechos fundamentales de los trabajadores.

En este sentido, se nombraba la doctrina emanada por el Tribunal Constitucional en su sentencia 6/1998, de 13 de enero[132], donde se establecía la posición prevalente de los derechos fundamentales en nuestro Ordenamiento Jurídico y la necesidad de respetar el principio de proporcionalidad ante cualquier medida restrictiva de derechos fundamentales, es decir;

> "si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad), si además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad), si la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)" (STC 6/1998).

En este caso, se concluía que la medida tomada por la empresa de instalar cámaras ocultas que controlaban exclusivamente la zona de caja superaba el juicio de proporcionalidad, pues era una medida justificada, al existir advertencias de otros trabajadores del proceder irregular de los cajeros y habían importante descuadres contables, era idónea para la finalidad pretendida por la empresa, pues se verificaba si algunos de los trabajadores cometían las irregularidades y así poder tomar las medidas oportunas, era necesaria, para tener un medio de prueba y, era equilibrada, pues las cámaras solo apuntaban a la zona de caja, por lo que se descartaba que se hubiera producido lesión en el derecho a la intimidad personal (art. 18.1 CE).

Por tanto, ponderando los intereses en juego y verificado el cumplimiento del principio de proporcionalidad, se permitía excepcionalmente un control con videocámaras ocultas, y, por tanto, sin conocimiento de trabajadores ni de sus representantes, pues existían serios indicios de determinadas actuaciones irregulares por parte de unos trabajadores, como así se acreditó gracias a las imágenes.

---

132 *"el necesario equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito –modulado por el contrato, pero en todo caso subsistente– de su libertad constitucional pues, dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, esa modulación solo deberá producirse en la medida estrictamente imprescindible para el correcto y ordenado respeto de los derechos fundamentales del trabajador y, muy especialmente, del derecho a la intimidad personal que protege el art. 18.1 CE, teniendo siempre presente el principio de proporcionalidad".*

Para el Tribunal Constitucional no se vulnero la intimidad del trabajador recurrente por grabarle prestando servicios en el centro de trabajo, pues no se trataba de una medida caprichosa, ni se pretendía divulgar su conducta, sino que se trataba de valorar el desempeño del trabajador, lo cual se encontraba justificado al existir fundadas sospechas de transgresión de la buena fe contractual por parte del trabajador. Se pretendía acreditar las irregularidades cometidas por el trabajador, fundadas en sospechas que finalmente se pudieron comprobar con las cámaras de videovigilancia y, por tanto, tener una prueba que sirva para justificar las medidas disciplinarias, para el caso de que el trabajador impugnase, como así lo hizo, la sanción de despido disciplinario que la empresa le impuso por tales hechos. A diferencia del caso juzgado en la STC 98/2000, no se trató de un control genérico del desempeño de los trabajadores, ni de escuchas indiscriminadas.

Al respecto de la falta de información a la representación de los trabajadores y a los propios trabajadores afectados, entiende el Tribunal que, no resulta relevante desde el punto de vista constitucional, pues la falta de dicha exigencia no generaría una vulneración de derechos fundamentales, tratándose de una cuestión de mera legalidad ordinaria, ajena por completo al objeto del recurso de amparo. (STC 186/2000, FJ 7).

Por último, se estableció que si no había lesión del artículo 18.1 CE, tampoco habría vulneración del derecho a la tutela judicial efectiva (art. 24.1 CE), pues, el convencimiento de los tribunales se alcanzó con otras pruebas diferentes a las grabaciones, como lo fueron las testificales de los detectives privados practicadas en el juicio oral, a los que sus letrados pudieron interrogar.

Con posterioridad se dictó la STC 292/2000, de 30 de noviembre, en la cual se abordaba el control empresarial a través de cámaras de videovigilancia desde una perspectiva de protección de datos de carácter personal y no tanto, del derecho a la intimidad de los trabajadores.

Dicha sentencia trataba el supuesto del distintivo informativo exigido por la AEPD. En concreto, juzgaba la instalación de una cámara de videovigilancia colocada en un lugar donde enfocaba un puesto de trabajo, la caja, y además se había colocado en el escaparate,

a la vista de todo el mundo, el distintivo informativo exigido por la instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de videocámaras (STC 292/2000). Esta sentencia estableció que el contenido del derecho fundamental a la protección de datos consistía en poder disponer y controlar los datos personales y, por tanto, permitía al trabajador decidir qué datos personales facilitaba a un tercero y con qué fin, cabiendo la posibilidad de que se opusiera a su uso o posesión. Por tanto, entiende el tribunal que la facultad de disponer y controlar los datos personales se va a concretar en otorgar el consentimiento para la recogida, la obtención y el acceso a los datos personales, incluyendo, además, su posterior almacenamiento y tratamiento, así como su uso por un tercero (STC 292/2000).

Respecto al consentimiento, la STC 292/2000, de 30 de noviembre, entiende que la clave del sistema de protección de datos de carácter personal e indica que la Ley Orgánica de Protección de Datos de carácter personal vigente en esa fecha (LOPJ 15/1999) establecía el principio general de que el tratamiento de los datos personales solamente sería posible con el consentimiento de sus titulares, salvo habilitación legal para que los datos puedan ser tratados sin dicho consentimiento. Por tanto, se concretaba que sería el legislador quien debía fijar cuándo concurría ese bien o derecho que justificaba la limitación del derecho a la protección de datos personales y en qué circunstancias podía restringirse y, además, debía hacerlo siguiendo unas reglas precisas que hicieran previsible al interesado la imposición de tal limitación y sus consecuencias.

En la vigente LOPD se establecía que para el tratamiento de los datos de carácter personal se requeriría del consentimiento inequívoco del afectado, en este caso del trabajador, salvo que la ley dispusiera otra cosa (art. 6.1). Excepciones que recogía el mismo artículo y donde se puntualizaba que no sería preciso ese consentimiento cuando los datos de carácter personal se refieran a las partes de un contrato laboral y sean necesarios para su mantenimiento o cumplimiento, o se recogieran para el ejercicio de las funciones propias de las Administraciones públicas o cuando el tratamiento de los datos tenga por finalidad proteger un interés sanitario vital (art.7.6), o cuando los datos figuraran en fuentes accesibles al público y su tratamiento fuera necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se

comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

Por tanto, conforme a dicha ley, el tribunal valoró el consentimiento y el contrato de trabajo, entendiéndose que el consentimiento del trabajador iba a pasar a un segundo plano, pues el consentimiento vendría implícito en la relación laboral, siempre que el tratamiento de datos de carácter personal fuera necesario para el mantenimiento y el cumplimiento del contrato laboral.

Tal excepción a exigir consentimiento también se recoge en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (art. 10.3 b)), donde se señala que los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado si el que recaba los datos es el responsable del tratamiento con ocasión de la celebración de un contrato de trabajo o de la existencia de una relación laboral (también negocial o administrativa) de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

Por ello, la excepción al consentimiento remite solo a los datos para poder llevar a cabo la relación laboral, es decir, los datos necesarios para el mantenimiento y cumplimiento de las obligaciones que derivan del contrato de trabajo. En este sentido, será válido un tratamiento de los datos personales del trabajador sin consentimiento dirigido al control de la relación laboral y, será necesario el consentimiento del trabajador cuando el tratamiento de datos se utilice con fines diferentes al cumplimiento del contrato de trabajo.

Sin embargo, una cosa es el consentimiento y otra cosa el deber de información, el cual seguirá existiendo, aunque no sea necesario el consentimiento, pues la información permitirá al trabajador afectado ejercer los derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o, en su caso, del representante (LOPD 15/1999, art. 5). El deber de información que exige la Ley Orgánica de protección de datos lo es sobre el uso y destino de los datos personales va a estar relacionado con el principio general de consentimiento para el tratamiento de los datos,

pues si no se conoce su finalidad y los destinatarios, difícilmente podrá poder prestarse el consentimiento. Para apreciar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información, se debe tener en cuenta si es necesario o no el consentimiento al tratamiento de datos.

Pero la falta de exigencia de consentimiento podrá tener incidencia en la calidad de los datos, que vienen recogidos en la Ley Orgánica de Protección de Datos de 2018, como otro de los principios de la protección de datos (art. 4)[133]. Aquí, solo se necesitará el consentimiento del afectado cuando la finalidad del tratamiento de datos no sea el mantenimiento, desarrollo y control de la relación laboral (art. 4).

Uno de los argumentos diferenciadores con la doctrina anterior es el relativo a que ante la falta de cumplimiento del deber de solicitar al trabajador su consentimiento o el deber de información para el tratamiento de datos, solo supone una vulneración del derecho fundamental a la protección de datos tras ponderar la proporcionalidad de la medida que se adopta, pues como establece nuestro Tribunal Constitucional, ningún derecho fundamental es ilimitado, y tampoco lo va a ser el derecho a la protección de datos, encontrándose sus límites en los otros derechos fundamentales y bienes jurídicos constitucionalmente protegidos conforme al principio de unidad de la Constitución y, ello, aunque la propia Constitución no imponga expresamente límites específicos, ni expida a los poderes públicos para que los determine, como si ocurre con otros derechos fundamentales.

Utilizando la doctrina expuesta, el consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario (STC 292/2000). La STC 292/2000, de 30 de noviembre concluyó que el empresario no

---

133 Artículo 4. Exactitud de los datos.
1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados. 2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos: a) Hubiesen sido obtenidos por el responsable directamente del afectado. b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado. c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica. d) Fuesen obtenidos de un registro público por el responsable.

necesitaba haber recabado el consentimiento expreso del trabajador para el tratamiento de las imágenes obtenidas a través de las cámaras de videovigilancia instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trataba de una medida dirigida a controlar el cumplimiento de la relación laboral y era conforme con el poder de dirección establecido en el artículo 20.3 ET[134].

No obstante, como se ha adelantado, aunque la medida de vigilancia que implica el tratamiento de datos no precise del consentimiento sí que resulta necesario el deber de información recogido en el artículo 5 de la LOPD 5/1999. En relación con esta afirmación se debe entender que al margen de posibles sanciones que pudieran derivar por la falta de consentimiento, para que el incumplimiento de este deber por parte del empresario conlleve una vulneración del art. 18.4 CE[135] exige primeramente confirmar si se ha producido o no la expuesta falta de información debida y, en todo caso, valorar la observancia o no del principio de proporcionalidad.

En el apartado dedicado a la normativa y régimen jurídico se mencionaba la instrucción 1/2006 de la Agencia Española de Protección de Datos, la cual surgió con la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de la propia LOPD 15/1999 y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos. Esa adecuación se debe realizar (*ex* artículo 3 de la Instrucción) colocando en las zonas donde se hayan instalado dispositivos de videovigilancia, uno o varios carteles ubicados en lugar suficientemente visible, tanto en espacios abiertos como cerrados y, además, se debe tener a disposición de los interesados los impresos en los que se detalle la información prevista en el art. 5.1 de la LOPD 15/1999 (art. 3). El contenido y el diseño del cartel o distintivo se ajustará a lo recogido en el anexo de esta Instrucción, de acuerdo con la cual, el cartel deberá incluir una referencia a la Ley Orgánica 15/1999 de protección de datos, la finalidad para la se tratan los datos (zona videovigilada) y la identificación del responsable del tratamiento, ante

134 Artículo 20.3 ET; *"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"*.

135 Art. 18.4 Constitución Española, *"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".*

quien podrán ejercitarse los derechos a los que se refieren los arts. 15 y siguientes de la mencionada Ley Orgánica.

En el caso enjuiciado en la STC 292/2000, de 30 de noviembre, la empresa colocó el mencionado distintivo en el escaparate del comercio donde la trabajadora prestaba servicios, por lo que esta podía conocer la existencia de las cámaras y la finalidad genérica para la que habían sido instaladas (información genérica). En este sentido, concluye la sentencia que no es necesario especificar más que la mera referencia a la genérica "vigilancia" pues lo importante para poder valorar vulneración a la protección de datos, será determinar si los datos obtenidos se utilizaron para la finalidad de control de la relación laboral o para otro propósito, porque solo si la finalidad del tratamiento de datos no guarda relación directa con el control de la relación laboral el empleador estaría vulnerando la protección de los datos de carácter personal de los trabajadores.

En consecuencia, al entender que la trabajadora tenía información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo (cumpliendo el deber de información *ex* art. 5 LOPD), y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el derecho a la protección de datos de carácter personal (art. 18.4 CE).

La siguiente doctrina fue la consecuente de la STC 29/2013 (Universidad de Sevilla), donde se estableció la protección de datos de carácter personal como una barrera absolutamente infranqueable.

En este asunto la Universidad de Sevilla, existiendo serios indicios de que un trabajador no cumplía con su jornada laboral, utilizó una instalación de videovigilancia instalada en el campus con la finalidad del control de acceso de las personas para controlar su prestación de servicios. Gracias a las cámaras del campus, la Universidad pudo confirmar que el trabajador no cumplía con la jornada que se recogía en las hojas de control de asistencia.

Por lo tanto, se desprende que la Universidad no utilizaba videovigilancia para el control laboral (tampoco de la jornada), sino que utilizó un sistema ya existente de control de

accesos para de forma puntual (al trabajador sospechoso y durante un tiempo limitado) realizar esa labor de control del cumplimiento de la jornada.

El trabajador impugnó la sanción ante los Juzgados de lo Social, siendo desestimada la impugnación por el Juzgado de lo Social nº 3 de Sevilla, ratificada posteriormente por el Tribunal Superior de Justicia de Andalucía (Sede Sevilla).

Dichas resoluciones se basaron en la doctrina del Tribunal Constitucional emanada de la sentencia 186/2000, en la que, valorando el cumplimiento del principio de proporcionalidad, se permitía excepcionalmente un control oculto, sin, por tanto, conocimiento de los trabajadores ni de sus representantes por la existencia de serios indicios de actuaciones irregulares por parte de algunos trabajadores.

Sin embargo, tras el conveniente recurso de amparo por parte del trabajador, el Tribunal Constitucional resuelve el asunto dando relevancia al derecho a la protección de datos de carácter personal (art. 18.4 CE) y a la información previa que debió realizarse a los trabajadores en materia de tratamiento de datos personales, y no tanto al hecho de que la instalación oculta vulneraba el derecho a la intimidad (art. 18.1 CE).

Así, entendió que las acciones dirigidas a la seguridad y vigilancia "no deben contravenir el derecho a la protección de datos personales, el cual tiene pleno protagonismo en estos terrenos de la captación y grabación de imágenes personales que permitan la identificación del sujeto, máxime si existe un contrato de trabajo" (STC 29/2013, FJ 5). Este asunto enjuiciaba el asunto desde la óptica del derecho de los trabajadores a la información y, por tanto, trayendo a colación la STC 292/2000, y no las SSTC 98/2000 y 186/2000, que estudiaban el conflicto desde la perspectiva del derecho a la intimidad y el juicio de proporcionalidad. Lo justifica entendiendo que se trataban de supuestos diferentes (vigilancia auditiva en el puesto de trabajo con conocimiento de los trabajadores y de sus representantes en la STC 98/2000, y de grabaciones secretas de la actividad laboral en la STC 186/2000, a diferencia del presente, que versaba sobre la utilización de las grabaciones de imágenes para un fin distinto al expresamente divulgado) y que en la 98 y 186/2000 ninguna referencia se hacía al art. 18.4 CE. En relación con este artículo, se argumentó que la Constitución quiso garantizar mediante el mismo no

solo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto, la intimidad y la propia imagen (STC 292/2000).

Además, se realizó una comparativa entre el derecho a la intimidad y a la protección de datos, concluyendo que tienen distinta función, objeto y contenido. En concreto, entiende que el derecho fundamental a la intimidad del art. 18.1 CE tiene la función de proteger frente a las intromisiones en el 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 el contrario, el derecho fundamental a la protección de datos persigue garantizar un poder de control (uso y destino) sobre sus datos personales, con la finalidad de evitar un tráfico ilegal de datos que lesionen la dignidad y los derechos de los afectados, aunque indica que 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.

Siguiendo la doctrina de la STC 292/2000, que se ha expuesto con anterioridad, la STC 29/2013 declaró el derecho a conocer en todo momento quien tiene los datos personales y que uso está realizando de los mismos, como un complemento indispensable del derecho fundamental del art. 18.4 CE. De ahí, nace la necesidad del derecho del afectado a ser informado de quién tiene esos datos y para qué los tiene. Dicho derecho a la información operará incluso cuando exista habilitación legal para recabar los datos sin necesidad de consentimiento, pues una cosa es la necesidad o no de autorización del afectado y otra, el deber de informarle sobre quien tiene los datos y cuál será el propósito del tratamiento. Sin embargo, conforme a dicha doctrina la exigencia relativa al deber de información no puede ser absoluto, pues cabe concebir limitaciones por razones constitucionalmente admisibles y legalmente previstas[136].

[136] SSTC 57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero, FJ 2, y en relación con el derecho a la protección de datos personales, STC 292/2000, FFJJ 11 y 16, *"no debe olvidarse que la Constitución ha querido que la ley, y solo la ley, pueda fijar los límites a un derecho fundamental, exigiendo además que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido".*

Esta sentencia, aplicando la mencionada doctrina, concluyó que no había ninguna norma que permitiera la omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito laboral, ni tampoco podría sustentarse en el control de la actividad laboral a través de sistemas de tratamiento de datos no informados o sorpresivos de tratamiento. En este sentido, se argumentaba que, conforme a los artículos 5.1 y 2 LOPD, ni siquiera la Administración podía obtener de los ciudadanos información relativa a sus datos amparándose en el interés público de sancionar infracciones administrativas, por lo que en menor medida el interés particular del empresario podrá justificar que el tratamiento de datos sea empleado en contra del trabajador sin mediar información previa sobre el control laboral efectuado.

Se entendió que las imágenes que habían captado las cámaras de videovigilancia del campus universitario eran datos de índole personal y, en consecuencia, se estableció a la Universidad como responsable del tratamiento de los datos, por lo que el hecho de realizar un control mediante cámaras sin previamente informar al trabajador sobre esa finalidad de supervisión laboral vulneraba el derecho a la protección de datos personales del trabajador (art. 18.4 CE). Los carteles genéricos que anunciaban la instalación de cámaras y captura de imágenes en el campus no fueron suficientes para entender que se realizó una información conforme a la LOPD, pues no se trataba, a juicio del Alto Tribunal, una información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

Se concluyó que, a la vista de la falta de información previa se vulneraba el derecho a la protección de datos (art. 18.4 CE) y no era preciso examinar el tratamiento de datos personales desde otros enfoques, como el de la proporcionalidad, por lo que se anularon las resoluciones judiciales impugnadas.

Entendemos que la doctrina de la STC 29/2013 hace una interpretación excesivamente rigorista, toda vez que enaltece en exceso una imagen del trabajador mientras presta servicios y utilizada en exclusiva para el control empresarial, sin difundir la misma. Entendemos que se debe hacer una interpretación exigente, pero en el caso de la Universidad, utilizando unas cámaras ya instaladas para el control empresarial en zonas

con poca expectativa de privacidad (vestíbulos y zonas de paso públicos) y durante poco tiempo, se respetaba el juicio de proporcionalidad y, por tanto, debería ser suficiente para no entender conculcado el derecho a la protección de datos del trabajador o por lo menos, aunque inseparables ambas situaciones, no haber anulado la prueba de la grabación. Es decir, entendería razonable una sanción de la Agencia Española de Protección de Datos por vulneración del deber de información, pero este ilícito no debería conllevar la anulación de una prueba tan determinante, única con la que contaba la Universidad para probar los incumplimientos del trabajador.

Y con la STC 39/2016**,** de 3 de marzo de 2016 (Bershka), cambia de nuevo la doctrina entendiendo como válido a efectos de información el distintivo informativo genérico de "Zona videovigilada" regulado por la Instrucción 1/2006 de la AEPD.

En este caso, se juzgaba la instalación de una cámara de videovigilancia en una tienda cuyos responsables sospechaban que tanto en la tienda como en la caja se estaban produciendo diferentes irregularidades. La cámara de videovigilancia se instaló apuntando a la caja y sin previa comunicación a los trabajadores, aunque en el escaparate de la tienda, situada en un lugar visible, se colocaría el distintivo informativo genérico.

Las imágenes captaron a una trabajadora apropiándose de dinero en efectivo de la caja en diferentes fechas y de forma habitual, por lo que fue despedida. La trabajadora recurrió en amparo alegando vulneración de los arts. 14, 15, 18.1, 18.4 y 24 CE.

A pesar de los artículos abducidos por la trabajadora en su recurso, el Tribunal Constitucional solo enjuiciará los artículos 18.1 y 18.4 CE, y, por tanto, el derecho a la intimidad y el derecho a la protección de datos de carácter personal.

El tribunal comienza con el estudio del derecho a la protección de datos (art. 18.4 CE), recordando que la imagen se considera un dato de carácter personal, pues la vigente LOPD en su artículo 3 establecía como dato de carácter personal cualquier información concerniente a personas físicas identificadas o identificables, y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la

mencionada LOPD, considera en su artículo 5.1 f) como dato de carácter personal la información gráfica o fotográfica.

Al tratarse de un dato de carácter personal, se resalta por parte del tribunal la necesidad del consentimiento del afectado (trabajador) para la recogida y tratamiento de sus datos personales, y se concreta que el consentimiento del afectado es la clave del sistema de protección de datos de carácter personal, pues la propia LOPD establece el principio general de que el tratamiento de los datos personales solamente será factible si media el consentimiento de sus titulares, con la excepción de la existencia de habilitación legal para que los datos puedan ser tratados sin dicho consentimiento (STC 39/2016, FJ 16)[137].

En esa misma línea se recuerda que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa" (LOPD, art. 6.1).

Será también el propio artículo 6.2 LOPD[138] el que recoja las excepciones a la necesidad del consentimiento, haciendo mención expresa al ámbito laboral. En relación con las excepciones el Tribunal Constitucional entendió, con apoyo en el Reglamento que desarrolla la LOPD, que en las relaciones laborales el consentimiento del trabajador no es lo principal pues el consentimiento se entiende implícito en la propia relación laboral (también negocial y administrativa), siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento de la relación laboral pactada a través de un contrato.

Para el Alto Tribunal, la excepción del consentimiento solo se refiere a los datos necesarios para el mantenimiento y cumplimiento del contrato de trabajo, implicando las

---

[137] STC 39/2016, FJ 16 *"(…) es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es el quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias".*

[138] Art. 6.2 LOPD 15/1999, *" No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".*

obligaciones derivadas de la relación laboral. Por lo que si se realiza un tratamiento de datos dirigido al control de la relación laboral deberá entenderse amparado por la excepción citada, no siendo necesario el consentimiento del trabajador afectado, dado que está dirigido al cumplimiento de esa prestación de servicios. Sin embargo, sí será necesario el consentimiento del trabajador cuando los datos sean tratados con una finalidad diferente lo convenido en el contrato, aunque es cierto que esta finalidad no será fácil de determinar.

Sin embargo, a pesar de entender que no será necesario el consentimiento en los casos señalados, el tribunal entiende que el deber de información sigue existiendo, pues este deber de información permitirá al trabajador ejercer los derechos de acceso, rectificación y cancelación y, además, saber quién es el responsable del tratamiento, conforme al artículo 5 de la LOPD.

El deber de información es esencial para poder otorgar el consentimiento. Si se desconoce su fin y sus destinatarios, es difícil que se preste el consentimiento, convirtiéndose en un evidente complemento de la necesidad de consentimiento. Por ello, como establece el Tribunal Constitucional, al momento de determinar si existe vulneración del derecho a la protección de datos por inobservancia del deber de información, la excepción del consentimiento al tratamiento de datos en puntuales supuestos tendrá que tomarse en consideración por el estrecho vínculo entre el deber de información y el principio general de consentimiento.

Pero ¿Cuáles serán los datos que el trabajador afectado podrá ceder sin necesidad de consentimiento? El punto que recoge la calidad de los datos en la LOPD 15/1999, dará respuesta a esta pregunta, indicando que solo cuando la finalidad del tratamiento de datos no sea el mantenimiento, desarrollo y control de la relación contractual se necesitará consentimiento del trabajador afectado (LOPD 15/1999, art. 4).

En todo caso, para el tribunal, el incumplimiento del deber de solicitar el consentimiento del afectado para el tratamiento de datos o del deber de información previa solo podrá suponer la vulneración del derecho fundamental a la protección de datos si previamente se ha valorado la proporcionalidad de la medida adoptada.

Por tanto, aplicando dicha doctrina el Tribunal Constitucional entendió en este caso que no era necesario recabar el consentimiento expreso del trabajador para el tratamiento de las imágenes obtenidas a través de las cámaras de videovigilancia 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, por tanto, estaba amparado el poder de control y dirección recogido en el artículo 20.3 ET[139], reflejo de los artículos 33 y 38 CE. Es de entender para el Alto Tribunal que el consentimiento se encuentre implícito en la propia aceptación del contrato, que incluye el reconocimiento del poder de dirección del empresario.

De esta forma, la exigencia de "finalidad legítima en el tratamiento de datos" (LOPD, art. 4.1)[140], que se refiere a la calidad de los datos, se encuentra implícita, en lo relativo a cámaras de videovigilancia utilizadas para el control empresarial, en esa facultad de control que se reconoce al empresario en el artículo 20.3 ET, siempre que esas facultades se ejerzan dentro de su ámbito legal y no lesionen los derechos fundamentales del trabajador (principio de proporcionalidad)**.**

Conforme a esta doctrina, además de la dispensa de falta de consentimiento y de la necesidad de información, para que la aplicación de la medida sea legítima debe respetar el principio de proporcionalidad, descrito claramente, pues la relevancia constitucional de la falta de información en los casos de videovigilancia laboral exige una ponderación individualizada de los derechos y bienes constitucionales en conflicto, esto es, entre el derecho a la protección de datos del trabajador y el poder de dirección empresarial. (SSTC 186/2000, FJ 5 y 170/2013, FJ 3).

Como se estableció en la STEDH de 12 de enero de 2016, caso Barbulesco vs Rumania, esta potestad de control empresarial recogida en la legislación es lo que legitima el control empresarial del cumplimiento de las tareas por parte de los trabajadores, sin perjuicio de

---

139 Artículo 20.3 ET, *"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".*

140 Artículo 4.1 LOPD, *"los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".*

que serán las circunstancias de cada caso las que finalmente determinen si el control llevado a cabo por el empresario ha vulnerado un derecho fundamental.

La sentencia comentada, valora la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre vigilancia a través de sistemas de cámaras o videocámaras, entendiendo que dicha Instrucción nace de la necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos y, más concretamente, para ajustar los tratamientos de imágenes con fines de vigilancia a los principios de la LOPD y garantizar los derechos de las personas a los que se tomaron imágenes.

Finalmente concluye el Tribunal en el caso juzgado que como la empresa dispuso el oportuno distintivo en el escaparate de la tienda donde prestaba servicios la trabajadora despedida, la misma conocía la existencia de las cámaras y su fin. El distintivo informativo de videovigilancia estaba colocado conforme a la Instrucción 1/2006 de la AEPD[141] y, por tanto, se cumplió con la obligación de información previa. En este sentido, conforme a la Instrucción mencionada, el cumplimiento del deber de información se colma con la simple colocación del distintivo. En el presente caso, la trabajadora conocía que en la empresa había un control por videovigilancia y eso fue suficiente para entender por el Tribunal Constitucional la existencia de información previa, sin que fuera necesario concretar el tipo de sistema (cámaras ocultas o visibles) ni la finalidad del control (seguridad, control laboral, etc.).

Aplicando el principio de proporcionalidad en lo que respecta a la confrontación entre la instalación de la videovigilancia y los derechos fundamentales de los trabajadores, se concluye por el Tribunal que, una vez constatado la idoneidad, necesidad y proporcionalidad de la medida de instalación de las cámaras de videovigilancia en la tienda en la que la trabajadora prestaba sus servicios, enfocando únicamente a la caja y colocando un cartel visible en el escaparate, pudieron captar su imagen cuando se

[141] El Artículo 3, Ins. 1/2006 exige a los responsables que cuenten con sistemas de videovigilancia cumplir con el deber de información previsto en el art. 5 de la Ley Orgánica 15/1999, y a tal fin deberán "colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados" y "tener a disposición de los/las interesados impresos en los que se detalle la información prevista en el art. 5.1 de la Ley Orgánica 15/1999". El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el anexo de la Instrucción, según el cual, el distintivo deberá incluir una referencia a la Ley Orgánica 15/1999, de protección de datos, una mención a la finalidad para la se tratan los datos ("zona videovigilada") y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los arts. 15 y siguientes de la Ley Orgánica 15/1999.

apropiaba de dinero y realizaba, encubriendo su proceder, operaciones falsas de ventas y de devoluciones de prendas, por lo que fue despedida, y no se conculcó ningún derecho fundamental de la trabajadora, toda vez que esta tenía información previa de la instalación de cámaras de videovigilancia y las imágenes captadas para el control de la relación laboral.

Por tanto, la nueva doctrina del Tribunal Constitucional se ampara en mayor medida en la LOPD y en el art 20.3 del ET, y permite la videovigilancia con una información genérica, si dicha videovigilancia forma parte del control de la actividad laboral, entendiendo, además, que el consentimiento se presupone con la firma del contrato de trabajo.

En esta sentencia[142] el voto particular del magistrado Fernando Valdés Dal-Ré disintiendo de la decisión adoptada explica perfectamente el cambio de doctrina del Tribunal Constitucional sobre el derecho a la protección de datos de carácter personal en supuestos de videovigilancia laboral.

En relación con el voto particular, dicho magistrado critica primeramente la forma del cambio, es decir, la falta de motivación o como dice;

> "sin aportar la obligada argumentación jurídico-constitucional sobre las razones que conducen a abandonar una jurisprudencia cuyo objetivo, primero y esencial, fue el fijar los límites del contenido esencial del derecho fundamental que el art. 18.4 CE confiere a los trabajadores" (STC 29/2013).

Seguidamente, este magistrado valora la nueva doctrina como un retroceso en la protección de los derechos fundamentales de los trabajadores y que él mismo ha denunciado en los últimos años a través de una sucesión de votos particulares, revelando, según su opinión, una orientación tendente a vaciar de contenido sustantivo un modelo constitucional, *ex* art. 1.1. CE, de relaciones laborales acorde con el Estado social y democrático de Derecho (STC 29/2013).

[142] STC 29/2013, de 11 de febrero (Universidad de Sevilla).

Continua su argumentación relatando que la STC 292/2000, de 30 de noviembre, ya recogía que el derecho a la protección de datos (art. 18.4 CE) no era ilimitado y podía encontrar condicionantes en el resto de derechos fundamentales y bienes jurídicos constitucionalmente protegidos, en casos de un ejercicio ordinario y ajustado a Derecho por el empresario de las facultades empresariales que le reconocen el art. 20.3 ET; sin embargo, para el magistrado disidente la nueva corriente doctrinal lo hace incluso cuando el poder empresarial ejercitado incurre en incumplimientos legales.

Para este magistrado, las facultades de vigilancia y control empresarial de la actividad laboral que regula el Estatuto de los Trabajadores conforman una fuente constitucional desde la que puede surgir un conflicto con los derechos fundamentales de los trabajadores, "con el efecto consiguiente de conducir la solución del recurso planteado a una lógica ponderativa sometida al principio de proporcionalidad" (STC 29/2013). A su juicio, basándose en la STC 88/1985 [143], entiende que:

> "el artículo 20.3 ET es solo una regla jurídica rectora de la relación contractual y por tanto, no es un parámetro de constitucionalidad que limita los derechos fundamentales en la empresa, ni tampoco los poderes o facultades empresariales son, sin excepción y de manera universal, expresiones directas e indefectibles de los arts. 33 y 38 CE que se deban ponderarse de manera mecánica con los derechos fundamentales de los trabajadores, ni las facultades del empresario y, menos aún si se ejercen de modo irregular o desviado, pueden restringir los derechos fundamentales de los trabajadores, especialmente, los recogidos en el artículo 18 CE".

Después, el magistrado realiza una crítica al juicio de proporcionalidad aplicado en la sentencia. En primer lugar, entiende que se ha antepuesto "de manera anómala" un nuevo juicio, de justificación, al triple juicio clásico de proporcionalidad (idoneidad, necesidad

[143] STC 88/1985, de 19 de julio, *"ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad ni la libertad de Empresa que establece el art. 38 del texto constitucional legitima el que quienes prestan servicios en aquéllas por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico constitucional. Las manifestaciones de 'feudalismo industrial' repugnan al Estado social y democrático de Derecho y a los valores superiores de libertad, justicia e igualdad a través de los cuales ese Estado toma forma y se realiza (art. 1.1)".*

y equilibrio), por lo que se ha generado una "inmediata confusión sobre el único canon que la propia resolución maneja" y, porque el juicio de necesidad que se efectúa acredita para este juzgador que la medida no era la menos invasiva de las posibles, al entender que podría haber sido menos agresiva para los derechos fundamentales del art. 18 CE, e igualmente eficaz para controlar la actividad desarrollada por el trabajador, que la grabación se hubiera llevado a cabo con información de la finalidad laboral destinada, y que su verdadero fin no era realmente el asegurar el cumplimiento de la actividad laboral, sino, obtener una prueba de las irregularidades.

Para este magistrado el debate constitucional de ponderación de derechos no es tal, pues solo se trata de un pretendido derecho a obtener pruebas para efectuar un despido con fundamento en el art. 20.3 LET y, por tanto, en los derechos a la propiedad y a la libertad de empresa (arts. 33 y 38 CE), objetivo conseguido a costa de la anulación de los derechos fundamentales del trabajador.

Al respecto, no compartimos dichas afirmaciones, pues como ya es cuestión pacífica entre la doctrina y se ha abordado a lo largo de esta tesis, ningún derecho fundamental es ilimitado y tampoco lo son los recogidos en el art. 18 CE. Además, la sentencia justifica sobradamente la existencia de información previa a través del distintivo genérico, pues era evidente para todos (y también para la trabajadora despedida) la existencia de cámaras de videovigilancia, que el consentimiento para el tratamiento de los datos se incluye en el contrato de trabajo, y también se justifican los motivos que llevan a entender que la medida de la videovigilancia cumplía con el principio de proporcionalidad, al margen de que evidentemente la medida se tomara para obtener pruebas, pues de lo contrario, no se hubiera utilizado la videovigilancia. De la misma forma, no podemos estar de acuerdo con este magistrado cuando dice que si la grabación se hubiera llevado a cabo con información del fin laboral al que se procuraba podría haber sido menos agresiva para los derechos fundamentales e igualmente eficaz para controlar la actividad laboral, pues entendemos que el magistrado confunde la forma de llevar a cabo la grabación, a través de una cámara que solo enfocaba la caja (juicio de necesidad), con la información previa. Es cierto, que se podría haber informado de forma más concreta, pero eso entendemos que no formaría parte del juicio de necesidad, sino del deber de información, superado

con el cumplimiento de las exigencias de la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre vigilancia a través de sistemas de cámaras o videocámaras.

De manera más clara pronuncia su voto particular el magistrado Juan Antonio Xiol Ríos, que critica la sentencia estudiando el derecho a la protección de datos en relación con el deber de información. En relación con la información, este magistrado pondera, si la misma debe facilitarse a los trabajadores especificando el fin de ese control de cumplimiento de la relación laboral; o si, el deber de información se cumple suficientemente mediante un anuncio hecho al público sobre la existencia de cámaras de seguridad en el establecimiento, como se ha establecido en la sentencia.

Apoyándose en la sentencia STC 29/2013 que, como hemos visto, establece la doctrina de que el deber de información vinculado a la instalación de cámaras de vigilancia en el establecimiento laboral debe concretar la finalidad de control de la actividad laboral, entiende que los precedentes que se indican en la sentencia como concluyentes, en especial la STC 292/2000, no son suficientes para justificar el fallo de la sentencia, pues en aquel se tratan de hallazgos casuales por las cámaras instaladas legalmente por razones de seguridad, mientras que en el presente caso se trata de una cámara dirigida específicamente a posiciones que ocupan los trabajadores para investigar determinados hechos. Además, entiende que los argumentos citados en la STC 292/2000 están obsoletos, pues son de hace 15 años y se fundaban en el derecho a la intimidad más que en el derecho a la protección de datos y en ese tiempo, además, se han dictado otras sentencias por el TEDH como la de 28 de enero de 2003, Peck c. Reino Unido, y 17 de julio de 2003, Perry c. Reino Unido.

Concluye el voto particular alegando que podría aceptar una información dirigida a los trabajadores que no especifique el fin concreto de vigilancia, pero nunca aceptaría que la información dirigida al público sea suficiente para cumplir el requisito de la información a los propios trabajadores, puesto que el art. 5 de la LOPD ordena, de una forma clara y específica, que la información se dirija a los interesados (en este caso, a los trabajadores), configurando con ello el contenido esencial del derecho, aunque podría haber considerado la justificación de la instalación de la cámara si se hubiese notificado, al menos, al comité de empresa para “evitar la frustración de la vigilancia” (en la línea, de la Sentencia del

Tribunal Superior de Justicia de la Comunidad de Madrid de 9 de febrero de 2015). En este sentido, considera que se ha dinamitado el contenido esencial del derecho fundamental a la protección de datos el hecho de admitir en la sentencia, que el empresario, ante cualquier sospecha que pueda abrigar, pueda instalar libremente (con carteles genéricos de aviso al público sobre la existencia de cámaras de seguridad) cámaras para el control del trabajo orientadas a determinadas posiciones ocupadas por los trabajadores.

Al contrario que estos magistrados, no me parece irrazonable el cambio de doctrina la cual, hasta este momento, y sobre todo con la STC 292/2000, era excesivamente proteccionista con el trabajador y limitaba notablemente el control empresarial bajo el sustento de la protección de datos. La razón de ser de una cámara oculta se encuentra en ser utilizada sin el conocimiento de los trabajadores, pues de lo contrario y en muchos casos, no sería posible coger "infraganti" al trabajador que comete una irregularidad y que no puede probarse de otra manera, pues evidentemente, lo que se busca con este tipo de actuación empresarial es acreditar, probar los hechos en un ulterior juicio. En este sentido, recordamos que el juez debe impartir justicia y para ello debe conocer la verdad y la grabación de una cámara a menudo no servía para ello, pues se entendía que la grabación era ilícita y, por lo tanto, nula e inservible para acreditar irregularidades cometidas por los trabajadores. No obstante, el juicio de proporcionalidad debe respetarse en todos los casos de videovigilancia, pero en mayor medida y con mayor rigor cuando se traten de cámaras ocultas.

En este contexto ha resuelto el Tribunal Superior de Justicia con sede en Málaga en su reciente sentencia de 20 de mayo de 2020, donde se trataba el caso de la residencia La Milagrosa. En este caso, se juzgaban 16 despidos a los trabajadores de la residencia una vez comprobadas las grabaciones de cámaras ocultas instaladas en el centro de trabajo por un detective privado y en las que se constata que varios trabajadores maltrataban y vejaban a residentes discapacitados. Al igual que en los casos comentados en esta tesis, el debate jurídico inicial no estará en los comportamientos de los trabajadores que se reflejan en las grabaciones, sino en la validez como prueba de estas, y en este caso, el Juzgado de lo Social no admitió como prueba las grabaciones pues no se había informado

a los trabajadores de la instalación de las cámaras, y ello vulneraba sus derechos fundamentales, aunque sin concretar cuáles.

En el presente caso, la residencia, dada cuenta la existencia de indicios de desatención y conductas de estrés inexplicables por parte de los usuarios de la residencia, procedió a la contratación de un detective privado para la instalación de cámaras ocultas de videovigilancia, no figurando cartel o aviso alguno de zona vigilada por cámara, ni comunicación a los trabajadores o sus representantes legales, ni tampoco su consentimiento.

En un primer momento, apoyándose en la sentencia de la Sala de lo Social del Tribunal Supremo de 1 de febrero de 2017, que se remite a la sentencia del Tribunal Constitucional de 39/2016**,** de 3 de marzo de 2016 (Bershka), aquí comentada, y de la sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2019, el Juzgado de lo Social de Málaga llega a la conclusión de que como no se comunicó a sus trabajadores, y a los representantes de los mismos, de forma explícita de la instalación de cámaras, ni se puso distintivo alguno de la existencia de estas ni de la zona que las mismas vigilaban, y además, las cámaras no eran perceptibles de manera notoria, y no constaba el consentimiento de los trabajadores a su instalación, ni que su instalación fuese dirigida a controlar la actuación de trabajadores concretos, ni que su instalación fuese a ser limitada en el tiempo, denegó la práctica de dicha prueba al no superar el principio de proporcionalidad exigido en las referidas sentencias ni concurrir los requisitos exigidos en las mismas.

Sin embargo, como ya se ha comentado en esta tesis, la jurisprudencia en la que se apoyaba fue modificada por la sentencia López Ribalda II de la Gran Sala, lo cual sirvió al Tribunal Superior de Justicia de Andalucía con sede en Málaga para admitir la prueba y, por tanto, apreciar nulidad de actuaciones. En este sentido, se entiende que cuando la empresa acredita la concurrencia de razones legítimas y de peso para recurrir, como medio más apropiado, a la instalación de cámaras sin el cumplimiento de la obligación de información previa (garantía de transparencia) a los trabajadores, para con ello averiguar si los empleados realizan el ilícito, no vulnera su expectativa de privacidad (ex artículo 8 del Convenio Europeo de Derechos Humanos).

Se concreta que, para juzgar la licitud de la actuación empresarial se debían valorar otros aspectos como las firmes y contundentes sospechas empresariales referentes a la comisión de graves irregularidades por diversos empleados, la imposibilidad racional de proceder eficazmente a la averiguación de tales comportamientos en el caso de comunicar previamente a los empleados la instalación de tales sistemas de vigilancia, la gravedad de los comportamientos detectados, que las sospechas vinieran referidas a la actuación de varios empleados, la necesidad de adoptar tales medidas de averiguación para llevar a cabo una adecuada protección de los usuarios y residentes del centro (discapacitados), y que la medida tomada por la empresa resultaba proporcionada y amoldada a la finalidad de garantizar la reputación de la empresa. Por ello, se entendió que el rechazo de la prueba de las grabaciones estaba injustificado y se dictamino nulidad de actuaciones.

Como novedad de esta sentencia cabe resaltar la justificación que se dió para la instalación de cámaras ocultas por la imposibilidad racional de proceder eficazmente a la averiguación de tales comportamientos caso de comunicar previamente a los empleados la instalación de tales sistemas de vigilancia. Es decir, se entiende que, si se comunica a los trabajadores incumplidores de la instalación de cámaras de videovigilancia oculta, se perderá el carácter sorpresivo de la ocultación y, por tanto, no se podrá sorprender “in fraganti” a los mismos, beneficiando a los incumplidores al prevenirles de la ocultación.

Recientemente se ha dictado sentencia por el Tribunal Supremo, de fecha 21/11/2021, donde se avala el uso de grabaciones para el despido de un conductor de autobús que dejaba viajar sin billete a una mujer y la realizaba tocamientos mientras conducía. En el autobús se habían instalado tres cámaras que grababan su interior, excepto el asiento del conductor, y todos los trabajadores conocían de su existencia, pues existían distintivos informativos genéricos dirigidos al público que advertían de la presencia de cámaras.

En este caso, el Tribual Supremo entendió justificada la limitación de derechos fundamentales, pues instalar cámaras de videovigilancia en el autobús era una medida "justificada" por razones de seguridad en un sentido amplio, en el que se incluye el control de la actividad laboral, por la naturaleza del trabajo del conductor, con los riesgos que supone para él y para los usuarios. También entiende que estas cámaras son "idóneas"

para detectar a posibles infractores y proceder a la sanción de sus conductas; "necesarias", por la ausencia de otros medios de menor tenor intrusivo para alcanzar el propósito; y "proporcionadas" al objetivo, por lo que satisfacen la proporcionalidad, sin detrimento de eventuales responsabilidades empresariales por parte de la Agencia Española de Protección de Datos, por las infracciones que posiblemente se hubiesen cometido en cuanto a lo dispuesto sobre la protección de datos.

Como se adelantaba, el Alto Tribunal concluyó que el trabajador tenía conocimiento de que se había instalado un sistema de control por videovigilancia a través del correspondiente distintivo genérico informativo por lo que no era necesario especificar la finalidad concreta de esa cámara. El conductor sabía que estaba siendo grabado cuando realizó las conductas reprochadas delante de las cámaras de grabación.

6.6.2. Jurisprudencia TEDH.

El proceso denominado como López Ribalda contra España en el que varias trabajadoras de Mercadona fueron despedidas por sustraer unos productos de un supermercado, usando la captación de imágenes para ello, es el mejor ejemplo de la evolución jurisprudencial vacilante del uso de las cámaras de videovigilancia para el control empresarial y la vulneración de los derechos fundamentales.

Los hechos se remiten al año 2009, cuando cinco trabajadoras de la empresa Mercadona en Barcelona fueron despedidas después de que la cadena de supermercados las grabara hurtando distintos productos y ofreciendo ayuda a otros para hurtar. De forma previa, la compañía instaló cámaras en determinados puntos para evitar hurtos de clientes, las cuales fueron informadas debidamente a los empleados con su ubicación exacta. Aunque, ante las diferencias existencias y ventas, con pérdidas en existencias de hasta 24.614 euros mensuales, otras cámaras se colocaron ocultas, con el fin de registrar posibles hurtos por parte de los empleados, y de ellas no se les informó. Las cámaras ocultas desvelaron que las cajeras escaneaban los productos de las cestas y seguidamente los anulaban, permitiendo a conocidos de ellas dejar la tienda llevándose productos por los que no

habían pagado. Las trabajadoras fueron llamadas a diferentes reuniones individuales donde se les mostraron los videos y tras admitir su participación en los hurtos, con presencia de los representantes sindicales y de la empresa, fueron despedidas por razones disciplinarias.

El Juzgado de lo Social nº 1 de Granollers dictó sentencia en fecha 20/1/2010 declarando los despidos como procedentes al entender la existencia de "infracción de la buena fe contractual, y un abuso de la confianza" en la conducta de las trabajadoras. Las principales pruebas en las que se basó para acreditar la procedencia de los despidos fueron las grabaciones de las cámaras ocultas y las declaraciones de testigos, entre los que estaban otros trabajadores, el delegado sindical y el representante de la empresa. Dicha sentencia, siguiendo la doctrina del Tribunal Constitucional en sentencia 186/2000 de 10 de julio de 2000, entendió que el uso de cámaras ocultas en el lugar de trabajo sin previo aviso a los trabajadores estaba en concordancia con el artículo 20 del ET, el cual permite al empleador utilizar todos los medios de vigilancia que considere oportunas para el control laboral de los trabajadores, siempre y cuando se respete la dignidad humana**.** Y ello, en base a la mencionada doctrina del Tribunal Constitucional, porque existía una sospecha sustancial de robo, circunstancias especiales que justificaron la injerencia en el derecho a la privacidad de un empleado, considerándose apropiado en lo que se refiere al objetivo legítimo buscado, necesario y proporcional.

Las trabajadoras recurrieron ante el Tribunal Superior de Justicia de Cataluña, dictándose sentencias el 28 de enero y el 24 de febrero 2011 por las cuales se ratificaban las sentencias dictadas por el Juzgado de lo Social, haciendo referencia a la mencionada jurisprudencia del Tribunal Constitucional, en el sentido de que la empresa estaba autorizada a realizar la videovigilancia encubierta de las cajas y que esta actuación fue justificada (al existir una sospecha razonable de robo), apropiada para el fin deseado, necesaria y proporcional.

Con posterioridad, las trabajadoras interpusieron sendos recursos de casación, que se declararon inadmisibles el 5 de octubre de 2011 y 7 de febrero de 2012 respectivamente. Después, las trabajadoras interpusieron recursos de amparo ante el Tribunal

Constitucional, los cuales también se inadmitieron el 27 de junio y 18 de julio de 2012 respectivamente, debido a la inexistencia de una violación de un derecho fundamental.

Por último, se interpusieron las demandas 1874/13 y 8567/13 contra el Reino de España interpuestas ante el Tribunal Europeo de Derechos Humanos en virtud del artículo 34 del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales por parte de las trabajadoras.

En consecuencia, en el denominado caso López Ribalda y otros contra España, el 9 de enero de 2018 se dictó sentencia por el TEDH en la que se reafirmaba el criterio sostenido en la sentencia anterior de 5 de septiembre de 2017 dictada por la Gran Sala TEDH (Barbulescu II). En ella, seis de los siete magistrados que integran el Tribunal condenaron a España por vulneración del artículo 8 del Convenio Europeo de Derechos Humanos (CEDH, sobre el derecho a la vida privada), al entender que la videovigilancia llevada a cabo por el empresario, que se desarrolló durante un periodo prolongado, no cumplió con las exigencias previstas en el art. 5 de la Ley Orgánica de Protección de Datos 15/1999, en particular, con la obligación de informar, previa, explicita y precisamente, sin ambigüedades, a los interesados sobre la exigencia y características particulares de un sistema de captación o recolección de datos personales, así como de las características especiales del mismo (cámaras ocultas).

En este punto, tal y como hizo el TEDH recordamos la normativa al respecto recogida en el Convenio Europeo de Derechos Humanos:

- “Todos tienen el derecho a que se respete su vida privada y familiar, así como su casa y correspondencia” (CEDH, art. 8.1).
- “Las autoridades no interferirán en el ejercicio de este derecho, excepto en lo que dicte la ley y cuando sea necesario en una sociedad democrática en interés de la seguridad nacional o pública o el bienestar económico del país, para la prevención del desorden o la ilegalidad, así como la salud o la moralidad, o para la protección de los derechos y libertades de otros” (CEDH, art. 8.2).

Considera el TEDH que los derechos del empleador podrían haberse satisfecho si se hubiera informado previamente a las demandantes, incluso de forma general, de la

instalación de un sistema de video vigilancia y proporcionándoles la información prevista en el artículo 5 de la Ley Orgánica de Protección de Datos de Carácter Personal. Es decir, las trabajadoras sabían que se instalaron cámaras en el supermercado para investigar posibles hurtos después de que el gerente notara descuadres entre existencias y ventas, pero también se instalaron cámaras ocultas, de las cuales no se informó a los trabajadores.

Por ello, el TEDH concluyó en este caso que los tribunales españoles no fueron capaces de establecer un equilibrio justo entre los derechos de las trabajadoras al respeto a su vida privada (conforme al Artículo 8 del CEDH) y el interés del empleador en la protección de sus derechos a la propiedad.

No obstante, este Tribunal falló por unanimidad la no vulneración del derecho a un juicio justo (art. 6 CEDH) porque las grabaciones ocultas no fueron la única prueba de la que se valieron los tribunales españoles para acreditar los hurtos, pues entre otras, contaron con diferentes declaraciones de testigos, y porque las propias trabajadoras afectadas tuvieron amplias oportunidades para impugnar tanto la autenticidad como el uso del material obtenido a través de los dispositivos a lo largo de todo el procedimiento judicial, y además, juzgados y tribunales abordaron sus objeciones a este respecto.

El 28 de mayo de 2018 el Panel de la Gran Sala aceptó una solicitud del Gobierno de España para que se remitiera el caso a la Gran Sala. Se celebró una audiencia el 28 de noviembre de 2018, y como consecuencia, el 17 de octubre de 2019 se dictaba una nueva sentencia, esta vez por la Gran Sala del TEDH, que contradijo la sentencia anterior.

En esta última sentencia, la Gran Sala ha entendido, catorce votos contra tres, que no ha habido ninguna violación del artículo 8 (derecho al respeto de la vida privada y familiar) del Convenio europeo sobre Derechos humanos y por unanimidad, que no hubo violación del Artículo 6 (derecho a un juicio justo).

Esta sentencia que rectifica el fallo de la sentencia de enero de 2018 relativo a la vulneración del derecho a la vida privada, se realiza en el mismo sentido que el voto particular efectuado por el Juez Dedov dela Sala del TEDH en la misma, el cual entendió que iba en contra de la anterior jurisprudencia del TEDH en casos como Barbulescu o

Köpke, siendo en este último caso la injerencia más grave al tratarse de un asunto que juzgaba la existencia de cámaras ocultas únicamente y el empleado no había sido informado en ningún momento de ninguna vigilancia.

Sin embargo, el Tribunal en este caso consideró infundada la denuncia. En la decisión de Köpke, el Tribunal aceptó la opinión de los tribunales nacionales de que no había otro medio igualmente eficaz para proteger los derechos de propiedad del empleador que hubiera podido interferir en menor medida con el derecho del demandante al respeto de su vida privada.

En relación con el presente caso, el TEDH indica que las cámaras de videovigilancia ocultas se instalaron en espacios públicos, y no privados y, además, la empresa utilizó los registros de ambos tipos de cámaras (ocultas y visibles) como pruebas de la comisión de un delito. Por lo tanto, las cámaras visibles también fueron necesarias para poder entender como se había organizado el hurto. De la misma forma, entendió que a pesar de que los empleados no habían sido informados sobre la vigilancia, la propia existencia de las cámaras, las cuales eran visibles, suponía y demostraba que un sistema de videovigilancia había sido instalado por el empresario, por lo que no se podía decir que los empleados no habían sido informados al respecto. Asimismo, entendió que el mero hecho de que las trabajadoras no hubieran podido anticipar que serían vigiladas en los lugares donde habían almacenado los artículos hurtados, no generaba una violación de derechos. Por último, entendió el tribunal que la decisión de adoptar medidas de vigilancia se había basado en una sospecha frente a todo el personal y que las pérdidas identificadas por la gerencia de la empresa habían sido de importantes cuantías (entre unos 8.000 y 25.000 euros al mes) para un supermercado minorista, donde los artículos individuales no eran demasiado caros, y las pérdidas aumentaban constantemente conforme pasaba el tiempo, por lo que podría razonablemente concluirse que las pérdidas podrían no haber sido causadas por una sola persona. Por todo ello, se determinó que no se podía concluir que la vigilancia fuera innecesaria, pues el único lugar donde se podían esconder los objetos hurtados era tras las cajas registradoras.

En su opinión, los medios utilizados por la empresa y, por tanto, las sentencias dictadas por los tribunales españoles no se consideraron abusivas, arbitrarias o desproporcionadas.

En el presente caso, se utilizó el pretérito principio por el cual los demandantes no deberían tener la posibilidad legal de beneficiarse de su propio delito (véase Riggs v. Palmer, 1889).

Volviendo a la sentencia propiamente dicha de la Gran Sala, esta justifica el cambio de doctrina indicando que aunque no quepa aceptar, con carácter general, que las meras sospechas de que las empleadas estuvieran cometiendo un delito justifiquen la instalación de cámaras encubiertas, la existencia de fundadas sospechas de que se ha cometido una infracción grave con pérdidas importantes en los bienes de la empresa, sí justificaría suficientemente las acciones de la empresa.

Y en el presente caso, como se justifica, el buen funcionamiento de la empresa estaba en riesgo no solo por la sospecha del mal comportamiento de un solo empleado, sino por la sospecha de una acción concertada por parte de varios empleados, lo que evidentemente generaba una atmósfera general de desconfianza en el centro de trabajo.

Concluye la Gran Sala, que a pesar de tratarse de grabaciones efectuadas con cámaras ocultas la privacidad de las trabajadoras no fue vulnerada, puesto que las grabaciones estaban justificadas por la sospecha fundada de hurto por parte de varios trabajadores y la cuantía de las pérdidas y, además, entiende que la empresa cumplió con el principio de proporcionalidad, pues concluye que solo se produjeron durante unos días y, en ningún caso, no fueron difundidas.

Explica, además, que la expectativa de privacidad que un empleado puede esperar en un lugar de trabajo tiene diferentes grados: elevado en baños y vestuarios, donde no es posible realizar una vigilancia, pudiéndose incluso eliminar; fuerte en los despachos y manifiestamente reducida en lugares visibles o accesibles a los compañeros de trabajo o al público en general, como es el caso del área de cajas en un supermercado.

Por ello, la sentencia falló que la intromisión en la vida privada de las trabajadoras no tenía un alto grado de gravedad, y que estas podían haber recurrido a la Agencia de Protección de Datos o presentar una reclamación ante los tribunales por sus derechos según la Ley de protección de datos y, sin embargo, no hicieron uso de ello.

Por lo tanto, la Gran Sala da un nuevo giro volviendo a la que había sido doctrina general, concretada en los asuntos Köpke y Bărbulescu II.

Desde luego estamos más cerca de la rectificación efectuada por la Gran Sala en esta sentencia de 17/10/2019 o del voto particular del Juez Dedov de la Sala del TEDH, pues estamos hablando de una cámara oculta instalada en el centro de trabajo, en lugares accesibles al público en general, como son las cajas, con la finalidad de vigilar a unos trabajadores por serias y fundadas sospechas frente a toda la plantilla (pérdidas importantes consecutivas durante varios meses y en aumento). Es cierto que se prolonga en el tiempo, lo que sirvió al TEDH para entender la vulneración de la privacidad en la sentencia de enero, pero también es cierto que es un medio idóneo para "pillar infraganti" a las trabajadoras y que la dificultad probatoria con otro medio era evidente.

Es necesaria la evolución jurisprudencial, pero lo cierto es que estos vaivenes jurisprudenciales dictados por el mismo Tribunal (aunque en diferentes Salas), generan una importante inseguridad jurídica.

En relación con esta inseguridad jurídica, esta sentencia de la Gran Sala llegó casualmente en el momento que nuestro Tribunal Constitucional prohíbe, como regla general, la vigilancia por cámaras ocultas en su sentencia de 25 de febrero de 2019. No obstante, es cierto que la mencionada sentencia del Tribunal Constitucional aborda la videovigilancia y la intimidad desde una perspectiva diferente al control empresarial, pues no confronta el derecho a la intimidad y el control empresarial, sino el derecho a la intimidad y la libertad de prensa o información. Y en este caso, se concluye que la Constitución Española excluye, por regla general, la utilización constante de cámaras ocultas, puesto que constituye una grave intromisión ilegítima en los derechos fundamentales a la intimidad personal y a la propia imagen de los trabajadores, aunque su utilización "podrá excepcionalmente ser legítima cuando no existan medios menos intrusivos para obtener la información" (STC 25/2/2019). Asimismo, aunque sin relevancia en el ámbito laboral, en materia de difusión de imágenes y libertad de información, concluye que esta solo alcanza a la información de relevancia pública, y que además, los medios de comunicación social que difundan imágenes obtenidas mediante cámaras ocultas deberán

distorsionar el rostro y la voz de las personas grabadas cuando su identificación no sirva al interés general de la información, y tampoco se podrán difundir imágenes que pudieran menoscabar innecesariamente la reputación de las personas.

Otra sentencia interesante, aunque quizás no tan relevante, fue la sentencia del TEDH de 28 noviembre 2017 en el caso Antović and Mirković. En esta sentencia, dictada después de Barbulescu II, se estudiaba el caso sucedido en la Universidad de Montenegro, cuando el decano de la Facultad de Matemáticas informó a los profesores, que se había instalado una cámara de videovigilancia en siete aulas en las que se impartían clases. En la comunicación se informaba de que el propósito consistía en garantizar la seguridad de las personas y de sus bienes, incluidos los estudiantes, y en la vigilancia de la docencia. A pesar de recoger que los datos recogidos se protegerían por unas claves solo conocidas por el decano y que se almacenarían durante un año, el TEDH entendió que se había violado el artículo 8 del Convenio, pues la supervisión de la docencia no estaba incluida en la ley de Montenegro como uno de los motivos que justificaban la videovigilancia. Por lo que, si no se cumplía la exigencia de que la restricción se encontrase contemplada en una la ley, vulneraba el artículo 8 del Convenio.

6.6.3. Conclusiones.

A la vista de la jurisprudencia relatada se puede concluir que existen dos doctrinas para tratar el asunto del control empresarial a través de cámaras de videovigilancia, la que pondera el derecho al control laboral del empleador con del derecho fundamental a la intimidad y la que lo hace con el derecho fundamental a la protección de datos de carácter personal. La primera, asentada en la actualidad, valorará con menor incidencia la información previa a los trabajadores y el consentimiento para el tratamiento de datos y en mayor medida al juicio de proporcionalidad, y la segunda, dará más relevancia a lo establecido en la Ley Orgánica de Protección de Datos en materia de información previa.

Por otra parte, a la hora de emitir cualquier tipo de conclusión al respecto, se debe tener en cuenta las diferentes formas de llevar a cabo la videovigilancia, es decir, la realizada a través de cámaras ocultas, donde la confrontación entre derechos del trabajador y

empresario serán más delicados, y la realizada con cámaras visibles, cuya incidencia en los derechos del trabajador será menor.

A la vista del camino doctrinal y jurisprudencial recorrido, se puede concluir que en esta materia de control empresarial, al existir la posibilidad de una limitación de derechos fundamentales, debe prevalecer el principio del equilibrio de derechos constitucionales[144], el cual vendrá exigido por una necesaria información previa al empleado de dicho control, y, por la superación del denominado juicio de proporcionalidad en el ejercicio del control empresarial, acuñado por el Tribunal Constitucional.

Para superar el test de proporcionalidad será necesario cumplir las cuatro condiciones exigidas para considerar si el sistema de vigilancia utilizado por el empresario para efectuar el control de sus trabajadores es adecuado y no excesivo para la satisfacción de los objetivos e intereses empresariales:

1. Que la medida sea idónea, es decir, que sea susceptible de conseguir el objetivo propuesto de controlar la actividad laboral y/o incumplimientos del trabajador. En este sentido, será idónea cuando se utilice para verificar si algunos trabajadores cometían las irregularidades sospechadas y poder adoptar las medidas disciplinarias pertinentes, pero no cuando se utilice para monitorizar la normal prestación de servicios.

2. Necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia. La necesidad va íntimamente relacionada con la prueba, es decir, será necesaria cuando las dificultades probatorias de los hechos hagan indispensable el uso de las cámaras y sin embargo, no lo será y resultará abusiva si se podría probar los hechos con medidas menos agresivas.

144 MIRÓ MORROS, D. y CRUZ DE PABLO, M. (2014). El uso de la video vigilancia en el ámbito laboral. *Actualidad Jurídica Aranzadi*. Nº 891/2014.

3. Ponderada o proporcional, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. Será proporcional cuando se utilice durante un tiempo limitado, enfocando a los trabajadores sospechosos y no a todos los trabajadores, o vaya dirigidos a captar las imágenes en lugares con expectativas de privacidad débiles. Por otra parte, no será proporcional y se entenderá excesiva si las cámaras se dirigen a todos los trabajadores o se filma en lugares con expectativas altas de privacidad, como aseos o vestuarios, si lo que se perseguía eran unos hurtos realizados en la caja.

4. Y, que sea justificada, esto es, si existen razones objetivas y motivadas que legitimen la decisión de control empresarial. Estará justificada cuando existan serías o razonables sospechas de graves irregularidades, perjuicio patrimonial del empresario y no lo estará y resultará excesiva cuando no existan sospechas ni datos objetivos que puedan sustentar la utilización de una medida tan invasiva como las cámaras de videovigilancia.

Y ello se establece porque los derechos fundamentales no son absolutos y porque su ejercicio se debe ponderar en atención a las circunstancias que concurren en cada supuesto, sobre todo cuando entran en colisión con otros derechos que también merecen la protección del ordenamiento jurídico.

En relación con la doctrina estudiada a lo largo de este artículo surgen una serie de cuestiones prácticas que se resuelven a continuación:

La primera cuestión es clara, ¿Es posible la utilización de videocámaras para realizar el control empresarial?

Después del estudio realizado en este artículo, evidentemente, la respuesta es sí, pero precisa de varias puntualizaciones. Se podrá utilizar siempre y cuando sea necesario y esté justificado. Es decir, que no haya otra forma o esta sea muy compleja para probar los hechos (incumplimientos del trabajador).

Sin embargo, esta respuesta es la genérica y se aplica a las cámaras de videovigilancia visibles, pues si lo que se plantea es la posibilidad de una cámara oculta, esta precisará, además, de la existencia de un daño importante. Por tanto, para instalar una cámara oculta, previamente debe existir un daño importante, que no pueda ser solucionado o probado por otro medio de prueba. Asimismo, y volviendo a la expectativa de privacidad explicada en este artículo, las cámaras ocultas no se podrán instalar en espacios privados, como aseos o vestuarios.

A la instalación y uso de cámaras ocultas, no afecta la siguiente puntualización relativa al uso de cámaras de videovigilancia, pues de lo contrario mermaría el carácter sorpresivo de las anteriores, como es la información previa a los trabajadores, incluyendo a su representación legal. Por tanto, para que el control empresarial se pueda llevar a cabo a través de cámaras de videovigilancia, se debe, primeramente, informar a los trabajadores.

En relación con la información previa y el tratamiento de datos de carácter personal, como se ha indicado, entra en juego también el consentimiento. Tanto para las cámaras ocultas como para las visibles podrá entenderse que el consentimiento del trabajador para la captación y tratamiento de datos de carácter personal, como es la imagen, viene implícito con la aceptación del contrato de trabajo, el cual lleva implícito el poder de dirección, organización y control del empresario, por el contrario, incluso en las cámaras ocultas se va a precisar la información previa a los trabajadores.

De ello, surge la siguiente cuestión, ¿Cómo debe realizarse la información?

Dicha información debe ser eficaz, y para ello, la comunicación donde se informe de la utilización de cámaras de videovigilancia para el control empresarial debe contener información previa y expresa, precisa, clara e inequívoca de los fines[145] a los que se dirige la captación de las imágenes, y, por tanto, se deben indicar tres notas claves:

[145] En el estudio de López Ahumada ("La tutela del derecho a la intimidad del trabajador y el control audiovisual de su actividad laboral", 2006), mucho antes de las sentencias estudiadas y de la nueva regulación en materia de protección de datos de carácter personal, ya se indicaba la necesidad del conocimiento por parte del trabajador de la propia existencia del control empresarial videográfico, y se concluía la conveniencia de "seguir teniendo presente, como pauta general, que la introducción del medio mecánico tiene que responder a un interés objetivo por parte de la empresa y que el trabajador tendrá que conocer la aplicación del sistema concreto de control del trabajo. Ello no supone que estemos ante requisito previo de tolerancia del medio de control por parte del trabajador, ni ante una especie de consentimiento tácito del trabajo. Concretamente, estamos

- Que los trabajadores van a ser grabados.
- Que dicha grabación puede ser utilizada para el control laboral.
- Y, que pueden ser sancionados por ello.

En el caso López y Ribalda contra España, esgrimido en este epígrafe para reflejar la evolución jurisprudencial de esta materia, se entendió finalmente, que las propias cámaras públicas y por tanto, visibles, suponían información a los trabajadores de que estaban siendo vigilados, sin embargo, dada cuenta de los múltiples vaivenes jurisprudenciales y la inseguridad jurídica reflejada, entendemos que realizar una información eficaz precisa de algo más que la mera visibilidad de las propias cámaras, incluso creo insuficiente la utilización de las pegatinas disuasorias que hacen referencia a la Ley Orgánica de Protección de Datos, si se pretende una utilización de cámaras de videovigilancia para el control empresarial.

Ello nos lleva a otra de las cuestiones, ¿Sirve el cartel-pegatina con referencia a la LOPD utilizadas para advertir a clientes (disuasorias) o de seguridad?

La Ley Orgánica de Protección de Datos 15/1999) establecía:

> "…el deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679" (art. 22.4).

ante una condición previa y necesaria para la aplicación de los aparatos que permiten el control videográfico. No obstante, es preciso destacar que, en algunos pronunciamientos judiciales, relativos al control de la actividad del trabajador por medio del video, se insiste en que la vulneración del derecho a la intimidad no se condiciona en todo caso al hecho de que los trabajadores tengan conocimiento previo de que su comportamiento laboral está siendo grabado. Como hemos indicado, este es un requisito general de referencia, sin embargo, su aplicación práctica puede modular dicha exigencia según la especialidad del supuesto de hecho". LÓPEZ AHUMADA, J. E. (2006) "La tutela del derecho a la intimidad del trabajador y el control audiovisual de su actividad laboral", Cuadernos electrónicos de Derechos Humanos y Democracia, núm. 3, enero-julio. Pág. 216.

La Agencia Española de Protección de Datos (AEPD) modificó el cartel de información sobre videovigilancia que hasta ahora se venía usando para señalar que una zona estaba siendo grabada. Este cambio, con motivo de la aplicación del Reglamento (UE) sobre Protección de Datos 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, difiere del anterior en el sentido que desaparece la referencia a la propia LOPD y se describe pormenorizadamente los requisitos para que se cumpla con la finalidad de informar. Sin embargo, esa información va destinada a consumidores de los establecimientos donde se exhiben y la validez a efectos de información eficaz a los trabajadores es más que discutible, aunque en ocasiones así haya sido.

Además de la desaparición de la referencia normativa a aplicar, se incluye un apartado para identificar claramente al responsable del tratamiento. Por tanto, habrá que indicar los datos del responsable de tratamiento (nombre, dirección e identificación fiscal) y, además, en el caso que sea necesario, el nombre y contacto del delegado de protección de datos.

146

[146] Pegatinas-carteles, relativos a la LOPD 15/1999 y la LOPD 3/2018.

Se hace una referencia expresa al ejercicio de protección de datos, donde habrá que indicar todos los datos necesarios para que el usuario sepa cómo proceder para ejercer sus derechos, recogidos en el RGPD: acceso, rectificación, cancelación, oposición y limitación del tratamiento. Se tendrá que indicar, además, tanto el canal que se va a usar (por correo ordinario, certificado, email, presencialmente, etc.), como la documentación necesaria para llevar a cabo este ejercicio de derecho (instancia, documento identificativo, etc.).

Además, aparece otro apartado, “Más información sobre el tratamiento de datos personales”, donde se deben indicar los datos necesarios sobre la finalidad del tratamiento, su legitimación, personas interesadas, cesiones o comunicaciones de datos, periodos de retención y toda la información accesoria necesaria para el cumplimiento del deber de informar.

Como es visible, la información sobre la existencia de un tratamiento de datos de videovigilancia se hace igual de exhaustiva que el resto de los tratamientos de datos, ya que el tratamiento de imágenes captadas a través de cámaras de videovigilancia también requiere de la adecuada información para que el usuario pueda conocer el destino de la información que se gestiona.

Sin embargo, el verdadero uso de estas pegatinas o carteles es la información a consumidores de la existencia de cámaras de videovigilancia y de que en ese preciso momento están siendo grabados. Por tanto, se puede entender que no hay una información previa eficaz, sino una información en el momento actual, y, por tanto, podría no resultar eficaz en términos de control empresarial, pues, aunque se entendiera que hay información sobre el hecho de grabar en sí mismo, no se estaría informando de que dicha grabación puede usarse para realizar un control laboral y que podrán ser sancionados por las imágenes que se visualicen.

Dicha explicación nos lleva a la siguiente cuestión, ¿Es posible el uso de cámaras de seguridad, cuya finalidad principal es evitar actuaciones delictivas, para realizar el control empresarial?

Siguiendo la jurisprudencia del caso López Ribalda, al ser visibles, sería posible su utilización para el control empresarial, pero deberían de darse unas circunstancias muy especiales, toda vez que no solo se podría entender que la información no es eficaz, pues, aunque se entendiera como informados a los trabajadores de la existencia de las cámaras y evidentemente, de que estaban siendo grabados, faltaría la precisión de los fines a los que se dirige la captación de las imágenes.

Dada cuenta los fines sancionadores del control empresarial, ¿Se podrá sancionar disciplinariamente a un trabajador por lo captado? Sí, pero siempre y cuando la captación de imágenes se haya realizado con información previa, y siempre que sea siguiendo el juicio de proporcionalidad. En este punto cobra especial atención la precisión de los fines a los que se dirige la captación de las imágenes, es decir, es por este motivo disciplinario por lo que se exige la información previa al trabajador.

En relación con la facultad disciplinaria del empresario y con la obtención de pruebas para ello, surge la duda de sí la declaración de una vulneración de un derecho fundamental al captar imágenes con cámaras de videovigilancia, conlleva necesariamente la declaración de nulidad del despido.

Recientemente se ha dictado una sentencia por el Tribunal Superior de Justicia de Andalucía, en fecha 1 de junio de 2020 (1146/2020), por la cual se declaraba la nulidad de la decisión empresarial por la cual se despedía a un vigilante de seguridad que veía películas y se dormía en su garita, pues la utilización de cámaras con fines de supervisión laboral sin haber mediado información al trabajador, vulneraba su derecho a la intimidad y a la protección de datos de carácter personal. Se concluye que la prueba obtenida es ilícita (al vulnerar un derecho fundamental) y no puede ser tenida en cuenta a la hora de valorar los hechos, pues concretamente, “se instaló una cámara de grabación en el centro de control donde prestaba su actividad profesional el vigilante, ocultando su ubicación y su existencia, y se grabaron imágenes no solo durante la prestación de su servicio, sino

también en momentos en los que se quitaba la camisa correspondiente al uniforme para ponerse la ropa de calle" (STSJ Andalucía 1146/2020), es decir, se trató de la utilización de una prueba obtenida a través de cámaras ocultas, por tanto sin información, situadas en lugares privados y con una expectativa de privacidad muy alta.

En este sentido, volvemos nuevamente a la esclarecedora sentencia del caso López Ribalda contra España, la cual, entendió que no se vulnero el derecho fundamental a un juicio justo, pues el despido se basó en otras pruebas y no solo en la grabación declarada nula. Por tanto, a pesar de utilizar un medio vulnerador de derecho fundamental para la comprobación del hecho constitutivo de despido, si este no ha sido el único medio para acreditar el despido, el despido no tiene por qué ser nulo, pudiéndose declarar procedente o improcedente, pues de lo anterior se extrae que prueba nula no es igual a despido nulo.

Por tanto, la conclusión que obtenemos de las cuestiones resueltas es que se permite la videovigilancia con cámaras visibles siempre y cuando exista una información eficaz (previa y expresa, precisa, clara e inequívoca de los fines a los que se dirige la captación de las imágenes) y se supere el test de proporcionalidad (idónea, necesaria, proporcionada y justificada), precisando para el caso de las cámaras ocultas, la existencia de un daño grave y se instalen en un lugar público, no privado.

Es sorprendente que en esta materia de control empresarial y de ponderación de derechos fundamentales se haya dado en ocasiones, como en la STC 29/2013 (Universidad de Sevilla) más importancia a la protección de datos de carácter personal y a la falta de información conforme a la LOPD que al derecho a la intimidad y a los propios hechos, normalmente incumplimientos contractuales graves. Entendemos como ya se ha avanzado, que en general y en esta materia de control empresarial, se da una excesiva relevancia a la LOPD. Con esto no quiero decir que no haya que informar a los trabajadores, sin embargo, lo que es evidente es que ante fundadas sospechas y siempre que se respete el juicio de proporcionalidad entendemos ajustada a derecho la utilización de cámaras ocultas de videovigilancia. En este sentido y con respecto al juicio de proporcionalidad, la grabación debe realizarse durante el tiempo estrictamente necesario, no ser indiscriminada con relación al resto de trabajadores y por supuesto, debe enfocar

a lugares del centro de trabajo donde la expectativa de privacidad no sea fuerte, como baños o vestuarios.

Resulta más llamativo si cabe cuando los incumplimientos realizados por los trabajadores no son simples hurtos o dejación de funciones, sino maltrato y vejaciones a discapacitados, como en el caso de la residencia La Milagrosa. Afortunadamente, como se ha comentado, el Tribunal Superior de Justicia de Andalucía, apoyándose en la doctrina europea comentada ha entendido válida la prueba de las cámaras de videovigilancia por existir firmes y contundentes sospechas de maltrato, por la gravedad de los comportamientos de los trabajadores y por la imposibilidad racional de descubrirlos si se hubiera avisado de la vigilancia.

En cualquier caso, dada cuenta los cambios de doctrina expuestos, la jurisprudencia vacilante y la casuística tan complicada en esta materia de la videovigilancia, lo más prudente a la hora de utilizar un sistema de videovigilancia será aunar las precisiones y requisitos establecidos en las doctrinas existentes, lo que permitirá que más difícilmente se vean vulnerados los derechos fundamentales de los trabajadores, pues "los demandantes no deberían tener la posibilidad legal de beneficiarse de su propio delito (Riggs v. Palmer, 1889)[147]".

Para ello, sería conveniente que en la empresa se estableciera un protocolo de actuación en este sentido, que culminara con la redacción de una cláusula contractual anexada al contrato laboral que previera la posibilidad de utilización de cámaras de videovigilancia para realizar el control empresarial y que expresamente disponga que podrán ser sancionados por las imágenes que se visualicen, cuyo consentimiento se ha otorgado con la firma del propio contrato. Asimismo, sería conveniente la colocación de dispositivos informando, conforme a la LOPD, que la zona está siendo vigilada.

[147] CARLOS L. BERNAL, (2009) "Un análisis de las decisiones judiciales con base en la teoría de los actos del habla". Pág. 5. *"El Tribunal mantuvo una interpretación alternativa del sistema jurídico: Señalo que la finalidad de las leyes, la intención del legislador, la aplicación de una interpretación racional y el principio o máxima del Common Law de acuerdo con el cual "Nadie puede aprovecharse de su propio fraude o sacar partido de su propia injusticia, o fundar demanda de su propia iniquidad o adquirir propiedad por su propio crimen (…)"*

Los convenios colectivos también pueden recoger las formas de uso de las nuevas tecnologías puestas a disposición de los trabajadores, sin embargo, para algunos autores[148], los escasos convenios que hasta el momento lo regulan, se limitan a hacer una referencia expresa al Reglamento de la UE y a la LOPD, y sólo hacen una llamada a los representantes legales para que negocien un protocolo de utilización de las nuevas tecnologías o para la elaboración de reglas de uso de medios informáticos, sin hacer un especial hincapié en las garantías de disfrute del derecho a la protección de datos.

Juana María Serrano García entiende que este tipo de clausulados o protocolos anexados al convenio deben ser negociados y pactados con la representación legal de los trabajadores, pues de lo contrario serían ilegales aquellas cláusulas de los convenios que recogieran unilateralmente lo establecido por la empresa en base al poder de dirección que le asiste.

6.7. Sistemas de geolocalización (GPS) vs Derecho a la intimidad.

Los dispositivos de geolocalización son uno de los sistemas más utilizados para la realización de un control laboral. Este tipo de control se da sobre todo en puestos de trabajo desarrollados fuera del centro de trabajo, como es el caso de conductores, repartidores o comerciales, aunque en la actualidad, dada cuenta del auge del teletrabajo motivado por la crisis del coronavirus, estos sistemas de control también se ejercen en otros sectores.

En este contexto, uno de los sistemas de control más extendido es el de la utilización de dispositivos de geolocalización, en concreto, el más utilizado es el que se realiza por GPS.

Como adelantábamos, toda vez que el trabajo a distancia es una realidad en nuestro sistema productivo y que el uso del GPS es un medio más que posee la empresa para realizar una labor de control en el desempeño de las tareas de sus empleados cuando las realizan fuera del centro de trabajo, resulta conveniente determinar el régimen jurídico y

[148] El trabajo de SERRANO GARCIA, J. Mª (2021) *"La Protección de datos y la regulación de los derechos digitales en la negociación colectiva y en la jurisprudencia*". Publicado en la Revista de derecho social nº 94, págs. 167-192 estudia el tratamiento del derecho a la protección de datos de carácter personal en diferentes convenios colectivos.

sus límites, pues desde luego, muchas veces va a estar en contraposición el derecho a la intimidad de los trabajadores y también sus datos personales.

Pueden identificarse dos tipos de actividades de control empresarial llevadas a cabo mediante sistemas de geolocalización: el control directo o «intencional», que tiene como objetivo recabar información relativa al cumplimiento de la prestación laboral del trabajador (control de presencia, desplazamientos…), y el control indirecto o difuso, que, estando destinado a satisfacer exigencias organizativas o de seguridad, permite controlar el comportamiento del trabajador[149]. Dentro de este último puede incluirse el denominado control defensivo, que tiene por finalidad verificar la autoría por parte del trabajador, o de cualquier otra persona, de algún ataque contra las personas o bienes, o la creación de una situación de peligro (finalidad disuasoria y probatoria). Estas medidas de control pueden ser arbitradas con carácter rutinario (sistemático), esto es, para cumplir con alguno de los objetivos indicados o *ad hoc* (ocasional), con la finalidad de averiguar si se ha cometido algún ilícito laboral por parte de los trabajadores cuando existan indicios de ello.

Como indicaba Kahale Carrillo en su estudio "La geolocalización como medio de control del trabajador" (2021)[150], la utilización de la geolocalización en las relaciones laborales tiene implicaciones, por una parte, en el derecho fundamental a la intimidad, y por otra, en la protección de datos personales. En cuanto a este último punto, el trabajador queda sujeto a la LOPD, puesto que será aplicable a cualquier tratamiento total o parcialmente automatizado de datos personales, según dispone el primer apartado del artículo 2[151]. Por consiguiente, los empleadores que utilicen la geolocalización tendrán que cumplir con lo establecido en aquella norma cuando corresponda a datos personales de la plantilla.

A lo largo del presente capitulo se estudiará el régimen jurídico y la jurisprudencia más relevante en materia de control laboral a través de los sistemas de geolocalización como

[149] GOÑI SEIN, J.L. (2009) «Controles empresariales: geolocalización, correo electrónico, internet, videovigilancia y controles biométricos», Justicia Laboral, núm. 3, Pág. 13.
[150] KAHALE CARRILLO, D.T. (2021) "La geolocalización como medio de control del trabajador" Revista andaluza de trabajo y bienestar social, Nº 57, Pág. 147.
[151] Art. 2.1. LOPD 3/2018, "Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

el GPS, determinándose los requisitos exigidos para la instalación de sistemas de vigilancia y control que permitan la geolocalización de los empleados salvaguardando los derechos fundamentales a la intimidad y a la protección de sus datos personales. También se estudiará la importancia y las diferencias entre el consentimiento y la información en esta materia de protección de datos, no resultando imprescindible recabar el consentimiento de los trabajadores, pero si será exigible, la información previa a la implantación de la medida de control.

6.7.1. Jurisprudencia española.

El Tribunal Constitucional (STC 292/2000, entre otras) así como la doctrina judicial de los diferentes Tribunales Superiores de Justicia (por ejemplo, STSJ Castilla la Mancha de 23/03/2015), en casos de vigilancia por GPS, han declarado la licitud de la utilización del GPS como medio de control y vigilancia de las instrucciones del empresario siempre que medie información previa a los trabajadores tanto de su instalación como de la finalidad que con la misma se persigue, siguiendo de alguna manera la misma doctrina que en los casos de videovigilancia. De la misma manera se ha pronunciado la Agencia Española de Protección de Datos en los procedimientos sancionadores AP/00032/2013 y AP/00040/2012, en los cuales se ha entendido infringido el deber de información sobre la instalación de estos dispositivos.

Por lo tanto, si la prestación de servicios por parte del trabajador se realiza fuera del centro de trabajo, las facultades de control de este por el empresario *ex* artículo 20.3 ET siguen siendo legítimas, siempre que la vigilancia se establezca exclusivamente a las "obligaciones y deberes laborales". Por ejemplo, en caso de usar un vehículo de la empresa por parte del trabajador para el desempeño de sus funciones, se entenderá que el vehículo es una herramienta más, propiedad de la empresa, y por ello, cabrá un control sobre el uso de este conforme al mencionado artículo 20.3 ET.

Uno de los medios más utilizados para el control empresarial cuando la actividad o parte de ella se desarrolla fuera del centro de trabajo es el sistema GPS. Sin embargo, la utilización del GPS como medio de control empresarial tiene unos límites, los cuales se han ido estableciendo jurisprudencialmente a través, y sobre todo, de las diferentes

sentencias dictadas por la Sala de lo Social del Tribunal Superior de Justicia de Madrid, como por ejemplo en la sentencia 739/2014, de 29 septiembre, donde se falló como vulneradora del derecho fundamental a la intimidad la medida de control empresarial de implantar un dispositivo GPS en un vehículo para su uso exclusivamente profesional, con la posibilidad de conocer en todo momento el lugar exacto en donde se hallaba la trabajadora, incluso fuera de la jornada laboral, sin ningún tipo de conocimiento por parte de la trabajadora. En el mismo sentido, previamente se dictó otra sentencia, STSJ de Madrid de 21/3/2014, la cual entendía conforme a la doctrina del Tribunal Constitucional, que el art. 18.1 CE impone un deber de información que protege frente a intromisiones ilegítimas en la intimidad, y justifica que lo hace, como regla de principio y, de forma añadida al resto de sus garantías, (sin perjuicio de los límites del derecho que ha ido fijando la doctrina del TC). En este sentido se dictó, por ejemplo, la STC 196/2004, de 15 de noviembre, según la cual se va a vulnerar la intimidad personal cuando su afectación no sea acorde con la Ley y no sea consentida, o cuando, aun autorizada, resulte diferente a los términos y el alcance para el que se otorgó el consentimiento, rompiendo la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida.

En este sentido (negativo, como control vulnerador del derecho a la intimidad) la sentencia dictada por la Sala de lo Social del Tribunal Supremo en fecha 5 de diciembre de 2003 entendía que el derecho a la libertad de empresa y el poder de dirección de la actividad laboral, que tiene reconocido el empresario constitucional y legalmente, deben de compatibilizarse con el respeto a los derechos fundamentales del trabajador, de los que sigue disfrutando cuando lleva a cabo trabajos por cuenta ajena, tal y como ha venido reconociendo de forma reiterada el Tribunal Constitucional en relación con diversos derechos fundamentales, y específicamente en referencia al derecho a la intimidad, en sus sentencias 98/2000, de 10 de abril, y 186/2000, de 10 de julio. Asimismo, se recoge en concreto, que la colocación de un sistema de monitorización en tiempo real del vehículo particular del demandante durante una semana en el que su contrato de trabajo estaba suspendido, afecta a una de las manifestaciones de su derecho a la intimidad, como es el derecho a que los demás no sepan cuáles son sus movimientos o que no dónde está en cada momento, como cita textualmente el tribunal, “el derecho a no estar localizado de manera continua por medios electrónicos colocados en sus bienes contra su voluntad”. Por tanto, según esta sentencia el empleo de ese mecanismo no respetaba el principio de

proporcionalidad, pues resultaba innecesaria con relación al objetivo perseguido de comprobar las actividades realizadas por el demandante en los espacios públicos y privados de acceso libre, lo que no justifica el uso de un medio tan invasor de la vida privada y, en consecuencia, reputaba ilícito la medida de seguimiento efectuado al trabajador mediante la ayuda de un localizador colocado en su vehículo particular, constituyendo una intromisión injustificada y desproporcionada en su esfera de intimidad.

En el mismo sentido se manifiesta el Tribunal Superior de Justicia de Castilla la Mancha en sentencia de fecha 10 de junio de 2014, donde declara vulnerado el derecho a la intimidad del trabajador, cuando la empresa colocó un dispositivo GPS en el teléfono móvil cedido al trabajador para su uso profesional, así como personal, con la posibilidad de saber en todo momento el lugar exacto donde se encontraba el trabajador. En este caso, la empresa no había informado al trabajador formalmente, mediante una condición particular, de la instalación del GPS, sino que se hizo a través de una condición general de un contrato de compromiso de confidencialidad. El tribunal entendió que el trabajador no dio consentimiento inequívoco para la captación de datos de carácter personal.

En este caso, la empresa era conocedora de que el trabajador utilizaba de modo privado el terminal móvil, lo que consentía y no prohibió nunca. No advirtió al trabajador para que apagase el teléfono fuera del horario de trabajo. En ningún momento la empresa comunicó de modo expreso y claro la instalación del GPS en el teléfono móvil, ni constaba aceptación del trabajador (falta, por tanto, de consentimiento) y tampoco se advirtió al trabajador para que apagase el teléfono fuera del horario laboral.

El Tribunal Superior de Justicia de Asturias, dictó una sentencia (27/12/2021) un tanto peculiar a colación de un conflicto colectivo planteado en la empresa ZENER COMUNICACIONES S.A., pues declaró la inexistencia de lesión del derecho a la intimidad de los trabajadores, pues los dispositivos GPS se habían instalado en los vehículos puestos a disposición de los trabajadores para su uso profesional, circunstancia conocida por los operarios y autorizada por la Agencia de Protección de Datos, pero por otro lado entendió vulnerada la intimidad de los trabajadores por estar activado el GPS también a partir de la finalización de la jornada laboral, sin el imprescindible consentimiento de los trabajadores en este supuesto.

Recuerda esta sentencia que una de las claves para entender lícito el control de los desplazamientos por medio de dispositivos GPS y del tratamiento de los datos personales obtenidos por su medio es la existencia de una relación laboral. Al existir la misma, se faculta a la empresa para, en el ejercicio de sus facultades de control y dirección, limitar algunos derechos fundamentales de los trabajadores. Sin embargo, esto deja de suceder cuando termina la jornada laboral, momento en el que dichas prerrogativas empresariales desaparecen y el contrato de trabajo deja de constituir el vínculo entre las partes que ampara al empresario para imponer las medidas implantadas de captación y tratamiento de datos. A partir del momento en el que se acaba la jornada de trabajo resultará imprescindible el consentimiento de los trabajadores para mantener en funcionamiento los dispositivos GPS y para el análisis automatizado de los datos personales que se genera, pues el supuesto deja de estar comprendido en la excepción prevista en el art. 6.2 LOPD y se rige por la regla general del art. 6.1 LOPD[152].

La sentencia dictada por el Tribunal Superior de Justicia de Andalucía, Sevilla (Sala de lo Social, Sección 1ª) de 19 julio de 2017 juzgó el despido disciplinario efectuado a un trabajador por ausencia injustificada a su puesto de trabajo teniendo como prueba los datos extraídos por la instalación de un dispositivo GPS en vehículo de la empresa. La Sala entendió que no había vulneración del derecho a la intimidad pues la instalación del dispositivo GPS era conocido por los trabajadores y, además, fue autorizado por la Agencia de Protección de Datos. La peculiaridad de este asunto y se refleja en la sentencia es que el trabajador era encargado y como tal, usaba la plataforma de localización para controlar a los trabajadores adscritos a su turno, por lo que conocía la instalación del GPS, por lo que cumplía con plenitud sus deberes constitucionales y legales, aunque el trabajador no pensara, por ser encargado, que también podría ser controlado, concluyendo el tribunal que no sería necesario especificar, más allá de la mera vigilancia, la finalidad

[152]Artículo 6 LOPD, 3/2018. Tratamiento basado en el consentimiento del afectado

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

exacta que se le ha asignado a ese control (STSJ, 2017).

En el mismo sentido se dictó la sentencia por el Tribunal Superior de Justicia de la Comunidad Valenciana, (Sala de lo Social, Sección 1ª) de 2 mayo de 2017 donde se valoraba el despido disciplinario efectuado a un comercial que no realizó correctamente sus funciones, basándose la empresa para efectuar el despido en la instalación en el vehículo de empresa de un sistema GPS de control y localización que emite un sonido al abrir la puerta del vehículo y se silencia cuando se introduce la llave. Además, el dispositivo de control y localización no se puede desactivar por los trabajadores, permaneciendo inactivo en horario de fines de semana y vacaciones. Se consideró por la Sala que la medida de control empresarial *ex* artículo 20 ET cumplía con el juicio de proporcionalidad, pues se trataba de una medida idónea para la finalidad pretendida por la mercantil de verificar que la correspondencia entre los partes emitidos por el trabajador sobre su prestación de servicios y el lugar en el que se encontraba, a la vista de las quejas de los clientes. En este sentido, le resulta de importancia a la Sala que el GPS permaneciera inactivo durante los días de vacaciones y fines de semana. Además, consideró la medida necesaria como prueba de tales irregularidades, ya que la aportación de datos del GPS se limitó a los días entre semana y con una duración limitada, sin que, a diferencia de otros supuestos, la grabación no tenía el propósito de vigilar y controlar genéricamente el cumplimiento por los trabajadores de sus obligaciones, sino confirmar unas sospechas concretas. A ello ha de añadirse que la colocación del dispositivo de GPS se ubicó en un vehículo de trabajo en el que no existía una razonable expectativa de privacidad al tener conocimiento el trabajador del mismo, ya que dicho dispositivo emitía un pitido cada vez que el coche se ponía en marcha.

La sentencia del Tribunal Supremo de 7 de febrero de 2018, establecía una contraposición entre derechos y deberes atribuidos al derecho a la protección de datos. Entiende que, a diferencia del derecho a la intimidad, el derecho a la protección de datos concede una serie de facultades cuyo ejercicio impone a terceros deberes jurídicos y, además, servirá para garantizar a la persona un poder de control y disposición sobre sus datos personales, lo que solo será posible y efectivo imponiendo los mencionados deberes jurídicos a terceros. Estas facultados o prerrogativas se concretan en el derecho al consentimiento previo para la recogida y uso de los datos personales, el derecho a saber y ser informado

sobre el destino y uso de esos datos, y el derecho a acceder, rectificar y cancelar dichos datos.

Conforme la doctrina constitucional, el trabajador no pierde sus derechos constitucionales como ciudadano por el hecho de realizar un trabajo, y conservará estos derechos también en el ámbito de la relación laboral.

La Sala de lo Social del Tribunal Supremo no ha tenido muchas ocasiones de pronunciarse sobre el control empresarial a través del GPS al faltar otros casos enjuiciados similares para poder darse el requisito de contradicción. La primera sentencia que se dictó en esta materia fue la de 21 de junio de 2012 y, en ella se estudiaba el caso de un empresario que controlaba las actividades de un trabajador en situación de incapacidad temporal mediante un GPS instalado por un detective privado en su vehículo particular. En dicho caso, el Alto Tribunal confirmó la nulidad del despido del trabajador por vulneración, entre otros, de su derecho fundamental a la intimidad.

En esta sentencia se entendió que al igual que la sentencia de instancia y el Tribunal Superior de Justicia de Bilbao que las pruebas utilizadas para acreditar el despido se habían obtenido con vulneración del derecho fundamental a la intimidad en relación con los derechos a la libertad de circulación y a la tutela judicial efectiva, pues se trataban de "medios electrónicos colocados" en los bienes del trabajador "contra su voluntad", lo que "no respeta el principio de proporcionalidad", además de tratarse de un medio de control innecesario al responder su aplicación a la mera conveniencia del detective.

En este recurso se presentó como sentencia contradictoria la dictada por la Sala de lo Social del Tribunal Superior de Justicia de Galicia de 27 de noviembre de 2003, en la que se juzgada el despido de un trabajador por una trasgresión de la buena fe contractual durante su incapacidad temporal. El trabajador fue vigilado por un detective privado en lugares públicos, siendo seguido y grabado en lugares públicos, a raíz de ser publicada en el diario “La Región” una fotografía en la que aparecía el actor realizando actividades de caza incompatibles con la situación de IT en la que se encontraba. El Tribunal entendió el despido como procedente al valorar que la empresa podía vigilar y comprobar el cumplimiento de los deberes laborales de sus empleados, utilizando de forma legítima los

adelantos técnicos y los servicios de agencias de investigación privada, pues, por una parte, existía un indicio de incumplimiento (la fotografía publicada en un medio informativo), el control tenía que realizarse, dado su objeto, fuera de la empresa y se desarrolló en lugares y espacios públicos "en días y en momentos concretos y en el exclusivo contexto de la investigación laboral" (STSJ, 2003). Sin embargo, en lo que se refiere al Recurso de Casación para la unificación de doctrina el Alto Tribunal no entendió, al igual que el Ministerio Fiscal, que se cumpliera el requisito de contradicción, pues se utilizaron medios de constatación diferentes, en uno se instaló por un detective privado un GPS en el vehículo del trabajador sin su conocimiento y, en el otro se filmó al trabajador por un detective privado.

En este sentido, resulta interesante analizar la más reciente sentencia del Tribunal Supremo de 8 de febrero de 2021, dictada en el conflicto colectivo por el que se impugnaba el Proyecto Tracker de Telepizza, en el que se establecían las condiciones y alcance de la obligación de los repartidores, durante su actividad de reparto, de estar geolocalizados por medio de una App que debía instalarse en su teléfono móvil personal. Entiende el alto tribunal que el proyecto es nulo, pues no supera el juicio de proporcionalidad y, por tanto, resulta vulnerador del derecho de privacidad de los trabajadores al poder utilizarse otros medios de menor injerencia.

El “Procedimiento interno Tracker” recogía diferentes apartados, como los repartos, los medios utilizados por el empleado, la forma de utilización, la responsabilidad del empleado, el régimen disciplinario, la remuneración compensatoria del uso de la herramienta. Por medio de la App y a través de la geolocalización, el cliente podía ver la ruta seguida por el repartidor, viendo la ubicación del pedido en tiempo real, de forma que envía datos mientras el repartidor tenga pedidos asignados y pendientes de entrega, con borrado de datos al día siguiente de la finalización del reparto. La App no tenía permiso para recoger datos del dispositivo, tales como número de teléfono, de serie, o código IMEI, si bien para su descarga era necesario proporcionar un número de teléfono móvil o dirección electrónica a fin de recibir el código de descarga. El proyecto imponía causas de suspensión y extinción del contrato en relación con el sistema de geolocalización.

El Alto Tribunal, al igual que entendió la Audiencia Nacional en primera instancia, no cuestiona que la geolocalización, por la que se va a tener un seguimiento del pedido, no sea un método adecuado o idóneo como control del empleado en el desempeño de su trabajo, sino que la configuración dada al mismo por la demandada no es conforme a derecho, pues no supera los criterios constitucionales ni legales, cuando existen otras formas de ejecutar ese sistema que no sea ese. Por ello, desde la perspectiva de los derechos fundamentales y del juicio de proporcionalidad, se entiende que, si supera el test de idoneidad, pero no el de necesidad, al existir otros medios menos invasivos.

Para el Tribunal Supremo el problema está en quien aporta el teléfono móvil, pues en el teléfono móvil del trabajador obran datos que debían de ponerse a disposición de la empresa. Explica el tribunal que no es lo mismo la aportación del trabajador de su móvil personal, que, si lo aporta la empresa, ni tampoco estamos ante una situación similar a la aportación de motocicleta propiedad del trabajador porque, la motocicleta no está vinculada a datos personales. Esto, unido a la falta de información a los trabajadores de los arts. 12 y 13 del Reglamento 679/2016 en materia de tratamiento de datos, conlleva la vulneración del derecho a la protección de datos personales de los trabajadores. De todos modos, aclara el Tribunal que podría admitirse el control a través del GPS instalado en el móvil de los trabajadores si hubiera mediado información sobre el tratamiento de los datos personales, y un acuerdo para el uso profesional del móvil personal, en lugar de haberse tratado de una decisión unilateral (Proyecto empresarial "Tracker"),

En sentido positivo, se indican a continuación diferentes sentencias que admitieron el uso del GPS en vehículos de la empresa para controlar el trabajo prestado, aunque en muchos casos poniéndolos en relación con otros medios de control como son los partes de trabajo, instrucciones previas y/o el informe de un detective privado.

El Tribunal Supremo en sentencia de fecha 15 septiembre 2020 entendió que el despido motivado por el seguimiento a través de un GPS no vulneraba la intimidad del trabajador si este conocía su existencia. En esta sentencia se estudiaba el caso en el que a través del GPS instalado en el coche de empresa se pudo comprobar que la trabajadora utilizaba el coche durante el descanso laboral y cuando estuvo de baja a sabiendas de que estaba prohibido. Además, se entiende que los datos que se recogen en el GPS no reflejan

circunstancias personales de la trabajadora y por ello el despido se calificó como procedente. Se trató, por tanto, de un despido por desobediencia probado con el GPS, que no vulneraba la privacidad pues solo se recogían los datos de la ubicación y movimientos del vehículo no de una persona y, además, la trabajadora conocía que el vehículo disponía de "un dispositivo de localización por GPS para garantizar la seguridad y coordinación de los trabajos" (STS, 2020).

Según determinado sector doctrinal[153], el interés de la sentencia radica en cómo se aborda la problemática de la geolocalización de un vehículo y sus efectos sobre la relación contractual aun cuando los datos utilizados por la empresa para proceder al despido de una trabajadora no derivan directamente de la prestación de trabajo, pues se realizó un control fuera del horario de trabajo y en situación de baja médica de la trabajadora.

El Tribunal Superior de Justicia de Andalucía declaró nulo el despido porque entendía que utilizar los datos del GPS durante la baja médica y el fuera del horario laboral vulneraba el derecho a la intimidad, sin embargo, el Tribunal Supremo revisó la sentencia y entendió que los datos que se obtuvieron con el GPS no eran personales y tampoco invadían la intimidad de la trabajadora, pues, aunque recogían la ubicación permanente del vehículo, no captaban circunstancia alguna de sus ocupantes, por lo que no existía la utilización de datos de carácter personal[154].

La revisión que efectúa el Alto Tribunal lo hace centrándose en el derecho fundamental a la protección de los datos personales, aunque sin abandonar el derecho fundamental a la intimidad personal. En este sentido, y en relación a las facultades de disposición sobre los datos de carácter personal se realizan dos precisiones; Que el derecho a la protección de datos de carácter personal no solo protege la utilización de los datos, sino también su

[153] Blog de Eduardo Rojo Torrecilla de 12/10/2020, http://www.eduardorojotorrecilla.es/2020/10/geolocalizacion-y-utilizacion-de.html

[154] Art. 4.1 del Reglamento (UE) núm. 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos: *"toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*

propia adquisición (STS de 21 de septiembre de 2015, 155) y que el tratamiento de los datos personales requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa (ex artículo 6.1 de la LOPD de 1999, aplicable al caso por razones cronológicas).

Además, entiende que se trataba de un vehículo de empresa con fines únicamente laborales y en el que expresamente se había establecido que el uso del vehículo asignado estaba limitado a la jornada laboral. Por tanto, la trabajadora era perfectamente conocedora de que solo lo podía utilizar para fines laborales y no lo debía de utilizar para fines ajenos al trabajo, por lo que concluía que, al no existir una situación de tolerancia del uso personal, tampoco existirá ya una expectativa razonable de intimidad, puesto que, si el uso personal de los instrumentos de la empresa era ilícito, "no podría exigírsele al empresario que lo soporte y que además se abstenga de controlarlo" (STS, 2020).

Sin embargo, surge la duda del conocimiento de los fines del GPS que tenía la trabajadora. Según el relato inalterado de los hechos probados, la trabajadora no había sido informada de que el GPS podría utilizarse para realizar un control laboral, pues solo se informaba de que de que el vehículo disponía de "un dispositivo de localización por GPS para garantizar la seguridad y coordinación de los trabajos" (STS, 2020), y por tanto, es posible que no se cumplieran realmente los requisitos de información previa recogidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que establece la necesaria obligación de informar de forma expresa, clara e inequívoca a los trabajadores, acerca de la existencia y características de estos dispositivos. De la misma forma, se deberá informar acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión (art. 90.2 LOPD).

Sin embargo, lo cierto es que los hechos ocurrieron bajo la vigencia de la derogada Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, cuyas exigencias eran menores. No obstante, para el Tribunal Supremo no fue necesario determinar para qué de la existencia del GPS en el vehículo, bastando el mero conocimiento de la

[155] Dicha sentencia consideró contrarias a la LOPD de 1999 las cláusulas-tipo de los contratos de trabajo que comprometían al trabajador a proporcionar a la empresa su teléfono móvil y su correo electrónico.

trabajadora, sin ser necesario un alarde informativo. Pronunciamiento en el mismo sentido que la nueva doctrina relativa a la videovigilancia que entiende licita la utilización de cámaras de videovigilancia para el control empresarial con la mera existencia de las pegatinas informativas de la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En otro asunto, la sentencia del Tribunal Superior de Justicia de Madrid (Sala de lo Social, sección 2ª) de 18 de mayo de 2004 entendió que se acreditaron un tiempo de paradas en el trabajo de veinte horas no justificadas en 26 días laborables y que los partes de trabajo no recogían las paradas, utilizándose el GPS como medio para probar los hechos y la consecuente la sanción impuesta al trabajador incumplidor.

Asimismo, en sentencia de 12 de junio de 2017, el Tribunal Superior de Justicia de Madrid consideró procedente el despido de una trabajadora de Cruz Roja que debía desplazarse en una unidad móvil de la empresa para atender a diferentes usuarios afectados de tuberculosis y VIH. La empresa, gracias a la instalación en el vehículo de un GPS, que la trabajadora conocía, detectó que el mismo se hallaba detenido durante la jornada laboral y ello sirvió como prueba del despido disciplinario. El Tribunal entiende lícito el seguimiento a través del sistema GPS como medio de prueba y no vulnerador del derecho a la intimidad de la trabajadora, dado que conocía la permanente transmisión de datos sobre su posición en las rutas de trabajo y, además, el GPS se limitaba a constatar únicamente cuándo arrancaba y se detenía el vehículo, así como cuál era su localización.

En el mismo sentido se pronunció la sentencia del Tribunal Superior de Justicia de Castilla-La Mancha (Sala de lo Social, sección 2ª), de 28 de mayo de 2009, que calificaba como procedente el despido de un vigilante nocturno, encargado de la conservación de diversas carreteras cuya función la realizaba circulando constantemente en un vehículo equipado con GPS, y con la obligación de parar para descansar durante 20 minutos cada dos horas. La Sala entendió que el trabajador se excedía deliberadamente y de forma exagerada en el tiempo de sus paradas generando un eventual riesgo para los usuarios de las vías, que se quedaban durante ese tiempo sin vigilancia (STSJ, 2009).

6.7.2. Jurisprudencia TEDH.

En esta materia, tanto la doctrina del Tribunal Constitucional y del Tribunal Supremo, como la jurisprudencia de los diferentes Tribunales Superiores de Justicia se han hecho eco de las sentencias del Tribunal Europeo de Derechos Humanos relativas a la videovigilancia, como la del caso Barbulesu I y II contra Rumanía o López Ribalda contra España, por lo que nos remitimos al expositivo anterior y recordamos la necesidad de superar el juicio de proporcionalidad en la imposición de la medida y de la necesidad de información previa, que no del consentimiento (implícito en la relación laboral), para no vulnerar ni la intimidad ni la protección de datos de carácter personal.

6.7.3. Conclusiones.

En la actualidad, dada cuenta del auge del teletrabajo y de las nuevas tecnologías, el uso de aplicaciones y programas informáticos que se basan en el sistema GPS son cada vez más frecuentes. Esto, unido a la nueva legislación en materia de desconexión digital y control horario[156] está generando múltiples conflictos.

La mayoría de estas aplicaciones se instalan en los teléfonos, por lo que lo primero que debemos preguntarnos es ¿Quién provee el teléfono?, ¿Quién abona la factura? Si el teléfono no lo provee el empresario, cabe la posibilidad de que se produzca un enriquecimiento injusto en favor de este. Esto es patente cuando las empresas utilizan el teléfono móvil y la tarifa de datos de Internet del trabajador para poder realizar ese control horario. Así, las empresas piden al trabajador que se descargue la aplicación de la empresa en el teléfono del trabajador y le pide que cuando entre y salga de trabajar se conecte a Internet, entre en la aplicación e indique o "clique" sus horas de entrada, salida y descanso. En estos casos los ahorros de costes de las empresas son evidentes, pues no tienes ni gastos de teléfonos móviles ni de las tarifas de datos de Internet.

[156] Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo.

En un primer momento pensé que la problemática del uso del teléfono particular en el trabajo era el enriquecimiento injusto que se generaba al empresario, pero tras la lectura de la jurisprudencia, he llegado a la conclusión que hay otro problema mucho más grave y generador de conflictos de más complicada solución, los datos de carácter personal. Al utilizar el móvil personal e instalar una aplicación del trabajo, se deben de dar diferentes datos de carácter personal, como el propio número de teléfono, de serie, o código IMEI, lo que va a generar un conflicto en materia de datos de carácter personal.

El Tribunal Supremo ha entendido que en el teléfono móvil particular del trabajador obran datos que al utilizarse en el trabajo se deben necesariamente que poner a disposición de la empresa. Explica el Tribunal que no es lo mismo la aportación del trabajador de un móvil personal, que, si lo aporta la empresa, ni tampoco estamos ante una situación similar a la aportación de motocicleta propiedad del trabajador porque, la motocicleta no está vinculada a datos personales.

Por lo tanto, si la empresa solicita el terminal del trabajador, o incluso su número de teléfono, deberá informar sobre el tratamiento de los datos personales recabados conforme al Reglamento General de Protección de Datos.

Una vez superado el problema que genera el uso del teléfono móvil particular, de la jurisprudencia existente se puede concluir que, para poder utilizar el mecanismo de control empresarial a través del GPS, deben darse los siguientes presupuestos para su admisión, conforme, como indica Kahale Carrillo (2021)[157], al marco legal establecido:

El primero, es el deber de información previa, no precisándose el consentimiento o autorización expresa del trabajador, que se entiende implícito en la relación laboral siempre que el tratamiento de los datos de localización sea necesario para el cumplimiento del contrato de trabajo (arts. 6.1.b) y 9.2.b) RGPD). Debe tratarse de una adecuada

[157] *"La facultad de control del empresario a través de la geolocalización se tiene que ejercer conforme al marco legal establecido al efecto y con los límites inherentes a aquel. La legitimidad de su uso en el ámbito laboral viene enfocada para que se cumpla con el marco legal aplicable en cada supuesto. Por tanto, los requisitos específicos es que el empleador informe a los trabajadores, por una parte, sobre el uso de un dispositivo GPS y las características de aquel. Por otra, informar, en su caso, a los representantes de los trabajadores. Por último, el derecho que tienen los trabajadores de ejercer los derechos de acceso, rectificación, limitación del tratamiento y supresión de los datos. Se destaca que no se precisa el consentimiento del trabajador, pero se requiere la información antes mencionada".* KAHALE CARRILLO, D.T. (2021) "La geolocalización como medio de control del trabajador" Revista andaluza de trabajo y bienestar social, Nº 57, Pág. 162.

información, en los términos de claridad y suficiencia que son exigibles a los efectos de evitar actuaciones sorpresivas. Asimismo, la medida debe respetar el juicio de proporcionalidad, no siendo lícito a priori un seguimiento durante los días no laborables. Podría ser lícito, como en la sentencia del Tribunal Supremo de 15 de septiembre de 2021, si hay información o conocimiento previo y no se recogen datos de carácter personal, pues en este caso solo se recogían datos del vehículo, no de la persona.

En segundo lugar, se debe tener en cuenta la finalidad del tratamiento de los datos de localización. El RGPD exige que la recogida de dichos datos personales se lleve a cabo dos principios (art. 5.1 RGPD), el de limitación de la finalidad y el de minimización de datos. Conforme al primero, los datos de localización han de ser obtenidos con fines legítimos, determinados y explícitos, es decir, que la geolocalización no podrá constituir un fin en sí misma, sino que deberá responder a un concreto objetivo que justifique la restricción de los derechos fundamentales de los trabajadores, seleccionado con un criterio restrictivo. Tal medida, además, deberá ser proporcional y necesaria para lograr el objetivo perseguido por el empleador, debiéndose informar con claridad al empleado sobre su alcance y consecuencias.

Por último, se debe recalcar el carácter imprescindible de los datos recogidos en relación con el objetivo perseguido por la monitorización. Los datos que recoja el sistema de geolocalización deberán ser exclusivamente los de posicionamiento del terminal, no estando permitida la obtención de otros datos personales. Por tanto, se excluye un control a través del GPS ilimitado.

En síntesis, se puede determinar que las claves para poder utilizar el mecanismo de control empresarial a través del GPS son, el conocimiento previo de la instalación de un GPS y que no recoja datos de carácter personal, y si lo hace, la información previa debe ser clara y suficiente conforme a la normativa en materia de protección de datos.

En relación con la videovigilancia, la instalación de los GPS como medida de control laboral tiene (o podría tener) menos intromisión en la esfera privada, toda vez que no siempre recogen datos de carácter personal al poder recoger solamente la ubicación y movilidad de un vehículo de empresa. Es cierto que otras veces se encuentra instalado en

el teléfono móvil y en este caso puede recoger la ubicación del trabajador lo que generaría una mayor intromisión en la esfera privada del trabajador por lo que para evitarlo sería conveniente que el teléfono fuera de la empresa. Por ello, también es importante donde se instala el GPS, generando menor intromisión en la intimidad de los trabajadores si se instala en el vehículo que en un teléfono, y mejor si este es propiedad de la empresa y no de un trabajador, pues como advertíamos en el teléfono particular obran datos que al utilizarse en el trabajo se deben necesariamente que poner a disposición de la empresa.

Quizás ya no estemos tan lejos de la implantación de un microchip bajo la piel de las personas para poder controlar nuestros movimientos, como sucede con las mascotas o en las películas de ciencia ficción. En este sentido, hay empresas en países europeos como Suecia o Bélgica donde se instalan microchip bajo la piel con la finalidad de abrir puertas, operar con impresoras o comprar alimentos en las máquinas "vending" con un movimiento de la mano, por lo que es probable que pronto se use esta tecnología para controlar a los trabajadores.

Desde luego, a día de hoy y de acuerdo con la jurisprudencia, parece una medida desproporcionada y excesiva comparada con las obligaciones que se contrajeron en el contrato de trabajo, aún con el consentimiento del trabajador, pero sin lugar a dudas, nos encontramos en el amanecer de una increíble revolución digital, con su consecuente impacto en la sofisticación tecnológica de los nuevos sistemas de control para el cumplimiento del trabajo, por lo que será preciso seguir de cerca estos avances y tomar nota del modo en que se vayan configurando las limitaciones a nivel jurídico, desde la jurisprudencia.

Antes de terminar este apartado conviene recordar al jurista Stefano Rodotà[158], que ante el avance de la ciencia y el aumento en la utilización de las máquinas en todos los ámbitos insistía en "la necesidad de que el Derecho frenara el mismo, preconizando que lo jurídico tuviese un papel destacado, en particular el constitucionalismo y los derechos a la

[158] 30/5/1933-23/6/2017

igualdad y a la dignidad de la persona", pues "no todo lo tecnológicamente posible es al mismo tiempo éticamente admisible, socialmente aceptable y jurídicamente legítimo"[159].

7.- Teletrabajo y el control empresarial.

El trabajo a distancia se entiende como el trabajo que se realiza fuera de los establecimientos y centros habituales de la empresa y del que el teletrabajo es una subespecie que implica la prestación de servicios con nuevas tecnologías[160].

López Ahumada[161] viene a entender al teletrabajo como un modelo de flexibilidad que hace que las empresas sean mucho más dinámicas y que se pueda contrarrestar el riesgo de una imposibilidad extraordinaria de los empleados de poder acudir a los centros de trabajo.

Con anterioridad a la pandemia motivada por el Coronavirus de 2020 la existencia del trabajo a distancia en nuestro país era una modalidad residual, sin embargo, esta forma de trabajar está generando un cambio está llamado a ocupar nuevos márgenes de aplicación y a tener una cuota de desarrollo del mercado de trabajo mucho más intensa. Además, el desarrollo del trabajo a distancia puede suponer una mayor generación de empleo y más riqueza. A su vez, el trabajo a distancia aumenta en sí mismo con el nivel de desarrollo económico de los países o de las regiones[162].

Dada cuenta del auge del teletrabajo y de la evolución tecnológica constante, el uso de aplicaciones y programas informáticos utilizados para monitorizar y controlar al empleado cuando presta servicios en la modalidad de teletrabajo es cada vez mayor y más habitual.

---

159 RODOTÀ, S (2003) "Democracia y protección de datos", Cuadernos de Derecho Público, núms. 19-20, mayo-diciembre de 2003, Págs. 15-26

160 Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.

161 LÓPEZ AHUMADA, J. E. (2023) "Reflexiones sobre el nuevo concepto de aplicación del teletrabajo", Noticias CIELO. Nº 2. Pág. 1.

162 LÓPEZ AHUMADA, J. E. (2023) "Reflexiones…" Ob. Cit Pág 1.

Sin embargo, esta posibilidad de teletrabajo va a generar conflictos entre el poder de dirección del empresario y diferentes derechos fundamentales, como son el derecho a la intimidad y a la protección de datos de carácter personal.

7.1. Régimen Jurídico.

El trabajo a distancia ha sido regulado de forma urgente a consecuencia de la crisis motivada por la pandemia sufrida en el año 2020 tanto en el ámbito interno como en el ámbito comunitario e internacional. En España se ha realizado, principalmente, a través de la Ley 10/2021, de 9 de julio, de trabajo a distancia.

En los diferentes países europeos también se han realizado reformas laborales recientes en relación con el trabajo a distancia, siempre con la base del Acuerdo Marco Europeo sobre Teletrabajo de 2002, que como se verá más adelante, define qué es el propio teletrabajo y recoge sus derechos básicos como la voluntariedad y la necesidad de formalizarse en un acuerdo escrito. En la mayoría de los países europeos se ha ido incluyendo en su legislación laboral la regulación del teletrabajo, y muchos de ellos, lo han plasmado en diferentes convenios colectivos. Países como España, Portugal y Francia regulan el teletrabajo de una forma muy específica en su propia legislación laboral, y otros países como el Reino Unido o Italia no han sido tan específicos y lo han regulado a través de la figura del trabajo flexible. Suecia, Finlandia o Alemania a través de la negociación colectiva desarrollaron las condiciones del trabajo a distancia.

En particular, en la Ley española sobre el Teletrabajo[163] se destaca la idea del carácter voluntario del teletrabajo y la igualdad de derechos de las personas que presten servicios en esta modalidad en relación con las que desarrollan su actividad en el propio centro de trabajo de la empresa, realizando una mención concreta a su derecho a la formación y la carrera profesional. Asimismo, dicha ley recoge el pleno ejercicio de los derechos colectivos de los teletrabajadores, la dotación de equipos a cargo de la empresa, la seguridad y la salud, y la gestión de la organización del trabajo por parte de la persona teletrabajadora en el marco de la legislación y convenios colectivos aplicables.

[163] Ley 10/2021, de 9 de julio, de trabajo a distancia.

Con anterioridad a esta Ley, la Organización Internacional del Trabajo regulaba, en su Convenio n.º 177 y en la Recomendación n.º 184, el trabajo a domicilio, definiéndolo como la actividad laboral que se realiza en el domicilio de la persona trabajadora o en otro local que esta escoja, distinto de los locales de trabajo de la empresa, a cambio de una remuneración y con el fin de elaborar un producto o prestar un servicio.

El Grupo de Trabajo del Artículo 29[164], en su Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, recordaba, entre otros aspectos, que deberá optarse por medios menos intrusivos que posibiliten las funciones de control laboral, posibilitándose al empleado poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo.

En lo que a España se refiere, la Ley 3/2012, de 6 de julio, de medidas urgentes para la reforma del mercado laboral, modificó la ordenación del anteriormente establecido como trabajo a domicilio para dar acogida al trabajo a distancia basado en la utilización permanente de las nuevas tecnologías. En esta ley ya se reconocía el teletrabajo como una forma particular de organizarse en el trabajo el cual permitía a las empresas favorecer la flexibilidad de su organización, aumentar las oportunidades de empleo y mejorar la conciliación del empleo con la vida personal y familiar. Conforme con esta modificación, el trabajo a distancia se recoge en el artículo 13 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, como aquel en que,

> "la prestación de la actividad laboral 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".

En la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se recogen entre los artículos 87 al 91 un compendio

[164] El Grupo de trabajo del artículo 29 está compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la UE, el Supervisor Europeo de Protección de Datos Y la Comisión Europea. Su nombre proviene de la Directiva de protección de datos (Directiva 95/46/CE) y fue lanzado en 1996.

de derechos relacionados con el uso de dispositivos en el ámbito laboral como son, entre otros, el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral y el derecho a la desconexión digital.

El artículo 87 recoge lo relativo al Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, estableciéndose que los trabajadores y los empleados públicos tendrán derecho a proteger su intimidad en el uso de los dispositivos digitales de la empresa. Además, se recoge la posibilidad de que el empleador pueda acceder a los concretos contenidos que se generen por el uso de los medios digitales facilitados a los trabajadores, pero siempre con la única finalidad de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de los propios dispositivos. Por último, se va a recoger la obligación empresarial de establecer protocolos sobre la utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos en nuestra legislación.

Si en un momento dado, el empleador admitiera un uso privativo de los dispositivos y, después pretendiera acceder al contenido de estos, deberá de modo preciso indicar que usos están autorizados y establecer garantías para preservar la intimidad de los trabajadores, como, por ejemplo, la determinación de los períodos de tiempo en que los dispositivos podrán utilizarse para fines privados, resaltando la necesaria información previa a los trabajadores de los criterios de utilización.

En el artículo 90 se va a recoger todo lo concerniente al Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Aquí, al igual que en lo relativo a los sistemas de videovigilancia, se establece la posibilidad de control empresarial *ex* artículo 20.3 ET a través de sistemas de geolocalización. Igualmente, se recoge la necesidad de información previa, expresa, clara e inequívoca a los trabajadores y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. De la misma forma se deberá informar a los trabajadores sobre el ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Por último, en el artículo 91 se va a recoger lo relativo a los Derechos digitales en la negociación colectiva, donde se va a indicar posibilidad de que los convenios colectivos establezcan mejoras o garantías añadidas de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

El Real Decreto-ley 6/2019, de 1 de marzo, de medidas urgentes para garantía de la igualdad de trato y de oportunidades entre mujeres y hombres en el empleo y la ocupación, modificó el artículo 34.8[165] del Estatuto de los Trabajadores relativo a la jornada, recogiendo el derecho a la conciliación de la vida familiar y laboral, incluyendo, el derecho a solicitar las adaptaciones de la duración y distribución de la jornada de trabajo conforme al artículo 37.6 ET[166].

En las Directrices Generales de la Estrategia Nacional frente al Reto Demográfico, aprobadas por Consejo de ministros el 29 de marzo de 2019 se indicaba la importancia del teletrabajo en la repoblación en zonas rurales y remotas, o pequeñas poblaciones, ayudando, por tanto, a favorecer el asentamiento y ayudar a revertir la población.

El artículo 5 del Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19, establece el carácter preferente del trabajo a distancia frente a otras medidas en relación con el empleo. En esta normativa excepcional y de vigencia limitada, se recogía el deber de la empresa de adoptar las medidas oportunas para establecer el teletrabajo en la empresa, si fuera técnicamente posible y si el esfuerzo de adaptación necesario resulta proporcionado.

En la Exposición de Motivos de la actual Ley 10/2021, de trabajo a distancia, se establece la insuficiencia de lo recogido en el artículo 13 del Estatuto de los Trabajadores para regular el teletrabajo, entendiendo que resulta exiguo para aplicarlo a todo lo que conlleva

---

165 Art. 34.8 ET "*Las personas trabajadoras tienen derecho a solicitar las adaptaciones de la duración y distribución de la jornada de trabajo, en la ordenación del tiempo de trabajo y en la forma de prestación, incluida la prestación de su trabajo a distancia, para hacer efectivo su derecho a la conciliación de la vida familiar y laboral. Dichas adaptaciones deberán ser razonables y proporcionadas en relación con las necesidades de la persona trabajadora y con las necesidades organizativas o productivas de la empresa".*

166 Derecho a reducción de jornada de trabajo diaria.

el teletrabajo, que requiere no solo de una prestación laboral fuera del centro de trabajo de la empresa, sino también de un uso importante y sistemático de las nuevas tecnologías informáticas y de la comunicación (TIC).

En el ámbito comunitario, la Unión de Confederaciones de la Industria y de Empresarios de Europa (UNICE), la Confederación Europea de Sindicatos (CES), el Centro Europeo de la Empresa Pública (CEEP) y la Unión Europea del Artesanado y de la Pequeña y Mediana Empresa (UNICE/UEAPME), firmaron en el año 2002 (posteriormente revisado en el año 2009), un Acuerdo Marco Europeo sobre el Teletrabajo, con el único fin de fijar una serie de pautas y prerrogativas que generaban una mayor seguridad a los trabajadores que optaban por el teletrabajo en los países de la Unión Europea. Este Acuerdo definió la modalidad del trabajo a distancia como una fórmula que modernizaba la organización del trabajo conllevando una mayor autonomía para el trabajador una mayor conciliación de la vida familiar.

Con el Acuerdo Marco Europeo sobre el Teletrabajo se establecían y recogían formalmente las condiciones laborales (flexibilidad y seguridad) a escala europea de los teletrabajadores. De un lado se establecía el evidente carácter flexible del teletrabajo, pero también se daba una seguridad al establecerse la misma protección en términos generales a los teletrabajadores que a los trabajadores presenciales. En este acuerdo se iba a definir el teletrabajo como una forma de organización o de realización del trabajo utilizando las tecnologías de la información, en el marco de un contrato o de una relación laboral, en la que un trabajo que también habría podido realizarse en los locales de la empresa, se ejecuta habitualmente fuera de estos.

La Directiva 2019/1158 (UE) del Consejo, de 20 de junio de 2019, relativa a la conciliación de la vida familiar y la vida profesional de los progenitores y los cuidadores, que derogaba la anterior[167], establece a través del uso de las formas flexibles de trabajo, como el trabajo a distancia, un auténtico derecho a la conciliación de la vida laboral y familiar.

[167] Directiva 2010/18/UE del Consejo, de 8 de marzo de 2010, por la que se aplica el Acuerdo marco revisado sobre el permiso parental, celebrado por BUSINESSEUROPE, la UEAPME, el CEEP y la CES, y se deroga la Directiva 96/34/CE.

La actual Ley 10/2021, de 9 de julio, de trabajo a distancia, nace de la necesidad de regular el teletrabajo el cual ha sido objeto de un auge desorbitado como consecuencia de la crisis del coronavirus, con el fin de garantizar el derecho al descanso y a la desconexión digital de los trabajadores. Como se ha indicado con anterioridad esta ley sobre el teletrabajo destaca la idea del carácter voluntario del teletrabajo y la igualdad de derechos de los trabajadores en empresa y teletrabajadores. Esta ley se divide en cuatro capítulos, las pertinentes disposiciones adicionales, transitorias y finales, a lo que se añade la relación de bienes necesarios para combatir los efectos del COVID-19 cuyo tipo impositivo aplicable del IVA a las entregas, importaciones y adquisiciones intracomunitarias será del cero por ciento.

La mencionada ley se aplicará a las relaciones laborales por cuenta ajena cuando se desarrollen a distancia de forma regular, esto es, un mínimo del 30% de la jornada en un periodo de referencia de tres meses, o el porcentaje proporcional según la duración del contrato de trabajo. Por lo tanto, si no se cumple el requisito de regularidad la presente ley no será de aplicación. Tampoco se aplicará en los contratos de trabajo celebrados con menores y en los contratos en prácticas, y para la formación y el aprendizaje, deberá ser mixto, garantizándose un mínimo del 50% de prestación de servicios de forma presencial, pudiéndose realizar una formación teórica de forma telemática.

Se definen tres situaciones, el trabajo a distancia, el teletrabajo y el trabajo presencial. En cuanto al trabajo a distancia, se entiende como la "realización de la actividad laboral conforme a la cual esta se presta en el domicilio de la persona trabajadora o en el lugar elegido por esta, durante toda su jornada o parte de ella, con carácter regular", siendo el presencial el que se presta en el centro de trabajo de la empresa. Por otro lado, se define el teletrabajo como el trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación.

Al tener un carácter voluntario, el trabajo a distancia deberá plasmarse en un acuerdo por escrito entre la empresa y el trabajador, no pudiendo imponer la empresa dicha modalidad empresarial, ni siquiera por conducto del artículo 41 ET, como modificación sustancial de condiciones de trabajo. El acuerdo de trabajo a distancia (ATD) deberá plasmar como mínimo los siguientes aspectos:

- Relación de los equipos, herramientas y medios necesarios para la realización del trabajo a distancia concertado, incluyendo los consumibles y los elementos muebles, así mismo, se debe indicar el periodo máximo para la renovación de estos.
- Inventario de los gastos en los que pudiera incurrir la persona trabajadora por el hecho de prestar servicios a distancia, reflejando la forma de cuantificación de la compensación que debe abonar la empresa obligatoriamente, y momento y forma para realizar la misma.
- Horario de trabajo y establecimiento de guardias o reglas de disponibilidad.
- Porcentaje y distribución de la jornada entre trabajo presencial y a distancia, en su caso.
- Centro de trabajo de la empresa al que queda adscrita la persona trabajadora a distancia y donde, en su caso, desarrollará la parte de la jornada de trabajo presencial.
- Lugar de trabajo a distancia elegido por la persona trabajadora para el desarrollo habitual del trabajo a distancia.
- Duración del acuerdo de trabajo a distancia, concretando los plazos de preaviso para el ejercicio de las situaciones de reversibilidad, en su caso.
- Medios de vigilancia y control de la actividad laboral que se utilizará.
- Protocolo de actuación en el caso de producirse dificultades técnicas o incidencia que impidan el normal desarrollo del trabajo a distancia.
- Instrucciones dictadas por la empresa, con la participación de la representación legal de las personas trabajadoras, en materia de protección de datos, específicamente aplicables en el trabajo a distancia.
- Instrucciones dictadas por la empresa, previa información a la representación legal de las personas trabajadoras, sobre seguridad de la información, específicamente aplicables en el trabajo a distancia.

En cuanto a los derechos de los trabajadores, la presente ley mantiene la igualdad de trato y no discriminación entre los trabajadores a distancia y los presenciales, y se realiza una especial protección en materia de Derechos relacionados con el uso de medios digitales. Así se recoge en su artículo 17, sobre el derecho a la intimidad y a la protección de datos y en su artículo 18, sobre el derecho a la desconexión digital.

El artículo 17 garantiza, de acuerdo con los principios de idoneidad, necesidad y proporcionalidad, el derecho a la intimidad y protección de datos en la utilización de medios telemáticos y en el control de la prestación laboral realizado a través de dispositivos electrónicos.

Se podría y debería pactar con el trabajador la utilización en el teletrabajo de los dispositivos propiedad del trabajador, sin embargo, la empresa no podrá exigir la instalación de programas o aplicaciones en dispositivos que sean propiedad de la persona trabajadora.

En relación con los dispositivos digitales propiedad de la empresa, se deberán establecer criterios de utilización de estos, en los que deberá participar la representación legal de los trabajadores.

Por último, se establece la posibilidad de que a través de la negociación colectiva se pacten usos por motivos personales de los equipos informáticos puestos a disposición por la empresa en el desarrollo del trabajo a distancia.

El último capítulo de la Ley 10/2021 recoge las facultades de organización, dirección y control empresarial en el trabajo a distancia, que no difieren de lo recogido en el Estatuto de los Trabajadores, pero especifica la obligación de los trabajadores de cumplir con las directrices establecidas en la empresa en materia de protección de datos y seguridad de la información también cuando trabajen a distancia. También se recoge la obligación de los trabajadores de cumplir con las instrucciones de uso y conservación de los equipos puestos a su disposición para trabajar a distancia.

En el artículo 22 se van a recoger las facultades de control del empresario, y va a permitir a la empresa que adopte las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones y deberes laborales, incluida la utilización de medios telemáticos, pero evidentemente, deben respetar la dignidad de los trabajadores, teniendo en cuenta, sus circunstancias personales y discapacidades.

Por tanto, ante la existencia de infinidad de programas para vigilar si los teletrabajadores cumplen con sus obligaciones, es posible que muchos de ellos resulten ilegales por vulnerar la intimidad de los trabajadores. Las empresas no podrán utilizar sistemas de fiscalización y control demasiado intrusivos, precisando realizar un control de proporcionalidad entre el medio utilizado y el fin de control, debiendo ser una medida idónea, necesaria y la menos invasiva posible. Asimismo, habrá que valorar la expectativa de intimidad que pudiera tener el trabajador, donde entra en juego la información dada al trabajador y los protocolos existentes en la empresa.

Los incumplimientos en esta materia, como la falta de protocolos, podrían conllevar sanciones que oscilarían entre 7.501 euros y 225.018 euros, en función de la gravedad y los hechos concurrentes en el caso.

En relación con la evolución normativa del teletrabajo, para algunos autores, como López Ahumada, habrá que ver si la nueva legislación en esta materia tiene la capacidad de adaptación a los cambios en la prestación de servicios, permitiendo que empresarios y trabajadores puedan acogerse a ella, pero la clave estará en conseguir que las nuevas leyes del teletrabajo puedan consolidar un régimen jurídico laboral que recoja las ventajas de esta modalidad de trabajo con las garantías jurídicas y los derechos reconocidos en la normativa básica[168].

7.2. Jurisprudencia.

La jurisprudencia en esta materia es bastante reciente y va a ir dando respuesta a los diferentes conflictos producidos por un control laboral del empresario realizado de forma excesiva o sin información previa.

Resulta propicio en este punto explicar la reciente Sentencia nº 4860 dictada por el Tribunal Superior de Justicia de Castilla y León (Valladolid) de 30/12/2021 en la cual se estudiaba el caso de una trabajadora del sector del telemarketing que fue despedida

[168] LÓPEZ AHUMADA, J. E. (2023) "Reflexiones…" Ob. Cit Pág 3.

mientras teletrabajaba tras comprobar mediante la monitorización de su ordenador que no estaba prestando el servicio y que estaba en un foro de Internet.

En la empresa para realizar su trabajo utilizaban la navegación por Internet de forma habitual y la aplicación Skype para comunicarse con los compañeros de trabajo y con los coordinadores. Para la realización del teletrabajo se instalaron en el ordenador privado de la trabajadora dos programas informáticos. El primero de ellos se trataba de un software de escritorio remoto con un acceso directo en el propio escritorio que precisaba la autorización de la trabajadora para que la empresa se pudiera conectar. El segundo de ellos se trataba de un software utilizado diariamente como soporte tecnológico por todos los operadores del contact center, susceptible de monitorización por el supervisor o coordinador de la empresa, para lo cual era preciso que la trabajadora hubiera entrado en el programa. Si la trabajadora estaba utilizando el software la empresa podía acceder a lo que estuviera en la pantalla y realizar una captura de pantalla. También podía escuchar las llamadas en línea, grabar las llamadas, controlar los tiempos de línea, pausas, descansos, tiempos y tiempos de codificación.

Las partes formalizaron un Acuerdo de Teletrabajo, donde se estableció una cláusula relativa a los equipos informáticos, que recogía que el trabajador utilizará un equipo informático de su propiedad, en su domicilio, conectándose por control remoto con el equipo informático del centro de trabajo a fin de controlar el desempeño de las funciones del teletrabajador. Por otra parte, se estableció una cláusula sobre el control y supervisión en la cual se indicaba que la empresa “controlará y supervisará la actividad del teletrabajador mediante medios telemáticos, informáticos y electrónicos".

La coordinadora de la empresa a través del sistema de control de llamadas se percató de que la teletrabajadora llevaba varios minutos sin codificar y accedió a través del software instalado en su ordenador a su pantalla para ver qué estaba haciendo, comprobando que la llamada estaba sin codificar y que la trabajadora estaba en un foro de Internet. Por ello, se despidió disciplinariamente a la teletrabajadora imputándole una conducta constitutiva de indisciplina y desobediencia en el trabajo, transgresión de la buena fe contractual, y disminución continuada y voluntaria en el rendimiento del trabajo.

Tras la consecuente demanda, el Juzgado de lo Social atendió a la petición subsidiaria de la trabajadora calificando el despido como improcedente, no entendiendo la nulidad del mismo. Tras el recurso de la trabajadora en la que se invocaba la jurisprudencia contenida en sentencia de 5-9-17 del TEDH (Gran Sala), caso Barbulescu contra Rumanía, por vulneración del derecho a la intimidad el Tribunal Superior de Justicia tampoco entendió la nulidad del despido pues diferenciaba la falta de respeto a la intimidad por el uso de una aplicación informática instalada en un ordenador personal de la trabajadora, y la vulneración de derechos fundamentales en la obtención de pruebas y lo que constituye despido con vulneración de derechos fundamentales o con móvil discriminatorio que es lo que da lugar a la nulidad, concluyendo que la información sobre los hechos imputados (indisciplina y desobediencia en el trabajo, transgresión de la buena fe contractual, y disminución continuada y voluntaria en el rendimiento del trabajo) no se había obtenido por el excesivo control efectuado a través de la aplicación, sino por otros medios. En este sentido entiende que las imputaciones eran tan genéricas que difícilmente se podían poner en relación con vigilancia del trabajo a través de la monitorización, de modo que no se podía entender vulnerada la intimidad, pues además, la trabajadora no solo fue informada de la instalación de la aplicación informática sino que autorizó la misma y al conocerla se permitió cuestionar su alcance.

Es decir, niega la nulidad no basándose en la intromisión del empresario a través de un medio desproporcionado y excesivo como es la instalación en un ordenador personal de un software que permite ver el escritorio en el ordenador propiedad de la trabajadora sino en que los genéricos hechos imputados en la carta de despido, al ser tan genéricos, no han podido ser extraídos de la monitorización del ordenador de la trabajadora. Entiende además que, de haberlo sido, tampoco entendería la nulidad pues la trabajadora fue debidamente informada.

La sentencia del Tribunal Superior de Justicia de Madrid de 18 de julio de 2022 declaró procedente el despido de un trabajador a distancia por una conducta constitutiva de transgresión de la buena fe contractual tras comprobar que el trabajador falseaba el registro de jornada. El Tribunal concluyó que la información reportada en los partes diarios de trabajo debía ser veraz y rigurosa para cumplir con su finalidad de permitir el control empresaria y al no serlo, constituía una transgresión de la buena fe contractual.

El Tribunal Superior de Justicia de Madrid en sentencia de fecha 24 de enero de 2022, consideró procedente el despido de un teletrabajador que se desconectaba por amplios periodos y de forma injustificada, incumpliendo con ello su deber elemental básico de realizar la tarea laboral encomendada durante la totalidad de su jornada.

La sentencia del Tribunal Superior de Justicia de Madrid de 2 de junio de 2022 resolvía el conflicto relativo a la forma en la que la empresa debía comunicarse y dar las directrices de teletrabajo al tratar el despido de una trabajadora que sacó expedientes de la empresa sin autorización que después perdería. El juzgado calificó el despido como improcedente al no existir en la empresa un protocolo escrito de actuación sobre el teletrabajo que estableciese criterios claros sobre qué información y documentación puede llevarse a casa y cuál no.

7.3. Teletrabajo, protección de datos y riesgos de ciberseguridad.

Como apunta Laura Sanz Martín[169], la aparición de las TIC en el mercado laboral, han favorecido la superación de la antigua concepción tradicional de las relaciones labores, para dar paso a un nuevo escenario desligado de condicionamientos dirigidos en exclusiva a la conciliación del trabajo con la vida personal y familiar.

La pandemia motivada por el Coronavirus ocurrida en el 2020 ha generado en nuestras empresas la práctica del teletrabajo como medida para el distanciamiento social y evitar contagios. Sin embargo, con el teletrabajo se van a incrementar los riesgos a los que se expone la información de la empresa y, además, se van a generar nuevos riesgos para esta, requiriendo en consecuencia, nuevas medidas para evitar posibles brechas de seguridad.

Por ello, tanto en materia de protección de datos como seguridad de la información, empresario y trabajador deben aumentar la cautela para evitar posibles brechas de seguridad.

[169] SANZ MARTIN, L. (2021) "El teletrabajo, Tecnoretos del Derecho". Coor. SANTAMARIA RAMOS, F.J. Valencia, España: Tirant lo Blanch. Pág. 211

7.3.1. Teletrabajo y protección de datos.

Ante los riesgos en materia de protección de datos y seguridad de la información en el trabajo a distancia, la empresa debe adoptar una serie de medidas garantizando igualmente los derechos digitales de los trabajadores, como el derecho a la desconexión digital o el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

La Ley 10/2021, de 9 de julio, de trabajo a distancia, nace de la necesidad de regular el teletrabajo, con el fin de garantizar el derecho al descanso y a la desconexión digital de los trabajadores, así como preservar el derecho a la intimidad en el uso de los dispositivos digitales.

Como se ha indicado con anterioridad, en esta ley sobre el teletrabajo destaca el carácter voluntario del teletrabajo y la igualdad de derechos de los trabajadores que preste sus servicios en el centro de trabajo y los teletrabajadores. Por ello, todos los trabajadores, incluidos los que realizan el trabajo a distancia, deben tener el mismo derecho a los descansos, vacaciones y demás, recogidos en la legislación.

En cuanto al derecho a la intimidad en relación con el uso de dispositivos digitales en el ámbito laboral, el artículo 17 (Ley 10/2021) garantiza el derecho a la intimidad y protección de datos en la utilización de los medios telemáticos y en el control de la prestación laboral realizado a través de dispositivos electrónicos, de acuerdo con los principios de idoneidad, necesidad y proporcionalidad, además del respecto a la protección de datos.

El último capítulo de la Ley 10/2021 recoge las facultades de organización, dirección y control empresarial en el trabajo a distancia, que no difieren de lo recogido en el Estatuto de los Trabajadores, pero especifica la obligación de los trabajadores de cumplir con las directrices establecidas en la empresa en materia de protección de datos y seguridad de la información también cuando trabajen a distancia. También, se recoge la obligación de los trabajadores de cumplir con las instrucciones de uso y conservación de los equipos puestos a su disposición para trabajar a distancia. Es decir, el trabajador debe respetar las políticas internas de la empresa en materia de protección de datos y, seguridad de la información (uso adecuado de dispositivos digitales, de contraseñas, de redes wifi,

actualización de antivirus, de software, almacenamiento seguro de datos, reporte de incidencias de seguridad, copias de seguridad, etc.).

En el artículo 22 se van a recoger las facultades de control del empresario, y va a permitir a la empresa que adopte las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones y deberes laborales, incluida la utilización de medios telemáticos, pero evidentemente, deben respetar la dignidad de los trabajadores, teniendo en cuenta, sus circunstancias personales y discapacidades. Es decir, la empresa podrá controlar el uso de sus dispositivos con las siguientes limitaciones:

- Únicamente podrá controlar en lo que al cumplimiento de las obligaciones laborales se refiere. Es decir, no podrá controlar páginas web en el descanso del trabajador o al final de su jornada laboral, salvo que se haya prohibido o las páginas web consultadas sean ilegales.

- El control efectuado por la empresa debe ser proporcional y dirigido a garantizar tanto el trabajo como la integridad de dichos dispositivos.

Ahora bien, si la empresa no pone a disposición de los trabajadores unos dispositivos digitales, no podrá controlar los dispositivos personales de los trabajadores para uso laboral ni podrá obligar a la instalación de aplicaciones o software.

7.3.2. Riesgos de seguridad en el teletrabajo.

El teletrabajo y el manejo de información de forma remota ha generado nuevos riesgos para la información de la empresa, requiriendo la toma de medidas adicionales para evitar posibles brechas de seguridad.

Estos nuevos riesgos son los virus informáticos, la interceptación de la información por phishing [170] o man in the middle attack[171], la pérdida o borrado de datos o incluso también la pérdida o robo de los propios dispositivos.

Estos riesgos se generan por errores de configuración, uso de redes no seguras, falta de formación tecnológica o falta de seguridad. Para evitarlos se pueden tomar diferentes medidas:

- Realizar copias de seguridad con frecuencia.
- Instalar antivirus y sus actualizaciones.
- Actualizar el software.
- Creación de contraseñas con altos niveles de seguridad.
- No usar redes públicas, etc.

Sin embargo, dichas medidas deberán estar protocolizadas en la empresa para esta las realice sistemáticamente y pueda sancionar a los trabajadores en caso de incumplimiento. Es decir, es totalmente recomendable realizar protocolos de seguridad informática además de formar a los trabajadores en materia tecnológica y de seguridad.

7.4. Conclusiones.

Con la crisis motivada por el Coronavirus el aumento del uso de la modalidad del teletrabajo fue exponencial, pues con anterioridad su uso en España era meramente residual. Sin embargo, tras la pandemia, aunque su utilización se ha venido moderando se está manteniendo en multitud de sectores como una alternativa real al trabajo presencial con el fin de mejorar la conciliación de la vida familiar. Este aumento, unido a la regulación de urgencia que se llevó cabo y a la utilización de diferentes sistemas de

[170] https://es.wikipedia.org/wiki/Phishing Phishing es el conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

[171] https://es.wikipedia.org/wiki/Ataque_de_intermediario En criptografía, un ataque de intermediario (MitM o Janus) es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado. El ataque MitM es particularmente significativo en el protocolo original de intercambio de claves de Diffie-Hellman, cuando este se emplea sin autenticación. Hay ciertas situaciones donde es bastante simple, por ejemplo, un atacante dentro del alcance de un punto de acceso wifi sin cifrar, donde este se puede insertar como intermediario.

monitorización para controlar el trabajo a distancia, conlleva una fuente generadora de nuevos conflictos laborales y de riesgos para la información de la empresa que la jurisprudencia deberá resolver.

La exigua y reciente jurisprudencia ha resuelto los primeros conflictos planteados con ocasión del control del trabajo a distancia y de los riesgos para la información de la empresa.

Por ejemplo, es posible instalar programas o aplicaciones de control de los empleados en los dispositivos electrónicos. En los dispositivos propiedad de la empresa puestos a disposición de los trabajadores, evidentemente sí, pero como hemos visto, también es posible en los dispositivos de los trabajadores. Para ello, no se puede imponer esta medida, pero si se puede acordar.

Otra de las cuestiones suscitadas es la forma en la que la empresa debe comunicarse y dirigir la actividad de los trabajadores a distancia. Evidentemente cualquier forma de comunicación es válida, ya sea verbal o escrita a través de las diferentes herramientas de comunicación existentes. No obstante, si lo que se va a pretender es despedir a un trabajador por desobediencia, al igual que a un trabajador del centro de trabajo, es necesario que la orden se realice de forma clara y por escrito, pues de lo contrario será muy difícil acreditar la orden y, por tanto, la desobediencia.

Por último, como se ha visto, del trabajo a distancia surgen nuevos casos de transgresión de la buena fe contractual o abuso de confianza. La desconexión injustificada y el falseamiento del registro de jornada pueden ser motivos de despido disciplinario.

En cualquier caso, tal y como se ha podido comprobar a través de la jurisprudencia, al igual que el control empresarial realizado a los trabajadores que prestan servicios en los centros de trabajo, para llevar a cabo un control legal y que no vulnere los derechos de los trabajadores a distancia, la información previa y el conocimiento de los dispositivos de control por parte del trabajador es absolutamente esencial.

8.- Redes Sociales y relaciones laborales.

Resulta interesante y necesario tratar en esta tesis la incidencia de las redes sociales en el entorno laboral, toda vez que de alguna u otra manera, forman parte de las nuevas tecnologías, y como tal, han sido incluidas en la negociación colectiva, introduciendo controles empresariales que, para algunos autores, como Juana María Serrano, exceden del art.20 ET, limitando, en ocasiones, el derecho fundamental a la intimidad o a la libertad de expresión[172].

En este apartado se estudiará la posibilidad de efectuar una sanción disciplinaria a un trabajador basándose únicamente en lo extraído de las redes sociales del trabajador sin vulnerar su derecho a la intimidad o a la libertad de expresión. Asimismo, se estudiará las nuevas formas de comunicación de los empleados con los trabajadores, su eficacia probatoria y su validez jurídica.

Antes de realizar el estudio jurisprudencial, resulta conveniente ver como se ha tratado esto en la negociación colectiva.

A continuación, se exponen los ejemplos más representativos de la incidencia de las redes sociales en el contrato de trabajo o, dicho de otro modo, los incumplimientos contractuales que pueden llegar a conocimiento del empresario a través de publicaciones en las redes sociales (Twitter, Instragram, etc.).

El primero y uno de los más típicos, y con más pronunciamientos de los tribunales es la realización de actividades incompatibles con la baja médica que se publican en las redes sociales. Aquí se valorará la posible intromisión al derecho a la intimidad de los trabajadores con el poder disciplinario del empresario.

[172] SERRANO GARCIA, J. Mª. (2019) "El Derecho a la libertad de expresión del trabajador a través de las nuevas tecnologías y el derecho a la reputación de la empresa", Revista Española de Derecho del Trabajo, nº 217, Págs. 101-127

En segundo lugar, se encuentran las publicaciones en redes sociales de comentarios en contra de la empresa. Aquí se estudiará la confrontación entre la libertad de expresión y el poder de control del empresario.

Por último, se encuentra la publicación de fotos o comentarios en el tiempo de trabajo.

En relación con la realización de actividades incompatibles con la baja laboral que se publican en las redes sociales, se han publicado diferentes sentencias, una de ellas la reciente del Tribunal Superior de Justicia de las Palmas de Gran Canaria de fecha 22/1/2016, que declaró la improcedencia de un despido por transgresión de la buena fe contractual de un trabajador en situación de incapacidad temporal por una lesión en el brazo, que colgó fotos en el Facebook tocando la guitarra y realizando labores de bricolaje en su casa, por entender que no eran actividades incompatibles con la situación de baja médica. El Tribunal entendió que el uso de la empresa como elemento probatorio de lo publicado por el trabajador en las redes sociales no vulneraba el derecho a la intimidad del trabajador, pues se trataban de imágenes tomadas con su permiso, que el propio trabajador compartía en su perfil de una red social de libre acceso. Esta sentencia también relata un elemento importante en relación con las redes sociales y la intromisión a la intimidad del trabajador, pues entiende que la investigación empresarial que supone la búsqueda en redes sociales (en este caso, fotos en Facebook) tampoco vulnera la intimidad del trabajador, pues no se trató de una actividad que excediera las facultades de control del empresario que puede hacer seguimiento también durante la suspensión del contrato por enfermedad, debiéndose respetar la buena fe contractual. Sin embargo, esta sentencia entendió que lo recogido en las redes sociales aportado como prueba en el juicio no acreditaban la transgresión de la buena fe contractual, pues para el tribunal no se acreditó la duración de tales actividades, ni su carácter contraproducente por retrasar su curación.

Por tanto, esta sentencia plasma la doctrina jurisprudencial consolidada en esta materia por la cual, investigar y aportar como prueba en juicio de lo publicado en redes sociales abiertas, aún fuera del tiempo de trabajo, no supone una intromisión a la intimidad del trabajador, pues se trata de lo expuesto públicamente y en abierto por el trabajador. Evidentemente, el uso que se le da debe tener relación con el contrato de trabajo no siendo

posible utilizar fotografías subidas a redes sociales durante el periodo descanso, si no estuviera en esa situación de IT.

En otro orden de cosas, en materia de incapacidad temporal, se requiere para que el despido se califique como procedente, que la actividad realizada durante la IT contravenga el tratamiento médico y dilate la curación de la dolencia.

En relación con las publicaciones en redes sociales de comentarios en contra de la empresa, destaca la sentencia del Tribunal Superior de Justicia de Cataluña de fecha 9 de septiembre de 2019 donde se juzgaba el caso de unas publicaciones de un jugador de baloncesto profesional del FC Barcelona. En este caso, el jugador publicó en sus redes sociales (Instagram) que venía arrastrando una lesión que le impedía jugar al máximo nivel, y que esa temporada estaba siendo la más dura de su carrera, ya que estaba jugando lesionado y sin poder rendir al máximo nivel. Por ello, y al entender el club que se estaba vulnerando su honor al realizar dicha publicación despidió al jugador. Tanto el Juzgado de lo Social como tras el recurso del Club, el Tribunal Superior de Justicia, calificaron el despido como nulo por vulneración del derecho a la libertad de expresión del trabajador, toda vez, que lo publicado no generaba una vulneración al honor o la imagen del Club. En relación con el conflicto reputación empresarial y los derechos de libertad de expresión e información, conviene ahondar en el estudio efectuado por Juana María Serrano en su artículo "El Derecho a la libertad de expresión del trabajador a través de las nuevas tecnologías y el derecho a la reputación de la empresa"[173], donde realiza una serie de reflexiones con ocasión de la sentencia dictada por el Juzgado de lo Social nº 8 de Palma de Mallorca en fecha 28 de febrero de 2018, que calificaba como procedente el despido de un trabajador por haber vertido opiniones, comentarios sarcásticos e imágenes desagradables por Facebook en relación con la Guerra de Siria identificando además a la empresa donde trabajaba. En este artículo se estudia el conflicto partiendo de la perspectiva de la negociación colectiva, pues en el caso se partió de la existencia de un código de conducta empresarial en el que el trabajador se comprometía a no realizar comentarios indignos o desagradables para las personas en las redes sociales.

[173] SERRANO GARCIA J. Mª. (2019) "El Derecho a la libertad de expresión del trabajador a través de las nuevas tecnologías y el derecho a la reputación de la empresa". Revista Española de Derecho del Trabajo nº 217, Págs. 101-127

Como señala este artículo, aludiendo a la STSJ de Cataluña de 16 de mayo de 2007, la finalidad del código de conducta de una empresa es velar por el buen desarrollo de las relaciones de trabajo y para ello sancionarán comportamientos que las dificulten o entorpezcan, sin tener en consideración si dichos actos del trabajador se han producid fuera o dentro de la empresa, por estas razones, estos códigos sancionan conductas, comentarios, opiniones o divulgaciones, que se realicen a través de cualquier vía, si se consideraran injuriosos o descalificadoras y perjudiciales para la empresa, para sus responsables o para su compañeros.

Sin embargo, algunas de las cláusulas de los códigos de conducta empresariales no solo velan por el buen desarrollo de las relaciones laborales en la empresa, sino por su reputación o imagen, lo que, a juicio de Juana María Serrano, limitan derechos fundamentales de los trabajadores, como la libertad de expresión. Acertadamente, concluye esta autora que las cláusulas genéricas establecidas en los convenios que sancionan cualquier declaración o comentario que pueda atentar a la reputación o imagen de la empresa deber ser interpretadas de forma muy restrictiva para no vulnerar el derecho a la libertad de expresión de los trabajadores. Del mismo modo, entiende que los controles empresariales que hacen las empresas a través de sus departamentos de control de publicaciones, sobre el uso que hacen sus trabajadores de las redes sociales, exceden del derecho recogido en el art. 20 ET y, por tanto, vulnerando la libertad de expresión de los trabajadores. Compartimos dichas afirmaciones, pero también entendemos que es evitable que el trabajador nombre a la empresa al momento de realizar sus opiniones y comentarios en redes sociales, y que si, de dichos comentarios donde se ha mantenido el nombre de la empresa, al final, dada cuenta la repercusión se genera un perjuicio a esta podría ser razonable la sanción más grave.

En relación con la publicación de fotografías y comentario en el tiempo de trabajo, destaca la sentencia del Tribunal Superior de Justicia de Castilla y León en fecha 15 de marzo de 2021 que declaró que la no vulneración por parte de la empresa del derecho a la intimidad del trabajador despedido de forma disciplinaria por hacerse fotografías mientras conducía un camión mientras trabajaba y que publicó posteriormente en sus redes sociales.

En la fotografía se acreditaba como el trabajador, conductor de camiones, circulaba con un vehículo de empresa a una velocidad de unos 90 kilómetros por hora, y que a la fotografía se acompañaba el comentario "A por la conquista de Asturias. Empezamos el domingo con alegría".

En un primer momento, el Juzgado de lo Social nº 3 de León entendió el despido como procedente, sin embargo, el Tribunal, que no entendió vulnerado el derecho a la intimidad pues no se trataba de imágenes relativas a la vida privada del trabajador, sino del registro fotográfico de una actividad dentro del marco de la prestación de servicios, realizada dentro del lugar de trabajo, en hora de trabajo y mientras se desarrolla la actividad laboral, calificó el despido como improcedente al no existir un incumplimiento grave y culpable del trabajador.

De las últimas sentencias en pronunciarse sobre publicaciones en redes sociales se encuentra la dictada por el Tribunal Superior de Justicia de Asturias de 18 de octubre de 2022, la cual estudiaba el despido de un trabajador de un supermercado por haber publicado un video en la red social TikTok donde con el uniforme de la empresa insultaba a los clientes que acudían al establecimiento a primera hora. En primera instancia el Juzgado de lo Social 3 de Gijón calificó el despido como nulo por haberse vulnerado el derecho fundamental a la libertad de expresión. Sin embargo, el Tribunal Superior de Justicia de Asturias revocó la sentencia anterior calificando el despido como procedente al considerar que la conducta del trabajador suponía una falta grave de respeto a los clientes y comprometía la imagen de la empresa.

Es innegable que las redes sociales han modificado la forma de relacionarse del ser humano y por ello, también la forma de relacionarse en el entorno laboral. Ahora es habitual que las empresas utilicen la aplicación Skype o formen un grupo en la aplicación Whatsapp para dar instrucciones, organizar y gestionar la empresa. Pero también son los trabajadores los que a través de estas aplicaciones se comunican con el empresario para indicarle que llegará más tarde, que está de baja e incluso que quiere dejar el trabajo.

En este sentido el Tribunal Superior de Justicia de Madrid, en sentencia dictada el 10 de junio de 2015, validó la dimisión de un trabajador vía WhatsApp: "Así, nos encontramos

con que la actora manifestó el 13-3-2014 que no quería trabajar para la empresa y que se iba, despidiéndose de las compañeras y abandonando el centro de trabajo, y no solo eso, sino que por la tarde la encargada de zona se comunicó con ella a través de la aplicación WhatsApp", reiterando la ahora recurrente que no iba a volver al trabajo (Hecho Probado Quinto). Todo ello reveló una terminante, clara e inequívoca voluntad de la actora de romper la relación laboral.

Tal y como viene entendiendo el Tribunal Supremo, la dimisión, o voluntad unilateral del trabajador de extinguir la relación laboral, puede manifestarse de forma expresa o tácita, no siendo preciso que se ajuste a una declaración de voluntad formal, pues resulta suficiente que la conducta seguida por el trabajador revele de forma indiscutible su opción por la ruptura o extinción de la relación laboral, si bien se exige una voluntad del trabajador "clara, concreta, consciente, firme y terminante, reveladora de su propósito", y en caso de que sea tácita "ha de manifestarse por hechos concluyentes, es decir, que no dejen margen alguno para la duda razonable sobre su intención y alcance".

Como exige el Tribunal Supremo en su sentencia de 21 de noviembre de 2000, dicha dimisión requiere una voluntad incontestable en tal sentido que puede manifestarse al exterior, para que necesariamente la conozca el empresario, de manera expresa con signos escritos o verbales que directamente explicitan la intención del interesado, lo que podrá realizarse a través de la aplicación de Whatsapp; o de manera tácita: comportamiento del cual cabe deducir clara y terminantemente que el empleado quiere terminar su vinculación laboral.

El Tribunal Superior de Justicia de Cataluña, entendiendo válida la prueba de comunicación a través de la aplicación de Whatsapp, dictó sentencia de 21 de marzo de 2016 en la que estimó la petición del trabajador, pues se acreditaba la intención de este de permanecer en la empresa a través de varias comunicaciones remitidas por medio de la mencionada aplicación.

Asimismo, el Tribunal Superior de Justicia de Madrid, en sentencia de 21 de diciembre de 2015, se valió de lo reflejado en la aplicación de Whatsapp para calificar el despido una trabajadora como procedente. Gracias a lo establecido la aplicación, lo que formó

parte de los hechos declarados probados, se constató que la trabajadora solicitó a la empresa que procediese a formalizar un despido simulado para extinguir el contrato y poder cobrar el paro, aunque luego solicitará por medio de burofax a la empresa que le diesen diferentes certificados para solicitar la baja por riesgo de embarazo.

En la sentencia del TSJ de Madrid, de 8 de junio de 2023 se confrontó la monitorización efectuada en el WhatsApp con el derecho al secreto de comunicaciones. En este caso, la empresa despidió a una trabajadora tras revisar conversaciones de Whatsapp obrantes en el teléfono facilitado por la empresa sin haber establecido (ni por ende) informado sobre los criterios de uso de los dispositivos informáticos puestos a disposición de la actora, para controlar su actividad. Se concluye en la instancia, que son conversaciones efectuadas en el ámbito laboral, pero de carácter privado, lo que constituye una lesión de la LOPD y del derecho fundamental al secreto de las comunicaciones.

Se argumentaba que, a pesar de entenderse el teléfono como parte del equipo de trabajo, y que, se entiende que lo es para un uso "determinado por el contrato de trabajo", con previsión de exclusivo uso profesional, la doctrina constitucional derivada del TEDH ha entendido que si el trabajador no estaba advertido de la posibilidad de que sus comunicaciones pudieran ser objeto de seguimiento por la empresa, podía razonablemente confiar en el carácter privado de sus conversaciones.

Aunque en primera instancia se calificó el despido como nulo, el TSJ entendió que no quedaba probado que el despido pretendiera la vulneración de derechos fundamentales, ni que el móvil del empresario al acordar el despido respondiera a una causa vulneradora de esos derechos fundamentales sino que el empresario, al intentar comprobar el comportamiento de su empleada y obtener pruebas de algunos de sus incumplimientos para tratar de justificar un despido, ha obtenido de forma ilícita tal prueba con vulneración de derechos fundamentales , no pudiendo de esta manera confundirse el despido con violación de derechos fundamentales con la infracción de derechos fundamentales para la obtención de la prueba de parte de los hechos en los que se basó la empleadora para adoptar tal sanción.

En la sentencia del Tribunal Superior de Justicia de Galicia de 28 de enero de 2016 se considera al Whatsapp no solo como un medio de prueba válido a pesar de no contemplarse en la Ley Reguladora de la Jurisdicción Social, sino que entiende que "ya ha tenido plasmación normativa". Sin embargo, como es lógico concluye que no basta con el pantallazo de la conversación, sino que requiere a los efectos de su consideración como documento en el proceso de la aportación de la transcripción de la conversación y la comprobación por un notario o secretario judicial que esta se corresponde con el teléfono y con el número correspondientes.

Otros tribunales se han mostrado menos rigoristas, como el Tribunal Superior de Justicia de Cataluña, que, en su sentencia de 16 de octubre de 2015, dio validez al pantallazo como prueba documental sin exigir un mecanismo adicional, llegando a modificar hecho declarado probado.

Es decir, ya hay importante jurisprudencia que ha utilizado como prueba válida las comunicaciones a través de Whatsapp, sin embargo, hay mucha otra que no ha estimado como suficiente prueba lo recogido en esta aplicación, pues no fueron autentificados por la compañía de telefonía y son fácilmente manipulables. En este sentido, se dictó la sentencia por el Tribunal Superior de Justicia de Navarra en fecha 19 de septiembre de 2016.

En el mismo sentido se ha pronunciado la sentencia del Tribunal Superior de Justicia de Madrid nº 817/2017, de 29 de septiembre de 2017 que indicó que hasta que WhatsApp no modifique la seguridad en el almacenamiento de los mensajes, no se podrá estar absolutamente seguro y tener la total certeza de que los mensajes no han sido manipulados.

Por tanto, y como siempre, debemos estar a la valoración de la prueba que realicen los jueces de instancia, sin embargo, lo reflejado en las comunicaciones a través de la aplicación Whatsapp u otras similares, serán una prueba más que deberán valorar los tribunales. Ello nos lleva a la siguiente cuestión, ¿Qué tipo de prueba son las conversaciones por Whastapp?

Esta pregunta nos lleva al siguiente punto de la tesis, como valorar la prueba electrónica en el proceso laboral.

9.- Valoración de la prueba electrónica en el proceso laboral.

En el proceso laboral, las reglas sobre la prueba vienen recogidas en los artículos 90 a 96 de la Ley Reguladora de la Jurisdicción Social, apenas se va a aplicar la Ley de Enjuiciamiento Civil, de aplicación subsidiaria a la anterior.

El artículo 90.1 de la LRJS realiza una definición amplia del concepto de prueba que puede ser utilizada para acreditar los hechos controvertidos, incluyendo,

> "los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos, que deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano jurisdiccional los medios necesarios para su reproducción y posterior constancia en autos".

Por su parte, la Ley de Enjuiciamiento Civil recoge en su artículo 299[174] lo relativo a los medios de prueba, haciendo igualmente una aplicación extensiva de los mismos.

Por tanto, tal y como se ha establecido a lo largo de la tesis, se permite la utilización de diferentes medios tecnológicos y telemáticos en el proceso laboral, sin embargo, se debe valorar como debe presentarse dicha prueba para poder ser tenida en cuenta como autentica y no manipulada, y que en su obtención no haya mediado vulneración de derechos fundamentales, pues como también se ha visto a lo largo de esta tesis, no serán admitidos como prueba los hechos obtenidos vulnerando derechos fundamentales.

---

[174] Artículo 299 LEC, Medios de prueba

1. *Los medios de prueba de que se podrá hacer uso en juicio son:*
- ***1.º*** *Interrogatorio de las partes.*
- ***2.º*** *Documentos públicos.*
- ***3.º*** *Documentos privados.*
- ***4.º*** *Dictamen de peritos.*
- ***5.º*** *Reconocimiento judicial.*
- ***6.º*** *Interrogatorio de testigos.*

2. *También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.*

Por ello, con el fin de acreditar lo reflejado en la prueba tecnológica es totalmente recomendable apoyar la prueba tecnológica adverada con otra prueba como el interrogatorio de la parte y/o la testifical. Por ejemplo, en la aportación de correos electrónicos como medio de prueba, es conveniente que estos sean reconocidos por testigos o por las propias partes, pues de lo contrario su valor probatorio puede ser irrelevante. En relación con los mensajes a través de la aplicación de Whatsapp sería conveniente una transcripción por un notario o Letrado de la Administración de Justicia del propio Juzgado donde se tramite el procedimiento, o bien, la autentificación de la compañía telefónica.

Ahora bien, dada cuenta del especialísimo recurso de suplicación propio de la Jurisdicción Social debemos de valorar si la prueba electrónica y telemática será tenida en cuenta como prueba documental o de otra índole.

9.1. Prueba documental.

El recurso de suplicación es un recurso extremadamente especial y concreto cuyo objeto viene recogido en el artículo 193 de la LRJS[175]. En su apartado b) se recoge la exigencia de que la revisión de los hechos declarados probados se hará solamente a la vista de pruebas documentales y/o periciales practicadas en el juicio.

Por tanto, no podrán revisarse los hechos declarados probados a la vista de otras pruebas que no sean documentales (o periciales), de ahí la suma importancia que tiene que la prueba tecnológica se valore como prueba documental, pues de lo contrario no se podrá inculcar la misma para formalizar el recurso de suplicación.

Reiterada doctrina del Tribunal Supremo en materia de revisión de hechos probados, tal y como se puede apreciar en las sentencias de la Sala Cuarta de 18/2/2014, de 3/7/2013,

---

175 *Art. 193 LRJS:*
a) Reponer los autos al estado en el que se encontraban en el momento de cometerse una infracción de normas o garantías del procedimiento que haya producido indefensión.
b) Revisar los hechos declarados probados, a la vista de las pruebas documentales y periciales practicadas.
c) Examinar las infracciones de normas sustantivas o de la jurisprudencia.

4/5/2013, y de 5/6/2011, ha fijado los requisitos para la modificación del relato de hechos, tanto en suplicación como en casación, partiendo del carácter extraordinario de estos recursos. Esta doctrina exige la concurrencia de los siguientes requisitos para que la revisión de hechos probados prospere:

En primer lugar, se deben indicar qué hechos han de adicionarse, rectificarse o suprimirse, sin valorar o incluir normas de derecho o su interpretación.

En segundo lugar, se debe citar la prueba documental que, por sí sola, demuestre la equivocación del juzgador, de una manera manifiesta, evidente y clara, y que servirá de base para la revisión de los hechos probados.

En tercer lugar, se debe precisar los términos en que deben quedar redactados los hechos probados y su influencia en la variación del signo del pronunciamiento, es decir, es necesario plasmar una redacción alternativa del hecho probado revisado.

Por último, la modificación planteada debe tener interés en el pleito, es decir, debe tener trascendencia para modificar el fallo de instancia (SSTS 14 mayo 2013 o 17 enero 2011);

Doctrina de antiguo recogida en similares términos en la STS de 25/3/1998 que indicaba que la revisión de hechos no faculta al Tribunal a efectuar una nueva valoración global y conjunta de la prueba practicada, sino que la misma debe operar sobre la prueba documental o pericial alegada que demuestre patentemente el error de hecho, bien entendido que su apreciación no puede entrañar denegación de las facultades valorativas de la prueba atribuidas al Juzgador "a quo", a quien corresponde, en virtud de lo dispuesto en el artículo 97.2 de la LPL (actual LRJS), apreciar todos los elementos de convicción aportados al proceso y declarar, en función de éstos, los que estime probados. No es posible admitir la revisión fáctica de la sentencia impugnada con base en las mismas pruebas que la sirvieron de fundamento, en cuanto no es aceptable sustituir la percepción que de ellas hizo el juzgador, por un juicio valorativo personal y subjetivo de la parte interesada (STS 16 de diciembre de 1967, 18 y 27 de marzo de 1968, 8 y 30 de junio de 1978, y 2 de mayo de 1985). En el supuesto de documento o documentos contradictorios y en la medida que de ellos puedan extraerse conclusiones contrarias e incompatibles,

debe prevalecer la solución fáctica realizada por el juez o Tribunal de Instancia, órgano judicial soberano para la apreciación de la prueba (STC 44/1989, 20 de febrero y 24/1990, de 15 de febrero.

La Ley 59/2003, de firma electrónica, en su artículo 3.5 define como documento electrónico a la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

De ello se podría entender que el documento electrónico es una prueba documental, sin embargo, el Tribunal Supremo realiza una interpretación restrictiva y no reconoce como prueba documental a la prueba electrónica. Más adelante se estudiará la jurisprudencia del Tribunal Supremo, pero dada cuenta de la aplicación restrictiva realizada por el Tribunal Supremo resulta recomendable e interesante llevar como prueba la transcripción íntegra o literal de esta prueba electrónica o telemática.

La sentencia del Tribunal Supremo de fecha 13/5/2014 desestima el recurso de casación de una empresa la cual había procedido a despedir disciplinariamente a una trabajadora a consecuencia de unos hechos grabados a través de una cámara de videovigilancia. Esta sentencia no solo entendió que la grabación sin consentimiento ni información previa era nula, pues vulneraba la protección de datos de carácter personal *ex* artículo 18.4 CE si no también, que las fotos extraídas del video y su grabación eran medios probatorios sin valor de prueba documental y, por lo tanto, no eran aptos, para la revisión de los hechos probados en el recurso de suplicación.

En esta sentencia el Magistrado Excmo. Sr. D. José Manuel López García de la Serrana emitió un voto particular al fallo de la sentencia, pues entendió que las imágenes captadas por la videocámara si debían valorarse como prueba documental y, por tanto, debían tenerse como aptos para la revisión fáctica en el recurso de suplicación. Argumenta el Magistrado que tanto la Exposición de motivos como el artículo 299.2[176] de la LEC

[176] Art. 299.2 LEC *"También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso".*

consideran esta prueba como análoga a la de prueba documental, aunque apunta, de la necesidad en su práctica de la adopción de procedimientos encaminados a garantizar su fiabilidad, al igual que ocurre con la emisión de certificaciones sobre la autenticidad de documentos públicos, conforme al artículo 318 LEC, y con el cotejo u otros procedimientos que sirvan para acreditar la veracidad de los documentos privados (ex. Art. 326 LEC). Esta consideración análoga a la de prueba documental, también se realiza en la doctrina de la Sala 1ª del Tribunal Supremo que los equipara a documentos privados[177]. En el mismo sentido se pronuncia el artículo 26 de Código Penal cuando considera como documento a todo soporte material que expresa o incorpora datos, hechos o narraciones. Es más, acertadamente, este Magistrado puntualiza que hoy día la mayoría de los archivos públicos y privados se encuentran en soportes informáticos, por lo que no darle la consideración de documentos, carece de sentido.

Por tanto, como bien explica el Magistrado, surge la paradoja de que unas imágenes tomadas por una videocámara tienen el valor de prueba documental en unas ramas del derecho, como la civil y penal, y para otras, como la social, no, generando, por tanto, una inseguridad jurídica. Concluye en este sentido que sería contradictorio que el video sirviera como documento para probar la comisión de una falta o de un delito y no lo fuera para probar un incumplimiento contractual laboral grave.

Por todo ello y amparándose en la sentencia del Tribunal Constitucional 212/2013[178], de 16 de diciembre, el Magistrado entiende que al negarse la práctica de esa prueba y no darle valor revisorio por no ser prueba documental se violó el derecho a la prueba que reconoce el artículo 24.2 CE., debiéndose anular las actuaciones.

Para terminar, trataremos los mensajes de la aplicación Whatsapp o similares, los cuales, dada cuenta la interpretación restrictiva de la doctrina jurisprudencial no se entenderá como prueba documental, perdiendo, por tanto, valor para revisar los hechos declarados probados.

---

[177] STS. (1ª) de 12 de junio de 1999.

[178] Esta sentencia se dictó en un procedimiento en el que se denegó el visionado de un DVD, prueba que se debió practicar con independencia del valor que se diera a su resultado. Ello motivó que nuestro más alto Tribunal anulara las actuaciones para la práctica de esa prueba, cuya naturaleza de prueba documental no pone en duda en su fundamento 4, donde se reitera la aplicación supletoria de la LEC.

Un claro ejemplo de la aplicación restrictiva es la sentencia del Tribunal Superior de Justicia de Madrid nº 817/2017, de 29 de septiembre de 2017 que entendió que ni los mensajes de la aplicación de mensajería instantánea (Whatsapp), ni los correos electrónicos son útiles como prueba para la impugnación de la sentencia en el Orden Social, ello, bien por la especial vulnerabilidad tanto externa como interna de aquel sistema, bien por la falta de literosuficiencia de los segundos que obliga a la parte recurrente a acudir a continuas conjeturas e hipótesis ajenas al cauce procesal elegido. Hasta que WhatsApp no modifique la seguridad en el almacenamiento de los mensajes, no se podrá estar absolutamente seguro y tener la total certeza de que los mensajes no han sido manipulados.

Como hemos indicado, la mayor parte de las Salas de lo Social no admiten estos documentos para sustentar la revisión de los hechos declarados probados en sentencia.

9.2. ¿Prueba nula igual a despido nulo? Debate normativo, procesal y jurisprudencial sobre la prueba ilícita.

Las pruebas obtenidas vulnerando directa o indirectamente derecho fundamentales han sido denominadas en nuestra legislación como pruebas ilícitas. En el debate procesal laboral habrá que valorar dos cuestiones, si se trata realmente de una prueba ilícita, es decir, si se ha obtenido con vulneración de derechos fundamentales (veremos el momento procesal para valorar la misma) y, las consecuencias en el pleito de despido, es decir, la calificación de despido nulo (por haberse vulnerado los derechos fundamentales del trabajador) o de improcedente (no haberse acreditado la causa del despido). Se parte de la base de que esta prueba es la única prueba con la que ha contado el empresario para la imputación de los hechos en la carta de despido, pues si existe otro medio de prueba, el despido se deberá calificar conforme a la prueba persistente.

9.2.1 Régimen Jurídico.

Como punto de partida resulta esencial exponer y tratar el artículo 11. 1 de la LOPJ que establece que “En todo tipo de procedimiento se respetarán las reglas de la buena fe. No

surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales".

Este artículo ha servido como base o argumento para sustentar a los defensores tanto de la tesis de la nulidad del despido como para los de la improcedencia, por lo que conviene estudiarlo.

Para algunos autores defensores de la nulidad se valora los términos "directa o indirectamente" de la Ley como el reflejo en nuestra normativa de la doctrina anglosajona del árbol envenenado. "La teoría de los frutos del árbol envenenado o emponzoñado", es una doctrina que entiende que cualquier prueba que directa o indirectamente y por cualquier nexo se pudiera relacionar con una prueba nula debe también considerarse nula. En este sentido esa prueba nula se convierte en ilegítima y su nulidad insubsanable, y en consecuencia arrastrará a todas aquellas otras pruebas directamente relacionadas y derivadas[179].

Sin embargo, Pico i Junoy en su libro "Aspectos básicos de la prueba en el proceso civil[180]" aclaró el origen del artículo 11.1 LOPJ. Este autor entiende que el origen del art. 11.1 LOPJ no es la doctrina del árbol envenenado sino otra doctrina, la fijada en la STC 114/1984, de 29 de noviembre, la cual establecía que "la hipotética lesión de los derechos reconocidos en el art. 18.3 de la Constitución Española no podría imputarse -con el carácter directo e inmediato- a las resoluciones judiciales, sino a los actos extraprocesales" (…) el acto procesal podrá haber sido o no conforme a Derecho, pero no cabe considerarlo como atentatorio, de modo directo, de los derechos reconocidos en el art. 18.3 de la Constitución". Lo que según Picó i Junoy hace el legislador al indicar en su texto "directa o indirectamente" es recoger la anterior doctrina constitucional, la cual establecía que resultaría "(…) ineficaz todo elemento probatorio para cuya obtención se

[179] En la sentencia del Tribunal Superior de Justicia de Cataluña de fecha 22/5/2015 se aplicó esta doctrina del árbol envenenado al entender nulo un informe de una empresa de seguridad basado en la grabación de unas imágenes obtenidas de forma ilícita, sin consentimiento ni información y, por tanto, vulnerando el derecho fundamental a la protección de datos de carácter personal ex art. 18.2 CE. En relación con la aplicación de la doctrina anglosajona del *"fruto del árbol envenenado o emponzoñado"*, constituye doctrina consolidada las sentencias del Tribunal Constitucional 98/2000 de 10 de abril, la 186/2000, de 10 de julio, la 29/2013 de 11 de febrero y la 39/2016 de 3 de marzo, y las sentencias del Tribunal Supremo de 5 de diciembre de 2003, de 7 de julio de 2016, de 31 de enero de 2017 y de 20 de junio de 2017.

[180] Pico i Junoy, J. "*Aspectos prácticos de la prueba civil*" Barcelona, Bosch Editor, 2006.

haya infringido directamente un derecho fundamental, así como también la ineficacia del medio de prueba a través del cual se intenta dar entrada en el proceso a dicho elemento probatorio, ya que ello supone indirectamente conculcar otros derechos fundamentales".

Por otra parte, para este autor la expresión "no surtirán efecto" recogida en el mencionado art. 11.1 LOPJ no conlleva la calificación de la improcedencia del despido.

El artículo 90 de la LRJS establece en su primer apartado la posibilidad de presentar las TIC como medio de prueba en el procedimiento judicial[181]. Teniendo en cuenta la aplicación supletoria de la LEC, hay que distinguir entre los diferentes medios de prueba electrónicos y sus reglas de valoración. Los documentos que se regulan en los artículos 382 a 384 (sección 8) de la LEC[182], si incorporan firma electrónica con certificado reconocido y producida por un medio seguro tienen el mismo valor que una firma manuscrita. Por su parte, las palabras, imágenes y sonidos captados por cámaras de filmación, grabación y semejantes serán valorados conforme a la sana critica.

---

[181] Art 90.1 LRJS "*1. Las partes, previa justificación de la utilidad y pertinencia de las diligencias propuestas, podrán servirse de cuantos medios de prueba se encuentren regulados en la Ley para acreditar los hechos controvertidos o necesitados de prueba, incluidos los procedimientos de reproducción de la palabra, de la imagen y del sonido o de archivo y reproducción de datos, que deberán ser aportados por medio de soporte adecuado y poniendo a disposición del órgano jurisdiccional los medios necesarios para su reproducción y posterior constancia en autos".*

[182] Sección 8 LEC.
Artículo 382 *Instrumentos de filmación, grabación y semejantes. Valor probatorio*
1. Las partes podrán proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes. Al proponer esta prueba, la parte deberá acompañar, en su caso, transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el caso.
2. La parte que proponga este medio de prueba podrá aportar los dictámenes y medios de prueba instrumentales que considere convenientes. También las otras partes podrán aportar dictámenes y medios de prueba cuando cuestionen la autenticidad y exactitud de lo reproducido.
3. El tribunal valorará las reproducciones a que se refiere el apartado 1 de este artículo según las reglas de la sana crítica.

Artículo 383 Acta de la reproducción y custodia de los correspondientes materiales
1. De los actos que se realicen en aplicación del artículo anterior se levantará la oportuna acta, donde se consignará cuanto sea necesario para la identificación de las filmaciones, grabaciones y reproducciones llevadas a cabo, así como, en su caso, las justificaciones y dictámenes aportados o las pruebas practicadas.
2. El material que contenga la palabra, la imagen o el sonido reproducidos habrá de conservarse por el Letrado de la Administración de Justicia, con referencia a los autos del juicio, de modo que no sufra alteraciones.

Artículo 384 De los instrumentos que permitan archivar, conocer o reproducir datos relevantes para el proceso
1. Los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, que, por ser relevantes para el proceso, hayan sido admitidos como prueba, serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar y de modo que las demás partes del proceso puedan, con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga.
2. Será de aplicación a los instrumentos previstos en el apartado anterior lo dispuesto en el apartado 2 del artículo 382. La documentación en autos se hará del modo más apropiado a la naturaleza del instrumento, bajo la fe del Letrado de la Administración de Justicia, que, en su caso, adoptará también las medidas de custodia que resulten necesarias.
3. El tribunal valorará los instrumentos a que se refiere el apartado primero de este artículo conforme a las reglas de sana crítica aplicables a aquéllos según su naturaleza.

En su apartado 2, el artículo 90 recoge la inadmisibilidad de pruebas que se hayan obtenido directa o indirectamente con violación de derechos fundamentales o libertades públicas. Esta cuestión, según este artículo, podrá plantearse por cualquiera de las partes o de oficio por el Juzgado en el momento de la proposición de la prueba. Al efecto, se oirá a las partes y en su caso se practicarán las diligencias que se puedan practicar en ese momento procesal o a través de diligencias finales si fuera necesario. Contra la resolución que se dicte sobre la pertinencia de la prueba solo cabrá recurso de reposición, que se interpondrá, dará traslado a las partes y resolverá en el mismo acto del juicio, quedando únicamente la posibilidad de impugnar la prueba ilícita en el recurso frente a la sentencia.

El estudio de la ilicitud de la prueba se puede realizar con anterioridad al acto del juicio o después de este. Del tenor literal de la Ley Reguladora de la Jurisdicción Social y la Ley de Enjuiciamiento Civil se desprende que debe realizarse en el propio acto del juicio, pues dichas leyes disponen que "no se admitirán las pruebas ilícitas (…)", por lo que se deberá plantear el incidente contradictorio del art. 90.2 LRJS y 287 LEC en el momento de la admisión de la prueba, lo cual puede realizarse antes del juicio, pero también en el mismo momento del acto del juicio. No obstante, también es permitido, como no podía ser de otra forma, plantear la ilicitud de la prueba a través del recurso contra la sentencia. En cualquier caso, como apuntan acertadamente diferentes autores como Abel Junch o Picó i Junoy, "no es posible que el tribunal pueda soslayar el incidente de ilicitud e inadmitir de oficio y ab limine una prueba por ilícita, como si puede hacer al inadmitir una prueba por impertinente o inútil".

Por su parte, si el juez advierte la ilicitud de la prueba en el momento de dictar sentencia, deberá decidir si valora la prueba ilícita para dictar sentencia o iniciar incidente contradictorio para que las partes puedan realizar alegaciones, lo que además de respetuoso con las partes, generaría una menor indefensión. Lamentablemente en la práctica esta posibilidad es muy remota, decantándose el juez casi siempre por la valoración de la prueba ilícita en la sentencia, debiendo impugnarse la ilicitud de la prueba a través del recurso.

El artículo 108 de la LRJS establece las posibles calificaciones del despido en la sentencia; procedente, cuando quede acreditado el incumplimiento alegado por el empresario en la carta de despido, improcedente, cuando no se haya acreditado las causas

alegadas en la carta de despido o no sea proporcional, y nulo, por tener como móvil alguna de las causas de discriminación prevista en la Constitución y en la ley, o, en lo que importa a esta tesis, se produzca con violación de derechos fundamentales y libertades públicas del trabajador. Los artículos 110 y 115 LRJS establecen los efectos de la declaración de improcedencia y nulidad respectivamente.

Recordamos que el despido, conforme al artículo 55.5 ET, es calificado como procedente cuando quede acreditado el incumplimiento alegado por el empresario en su escrito de comunicación, y será improcedente en caso contrario o cuando en su forma no se ajustara a lo establecido en el apartado 1. Por su parte, será calificado como nulo cuando se produzca con violación de derechos fundamentales y libertades públicas del trabajador.

En última instancia, resulta adecuado mencionar la aplicación supletoria en el proceso social de la Ley de Enjuiciamiento Civil. En esta materia de ilicitud de la prueba del artículo 287 de la LEC establece que "1. Cuando alguna de las partes entendiera que en la obtención u origen de alguna prueba admitida se han vulnerado derechos fundamentales habrá de alegarlo de inmediato, con traslado, en su caso, a las demás partes.

Sobre esta cuestión, que también podrá ser suscitada de oficio por el tribunal, se resolverá en el acto del juicio o, si se tratase de juicios verbales, al comienzo de la vista, antes de que dé comienzo la práctica de la prueba.

A tal efecto, se oirá a las partes y, en su caso, se practicarán las pruebas pertinentes y útiles que se propongan en el acto sobre el concreto extremo de la referida ilicitud.

Contra la resolución a que se refiere el apartado anterior solo cabrá recurso de reposición, que se interpondrá, sustanciará y resolverá en el mismo acto del juicio o vista, quedando a salvo el derecho de las partes a reproducir la impugnación de la prueba ilícita en la apelación contra la sentencia definitiva".

9.2.2 Jurisprudencia.

Partiendo de la base normativa anteriormente mencionada, se realiza a continuación una valoración de la jurisprudencia de la que aparecen dos corrientes; los partidarios de que la ilicitud de la prueba digital genera que los hechos que probaron devienen no acreditados, dando como resultado la calificación del despido como improcedente, y los partidarios de conllevar la nulidad de la prueba con el resultado de la calificación como despido nulo. Ante esta disyuntiva cabe recordar que no hay jurisprudencia en unificación de doctrina en esta materia.

9.2.2.1. Calificación del despido como improcedente.

Parecen ser mayoría los partidarios de la improcedencia, resaltando a modo de ejemplo, la sentencia del Tribunal Superior de Justicia de Castilla La Mancha (Albacete) de 12 de enero de 2018, en la que se enjuiciaba el despido de un vigilante de seguridad por unos hechos grabados con una cámara de videovigilancia instalada en su caseta sin previa advertencia de su colocación. Entiende que la prueba es ilícita al no superar el juicio de proporcionalidad, y valorando si conllevase la nulidad conforme al artículo 55.5 ET o la improcedencia con base en los artículos 90.1 LRJS, 287 LEC, 11 de la LOPJ, concluye que el despido debe ser calificado como improcedente pues "la no admisión del medio contaminado no conlleva a que la decisión extintiva, en sí misma considerada, pretendiera la vulneración de un derecho fundamental o libertad pública del trabajador, que llevara aparejada la calificación de nulidad del mismo (art. 55.5 ET) (…) pensamos que la sanción de nulidad tiene su fundamento en el móvil del empresario cuando el despido en sí mismo responde a una causa vulneradora de un derecho fundamental, de ahí la prescripción del artículo 55.5 ET, pero no cuando la finalidad del empresario es comprobar un comportamiento del trabajador para obtener la prueba de la causa alegada para justificar el despido, en cuyo caso, procede la nulidad de dicha prueba obtenida con vulneración de derechos fundamentales o libertades públicas, sin que tal nulidad pueda extenderse a la calificación del despido que podrá ser improcedente o incluso procedente, si una vez desechados los hechos acreditados mediante la prueba ilegal o ilegítima, aun resultan probados, mediante prueba hábil e idónea hechos que constituyen un incumplimiento grave y culpable del trabajador".

En el mismo sentido se pronunció la sentencia del Tribunal Superior de Justicia de Andalucía (Sevilla) de 9 de marzo de 2001 donde en base al móvil o intención vulnerados de un derecho fundamental parte del empresario, califica el despido como improcedente y no nulo, pues el despido se basó en "la conducta del trabajador y no en el móvil atentatorio a su derecho a la intimidad". En este caso se matizó que no se traslada la doctrina del "árbol envenenado" al no juzgarse la ineficacia de un procedimiento penal.

Discrepamos de esta doctrina (de la intención vulneradora de DDFF por parte del empresario) que pretende conocer cuál ha sido el móvil del empresario, cosa prácticamente imposible, salvo torpeza extrema en su interrogatorio, pues dicho móvil vulnerador de un derecho fundamental no se va a indicar en la carta de despido, por lo que se exigiría realizar una actividad adivinatoria a los juzgadores más propia de videntes que de magistrados.

Otra corriente dentro de los partidarios de la improcedencia, más simple y superficial, pero que no requiere un alarde adivinatorio, es la que propugna que el despido debe ser calificado como improcedente al no haberse acreditado la causa del despido al no haberse admitido la prueba que vulnera derechos fundamentales. En este sentido, la sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de fecha 21 de marzo de 2017, que estudiaba el caso de un despido acreditado únicamente con una grabación por cámaras de videovigilancia genéricas sin conocimiento por parte de los trabajadores entendió que "(…) es igualmente ajustado el razonamiento de la Sentencia de instancia que al considerar que no son válidas a efectos probatorios las grabaciones aportadas, y no aportando la empresa algún otro medio de prueba acreditativo de la comisión de los hechos imputados a la actora en la carta de despido, procede declarar la improcedencia del despido".

En el mismo sentido se pronunció la sentencia del Tribunal Superior de Justicia de Madrid, de 7 de marzo de 2014, que calificaba el despido como improcedente al basado en la información obtenida de un GPS situado en el vehículo profesional que permitía conocer el posicionamiento incluso fuera de la jornada sin el conocimiento de la empleada. De la misma manera se pronunció nuevamente el Tribunal Superior de Justicia

de Madrid en fecha 20 de enero de 2020 en la que se juzgaba despido de un trabajador tras prueba pericial informática que analizaba los instrumentos de trabajo propiedad de la empresa puestos a disposición del trabajador con prohibición de uso para actividades extralaborales y sin expectativa de intimidad para este. El Tribunal estableció que "El que la sentencia no de credibilidad a la prueba empresarial, que por otra parte solo afectó a una de las imputaciones contenidas en la carta -la competencia ilegal- pero el despido contiene otra imputación grave, sobre la que se practica una prueba de cargo distinta, una prueba testifical, que se rechaza porque no han << quedado claras las posturas de las partes. Esta imputación, que se intentó probar con testifical, puede justificar la declaración de improcedencia, pero no la nulidad. De hecho, la naturaleza de las imputaciones permite explicar la medida previa de suspensión preventiva si las relacionamos con la categoría laboral del actor. Así las cosas, es también evidente que no hay hechos probados en el relato fáctico que justifiquen la procedencia del despido, pero ello conlleva la improcedencia de este y no su nulidad. Ello supone también la estimación del motivo 6º del mismo -por infracción de los artículos 179.3, 182.1 d), 183.1 y 2 de la LRJS, 9.2, 24.1 y 120 de la CE y 11 y 248.1 de la LOPJ y 218 de la LEC sobre la improcedencia de la indemnización complementaria por infracción de derechos fundamentales.

Tampoco supone una infracción del derecho de intimidad del trabajador la exigencia de que durante este breve periodo de suspensión retribuida deje de disponer -y entrego a la empresa- << el ordenador, el móvil y el resto de material propiedad de la empresa >> máximo cuando existe un protocolo (hecho probado 7º que hemos admitido) que prohíbe la utilización de estos instrumentos para actividades personales. No se observa trato degradante alguno -que no lo es sin más la mera suspensión breve y retribuida referida- pues el actor deja de acudir a la empresa manteniendo su retribución y categoría, ni se identifica la supuesta invasión de la intimidad por la sentencia que no puede presumirse sin más por el hecho de devolver transitoriamente, durante el periodo de inasistencia, el material de la empresa cedido con la exclusiva finalidad de ser empleado con motivo y durante la actividad laboral. Además, es la sentencia la que tiene que indicar que garantía ha infringido la empresa al utilizar la prueba pericial, que en todo caso no es un motivo de resolución contractual -si no se indica la concreta infracción de la intimidad- sino, en su caso, un elemento de ineficacia probatoria de la pericial o de falta de credibilidad de los emails (…)". Es decir, el Tribunal en esta sentencia separa los diferentes hechos

relatados en la carta de despido y cada uno de los elementos probatorios aportados al plenario, sin que si una de las pruebas es ilícita conlleva la nulidad del despido (como sería si se aplicara la doctrina del árbol envenenado), sino que la ilicitud de una prueba conlleva solo la anulación de la misma con el resultado de no acreditación de los hechos, quedando pendiente valorar otros hechos de la carta y otras pruebas practicadas (p.ej. testifical).

Recientemente se ha dictado una sentencia en este sentido por el Tribunal Superior de Justicia de Madrid de 8 de junio de 2023 donde se concluía la prueba ilícita no implicaba directamente la calificación como despido nulo.

Esta sentencia examinó las consecuencias jurídicas en relación con la calificación del despido, esto es, si la nulidad del mismo aplicando el art. 55 ET o las que se derivan de la obtención de una prueba ilícita con arreglo al artículo 11.1 LOPJ, que serán la procedencia o improcedencia del despido, según hayan quedado o no probados los incumplimientos contractuales alegados en la carta de despido, una vez eliminados los hechos obtenidos de tal modo.

Entendió que no procedía la calificación de despido nulo de conformidad puesto que no se ha probado que la decisión extintiva acordada por la empresa demandada, en si misma considerada, pretendiera la vulneración de derechos fundamentales o libertades públicas de la trabajadora, ni que el móvil del empresario al acordar el despido respondiera a una causa vulneradora de esos derechos fundamentales lo que legalmente llevaría aparejada la nulidad del despido según dispone la norma Estatutaria.
Otra cosa es que el empresario, al intentar comprobar el comportamiento de su empleada y obtener pruebas de algunos de sus incumplimientos para tratar de justificar un despido, ha obtenido de forma ilícita tal prueba con vulneración de derechos fundamentales , no pudiendo de esta manera confundirse el despido con violación de derechos fundamentales con la infracción de derechos fundamentales para la obtención de la prueba de parte de los hechos en los que se basó la empleadora para adoptar tal sanción.

9.2.2.2. Calificación del despido como nulo.

Dentro de los partidarios de la nulidad, hay quien sigue la doctrina del árbol envenenado en la cual, prueba ilícita por vulnerar derecho fundamental conlleva la nulidad del despido. En la sentencia del Tribunal Superior de Justicia de Cataluña de fecha 22 de mayo de 2015 se aplicó esta doctrina del árbol envenenado al entender nulo un informe de una empresa de seguridad basado en la grabación de unas imágenes obtenidas de forma ilícita, sin consentimiento ni información y, por tanto, vulnerando el derecho fundamental a la protección de datos de carácter personal ex art. 18.2 CE. En relación con la aplicación de la doctrina anglosajona del "fruto del árbol envenenado o emponzoñado". En concreto, dicha sentencia entendió que "Por tanto, debemos confirmar la resolución recurrida, en el sentido de que la obtención de la fuente de prueba consistente en las grabaciones de vídeo fue ilícita por vulnerar el derecho fundamental a la protección de datos de carácter personal (art. 18.4 CE), y con carácter derivado, por aplicación de la doctrina de los frutos del árbol prohibido (vid. art. 11.1 LOPJ); la prueba consistente en el informe de Securitas, causalmente derivada de las grabaciones de vídeo, y en clara conexión de antijuridicidad con la misma, puesto que la prueba refleja no se hubiera obtenido razonablemente, sin la vulneración del derecho y existe, cuanto menos, negligencia grave del que se beneficia de la prueba que obvia toda garantía de jurisdiccionalidad en su obtención (art. 90.4 LRJS) y utiliza para fines distintos a los declarados (seguridad vs. control de la actividad laboral) los datos personales de los trabajadores".

En el mismo sentido se posicionó el Tribunal Superior de Justicia del País Vasco en su sentencia de fecha 10 de mayo de 2011, que valoraba como ilícita la prueba obtenida por unos detectives privados a través de un GPS para despedir a un trabajador y concluye que "encuentran cobijo no solo los supuestos en que el cese se produce como consecuencia del ejercicio legítimo de un derecho fundamental, sino también aquellos otros en que los hechos que lo sustentan han sido conocidos por el empresario mediante métodos que conculcan los derechos fundamentales del afectado".

Siguiendo esta doctrina se encuentra también la sentencia del Tribunal Superior de Justicia de Andalucía (Málaga), de fecha 5 de abril de 2017 que juzgaba el despido de un trabajador basado en pruebas obtenidas con cámaras de videovigilancia, calificando el despido como nulo.

En el mismo sentido, se dictó la Sentencia del Tribunal Superior de Justicia de Asturias de 30 de noviembre de 2013, cuando juzgaba el despido de una trabajadora motivado por el acceso a correos electrónicos vulnerando el derecho a la intimidad y concluyó que

> "La decisión de sacar el contenido de los correos electrónicos enviados por la recurrente del ámbito privado en que se había producido y su utilización como causa de despido, al igual que su vulneración al presente proceso, vulnera frontalmente su derecho a la intimidad y al secreto de las comunicaciones (…) con independencia de que el contenido del mensaje transmitido pertenezca o no al ámbito de lo personal, lo íntimo o lo reservado, por lo que resulta forzoso declarar como nulo el despido, de conformidad con lo dispuesto en el artículo 55.5 ET".

9.2.3 Conclusiones.

Ha quedado patente que la normativa establecida al efecto no da una respuesta clara a la calificación del despido cuando la única prueba en la que se basa el despido se ha obtenido con vulneración de algún derecho fundamental de los trabajadores. Por una parte, está el artículo 11 de la LOPJ que dispone que no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales. De la misma forma se dispone en el artículo 90.2 de la LRJS, pero lo hace desde el punto de vista de la admisibilidad y concreta que resultan inadmisibles las pruebas que se hayan obtenido directa o indirectamente con violación de derechos fundamentales o libertades públicas. Esta cuestión, podrá plantearse por cualquiera de las partes o de oficio por el Juzgado en el momento de la proposición de la prueba.

Por tanto, al no existir una normativa clara al respecto, corresponde al Juez la calificación del despido como nulo, procedente o improcedente. Esta intervención del juez no solo opera a petición de la parte, conforme al principio de justicia rogada, sino también de oficio, sin incurrir por ello en incongruencia ni infracción procesal alguna, estando además obligado, si se evidencia infracción de derechos fundamentales en la actuación

extintiva del empleador, a emitir una calificación acorde con esa violación (TSJ Castilla-La Mancha 18-5-04).

En relación con la jurisprudencia es importante indicar que en esta materia no hay en unificación de doctrina, por lo que, hay cierta inseguridad jurídica al respecto.

Como hemos visto, existen dos corrientes, los que concluyen que la prueba ilícita conlleva la nulidad del despido y para los que genera la improcedencia del despido. Dentro de los partidarios de la improcedencia, existe cierta jurisprudencia basada en la intención vulneradora de los derechos fundamentales del trabajador por parte del empresario, lo que resulta, al menos desde mi punto de vista, una labor prácticamente imposible, salvo torpeza extrema del empresario, ya sea indicándolo en la carta de despido o al declarar en el acto del juicio. Esta corriente pretende conocer la intención del empresario exigiendo realizar una actividad adivinatoria a los juzgadores más propia de videntes que de magistrados.

Por otro lado, existe una corriente más simple y superficial, pero que no requiere un alarde adivinatorio, la que propugna que el despido debe ser calificado como improcedente al no haberse acreditado la causa del despido al no haberse admitido la prueba que vulnera derechos fundamentales.

Por otra parte, está la doctrina que califica al despido como nulo si la decisión de extinguir por causas disciplinarias el contrato de trabajo se basó exclusivamente en las conclusiones obtenidas de un informe cuyos datos fueron obtenidos de manera ilícita con infracción de derechos constitucionales, el informe no solo resulta ineficaz, calificando la prueba como nula, sino que serán nulos cuantos actos y medidas traigan causa de ella, por lo que el despido también será calificado como nulo.

Sin embargo, a pesar de utilizar un medio vulnerador de derecho fundamental para la comprobación de un hecho constitutivo de despido, si este no ha sido el único medio para acreditar el mismo, el despido no tiene por qué ser nulo, pudiéndose declarar procedente o improcedente, pues pueden existir otras pruebas que acrediten los hechos constitutivos de despido.

En cualquier caso, a la vista de la doctrina mencionada parece prevalecer la vulneración de un derecho fundamental a la verdad material.

9.3. La prueba pericial informática.

Dada cuenta los temas que se están tratando en esta tesis, y especialmente en este apartado sobre la valoración de la prueba electrónica en relación con el control empresarial efectuado a través de las nuevas tecnologías de la información y comunicación, resulta conveniente hacer un breve estudio de la prueba pericial informática, pues esta es en muchos casos clave para realizar el control empresarial y determinar las infracciones de los trabajadores.

Además, como se ha indicado en el apartado 8.1. de esta tesis, para poder modificar los hechos declarados probados a través del recurso de suplicación es preciso basarse en pruebas documentales o periciales practicadas en el juicio, por lo que esta pericial informática, cobra especial relevancia[183].

En relación con la prueba pericial, el artículo 93 de la Ley Reguladora de la Jurisdicción Social establece su apartado 1 que,

> "La práctica de la prueba pericial se llevará a cabo en el acto del juicio, presentando los peritos su informe y ratificándolo. No será necesaria ratificación de los informes, de las actuaciones obrantes en expedientes y demás documentación administrativa cuya aportación sea preceptiva según la modalidad procesal de que se trate".

Por su parte, la Ley de Enjuiciamiento Civil establece en su artículo 632 que "Los Jueces y los Tribunales apreciarán la prueba pericial según las reglas de la sana crítica, sin estar

[183] Art. 193 LRJS:
a) Reponer los autos al estado en el que se encontraban en el momento de cometerse una infracción de normas o garantías del procedimiento que haya producido indefensión.
b) Revisar los hechos declarados probados, a la vista de las pruebas documentales y periciales practicadas.
c) Examinar las infracciones de normas sustantivas o de la jurisprudencia.

obligados a sujetarse al dictamen de los peritos", por tanto, como ha entendido la jurisprudencia, el juez será quién valore a través de lógica y sentido común los informes periciales que se planteen, pero aún ratificados por sus autores no resultarán en ningún caso vinculantes para el juzgador de instancia.

La propia exposición de motivos de la Ley de Enjuiciamiento Civil ya adelantaba que "Con las excepciones obligadas respecto de los procesos civiles en que ha de satisfacerse un interés público, esta Ley se inclina coherentemente por entender el dictamen de peritos como medio de prueba en el marco de un proceso, en el que, salvo las excepciones aludidas, no se impone y se responsabiliza al tribunal de la investigación y comprobación de la veracidad de los hechos relevantes en que se fundamentan las pretensiones de tutela formuladas por las partes, sino que es sobre estas sobre las que recae la carga de alegar y probar. Y, por ello, se introducen los dictámenes de peritos designados por las partes y se reserva la designación por el tribunal de perito para los casos en que así le sea solicitado por las partes o resulte estrictamente necesario".

Una vez determinado el régimen jurídico, la prueba pericial se puede definir como un compendió de información con la opinión final o dictamen de un perito, que no es otra cosa que un experto en una materia determinada debidamente titulado, proporcionando al procedimiento y al juzgador de instancia unos conocimientos técnicos que van a permitir valorar unos hechos controvertidos, pero no van a dar un conocimiento directo sobre cómo ocurrieron los hechos, como un atestado o un informe de la Inspección de Trabajo.

En este sentido, la jurisprudencia ha venido entendiendo que el perito es un auxiliar experto que provee al procedimiento y al juzgador de instancia conocimientos especializados de carácter científico o técnico, de los que él no dispone, y que son necesarios para formar criterio y emitir la correspondiente sentencia. (Por ejemplo, la STS de 26 de septiembre de 2005).

En lo que afecta a la pericial informática, esta debe desarrollarse, al igual que otras periciales, por un experto debidamente titulado, normalmente en los casos de periciales informáticas, será un Ingeniero Informático. En este sentido tanto el artículo 87 de la LRJS como el artículo 340.1 y 2 de la LEC disponen que los peritos deberán estar

debidamente titulados, en posesión de un título oficial correspondiente a la materia objeto de su informe. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias. Podrá asimismo solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia, pudiendo, por tanto, emitir dictamen las personas jurídicas legalmente habilitadas para ello.

Como hemos adelantado, las periciales informáticas tienen especial relevancia en el uso de las nuevas tecnologías tanto por los trabajadores como por el empresario al realizar un control de la prestación del servicio. Estás periciales van a intentar acreditar una serie de hechos encontrados en un ordenador, por lo que, como se ha indicado en el apartado 6.8 de esta tesis, el análisis de un hardware debe conllevar que se garantice la cadena de custodia para evitar posibles manipulaciones. Como se advertía en el mencionado apartado, para garantizar la cadena de custodia la empresa debe, en presencia de un notario y en el centro de trabajo o lugar donde el trabajador tenga el ordenador o hardware a analizar, precintar el ordenador para luego ser depositado ante la correspondiente Notaría. Será en la propia notaría donde el ordenador deba permanecer y donde se deba analizar el mismo o extraer las copias necesarias. Si se siguen estos pasos de intervención, sellado, depósito y copias, se garantizará adecuadamente la custodia de la información obrante en el ordenador propiedad de la empresa que fue puesto a disposición del trabajador como herramienta de trabajo (Por ej. Sentencia de TSJ de Madrid, de 13 de mayo de 2016 o de 14 de enero de 2020).

Las periciales informáticas van a versar principalmente sobre la eliminación de archivos en los ordenadores, intentando acreditar quien, donde y cuando se realizó, acceso o apropiación de bases de datos de empresas, verificación de correos electrónicos, espionaje corporativo, certificación de desarrollo de software o manipulación de archivos audiovisuales.

Para la elaboración de una pericial de este tipo, se va a tener que realizar un análisis preliminar de la prueba informática que se quiere obtener, garantizar la cadena de custodia de la misma y, por último, realizar el análisis forense de la información.

El análisis digital forense ha sido definido por algunos autores[184], como "la aplicación de técnicas científicas y analíticas especializadas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal".

La norma internacional ISO/IEC 27037:2012 es la norma donde se establecen las directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas o digitales. Estos procesos deben diseñarse con la finalidad de conservar la integridad de la prueba y seguir una metodología concreta para contribuir a su admisibilidad en procesos legales. De acuerdo con esta norma internacional la evidencia digital se rige por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital. Esta norma también va a proporcionar las directrices generales para la obtención de pruebas no digitales que pueden ser útiles en la etapa de análisis de la evidencia digital. La norma pretende orientar a aquellos responsables de la identificación, recolección, adquisición y preservación de potencial evidencia digital, asegurando que las personas responsables de gestionar potencial evidencia digital lo hagan con prácticas aceptadas en todo el mundo, con el objetivo de realizar la investigación de una manera sistemática e imparcial, preservando su integridad y autenticidad. La evidencia digital puede obtenerse de diferentes tipos de dispositivos digitales, redes, bases de datos, etc. La rigurosidad de la aplicación de una metodología adecuada se debe a la fragilidad de la evidencia digital[185].

Por tanto, a la vista de lo relatado el Juzgador de instancia deberá valorar la prueba pericial en base a las reglas de la sana crítica, la cual, según la doctrina jurisprudencial, se sujeta en los siguientes parámetros:

En primer lugar, se debe valorar la cualificación del perito y su propia especialización sobre el concreto supuesto a enjuiciar. En este sentido tanto el artículo 87 de la LRJS

[184]ROATTA, S., CASCO, M.E., y FOGLIATO, M. (2012) "El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012", publicado en https://core.ac.uk/download/pdf/296383939.pdf o http://sedici.unlp.edu.ar/bitstream/handle/10915/46243/Documento_completo.pdf?sequence=1&isAllowed=y

[185]ROATTA, S., CASCO, M.E., y FOGLIATO, M. (2012) "El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012", publicado en https://core.ac.uk/download/pdf/296383939.pdf o http://sedici.unlp.edu.ar/bitstream/handle/10915/46243/Documento_completo.pdf?sequence=1&isAllowed=y

como el artículo 340.1 y 2 de la LEC disponen que los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de este.

En segundo lugar, se debe tener en cuenta el método seguido por el perito a la hora de realizar la pericial. La Norma ISO/IEC 27037:2012 es una norma internacionalmente reconocida donde se establecen las directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas o digitales. Asimismo, junto con el dictamen pericial, se puedan aportar la documentación, instrumentos o materiales adecuados para exponer lo que haya sido objeto de pericia.

En tercer lugar, se valorarán las condiciones de observación y de reconocimiento en las que se han estudiado las evidencias digitales.

En cuarto lugar, se valorará la objetividad del perito, es decir, la mayor o menor vinculación del perito con las partes. En este sentido, ninguna norma otorga mayor credibilidad probatoria al dictamen de un perito judicial que uno de parte, pues como se está viendo, ha de atenderse a su resultado, el nivel de conocimientos de perito, el desarrollo de las operaciones periciales y sus conclusiones. Sin embargo, en la práctica si se valora de mejor manera los peritos judiciales que los de parte.

Otro de los factores a tener en cuenta es la simple proximidad en el tiempo, dándole mayor credibilidad al dictamen se emita con cierta proximidad al hecho que lo fundamenta.

La concordancia entre el contenido y el objeto del dictamen será otro parámetro importante a tener en cuenta por el Juzgador, valorando las posibles extralimitaciones del perito o si no se recoge parte de la controversia.

El interrogatorio efectuado a los peritos en Sala también se tendrá en cuenta, valorándose la espontaneidad, razonabilidad o base científico-técnica de la explicación.

Por último, de existir varios dictámenes periciales, se aplicará el criterio de la mayoría coincidente, donde el dictamen de varios peritos coincidentes va a prevalecer sobre el contrario.

9.4. Análisis del Hardware de la empresa vs derecho a la intimidad y cadena de custodia.

Además de la supervisión del correo electrónico, el empresario puede pretender el análisis del propio hardware puesto a disposición del trabajador. En cualquier caso, parece que el análisis del hardware va encaminado a revisar el software, pues el hardware no se va a poder analizar en sí mismo, sino que se debe profundizar en su contenido, el software. A fin de facilitar la comprensión, conviene definir los conceptos hardware y software.

"El hardware, (equipo o soporte físico)[186] en informática se refiere a las partes físicas, tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Los cables, así como los muebles o cajas, los periféricos de todo tipo, y cualquier otro elemento físico involucrado, componen el hardware o soporte físico; contrariamente, el soporte lógico e intangible es el llamado software" (Wikipedia, 2022).

Constituye el «Conjunto de los componentes que integran la parte material de una computadora» (RAE, 2022).

Se va a considerar hardware también, a los teléfonos móviles, las cámaras fotográficas o cualquier otro dispositivo electrónico.

Se denomina software, logicial o soporte lógico[187] al "sistema formal de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware. La interacción entre el software y el hardware hace operativo un ordenador (u otro dispositivo), es decir, el software envía instrucciones que el hardware ejecuta, haciendo posible su funcionamiento" (Wikipedia, 2022).

[186] https://es.wikipedia.org/wiki/Hardware

[187] https://es.wikipedia.org/wiki/Software

Los componentes lógicos incluyen, entre otros, el sistema operativo (Windows, Linux, IOS) las aplicaciones informáticas, los procesadores de texto, y las hojas de cálculo.

Por tanto, en el hardware no hay realmente nada, sino que será en el software donde se encuentre las aplicaciones, correos electrónicos, y demás, donde se encontrará la información sensible. Sin embargo, para analizar el software se precisa el hardware, por lo que en este apartado estudiaremos como el empresario debe recuperar los diferentes dispositivos y poder analizarlos, con el fin de no romper la cadena de custodia y evitar posibles manipulaciones.

Para ello, es preciso tener en cuenta y recoger en el informe, un identificador univoco de la evidencia (número de serie o similar), los datos de acceso a la evidencia, es decir, quién, cuándo y dónde se accede a la misma, los traslados de la evidencia, las tareas realizadas en la misma y, por último, el registro de todo cambio potencial en la evidencia digital con el nombre del responsable y la justificación de las acciones realizadas[188].

Por tanto, para garantizar la cadena de custodia la empresa debe, en presencia de un notario y en el centro de trabajo o lugar donde el trabajador tenga el ordenador o hardware a analizar, precintar el ordenador para luego ser depositado ante la correspondiente Notaría. Será en la propia notaría donde el ordenador deba permanecer y donde se deba analizar el mismo o extraer las copias necesarias. Si se siguen estos pasos de intervención, sellado, depósito y copias, se garantizará adecuadamente la custodia de la información obrante en el ordenador propiedad de la empresa que fue puesto a disposición del trabajador como herramienta de trabajo. En este sentido, se dictó la sentencia de TSJ de Madrid, de 13 de mayo de 2016 o de 14 de enero de 2020, la cual se comenta a continuación.

En esta sentencia, se estudiaba el despido de un trabajador efectuado por la empresa a la luz de unas comunicaciones realizadas por el trabajador a través de la aplicación Yahoo Messenger. Al margen de valorar la posible intromisión al derecho a la intimidad y al secreto de las comunicaciones el tribunal estudia la posible rotura de la cadena de custodia

[188] Norma ISO/IEC 27037/2012

en la intervención del ordenador propiedad de la empresa puesto a disposición del trabajador como herramienta de trabajo. En este sentido, el tribunal concluye que no se dieron las condiciones básicas que exige la legislación y la jurisprudencia en la entrega del ordenador y el móvil por parte del trabajador, ya que se le priva de conocer la razón de su permiso retribuido, trato que ya de por sí es degradante y atentatorio contra la dignidad del trabajador, sino que además se tiene pleno acceso al ordenador y el móvil del trabajador sin garantías, y pese a que se ha realizado por perito, este es de parte, y no se ha acreditado en modo alguno que el análisis del ordenador y el móvil se hayan realizado con todas las garantías legales que ya hemos visto que hay que tener en cuenta, ni siquiera sabemos si los emails se han podido manipular o no, ya que el trabajador no estaba presente ni tampoco fedatario público que pudiera avalar este hecho ni representante de los trabajadores, por lo que la prueba pericial queda invalidada por estas circunstancias de vulneración de derechos fundamentales.

9.5. Detectives privados y derecho a la intimidad.

Llegamos a este punto, resulta apropiado hacer un pequeño estudio de la posible intromisión en el derecho a la intimidad de los trabajadores de las investigaciones efectuadas por detectives privados contratados por las empresas.

La doctrina del Tribunal Constitucional[189], configura al derecho a la intimidad como un derecho fundamental estrictamente vinculado a la propia personalidad y que deriva, sin ningún género de dudas, de la dignidad de la persona ex artículo 10.1 CE, que reconoce e implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana".

Por tanto, lo que hace el Tribunal Constitucional es establecer la necesidad 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, pero en todo caso subsistente- de su libertad constitucional", y ello, en base a la posición

[189] SSTC 170/1997, de 14 de octubre, 231/1988, de 1 de diciembre; 197/1991, de 17 de octubre; 57/1994, de 28 de febrero; 143/1994, de 9 de mayo; 207/1996, de 16 de diciembre; y 202/1999, de 8 de noviembre; etc.

preferente que ocupan los derechos fundamentales en nuestro ordenamiento jurídico, especialmente del derecho a la intimidad.

Por su parte, el Tribunal Supremo[190] ha entendido que los informes emitidos por detectives privados no podrán tacharse genéricamente como prueba nula por vulnerar el derecho a la intimidad personal, ni atentar a la dignidad personal del trabajador o intimidad, por cuanto sostener lo contrario supondría vaciar de contenido el derecho de dirección de la empresa y la propia intervención de este colectivo en el ámbito laboral, aunque siempre se deberá valorar el principio de proporcionalidad.

En esta materia, resulta esclarecedora la sentencia dictada por el Tribunal Superior de Justicia de Madrid de 28 de octubre de 2011, que estudiaba el caso de un despido disciplinario efectuado tras la contratación de un detective privado por la empresa para investigar la conducta de un trabajador en lugares públicos mientras estaba en situación de baja médica.

Aplicando el principio de proporcionalidad, la Sala entendió que la investigación era una medida justificada, y que no vulneraba el derecho a la intimidad del trabajador, pues existían razonables sospechas de un proceso fraudulento de incapacidad temporal, idónea para la finalidad pretendida por la empresa (que no era otra que verificar si la trabajadora simulaba o no una situación de baja médica, y en su caso adoptar la medida disciplinaria de despido), necesaria (ya que el informe del detective privado y la ratificación del mismo en el acto de juicio, constituía una prueba útil y adecuada para acreditar la conducta del trabajador); y equilibrada (pues el informe del detective privado y la grabación de imágenes se limitó a unos días en concreto con el único objetivo de comprobar que actividades realiza diariamente para concluir si se corresponden con las de una persona lesionada o enferma o de lo contrario pudieran existir indicios de fraude o simulación en su comportamiento.

Concluyó la Sala que no se vulnera el derecho a la intimidad de la trabajadora por el mero hecho de ser investigada por un detective privado durante un breve lapso temporal con el

[190] Sentencias del Tribunal Supremo de fechas 01/12/1986 y 24/07/1990

objeto de verificar su comportamiento durante su situación de incapacidad temporal, pues dicha medida no era arbitraria ni caprichosa, y además, se desarrolló en un estricto marco de confidencialidad y de secreto profesional por un detective privado debidamente habilitado a tal efecto, con el objeto comprobar si las actividades que realizaba se correspondían con las de una persona lesionada o se trataba de una simulación, y por tanto, constituían una transgresión de la buena fe contractual.

10. Transgresión de la buena fe y desobediencia.

Los incumplimientos laborales relacionados con el uso inadecuado de las nuevas tecnologías por el trabajador podrán constituir una transgresión de la buena fe contractual, o incluso desobediencia, si la empresa había informado previamente del uso que puede hacerse de las herramientas y medios tecnológicos puestos a disposición de los trabajadores.

Tanto la transgresión de la buena fe contractual como la desobediencia son conceptos jurídicos indeterminados, que no han sido definidos en nuestra legislación, sin embargo, si se recogen como causa de despido en el Estatuto de los Trabajadores.

La transgresión de la buena fe viene recogida en el artículo 54.2. d) junto al abuso de confianza en el desempeño del trabajo, y por su parte, la desobediencia viene reflejada en el artículo 54.2. b) junto con la indisciplina.

Para poder definir la transgresión de la buena fe, se debe definir previamente que se entiende por buena fe en el ámbito de las relaciones laborales. La buena fe, tal y como se ha entendido por el conjunto de la jurisprudencia, puede definirse como el cumplimiento de la legislación o de los acuerdos suscritos entre la empresa y el trabajador, o el cumplimiento de los protocolos a seguir en la empresa.

Por tanto, a la espera de una delimitación y matización del concepto jurídico por nuestra jurisprudencia, se puede definir la transgresión de la buena fe contractual como la pérdida de confianza para con el trabajador por incumplimiento de sus obligaciones.

La Sala de lo Civil de nuestro Alto Tribunal ha definido el concepto de "buena fe contractual", por ejemplo, en la sentencia de 15/06/2009, que la define de la siguiente forma:

> "(…) la buena fe, en su sentido objetivo consiste en dar al contrato cumplida efectividad en orden a la realización del fin propuesto, por lo que deben estimarse comprendidas en las estipulaciones contractuales aquellas obligaciones que constituyen su lógico y necesario cumplimiento, también se ha sentado por la misma que el carácter genérico del artículo 1258 Cc. ha de armonizarse con los más específicos que para cada contrato y en cada supuesto contiene el Código Civil y que la posibilidad de ampliar o modificar, a su amparo, lo estrictamente convenido, ha de admitirse con gran cautela y notoria justificación, es decir, que la expansión de los deberes al amparo del artículo 1258 Cc. debe ser lo más restringida posible, porque no puede escindirse este artículo del contenido del artículo 1283 Cc., según el cual en los términos de un contrato no deberán entenderse comprendidos cosas distintas ni casos diferentes de aquellos sobre los que los interesados se propusieron contratar",

Además, entiende que la buena fe es un criterio objetivo, constituido por una serie de pautas coherentes con el comportamiento en las relaciones humanas y negociales, que en las relaciones laborales no va a funcionar solo como una expresión de la voluntad reflejada en el consentimiento, sino también como una fuente de integración del contenido normativo del contrato, que "actúa por vía dispositiva, a falta de pacto y abstracción hecha de la intención o de la voluntad de las partes", de tal manera que estas derivaciones que complementan el contrato encuentran su en lo establecido expresamente en el contrato, sino también, en la norma o principio general de la buena fe.

Por su parte la Sala de lo Social del Tribunal Supremo ha venido matizando los elementos básicos constitutivos de la transgresión de la buena fe contractual:

En primer lugar, el trabajador tiene que cometer el acto con plena conciencia de que su conducta afecta al elemento espiritual del contrato, consistiendo esa transgresión en la

eliminación voluntaria de los valores éticos que deben inspirar al trabajador en el cumplimiento de los deberes básicos derivados del contrato laboral.

En segundo lugar, debe prevalecer un equilibrio entre la significación y alcance del acto u actos concretos determinantes del despido con las demás circunstancias concurrentes, atendiendo al momento en que se producen los hechos y a los efectos que causan.

En tercer lugar, resulta absolutamente necesario relacionar la conducta y sus antecedentes con la propia transgresión y la gravedad del despido, y ello para que exista adecuación entre el acto y la sanción.

Por último, resulta clave la naturaleza dolosa o culposa de la infracción para calificar de grave la conducta y, por tanto, que se respete el valor constitucional de la justicia que exige, la proporcionalidad y el equilibrio.

Una de las notas características y diferenciadoras de la transgresión de la buena fe contractual y la desobediencia, es el carácter gradualista de la transgresión, por lo que se debe estudiar la aplicación del criterio gradualista existente en nuestra jurisprudencia, por la cual, como veremos, se valora de forma individualizada los incumplimientos laborales cometidos por el trabajador teniendo en cuenta otras circunstancias que permitan matizar el enjuiciamiento, como la categoría profesional del trabajador, su antigüedad en la empresa, los antecedentes, perjuicios económicos o de otra naturaleza, etc.

Para poder definir la teoría gradualista debemos tener en cuenta los deberes y obligaciones laborales de los trabajadores y las potestades del empresario.

Los deberes laborales básicos se establecen en el artículo 5 del Estatuto de los Trabajadores, y en lo que respecta a la transgresión de la buena fe, se recoge el deber de cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia, y cumplir las órdenes e instrucciones del empresario en el ejercicio regular de sus facultades directivas.

Asimismo, el artículo 20.1 ET también recoge como obligación del trabajador, realizar el trabajo convenido bajo la dirección del empresario, debiéndole, además, *ex* art. 20.2 ET, la diligencia y la colaboración en el trabajo que se establezcan en la ley, en los convenios colectivos, usos y costumbres, además del seguimiento de las órdenes o instrucciones adoptadas por el propio empresario en el ejercicio regular de sus facultades de dirección, sometiéndose en sus prestaciones recíprocas a las exigencias de la buena fe. Por tanto, se establece la buena fe como exigencia tanto para el trabajador en la prestación del servicio como al empresario en su dirección del negocio.

Por su parte, el artículo 58, que recoge las faltas y sanciones de los trabajadores, establece la potestad sancionadora por incumplimientos laborales tiene la empresa. Esta facultad sancionadora, como establece el apartado 2 del mencionado artículo 58, estará sujeta al control judicial.

Las sanciones podrán ser leves, graves o muy graves, siendo la sanción más grave el despido. Para que un despido sea calificado judicialmente como procedente se requiere que la falta imputada y más tarde acreditada conlleve un incumplimiento grave y culpable del trabajador.

El resultado de aplicar la tesis gradualista cuando concurren circunstancias a valorar en cada caso concreto incide directamente en la valoración de la prueba, lo que excede del ámbito del recurso de casación para unificación de doctrina, y, además impide la existencia del presupuesto de contradicción, como ha expuesto, entre otras, la sentencia del Tribunal Supremo de 15/01/2009, y las en ella citadas.

En relación con la valoración de la prueba, es doctrina consolidada (por ejemplo STS 24/05/2005) que al valorarse la prueba en cada caso concreto con el fin de valorar si las conductas son merecedoras de la sanción más grave no es materia propia de la unificación de doctrina, pues resulta altamente improbable que se den situaciones o conductas sustancialmente iguales después de un veredicto basado en una valoración individualizada de circunstancias variables, que normalmente no permite la generalización de las decisiones fuera de su ámbito específico, pues “para llegar a la conclusión de que un incumplimiento contractual es grave y culpable se deben, como regla, valorar todas las circunstancias concurrentes no solo en lo afectante al hecho

cometido, sino también en lo relativo a la conducta y persona del trabajador y al entorno empresarial en que acontece" (STS 13/11/2000, FJ 6). El recurso de casación para la unificación de doctrina no se podrá plantear basándose en juicios empíricos de valoración de la conducta humana, porque en estos juicios los elementos circunstanciales de dicha valoración adquieren toda la importancia, existiendo además un elemento de discrecionalidad que no es susceptible de unificación. En este sentido se pronunció el Auto de 5 de noviembre de 1998 (rec. 4546/1997) cuando inadmitiendo el recurso de casación para la unificación de doctrina interpuesto alego que no era materia propia de la unificación de doctrina pues la decisión partía necesariamente de una valoración individualizada que no permitía establecer criterios generales de interpretación. Por lo tanto, la valoración de la prueba en cada caso concreto en consonancia con la aplicación de la tesis gradualista en asuntos de despidos por transgresión de la buena fe contractual y el abuso de confianza hace que estos pleitos carezcan de interés casacional y, por tanto, no se admitan los recursos de casación para la unificación de doctrina.

Como se ha adelantado en el principio de este apartado, y así se recoge en el artículo 54 ET, tanto la desobediencia como la transgresión de la buena fe son causas de despido, pero su definición legal es exigua, debiendo acudir a la jurisprudencia para poder encontrar los diferentes supuestos que componen la transgresión de la buena fe como la desobediencia.

La antigua sentencia del Tribunal Supremo de 16/10/1986 fue una de las pioneras en tratar la transgresión de la buena fe y los perjuicios económicos de la empresa. En esta sentencia se estudiaba el caso de un camarero despedido por no registrar las consumiciones servidas y cobradas, recogiéndose como hecho probado que:

> "de manera consciente y deliberada en lugar de ticar en la caja el valor de las consumiciones servidas, no lo verificó, ni el importe de las bebidas lo ingresó en ella, con lo que de modo grave y culpable transgredió la buena fe contractual, esto es, la fidelidad y lealtad que todo empleado ha de tener para con la empresa que remunera su trabajo, sin que la cuantía de las consumiciones servidas, a tales fines, tenga repercusión para atenuar el sancionable proceder del actor, ya que esta Sala tiene declarado, sentencias de 29 de marzo de 1985 y 24 de junio último, entre

> otras muchas, que la inexistencia de perjuicios o la escasa importancia de estos derivados de la conducta del trabajador, enerve la conclusión expuesta, al no ser trascendente a los fines debatidos... que no se hayan causado perjuicios económicos a la empresa, al no ser requisito indispensable para apreciar la comisión de tal falta, que se configura por la carencia de valores éticos en quien comete tal infracción".

Por tanto, define la transgresión de la buena fe contractual como la fidelidad y lealtad del empleado con su empresa resultando irrelevante causar daños o un perjuicio económico a la empresa.

Por su parte, la sentencia del Tribunal Supremo de 26/01/1987, que trataba el despido de un cajero que no pudo justificar los desajustes de caja, procedía de igual forma, definiendo la buena fe como "directivas equivalentes a lealtad, honorabilidad, probidad y confianza". Esta sentencia concluyó que la transgresión de la buena fe contractual constituía un incumplimiento que, cuando resulta grave y culpable, es causa que justifica el despido aunque no se acredite la existencia de un lucro personal, ni haber causado daños a la empresa y con independencia de la mayor o menor cuantía de lo defraudado, pues resulta suficiente el quebranto de los deberes de fidelidad y lealtad implícitos en la relación laboral, deberes que han de ser más rigurosamente observados por quienes desempeñan puestos de confianza y jefatura en la empresa, aplicándose por tanto la tesis gradualista al valorar de forma más severa al hecho de tratarse de un cargo de confianza.

También se calificó como procedente en la sentencia del Tribunal Supremo de 19/12/1990 el despido de un trabajador por apropiarse de materiales de construcción propiedad del cliente y entendió que dicha conducta constituía una transgresión de la buena fe contractual y abuso de confianza en el desempeño de su trabajo. En este caso, además del quebranto de los deberes de fidelidad y lealtad para con la empresa, existía un lucro a favor del trabajador.

La sentencia del Tribunal Supremo de 4/02/1991 juzgaba el despido de una empleada de banca que fue despedida por realizar operaciones bancarias sin la debida autorización. Esta sentencia resalta la innecesaridad de existencia de concreto perjuicio como a la de

una concreta voluntad de ser desleal, y sin destacar la posible existencia de circunstancia alguna de atenuación de responsabilidad, destacando que "es suficiente para la estimación de la falta el incumplimiento grave y culpable, aunque sea por negligencia, de los referenciados deberes inherentes al cargo", pues en este caso, la empleada hizo asumir a la entidad bancaria unos riesgos injustificados e innecesarios, sin valorar el perjuicio que generaba a la empresa. Por tanto, entendió que los hechos probados eran constitutivos de transgresión de la buena fe contractual, con independencia de que el empleado haya querido o no, consciente y voluntariamente, quebrantar los deberes de lealtad. Entiende suficiente para la calificación como procedente del despido el incumplimiento grave y culpable, aunque sea por negligencia, de los referenciados deberes inherentes al cargo, con independencia igualmente de que el perjuicio económico haya llegado o no a producirse.

En relación con la transgresión de la buena fe y el abuso de confianza con las técnicas de la información y la comunicación (TIC), citaremos una serie de sentencias que tuvieron en cuenta estas nuevas tecnologías para acreditar los despidos. En este sentido, reiteramos que el carácter subjetivo de la transgresión de la buena fe contractual va a imponer la necesidad de valorar cada caso a fin de considerar si una acción del trabajador es merecedora de sanción, no permitiendo a priori establecer hechos o circunstancias constitutivas de transgresión de la buena fe contractual, con la excepción del “robo/hurto” y de la “competencia desleal”, considerando este último como el comportamiento del trabajador que realiza, sin consentimiento de su empresa, un trabajo ya sea por cuenta ajena o por cuenta propia que compite directamente con la empresa que le tiene contratado. De esta forma, se dictó sentencia por el Tribunal Superior de Justicia de Madrid de fecha 26/3/2019 que establece que “los hechos imputados al demandante y que han resultado acreditados constituyen conductas expresamente tipificadas en la Ley de Competencia desleal como comportamientos objetivamente contrarios a las exigencias de la buena fe, y que llenan de este modo el concepto jurídico indeterminado de “transgresión de buena fe contractual recogido en el artículo 54.2 ET cuyos elementos constitutivos básicos, recogidos en la jurisprudencia del Tribunal Supremo, concurren en este caso”. Resulto acreditado para el Tribunal que el demandante tenía plena conciencia de que su conducta afectaba al elemento espiritual del contrato que le vincula con la demandada, y omite el cumplimiento de la normativa interna existente al efecto de regular los supuestos

de conflictos de intereses. Recuerda el Tribunal que el elemento esencial del incumplimiento del deber de abstención, a efectos de que se incurra o no en competencia desleal, no está en el daño efectivamente producido a la empleadora, sino en la intención del trabajador al actuar sin el consentimiento del empresario y sin importarle la lesión de los intereses de este (en este sentido la STSJ Sevilla 5/5/2016), y a este respecto dicha intención fue clara, aunque no constara acreditado un daño concreto producido a la empresa.

En la sentencia del Tribunal Superior de Justifica de Canarias (Santa Cruz de Tenerife) de 3/11/2011 se declara la procedencia del despido de una cajera de un supermercado que mediante cámaras de seguridad se había grabado como sustraía dinero de la caja. La intimidad de la trabajadora no resultó vulnerada y se entendió que la actuación profesional de la trabajadora era constitutiva de transgresión a la buena fe contractual.

En sentido contrario y, por tanto, aplicando la tesis gradualista, pero entendiendo no vulnerador de la transgresión de la buena fe contractual se indican las siguientes sentencias:

La sentencia del Tribunal Supremo de 21/1/1991 calificó el despido de un trabajador por usar incorrectamente horas sindicales como improcedente, aplicando la tesis gradualista, al entender que los hechos no tenían la gravedad ni la importancia para considerarse como vulneradores de la buena fe contractual ni abuso de confianza, entendiendo que solo sería constitutivo de despido si el uso propio del crédito horario se realiza de forma manifiesta y habitual, "poniendo en peligro el derecho legítimo de la empresa a que los representantes formen cuerpo coherente con los representados."

En este sentido, la sentencia del TSJ Madrid de 26/1/2020 entendió que no suponía trasgresión de la buena fe contractual o abuso de confianza en el desempeño del trabajo los comentarios vertidos a los compañeros de trabajo en relación a su actitud de colaboración con la empresa (decirle a dos compañeros que debían haber tardado más en regresar de sus reconocimientos médicos, o que no debían haber accedido a acompañar al Jefe a realizar una actividad que podría suponer un retraso de la hora de salida) ni son ejemplares ni denotan una especial implicación del trabajador en la empresa, pero

tampoco constituyen una trasgresión de la buena fe contractual ni abuso de confianza en el desempeño del trabajo, pues los deberes laborales propios del contrato de trabajo pueden cumplirse sin que sea exigible contractualmente una implicación en la empresa que vaya más allá de aquéllos que constituyen el núcleo de la relación laboral entre las partes. O, dicho de otro modo, no constituye infracción muy grave el incumplimiento de deberes que no forman parte del contenido del contrato de trabajo.

Por tanto, en relación con la transgresión de la buena fe contractual y/o el abuso de confianza en el desempeño del trabajo y los incumplimientos graves y que lo generan, podemos concluir que:

Va a formar parte esencial del contrato de trabajo el principio general de la buena fe, integrando el contenido normativo del contrato, y limitando el ejercicio de los derechos subjetivos de las partes contratantes con el fin de impedir la lesión de los intereses de la otra parte, sino ajustándose a las reglas de lealtad, honradez y mutua confianza.

La buena fe servirá como un criterio para la valoración de conductas al que debe ajustarse el cumplimiento de las obligaciones de los contratantes, resultando como una exigencia de comportamiento ético jurídicamente protegido y exigible en el ámbito contractual la buena fe y a la mutua fidelidad entre empresario y trabajador.

Resultará irrelevante la falta de perjuicios para la empresa o el lucro personal del trabajador para que los hechos se puedan calificar como transgresores de la buena fe contractual.

Tampoco será relevante el componente de voluntariedad. Servirá el incumplimiento grave por negligencia de los deberes inherentes a la relación laboral o al cargo ostentado para calificar el comportamiento como contrario a la buena fe contractual, no siendo necesaria la falta de voluntad del trabajador de comportarse de forma infiel o desleal.

La transgresión de la buena fe contractual comporta un tipo de incumplimiento que admite diferentes graduaciones a la hora de ser sancionada. En este sentido, cuando se califique como grave y culpable será causa que justifique el despido disciplinario, pues dada cuenta

la vulneración se justifica que la empresa no siga confiando en el trabajador que realiza la conducta abusiva o contraria a la buena fe.

Se debe valorar y aplicar la tesis gradualista, por la cual, los trabajadores que desempeñan puestos de confianza y responsabilidad en la empresa estarán más estrictamente observados en el desempeño de las facultades conferidas. En este sentido, la sentencia del Tribunal Supremo de 27/01/2004 estableció que "el enjuiciamiento del despido debe abordarse de forma gradualista buscando la necesaria proporción ante la infracción y la sanción, y aplicando un criterio individualizador que valore las peculiaridades de cada caso concreto (sentencias de 19 y 28 febrero 6 abril y 18 de mayo de 1990, 16 mayo 1991 y 2 de abril y 30 de mayo de 1992, entre otras)".

En relación con el despido, debe efectuarse una interpretación restrictiva de la transgresión de la buena fe, debiéndose aplicar otras sanciones menos graves si del examen de los hechos y circunstancias concurrentes resulta que los hechos imputados, si bien son sancionables, pero no son tan graves, como para sancionar con el despido.

Por otra parte, la desobediencia se define en la RAE como “la acción y efecto de desobedecer”, entendiéndose por desobedecer como la acción de “No hacer lo que ordenan las leyes o quienes tienen autoridad”. Por lo tanto, y en lo que al ámbito laboral se refiere, se debe ir en contra de las directrices emanadas por la empresa. De este modo, para que exista desobediencia debe haber una orden o mandato expreso por la empresa y la falta de tolerancia ante su falta de hacer, de lo contrario, dicha tolerancia impedirá tomar medidas frente a los infractores.

En relación con el control empresarial a través de las TIC y el despido por desobediencia, se ha comentado en el apartado relativo al GPS y al derecho a la intimidad, la sentencia del Tribunal Supremo de fecha 15 septiembre 2020, la cual avaló el uso de un GPS para despedir a una trabajadora, entendiendo que no vulneraba su intimidad si este conocía su existencia. El Alto Tribunal pudo comprobar que la trabajadora utilizaba el coche durante el descanso laboral y cuando estuvo de baja a sabiendas de que estaba prohibido. Al acreditarse la información y la prohibición del uso extralaboral y no existir ninguna tolerancia, se produjo un despido por desobediencia y transgresión de la buena

contractual. Lo determinante para que el Tribunal Supremo calificara el despido como procedente fue la desobediencia, pues entendió que la trabajadora era conocedora de la prohibición de conducción del vehículos fuera de la jornada laboral y, que el vehículo tenía instalado un GPS por lo que era fácilmente controlable y localizable por lo que no apreciarían ninguna invasión en los derechos fundamentales de la trabajadora con la constatación de los datos de geolocalización que permitieron comprobar y acreditar que el vehículo estaba siendo utilizado desobedeciendo las instrucciones de la empresa "(…). Había conocimiento previo y no se aprecia invasión de la esfera privada de la trabajadora, al afectar exclusivamente a la ubicación y movimiento del vehículo del que, eso sí, ella era responsable y debía utilizar con arreglo a lo pactado (…)".

En este mismo sentido se dictó sentencia por el Tribunal Superior de Justicia de Castilla y León (Valladolid) en fecha 4/12/2012 en la cual se estudiaba el caso de un despido a un trabajador por desobedecer reiteradas veces las órdenes y prohibiciones expresas de la empresa de no utilizar Internet para actividades privadas. Se acreditaron, además, quejas de los clientes por la lentitud del sistema motivado por ese uso inadecuado, lo que supuso un perjuicio en forma de mala prestación de servicios por la empresa. Además de la desobediencia, el tribunal entendió que el hecho de destinar reiteradamente el empleo de tiempo de trabajo durante la jornada laboral en actividades personales suponía quebrantar la buena fe contractual, pues el uso no fue escaso y limitado en el tiempo sino generalizado.

Por tanto, en relación con el uso inadecuado de las nuevas tecnologías por el trabajador, estas podrán constituir una transgresión de la buena fe contractual, o una desobediencia si la empresa había informado previamente del uso que puede hacerse de las herramientas y medios tecnológicos puestos a disposición de los trabajadores.

La desobediencia no es gradualista, ni precisa de la existencia de los mismos requisitos para su constitución que la transgresión de la buena fe, por lo que será más fácil defender la sanción a un trabajador por desobediencia que por transgresión de la buena fe. Es importante concluir indicando que a pesar de que la desobediencia no sea gradualista, si debe ser grave para constituir una infracción laboral muy grave.

11.- Objetivo: Orientaciones y Soluciones para que el control del empresario se realice sin vulneración los derechos fundamentales de los trabajadores.

El objetivo de esta tesis ha sido analizar la jurisprudencia sobre el control empresarial efectuado a través de las nuevas tecnologías de la información y la comunicación, y valorar su incidencia en los diferentes derechos fundamentales de los trabajadores, además de analizar el control empresarial efectuado en las propias herramientas tecnológicas que la empresa ha puesto a disposición de los trabajadores, determinando si la prueba extraída a través de estos medios es lícita.

El aumento en el uso de las nuevas tecnologías de la información y la comunicación (TIC) no ha generado conflictos diferentes a los ya planteados relativos al uso privativo de herramientas facilitadas por la empresa y el derecho de los empresarios de controlar tal utilización, sin embargo, las nuevas TIC han permitido aumentar exponencialmente las posibilidades de efectuar el control empresarial y, la inspección y control de la prestación de servicios. Con estas nuevas tecnologías se va a poder monitorizar los ordenadores, el correo electrónico y la navegación por Internet, lo que permitirá realizar controles más directos y con menor esfuerzo por parte del empresario. Esos controles, aun siendo realizados dentro del más riguroso respeto al Derecho, pueden llegar a poner en riesgo diferentes derechos fundamentales que asisten a los trabajadores.

El interés del empresario para realizar ese control ha quedado patente, no solo por una labor de control de la producción, sino por el deber que le exige el propio Código Penal, afectando “la responsabilidad penal de las personas jurídicas, de prevenir de riesgos penales” (CP, 2015), y que podrían ser cometidos por sus empleados al utilizar las TIC como herramientas de trabajo.

Como consecuencia del uso por los trabajadores de las nuevas tecnologías de información y comunicación (ordenador, dispositivos móviles, correo electrónico, internet, etc.) puestas a su disposición por el empresario y el control ejercido por este sobre el uso que se hace de las mismas, se van a generar diferentes conflictos.

El artículo 20.3 ET establece el derecho del empresario a la adopción de medidas que considere oportunas para vigilar y controlar el trabajo. Eso sí, debe adoptarlas y aplicarlas considerando debidamente su dignidad (SSTC 98/2000, de 10 de abril, FJ 5, 186/2000, de 10 de julio, FJ 5, y 241/2012, de 17 de diciembre, FJ 4). Y es aquí donde encontramos una laguna a nivel normativo, sin que la legislación actual avance al mismo ritmo en que avanza la sociedad de la información. Además, es conveniente indicar que nuestra Constitución no recoge expresamente una protección de los derechos fundamentales frente a la intromisión efectuada a través de las nuevas tecnologías de la información y comunicación.

Por ello, deben ser los tribunales quienes den una solución individualizada a cada conflicto planteado, pues los convenios colectivos o no regulan esta materia o lo hacen de tal forma que rápidamente quedan obsoletos[191]. Se hace necesaria, por tanto, una delimitación de determinados bienes e intereses de relevancia constitucional en el marco de estas relaciones laborales, donde se encuentran especialmente afectados los derechos del trabajador a la intimidad (art. 18.1 CE) y el secreto de las comunicaciones (art. 18.3 CE), frente al poder de dirección y organización del empresario (arts. 33 y 38 CE).

Sin embargo, el poder de dirección del empleador no es absoluto ni ilimitado. Por esta razón, nuestra jurisprudencia ha establecido ciertos requisitos para poder realizarlo sin vulnerar los derechos fundamentales los trabajadores.

1. En primer lugar, ha de ejercitarse respetando los límites establecidos en la Constitución, las leyes, los convenios colectivos y los contratos de trabajo (STS, 5 de febrero de 2008), es decir, que su ejercicio sea conforme a Derecho, excluyendo la ilegalidad, la vulneración de derechos fundamentales de los trabajadores y la actuación torticera por parte del empresario, contraria a su deber de buena fe[192].

[191] SAN MARTÍN MAZZUCCONI, C. (2007) "El uso y el control empresarial de las nuevas tecnologías en el ámbito laboral". Revista Doctrinal Aranzadi. Nº 7/2007 - 8/2007.

[192] MOLERO, C. (2003). Manual de Derecho del Trabajo. 3ª. Ed. Madrid, España: Editorial Civitas. Pág. 257

2. La dignidad del trabajador va a ser el límite principal de este poder de dirección del empresario, aunque también lo serán el resto de los derechos fundamentales de los trabajadores, y el deber de la buena fe contractual (STSJ Cataluña, 18 de septiembre de 2001).

Por su parte, el contrato de trabajo no puede considerarse como un título que genere permita recortar los derechos fundamentales que el trabajador posee como ciudadano, el cual no va a perder esa condición por trabajar en una empresa (STC 88/1985, de 19 de julio, FJ 2). Partiendo de este principio, no puede desconocerse tampoco, como estableció la STC 99/1994, de 11 de abril, FJ 4, que el paso a una organización empresarial modulará aquellos derechos del trabajador en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva; reflejo, a su vez, de derechos empresariales consagrados en la Constitución (arts. 38 y 33 CE).

El Tribunal Constitucional ha establecido la doctrina sobre el alcance de los derechos fundamentales en el marco de la relación laboral y la necesaria proporcionalidad de sus restricciones o limitaciones. En este sentido, los trabajadores no van a dejar de ser ciudadanos por el hecho de realizar una actividad laboral para un empresario, ni los derechos fundamentales que la Constitución reconoce a todos los ciudadanos van exluirse por la existencia de una relación laboral[193].

Ahora bien, tampoco podrá el trabajador en su relación laboral mantener sus derechos de una forma incondicional. La formalización de un contrato de trabajo y el ingreso en la unidad productiva de la empresa comporta una pequeña pérdida o al menos una reducción de la intimidad de las personas trabajadoras, soportando cierta compresión de los derechos de los que el individuo es titular[194], sin que con ello se permita justificar medidas incompatibles con la dignidad de los trabajadores.

[193] SEMPERE NAVARRO, A.V y SAN MARTÍN MAZZUCCONI, C. (2012) Sobre el control empresarial de los ordenadores. Revista Doctrinal Aranzadi Social. Nº 3/2012. Pág. 12.

[194] FERNÁNDEZ LÓPEZ, M.F., 1985. Libertad ideológica y prestación de servicios, en Relaciones Laborales Nº 7, Pág. 65.

Al respecto, cualquier límite que sufra un derecho fundamental debe ser proporcionado y el estrictamente necesario para lograr un fin constitucionalmente legítimo. (STC 115/2013, de 9 de mayo, 143/1994, de 9 de mayo y 70/2002, de 3 de abril). El Tribunal Constitucional ha venido entendiendo que, ante un conflicto de intereses, los derechos fundamentales de los trabajadores deben prevalecer y, por tanto, cualquier limitación en los mismos procedente del control empresarial solo va a poder "derivar del hecho de que la propia naturaleza del trabajo contratado implique la restricción del derecho" (SSTC 99/1994, de 11 de abril; 6/1995, de 10 de enero, y 136/1996, de 23 de julio). Según esta doctrina, en la que la relación laboral conlleva la perdida de ciertos parámetros de la actividad humana de los trabajadores, se debe valorar si es preceptivo el equilibrio entre el interés del trabajador y el de la empresa, donde, además, el trabajador ha admitido voluntariamente, a través de su aceptación, el contrato de trabajo. Por tanto, la clave para valorar las posibles intromisiones en los derechos de los trabajadores estará en el propio objeto del contrato de trabajo, y en las limitaciones que podrían derivarse del mismo, teniendo en cuenta la satisfacción del interés que llevó a las partes a formalizar ese contrato de trabajo. Y ello porque según esta doctrina hay actividades o trabajos que llevan implícitas una restricción en el derecho a la imagen de los trabajadores que las realicen, por la propia naturaleza de estas, como son las actividades en contacto con el público. De esta forma, el que en su día aceptará realizar un trabajo de atención al público, no podrá invocar la vulneración de la propia imagen para no realizar el trabajo.

Es doctrina consolidada de nuestro Tribunal Constitucional que el ejercicio de cualquier derecho fundamental consagrado en nuestra Constitución no es de carácter absoluto, sino que se debe contraponer con el ejercicio de otros derechos o bienes jurídicos protegidos, siendo función de los órganos jurisdiccionales preservar el equilibrio necesario ante una posible colisión de intereses contrapuestos. (STC 213/2002, de 11 de noviembre, FJ 7; o SSTC 20/2002, de 28 de enero, FJ 4; 151/2004, de 20 de septiembre, FJ 7).

Para comprobar si una medida empresarial es restrictiva de un determinado derecho fundamental, ésta deberá superar, lo que el TC denomina el juicio de proporcionalidad, es decir, que la medida sea susceptible de conseguir el objetivo propuesto (juicio de idoneidad), que no exista otra medida más moderada para la consecución de tal propósito (juicio de necesidad) y finalmente, que la misma sea proporcional de acuerdo con los

bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto) (SSTC 96/2012, de 7 de mayo y 241/2012, de 17 de diciembre, 170/2013, de 7 de octubre de 2013, 66/1995, de 8 de mayo; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8).

En lo que respecta a las garantías aplicables al control empresarial de los diversos instrumentos informáticos puestos a disposición de sus empleados, el Tribunal Supremo en su sentencia de la Sala Cuarta de 26 de septiembre de 2007 precisaba la forma en que la empresa debía realizar su control sin vulnerar los derechos fundamentales de los trabajadores, partiendo de las exigencias de buena fe. Para ello, debe establecer previamente las reglas de uso de esos medios (con aplicación de prohibiciones absolutas o parciales), informar a los trabajadores de que va a existir control y de los medios que van a utilizarse para realizarlo y, en su caso, acceso a la información generada, emitida o consultada por los empleados con los medios facilitados por el empresario (en el mismo sentido, STS de 6 de octubre de 2011). Al realizar el control empresarial de esta manera desaparece toda expectativa razonable de intimidad o confidencialidad.

Por lo tanto, para poder realizar un control adecuado por parte de la empresa sin interferir en los derechos fundamentales de los trabajadores, se recomienda que la creación de un código de conducta telemático, clausulas anexas al contrato de trabajo o de diferentes protocolos internos por los cuales se informe a los trabajadores y se establezcan las pautas de actuación de los trabajadores en relación con las herramientas tecnológicas a su disposición.

Un código de conducta de este tipo deberá concretar, principalmente, los usos permitidos y prohibidos de los distintos tipos de equipos y herramientas; las facultades, medios y medidas de control del empresario; así como aspectos relativos a la protección de datos y a la propiedad intelectual e industrial.

Las empresas, a través de la información previa a los trabajadores y a sus representantes legales de las reglas de uso de los medios informáticos, telemáticos puestos a su disposición, y de que va existir un control empresarial de los mismos o a través de esos medios (cámaras, GPS, monitorización, etc.), van a impedir que se produzca una situación de tolerancia con el uso personal de dichos medios, la cual justificaría una “expectativa

razonable de confidencialidad", lo que podría conllevar la invalidez de la prueba obtenida por vulneración de derechos fundamentales.

Incluir en la normativa interna o a modo de clausulado adicional al contrato una política que regule las manifestaciones de los trabajadores en las redes sociales también servirá para poder sancionar por desobediencia, al margen de la transgresión de la buena fe, más difícil de acreditar por la denominada tesis gradualista.

Para terminar, es patente que la complejidad de las nuevas tecnologías y la aparición continúa de novedades dificultan establecer criterios firmes y unánimes en nuestra jurisprudencia, por lo que las cuestiones estudiadas en la presente tesis tendrán una evolución y habrá que realizar un seguimiento, pues como se ha visto, están en juego derechos fundamentales.

A continuación, se establecen modelos de cláusulas contractuales adicionales que servirán para que el control empresarial se realice sin vulnerar los derechos fundamentales de los trabajadores.

Anexo I. Ejemplo de cláusula adicional al contrato sobre los usos de herramientas informáticas facilitadas por el empresario al trabajador:

"8.- UTILIZACIÓN DE LOS MEDIOS INFORMÁTICOS

Los medios informáticos, incluido el correo electrónico, son herramientas de trabajo propiedad de la empresa, tanto en relación con el hardware y con el software instalado como en relación con los contenidos, y como tales herramientas deben ser considerados, estando destinados los mismos al uso estrictamente profesional. Si, a pesar de ello, el trabajador utilizase los equipos informáticos para guardar documentos o información de carácter privado, la empresa no se hace responsable de una posible pérdida o deterioro de los mismos.

El trabajador será responsable de sus contraseñas personales, así como de la custodia de todos los documentos existentes en su ordenador, no pudiendo hacer uso de su contenido para fines distintos de los laborales, revelar o difundir su contenido ni obtener copias mediante cualquier procedimiento para utilizarlas fuera del ámbito de la empresa, salvo que tenga autorización expresa de la empresa para ello.

Por ello, y en base al poder de Dirección que asiste al empresario conforme al artículo 20 del ET, este podrá revisar el contenido de los medios informáticos propiedad de la empresa, incluido el correo electrónico, la navegación por Internet y el teléfono, a los fines de realizar una labor de control laboral, respetando los principios de idoneidad, necesidad y proporcionalidad.

Cualquier incumplimiento de lo regulado en los apartados anteriores será considerado como falta muy grave a efectos laborales".

En relación con la instalación de cámaras de videovigilancia y de los sistemas de geolocalización, se indica a continuación unos ejemplos de información clara y eficaz para poder realizar un control a través de dichos dispositivos sin vulneración de derechos fundamentales:

Anexo II. Comunicación empresarial informando sobre la instalación de cámaras de videovigilancia para realizar un control de la actividad profesional.

"La EMPRESA con CIF _____ y domicilio en _____por medio de la presente COMUNICA:

Que se ha instalado un sistema de vigilancia mediante cámaras en el interior del local situado en _____ para garantizar la seguridad de los trabajadores, clientes, usuarios y todas aquellas personas que concurran al interior de las instalaciones de la empresa, así como para realizar un control laboral, respetando los principios de idoneidad, necesidad y proporcionalidad.

Que la información obtenida y almacenada mediante el sistema de grabación se utilizará exclusivamente para fines de prevención, seguridad y protección de personas y bienes que se encuentren en el establecimiento o instalación sometida a protección.

Que la anterior información se somete a los derechos que le reconoce el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como a su legislación de desarrollo".

Anexo III. Modelo de información a los trabajadores de la instalación del GPS.

La empresa_____, con CIF_____ y domicilio en _____ por medio de la presente COMUNICA:

Que se ha instalado un sistema de vigilancia mediante GPS en los vehículos de la empresa para garantizar la seguridad y control de los trabajos, así como para realizar un control laboral, respetando los principios de idoneidad, necesidad y proporcionalidad.

En consecuencia, los datos obtenidos también podrán utilizarse para justificar una sanción disciplinaria (e incluso el despido).

Que la anterior información se somete a los derechos que le reconoce el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como a su legislación de desarrollo".

Asimismo, se les informa de su derecho de acceso, rectificación, limitación del tratamiento y supresión de los datos extraídos.

Estas informaciones o comunicados deben incluir:

1. Identificación del responsable del tratamiento.
2. Dejar constancia de la instalación de las tecnologías (cámaras, GPS, etc.).
3. Indicar la finalidad del tratamiento, en este caso la prevención, seguridad y protección de personas y bienes presentes en las instalaciones, pero también control de los trabajos.
4. Reconocimiento del sometimiento de la anterior información a los derechos de los trabajadores recogidos en la LOPD.
5. Fecha, nombre del trabajador y su firma, a fin de acreditar la recepción de la información.

Por otra parte, con el fin de respetar la nueva ley de trabajo a distancia y garantizar el derecho al descanso y a la desconexión digital sería conveniente realizar un protocolo o normativa interna que regule el teletrabajo, donde se recojan las formas de control (sistemas de seguimiento), los medios técnicos, las condiciones de prestación del mismo, etc.

Anexo IV. Modelo de Acuerdo Empresarial de trabajo a distancia.

ACUERDO TELETRABAJO EN LA EMPRESA

PREÁMBULO.

El Convenio Colectivo único para todos los centros de trabajo de la empresa (BOE del 31 de diciembre de 2020) menciona el teletrabajo en el capítulo III, Organización del trabajo. Igualmente, en la disposición adicional séptima remite a la negociación colectiva para el estudio de medidas relativas al teletrabajo, al tiempo que recoge el compromiso de celebrar en el plazo de un año un programa experimental en consonancia con las recomendaciones de la Comisión Europea que entiende el teletrabajo como un medio de organización del trabajo y para facilitar la conciliación de la vida profesional y personal y la mayor autonomía en el cumplimiento de las tareas. La declaración del estado de alarma como consecuencia de la crisis sanitaria causada por la COVID-19 interrumpió el mandato que contiene la disposición adicional citada y provocó la asunción súbita del teletrabajo en la empresa, al amparo del artículo 5 del Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social de la COVID-19, que establece el carácter preferente del teletrabajo en las empresas que pudieran adoptarlo. De esta forma, lo que inicialmente estaba previsto como un programa experimental, por definición parcial y de impacto residual en la organización, se convirtió en la forma obligada de asumir la prestación laboral. El esfuerzo de la empresa para cambiar sin planificación previa la forma de organización del trabajo, que en la sede social los primeros meses de la pandemia fueron exclusivamente bajo la modalidad de teletrabajo y especialmente la responsabilidad de todos los empleados que, desempeñando su función mediante teletrabajo o de manera presencial, según los centros y el tipo de actividad, permitieron que la actividad de la empresa en la primera etapa de la pandemia no se viera apena l afectada. Así, el programa experimental se convirtió por la COVID-19 en una forma obligada de prestación laboral, mayoritariamente extendida en los centros de trabajo en los que tal organización se consideró idónea. La evolución de la pandemia permitió situar al teletrabajo como una fórmula habitual de prestación laboral adoptada por muchas empresas como fórmula de

adaptación a las nuevas circunstancias impuestas en la crisis sanitaria. Tal alcance tuvo la extensión del teletrabajo que en algo más de seis meses desde la declaración del estado de alarma y aún durante su vigencia se reguló el teletrabajo en primer lugar mediante el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, convalidado por la Ley 10/2021, de 9 de julio, con idéntica denominación. En el mismo sentido se aprobó para el ámbito de las Administraciones Públicas el Real Decreto-Ley 29/2020, de 29 de septiembre. La experiencia acumulada en la empresa después de más de dieciséis meses con régimen de teletrabajo motivado por la COVID-19 y amparado en la disposición transitoria tercera de la Ley 10/2021, de 9 de julio, ha permitido concebir el teletrabajo como una forma normalizada de prestación laboral, al igual que ha ocurrido en organizaciones del ámbito público y privado y ha logrado despejar los obstáculos para la negociación de un régimen estable de teletrabajo no condicionado a la pandemia y bajo la plena aplicación de la reciente normativa. Por otra parte, la experiencia también ha aconsejado abordar un programa experimental de teletrabajo acordado en el seno de la Comisión Paritaria del convenio que anticipará la aplicación del propio contenido de este acuerdo y que contribuirá sin duda a su mejor aplicación y adaptación a las características de los centros y los puestos de trabajo. En suma, el teletrabajo lejos de retornar a la implantación residual o nula que tenía antes de la pandemia, se ha convertido en una forma más de organizar el trabajo, porque viene a satisfacer objetivos que las partes hacen suyos y que son:

- Contribución a las metas de la Agenda 2030 para el Desarrollo Sostenible por su clara vinculación con el uso más eficiente de los recursos materiales.

- La reducción de emisiones de carbono mediante la reducción de la circulación de vehículos para la asistencia presencial.

- Reducción del consumo de papel por digitalización de procesos asociados al teletrabajo, del consumo de electricidad, de otros consumos y de la generación de residuos.

- Optimización del uso del espacio tanto en los despachos como en salas de reuniones y el aparcamiento, que ya ofrecía dificultades en muchos casos, que se agrava con las

nuevas incorporaciones ya realizadas o las previstas.

- Mejora de la conciliación de la vida personal y laboral (cuanto menos, en lo referido al ahorro de tiempo de transporte) y en suma del bienestar de los empleados. Las partes entienden que la continuidad es un valor para adoptar en este acuerdo un modelo de teletrabajo en la empresa, no solo uniforme para todos los centros, sino en líneas generales similar al adoptado durante la pandemia. Entienden que es necesario consolidar el teletrabajo en la forma en la que se está desarrollando, destacando el valor de la presencialidad para el conjunto de la organización, pero ahora revestido de las garantías y legitimidad que ofrece la negociación colectiva para lo que la Ley 10/2021 las ha emplazado.

El análisis del impacto de este modelo en el conjunto de la organización y la evolución de este determinarán los cambios que haya que asumir en el futuro. Por todo lo anterior, la representación de la Dirección y de los trabajadores, en Madrid, a 14 de junio de 2021, ACUERDAN:

1.- ÁMBITO OBJETIVO

El presente acuerdo regula el contenido de la prestación laboral que incluye en su jornada semanal una parte que se presta en la modalidad de teletrabajo en los términos descritos en el punto 5 que supone el uso de medios y sistemas informáticos, telemáticos y de telecomunicación. En el ámbito de este acuerdo se equipará el trabajo a distancia a teletrabajo. Se considera teletrabajo a los efectos de este acuerdo cuando la prestación laboral se realiza por medios y sistemas informáticos y de telecomunicación un mínimo de un treinta por ciento de la jornada semanal. No forman parte de este acuerdo las modalidades de teletrabajo en las que la prestación laboral se pueda desempeñar a distancia con carácter temporal, excepcional e individual por causa de conciliación familiar y laboral, que se resolverán por la Dirección de Organización y Recursos Humanos, previo informe de la dirección correspondiente. Tampoco forma parte de este acuerdo la modalidad de teletrabajo ocasional para personas que no se acojan al teletrabajo regulado el apartado 5. Para esta modalidad el director, jefe de Departamento o jefe de servicio/unidad correspondiente podrá autorizar jornadas de trabajo de lunes a

viernes, excepto el mes de agosto, y que no supere un máximo de 25 jornadas al año natural en esta modalidad. La implantación del régimen de teletrabajo se llevará a cabo sobre los puestos de trabajo, cuyas funciones, en general no requieren de forma continuada de presencia física de la persona trabajadora para su desempeño y sean susceptibles de realizarse por medios telemáticos. Las características funcionales que deben reunir los puestos y que servirán como criterios para el análisis de los puestos para determinar si son teletrabajables, son:

- Que la mayoría de los contenidos funcionales de los mismos puedan desarrollarse a distancia con medios informáticos.
- Que no requieran para su normal desempeño de la presencia o colaboración física con otras personas.
- Que permitan obtener los resultados sin exigir una presencia o ubicación específica determinada.
- Que una parte significativa de su actividad se pueda desarrollar con medios informáticos.
- Que no requieran de acceso frecuente a material no informatizado.
- Que no conlleven la supervisión diaria, presencial y continuada de puestos no teletrabajables.
- Que el cumplimiento de las funciones sea verificable mediante los sistemas de seguimiento y evaluación que se establezcan. La determinación de estos puestos en función de su contenido funcional corresponderá a la empresa.

2.- ÁMBITO SUBJETIVO

El trabajo a distancia lo podrán desempeñar personas trabajadoras que ocupen puestos cuyas funciones sean susceptibles de ser realizadas de manera no presencial, total o parcialmente y que estén determinados en este sentido conforme el apartado anterior. La empresa manifiesta su intención de extender la modalidad de teletrabajo con los requisitos establecidos en el presente acuerdo el personal sujeto al convenio colectivo único de la empresa y el personal fuera de convenio, sin perjuicio de la disponibilidad presencial y horaria que este último tipo de puestos requiere.

3.- ÁMBITO TERRITORIAL

El modelo de teletrabajo del presente acuerdo es aplicable a todos los centros de trabajo de la empresa.

4.- ÁMBITO TEMPORAL

El presente acuerdo será aplicable cuando la Dirección de Organización y Recursos Humanos indique que se han cumplido los trámites relativos a la formalización de los acuerdos individuales de teletrabajo y considere oportuno que decaiga el trabajo a distancia como medida de contención sanitaria derivada de la COVID-19, a que se refiere la disposición transitoria tercera de la Ley 10/2021, de 9 de julio, de trabajo a distancia, en la que se encuentra la empresa. El acuerdo tendrá una duración hasta el 31 de diciembre de 2023 y podrá ser prorrogado automáticamente por periodos anuales, salvo denuncia expresa de alguna de las partes. Las modificaciones a este acuerdo en el periodo de su vigencia se acordarán en la Comisión Paritaria de seguimiento, vigilancia, interpretación y estudio del convenio a propuesta de la Comisión de Seguimiento que se crea en el apartado 16 de este acuerdo.

5.- MODALIDAD DE TELETRABAJO EN LA EMPRESA

El modelo de teletrabajo en la empresa será homogéneo para todo el personal que se acoja voluntariamente a este y consistirá en la prestación de teletrabajo de dos días a la semana, por lo que los tres restantes se desempeñarán en régimen presencial. La jornada de trabajo diaria no se podrá fraccionar en ningún caso en las dos modalidades de prestación de servicio, presencial y de teletrabajo. Los días de teletrabajo se prestarán en el horario que para cada centro de trabajo se establece en el convenio colectivo único.

6.- VOLUNTARIEDAD Y REVERSIBILIDAD DEL TELETRABAJO

El trabajo a distancia será voluntario, y reversible, para la persona trabajadora y para la empresa y requerirá la firma por ambas partes del acuerdo de teletrabajo individual que

se anexa a este acuerdo. La negativa de la persona trabajadora a trabajar a distancia, el ejercicio de la reversibilidad al trabajo presencial y las dificultades para el desarrollo adecuado de la actividad laboral a distancia que estén exclusivamente relacionadas con el cambio de una prestación presencial a otra que incluya trabajo a distancia, no serán causas justificativas de la extinción de la relación laboral ni de la modificación sustancial de las condiciones de trabajo. La decisión de teletrabajar desde una modalidad de trabajo presencial será reversible para la empresa y la persona trabajadora. El ejercicio de esta reversibilidad se deberá realizar por escrito motivado a la otra parte, al menos con quince días naturales de antelación. La reversibilidad implicará la vuelta a la situación de presencialidad en la prestación laboral.

Serán causas de reversibilidad:

1. Decisión organizativa individual adoptada por la empresa, a propuesta del titular de la Dirección en la que desempeña sus funciones la persona trabajadora con al menos quince días naturales de antelación a su fecha de efectos.
2. Desistimiento del trabajador que deberá comunicar por escrito a la empresa, al menos con quince días naturales de antelación a la fecha de efectos.
3. Mutuo acuerdo, formalizado por escrito.
4. Decisión organizativa general por causas excepcionales adoptada por la empresa que deberá ser comunicada a la plantilla afectada con dos meses de antelación a la fecha de efectos e informada justificativa y previamente en la Comisión de Seguimiento. La empresa podrá suspender temporal y/o parcialmente la prestación de teletrabajo por causas excepcionales y de fuerza mayor.

7.- CONDICIONES DE LA PRESTACIÓN DE TELETRABAJO

Las personas que desarrollen el trabajo a distancia tendrán los mismos derechos que si prestasen los servicios de manera exclusivamente presencial; y no podrán sufrir perjuicio en ninguna de sus condiciones laborales, incluyendo retribución, estabilidad en el empleo, tiempo de trabajo, formación y promoción profesional. Sin perjuicio de lo previsto en el párrafo anterior, las personas que se encuentren en régimen de teletrabajo tendrán derecho a percibir, las mismas retribuciones que si prestasen servicios de manera

exclusivamente presencial. Las personas que se encuentren en régimen de teletrabajo no podrán sufrir perjuicio alguno ni modificación en las condiciones pactadas, en particular en materia de tiempo de trabajo o de retribución, por las dificultades, técnicas u otras no imputables a la persona trabajadora, que eventualmente pudieran producirse. Las condiciones de ordenación de la prestación del teletrabajo, sin perjuicio de las que se vayan aplicando conforme se analice el impacto de la implantación, serán:

a) Domicilio de la persona teletrabajadora: será el que elija la persona trabajadora para la prestación laboral por teletrabajo con carácter ordinario y que se fijará en el acuerdo individual de teletrabajo y que tendrá conexión por vía telemática entre los equipos informáticos de la empresa y de la persona trabajadora, en su caso. Cualquier modificación permanente de este domicilio deberá notificarlo por correo electrónico a la empresa con una antelación mínima de siete días a la fecha de efectos y la declaración de que dispone en el nuevo domicilio de las mismas condiciones del anterior domicilio en cuanto a protección de datos, seguridad de la información y prevención de riesgos laborales necesarias para el desempeño de sus funciones.

b) Requerimiento de presencia a la persona teletrabajadora: por necesidades del servicio, que deberán ser debidamente justificadas, podrá ser requerida su presencia en el centro de trabajo, preavisando con una antelación mínima de 24 horas. En situaciones de excepcionalidad acreditada, que requieran de la presencia ineludible de la persona que se encuentre en la modalidad de trabajo a distancia se podrá recabar su presencia sin la antelación mínima señalada.

c) Domicilios de teletrabajo temporales distintos al elegido: la persona teletrabajadora podrá elegir temporalmente un domicilio de teletrabajo, que tendrá que comunicar con una antelación de quince días naturales a la fecha de sus efectos, siempre que pueda cumplir con lo dispuesto en el apartado anterior respecto al eventual requerimiento de presencia y que cumple con las condiciones del domicilio elegido.

d) Los días de teletrabajo serán fijados entre la persona teletrabajadora y el responsable directo, en atención a las necesidades organizativas del servicio.

e) Teletrabajo y vacaciones o festivos. No se podrá intercalar habitualmente días de vacaciones en periodos de teletrabajo salvo necesidades del servicio.

f) Dificultades técnicas. En caso de producirse dificultades técnicas que impidan el normal desarrollo del trabajo a distancia, la persona trabajadora deberá ponerlo inmediatamente en conocimiento de su superior jerárquico y procurar su solución inmediata. Si la dificultad se mantuviera más de 24 horas, la empresa podrá suspender el régimen de trabajo a distancia hasta su subsanación.

g) La incorporación al régimen de teletrabajo, una vez se haya iniciado este con carácter general podrá ser solicitada por la persona trabajadora, en cualquier momento.

h) Para incorporarse al régimen de teletrabajo habrá de contarse con al menos seis meses de antigüedad en el puesto de trabajo.

El plazo general del acuerdo individual de teletrabajo será de seis meses, prorrogables tácitamente por periodos de seis meses.

8.- OBLIGACIONES FORMALES DEL ACUERDO DE TELETRABAJO

El acuerdo de teletrabajo entre la empresa y la persona trabajadora deberá realizarse por escrito, y formalizarse antes de que se inicie el trabajo a distancia; utilizando para ello el modelo que se anexa al presente acuerdo. La Dirección de Organización y Recursos Humanos entregarán a los representantes de los trabajadores de cada ámbito una copia de los acuerdos de trabajo a distancia que se firmen en estos y de sus actualizaciones, excluyendo aquellos datos que, de acuerdo con 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, pudieran afectar a la intimidad personal, de conformidad con lo previsto en el artículo 8.4 del Estatuto de los Trabajadores. El tratamiento de la información facilitada estará sometido a los principios y garantías previstos en la normativa aplicable en materia de protección de datos. Esta copia se entregará por la empresa, en un plazo no superior a diez días desde su formalización, a la representación de los trabajadores, que la firmará a efectos de acreditar que se ha producido la entrega. Posteriormente, dicha copia se

enviará a la oficina de empleo.

9.- MEDIOS TÉCNICOS Y GASTOS DERIVADOS DEL TELETRABAJO

La persona trabajadora deberá poseer los conocimientos informáticos suficientes que requiere el ejercicio de las funciones objeto de la prestación en modalidad de trabajo no presencial. La empresa dotará a las personas que accedan al teletrabajo de los equipos informáticos para el ejercicio de su función. Corresponde igualmente a la empresa el mantenimiento de los medios técnicos que se hayan puesto a disposición de la persona trabajadora. La persona trabajadora deberá utilizar las herramientas y sistemas de información corporativos que la empresa ponga a su disposición para el teletrabajo, de los que deberá realizar un uso responsable y ajustado a la finalidad para los que han sido entregados.

La persona trabajadora, al acogerse a este acuerdo reconoce que con los medios que la empresa pone a su disposición y con los propios de su lugar de teletrabajo, cuenta con medios físicos suficientes y adecuados para desarrollar sus funciones desde el domicilio elegido para realizar la prestación laboral por teletrabajo. Las partes entienden que los posibles gastos derivados del teletrabajo a que hace referencia el artículo 12 de la Ley 10/2021, de 9 de julio, de trabajo a distancia se encuentran compensados por este régimen de prestación laboral, sin perjuicio de los criterios que puedan dictar los organismos competentes en esta materia.

10.- SISTEMAS DE SEGUIMIENTO

El seguimiento del cumplimiento de las tareas y trabajos que realice la persona que desempeñe su actividad por teletrabajo se llevará a cabo por el responsable directo de la unidad organizativa a la que esté adscrita conforme a lo regulado en los artículos 20 y 34.9 del ET. La jefatura de la unidad organizativa de la persona teletrabajadora deberá cumplimentar de manera semestral un informe en el que se analice el grado de cumplimiento de las funciones y tareas asignadas, el cumplimiento de objetivos y la valoración de la conveniencia o no de continuar prestando servicios en esta modalidad de trabajo. Este informe deberá ser conocido por el teletrabajador para realizar las

alegaciones que considere oportunas. La Dirección de Organización y Recursos Humanos aportará un modelo para la cumplimentación de este informe que incluirá, entre otros aspectos, la valoración de la desconexión digital. Por la Dirección de Organización y Recursos Humanos se articulará la implantación de un método de registro de jornada adaptado al régimen mixto de prestación laboral presencial y de teletrabajo que tendrán los centros de trabajo de la empresa. En todo caso el método de control establecido garantizará los derechos de la persona trabajadora a la intimidad, la propia imagen y a la protección de datos.

11.- SEGURIDAD Y SALUD LABORALES

Las personas que teletrabajan tienen derecho a una adecuada protección en materia de seguridad y salud en el trabajo, de conformidad con lo establecido en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, y su normativa de desarrollo. La evaluación de riesgos y la planificación de la actividad preventiva del trabajo a distancia deberán tener en cuenta los riesgos característicos de esta modalidad de trabajo, poniendo especial atención en los factores psicosociales, ergonómicos y organizativos, así como a los trastornos musculoesqueléticos, fatiga visual y estrés. En particular, deberá tenerse en cuenta la distribución de la jornada, los tiempos de disponibilidad y la garantía de los descansos y desconexiones durante la jornada. El servicio de prevención propondrá el contenido de las evaluaciones de riesgos laborales de I s personas que trabajan en su puesto a distancia a los comités de seguridad y salud y se ejecutarán conforme se establezcan en su planificación correspondiente.

La persona teletrabajadora, al acogerse a este acuerdo, consiente en la realización de la evaluación de riesgos laborales del puesto de trabajo, mediante la modalidad que determine el Servicio de Prevención propio de la empresa, pudiéndose realizar una autoevaluación realizada voluntariamente por la propia persona trabajadora. La evaluación de riesgos únicamente debe alcanzar al puesto de trabajo habilitado para la prestación de servicios en la modalidad de trabajo a distancia, no extendiéndose al resto de zonas del lugar de trabajo. Es responsabilidad de la persona que realiza la modalidad de trabajo a distancia cumplir con los requisitos de prevención de riesgos laborales que establezca el Servicio de Prevención.

12.- FORMACIÓN

La empresa deberá adoptar las medidas necesarias para garantizar la participación efectiva en las acciones formativas de las personas que trabajan a distancia, en términos equivalentes a los de las personas que prestan servicios de manera presencial, debiendo atender el desarrollo de estas acciones, en lo posible, adecuadas a las características de su prestación de servicios a distancia. La empresa deberá garantizar a las personas teletrabajadoras la formación necesaria para el adecuado desarrollo de su actividad tanto al momento del inicio del trabajo a distancia como cuando se produzcan cambios en los medios o tecnologías utilizadas. Igualmente, la persona teletrabajadora podrá ser convocada y participar en los cursos presenciales y/o a distancia que le aporten su permanente actualización profesional y las oportunidades de desarrollo de la carrera profesional, en las mismas condiciones que las personas que trabajen de manera presencial.

13.- PROTECCIÓN DE DATOS

Por lo que se refiere a los ficheros que contengan datos de carácter personal, se estará a lo que disponga el Reglamento Europeo de Protección de Datos RGPD (UE) 2016/679, así como la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos. La persona trabajadora, en el desarrollo del trabajo a distancia, deberá cumplir las instrucciones determinadas por la empresa en el marco de la legislación vigente sobre protección de datos y sobre seguridad de la información.

14.- DESCONEXIÓN DIGITAL

Las personas teletrabajadoras tienen derecho a la desconexión digital fuera de su horario de trabajo en los términos establecidos en el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre. La empresa velará por el derecho a la desconexión digital tanto para las personas trabajadoras que se encuentren en régimen de teletrabajo como para las que realicen su prestación laboral en régimen exclusivamente presencial, con respeto de la duración máxima de la jornada y otros límites convencionales aplicables.

Para ello las partes entienden conveniente que se adopten las siguientes pautas de actuación:

- Evitar el envío de comunicaciones y realizar llamadas fuera del horario laboral.
- Evitar el envío de comunicaciones y realización de llamadas durante el disfrute de vacaciones y permisos salvo circunstancias excepcionales y justificadas.
- Procurar la planificación de las reuniones con al menos 24 horas de antelación.

15.- DERECHOS DE REPRESENTACIÓN COLECTIVA

La prestación de servicios en régimen de teletrabajo no supondrá menoscabo de los derechos de representación colectiva de la persona que lo desempeñe. Las personas teletrabajadoras tendrán derecho a ejercitar sus derechos de naturaleza colectiva con el mismo contenido y alcance que el resto de las personas trabajadoras del centro al que están adscritas. A estos efectos, la negociación colectiva podrá establecer las condiciones para garantizar el ejercicio de los derechos colectivos de las personas trabajadoras a distancia, en atención a las singularidades de su prestación, con respeto pleno al principio de igualdad de trato y de oportunidades entre la persona trabajadora a distancia y la que desempeñe tareas en el establecimiento de la empresa.

16.- COMISIÓN DE SEGUIMIENTO

Se crea una Comisión para el seguimiento del presente acuerdo. Estará compuesta por cuatro representantes de la empresa y cuatro representantes por la parte social.
Serán funciones de la Comisión de seguimiento:

a) Conocer el resultado de la aplicación del apartado a) del punto 17.
b) Análisis del impacto de la implantación del régimen acordado de teletrabajo en la empresa.
c) Ser informados de las solicitudes denegadas de teletrabajo.
e) Proponer a la Comisión Paritaria modificaciones al presente acuerdo.
f) Conocer previamente las suspensiones temporales del régimen de teletrabajo por causas excepcionales o la reversibilidad general del teletrabajo en la empresa.

g) Estudiar la aplicación de criterios que puedan dictar los organismos competentes en materia de teletrabajo.

17.- PROCEDIMIENTO DE IMPLANTACIÓN DEL MODELO DE TELETRABAJO

La implantación del régimen del teletrabajo pactado en el presente acuerdo se realizará con las siguientes fases:

Fase previa. Análisis de las funciones de los puestos para determinar si son teletrabajables, mediante informe de las direcciones, con los criterios que establezca la Dirección de Organización y Recursos Humanos.

b) Fase del ejercicio de la voluntad para teletrabajar por parte de las personas trabajadoras.

c) Fase de fijación de los. Dos días de teletrabajo para cada persona teletrabajadora en su departamento/servicio.

d) Fase de formalización de los acuerdos individuales de teletrabajo.

e) Comunicación de aplicación efectiva y de entrada en vigor del régimen de teletrabajo pactado.

Anexo IV. Contrato-Acuerdo teletrabajo. Empresa-trabajador.

ACUERDO TRABAJO A DISTANCIA (teletrabajo)

RD-ley 28/2020, de 22 de septiembre

REUNIDOS

En _____, a _____ de _____ de _____

De una parte, D. _____, que interviene en nombre y representación de la empresa _____, en su calidad de _____ .

De otra parte, D. _____, como persona trabajadora de la empresa _____.

Ambas partes reconociéndose capacidad legal suficiente para el otorgamiento del presente documento,

MANIFIESTAN

PRIMERO.- Que el objeto del presente documento es formalizar voluntariamente un acuerdo de trabajo a distancia en la modalidad de teletrabajo, de conformidad con lo establecido en el artículo 5.1 del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia (BOE del 23-09-2020).

SEGUNDO.- El trabajo a distancia se llevará a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación.

A tales efectos se establece el siguiente inventario de los medios, equipos y herramientas que exige el desarrollo del trabajo a distancia concertado, así como los consumibles y elementos muebles:

-

-

La vida útil o periodo máximo para la renovación de estos se establece en un periodo temporal de:

-

La persona trabajadora deberá cumplir las condiciones e instrucciones de uso y conservación establecidas en la empresa en relación con los equipos o útiles informáticos, y tiene la obligación de cuidado de los equipos suministrados, y el uso adecuado y responsable del correo electrónico corporativo y no podrá recolectar o distribuir material ilegal a través de Internet, ni darle ningún otro uso que no sea determinado por el contrato de trabajo.

La persona trabajadora se compromete a cuidar los elementos de trabajo, así como las herramientas que la empresa ponga a su disposición y a utilizarlas exclusivamente con los fines laborales que previamente se hayan fijado.

Finalizado la modalidad de trabajo a distancia en teletrabajo se deberá reintegrar los equipos informáticos que se le haya asignado.

TERCERO.- El lugar de trabajo a distancia elegido por la persona trabajadora para el desarrollo del trabajo a distancia está ubicado en :

-

Cualquier cambio del lugar de trabajo deberá ser comunicado con carácter previo y con plazo temporal suficiente a la empresa, para poder dar cumplimiento a las obligaciones legales en materia de prevención de riesgos laborales.

A los efectos de la obligación empresarial de evaluación de riesgos y planificación preventiva, las visitas necesarias al domicilio del trabajador, requerirá, en cualquier caso, el permiso de la persona trabajadora, o de la persona titular del mismo.

La persona trabajadora debe cumplir las condiciones especiales sobre la prevención de riesgos laborales que se encuentren definidas en la evaluación de riesgos y en la planificación de la actividad preventiva.

CUARTO.- La duración de este acuerdo de modalidad de trabajo a distancia se establece en :

-

No obstante, la duración pactada, la empresa y la persona trabajadora podrán revertir el acuerdo de trabajo presencial a distancia en los siguientes supuestos:

-

-

Se establece un de plazo de preaviso de _____ para el ejercicio de las situaciones de reversibilidad.

QUINTO.- El horario de trabajo de la persona trabajadora se desarrollará de:

-

Estableciéndose las siguientes reglas de disponibilidad: (optativo)

Se establece que el porcentaje y distribución entre trabajo presencial y trabajo a distancia, será el siguiente: (optativo) _____.

SEXTO.- Los gastos que pude tener la persona trabajadora por el hecho de prestar servicios a distancia, son los siguientes:

-

-

Estos gastos se cuantifican de la siguiente forma:

-

La compensación que abonará la empresa será por un importe:

-

El importe se abonará en los siguientes plazos temporales y forma siguientes:

-

SÉPTIMO.- La persona trabajadora queda adscrita al centro de trabajo de la empresa sito en _____, donde desarrollará la parte de la jornada de trabajo presencial en caso de existir la misma.

OCTAVO.- El procedimiento a seguir en el caso de producirse dificultades técnicas que impidan el normal desarrollo del trabajo a distancia, será el siguiente:

-

-

NOVENO.- Se establecen en materia de protección de datos y sobre seguridad de la información, las siguientes instrucciones:

Solo los sistemas de comunicación aprobados por la empresa pueden ser usados para llevar a cabo sus actividades. Toda la información y equipos de la empresa deben mantenerse seguros en todo momento. Si la información se almacena temporalmente en su domicilio, debe estar bajo llave en lugar seguro o protegida adecuadamente por otros medios.

El acceso a los diferentes entornos y sistemas informáticos de la persona trabajadora será efectuado siempre y en todo momento bajo el control y la responsabilidad de la misma, siguiendo los procedimientos establecidos por la empresa que se hacen parte integral del presente acuerdo.

DÉCIMO.- La persona trabajadora se compromete a respetar la legislación en materia de protección de datos, las políticas de privacidad y de seguridad de la información que la empresa ha implementado, como también a:

- Utilizar los datos de carácter personal a los que tenga acceso único y exclusivamente para cumplir con sus obligaciones para con la empresa

- Cumplir con las medidas de seguridad que la empresa haya implementado para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso, así como no a no ceder en ningún caso a terceras personas los datos

de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación.

UNDÉCIMO.- La empresa establece como medidas de vigilancia y control para verificar el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales, las siguientes:

-

-

DUODÉCIMO.- La persona trabajadora se compromete a guardar la máxima reserva y confidencialidad sobre las actividades laborales que desarrolle. Se considerará Información confidencial la información de propiedad de la empresa y la información que genere la persona trabajadora en virtud del contrato de trabajo. Comprometiéndose a no divulgar dicha Información confidencial, por ningún medio físico o electrónico, así como a no publicarla ni ponerla a disposición de terceros, a no ser que cuente con el consentimiento de la empresa

DECIMOTERCERO.- Se garantiza a la persona trabajadora el derecho a la desconexión digital fuera de su horario de trabajo en los términos establecidos en el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre.

Fdo.- La empresa Fdo.- El trabajador

Anexo V. Protocolo interno regulador del derecho a desconexión digital en la empresa:

POLÍTICA INTERNA REGULADORA DEL DERECHO A LA DESCONEXIÓN DIGITAL DE LAS PERSONAS TRABAJADORAS

1.- NUEVAS FORMAS DE TRABAJO y DESCONEXIÓN DIGITAL

1.1 UN NUEVO ESCENARIO

Las nuevas tecnologías han puesto a nuestra disposición herramientas de trabajo y de comunicación que permiten a las personas estar conectadas en cualquier momento y en cualquier lugar, pudiendo realizar así un creciente número de tareas fuera del centro de trabajo. En el marco de la transformación digital, muchas empresas están avanzado hacia un modelo de organización del trabajo más flexible, que les permite ganar agilidad y eficiencia y dar un mejor servicio a sus clientes, y que, a su vez, fomenta la conciliación familiar y, por tanto, un equilibrio de la vida laboral y personal de la plantilla, potenciando su compromiso con la empresa. Pero la posibilidad de estar siempre conectado, que permite esta nueva organización del trabajo y desdibuja los limites tradicionales de la jornada laboral, puede tener como consecuencia que las comunicaciones e interacciones que antes se hacían en un horario cerrado y habitualmente en la oficina, ahora se produzcan en cualquier momento del día y en cualquier lugar, lo que en ocasiones puede interferir con el descanso y el disfrute del tiempo libre de las personas. En este contexto nace el concepto de Desconexión Digital en el ámbito laboral, que hace referencia a la necesidad de poder desconectar de las herramientas de trabajo y de comunicación para poder disfrutar del descanso necesario para el bienestar físico y mental.

2.- DESCONEXIÓN DIGITAL

2.1 UNA CULTURA DE RESPETO AL TIEMPO DE LOS DEMÁS

La empresa lleva tiempo trabajando en sistemas de trabajo flexibles que puedan

facilitarnos el acercamiento al cliente, mejorar la captación y retención de talento, y dotarnos de una mayor agilidad en la gestión, a la vez que favorezcan la conciliación de la vida personal y laboral de las personas trabajadoras. Este modelo de trabajo flexible se establece sobre una cultura organizacional construida sobre el respeto, la confianza, la flexibilidad y la eficiencia y debe estar dirigido hacia unos sistemas de trabajo basados en objetivos medibles y orientados a resultados y que respeten el marco legal aplicable. Esto permite a esta empresa contar con una organización del trabajo que no comprometa el tiempo libre de las personas trabajadoras. En este sentido, y en base al compromiso con el bienestar su plantilla, esta empresa reconoce expresamente el derecho de las personas trabajadoras a desconectarse de las herramientas de trabajo y comunicación provistas por la empresa, fuera de la jornada de trabajo. Además, esta empresa se compromete a implantar una serie de pautas que nos permitan seguir avanzando en una cultura de respeto al tiempo de los demás (tanto en horario laboral como en el tiempo libre).

2.2. MEDIDAS PARA EL EJERCICIO DEL DERECHO A LA DESCONEXIÓN

Se establecerá en la organización las siguientes pautas:

- Se garantiza el derecho a la desconexión digital tanto a las personas trabajadoras que realicen su jornada de forma presencial como a los supuestos de realización total o parcial del trabajo en remoto bien sea a través de trabajo en movilidad o en régimen de teletrabajo.

- Se evitará enviar comunicaciones y realizar llamadas fuera del horario laboral, salvo que concurran circunstancias excepcionales justificadas y, en todo caso, se considerará como Tiempo de Respeto al Tiempo Libre:

    • De lunes a jueves entre las 18:30 y las 09.00 horas.
    • Fines de Semana desde las 15.00 horas del viernes y hasta las 09.00 horas del lunes.
    • Festivos durante todo el día.

Estos límites no aplicarán a personas cuyas funciones deban desarrollarse en festivos ni aquellas que desarrollen su trabajo en horarios especiales en cuyo caso se evitará el envío de comunicaciones una vez finalizada la jornada laboral del destinatario y antes del inicio de la siguiente. En caso de que se envíen comunicaciones durante el Tiempo de Respeto al Tiempo Libre, no debe esperarse respuesta a los mensajes enviados dentro de dicho tiempo. Por lo que, en los casos de circunstancias excepcionales justificadas, siempre se valorará la llamada como primera opción.

- Igualmente se evitará enviar comunicaciones y realizar llamadas salvo que se den circunstancias excepcionales justificadas durante el disfrute de permisos y vacaciones, del receptor, siempre que se conozca esta situación.

- En caso de que se envíen comunicaciones en las situaciones anteriormente mencionadas, la persona trabajadora tiene derecho a no responder por lo que no debe esperarse respuesta mientras duren dichas circunstancias por lo que en los casos de urgencia siempre se valorará la llamada como primera opción.

- En este sentido, se recuerda la necesidad, siempre que sea posible, de activar el aviso de fuera de oficina en nuestra ausencia indicando los datos de contacto de compañeros que están disponibles y puedan atender las cuestiones que se requieran en ausencia de la persona trabajadora. Siempre se respetará lo indicado en el "fuera de oficina" respecto a la persona responsable en ausencia de la persona a la que se dirige el mensaje y en caso de necesitar contactar con el "titular" siempre se valorará la llamada como primera opción.

- En los casos en que concurran circunstancias de causa de fuerza mayor o que supongan un grave, inminente y evidente perjuicio empresarial o del negocio cuya urgencia temporal necesite de una respuesta inmediata, quedarán sin efecto las medidas que garantizan el derecho a la desconexión digital hasta que dicha situación haya sido resuelta.

- Se recomienda planificar las reuniones con al menos 24 horas de antelación y

estableciendo el tiempo aproximado de duración de estas. Las reuniones se convocarán, atendiendo a las diferentes necesidades de las áreas, a partir de las 09:30 y hasta las 18.30 horas y excepcionalmente hasta las 19:00 horas de lunes a jueves y hasta las 14:00 horas los viernes.

- Con el objetivo de que las reuniones y las sesiones de formación sean lo más productivas posibles se recomienda la desconexión de cualquier otro dispositivo que no sea necesario para el desarrollo de esta.

3.- ACCIONES DE SENSIBILIZACIÓN Y FORMACIÓN

Para trasladar estas pautas a la plantilla e impulsar una cultura favorable al descanso, se desarrollará un Plan de gestión del cambio alineado con el que se realice para el conjunto del Proyecto de nuevas formas de trabajo, llevándose a cabo las siguientes acciones:

- Formación y recursos relacionados con la desconexión y el descanso.
- Formación y recursos sobre un uso razonable de los medios de trabajo tecnológicos y adicción a las nuevas tecnologías.
- Campañas de sensibilización en el respeto al tiempo de descanso personal.

12.- Bibliografía, sistema APA 2017 de citación

- ABEL LLUNCH, X. (2005) Iniciativa probatoria en el proceso civil. Barcelona, España: BOSCH.
- ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F. (2006). El Derecho de los Trabajadores a la Intimidad. Navarra, España: Aranzadi, S.A.
- AVILÉS, J.A.F y ROLDÁN, V.R.R. (2016) "Nuevas tecnologías y control empresarial de la actividad laboral es España", Revista Labour & Law Issues, Vol. 2, nº 1.
- CALONGE CRESPO, I. (2011) Videovigilancia y seguridad pública. [Videovigilancia: ámbito de aplicación y derechos fundamentales afectados. En particular la protección de los datos personales]. Coor. ETXEBARRIA GURIDI, J.F. y IXUSCO ORDEÑANA, G. País Vasco, España: Tirant lo Blanch. Págs. 81-106.
- CARDONA RUBERT, M. B. (2003) "Las relaciones laborales y el uso de las tecnologías informáticas". Revista de Relaciones Laborales, Nº Extra-1. Págs. 157-173.
- CASTELLS, M. (2000) La sociedad red: Una visión global (2ª.ed) Madrid, España: Alianza Editorial.
- CARRILLO, J. Mª. (2019) "El Derecho a la libertad de expresión del trabajador a través de las nuevas tecnologías y el derecho a la reputación de la empresa". Revista Española de Derecho del Trabajo nº 217, Págs. 101-127.
- CHACARTEGUIJÁVEGA, C. (2013) Dignidad de los trabajadores y derechos humanos del trabajo según la jurisprudencia del Tribunal Europeo de Derechos Humanos. Albacete, España: Bomarzo.
- COLÀS NEILA, EI. (2012) Derechos fundamentales del trabajador en la era digital: una propuesta metodológica para su eficacia. (1ª.ed). Albacete, España: Bomarzo.
- DE REBECQUE, B. C. (2019) "La libertad de los modernos" Madrid, España: Alianza Editorial. Trad. RIVERO RODRIGUEZ, A.
- DIAZ REVORIO, F. J. (2006). El derecho fundamental al secreto de las comunicaciones. Revista de la Facultad de Derecho, Nº 59, págs. 159-175.

- FERNÁNDEZ ESTEBAN, M. L. (1998) Nuevas tecnologías, Internet y Derechos Fundamentales. Madrid, España: McGraw Hill.
- FERNÁNDEZ LÓPEZ, M.F., (1985) "Libertad ideológica y prestación de servicios", en Revista de Relaciones Laborales, nº 7. Págs. 177-198.
- GARCÍA MEXÍA, Pablo (2005) El Derecho de Internet, Valencia, España: Tirant lo Blanch,
- GAYO (2009) Instituciones, Madrid, España: CIVITAS.
- GOÑI SEIN, J L. (1988) El respeto a la esfera privada del trabajador: un estudio sobre los límites del poder de control empresarial. Madrid, España: Civitas.
- GOÑI SEIN, J.L. (2009) «Controles empresariales: geolocalización, correo electrónico, internet, videovigilancia y controles biométricos», Justicia Laboral, núm. 3, pág. 13.
- HERRERO-TEJEDOR, F. (1990) "Honor, Intimidad y Propia Imagen", Madrid, España: Colex.
- KAHALE CARRILLO, D.T. (2021) "La geolocalización como medio de control del trabajador" Revista andaluza de trabajo y bienestar social, Nº 57 págs. 141-166.
- LE GOFF, J. (2007) La Edad Media explicada a los jóvenes. Barcelona, España: Paidos.
- LOCKE, J., (1969) Ensayo sobre el gobierno civil, Aguilar, Madrid, España: Aguilar.
- LÓPEZ AHUMADA, J. E. (2006) "La tutela del derecho a la intimidad del trabajador y el control audiovisual de su actividad laboral", Cuadernos electrónicos de Derechos Humanos y Democracia, núm. 3, enero-julio.
- LÓPEZ AHUMADA, J. E. (2023) "Reflexiones sobre el nuevo concepto de aplicación del teletrabajo", Noticias CIELO. Nº 2.
- LLUCH CORELL, F.J. (2017) "El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador, El Derecho, disponible en http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronicotrabajador _11_1045180003.html

- MARTÍNEZ FONS, D. (2002) “Uso y control de las tecnologías de la información y comunicación en la empresa”. Revista de Relaciones Laborales. Nº 2. Págs. 1311-1344.
- MARTÍNEZ LÓPEZ, F. J.; LUNA HUERTAS, P.; MORO INFANTE, A. Y MARTÍNEZ LÓPEZ, L. (2003). “Los sistemas de control de la actividad laboral mediante las nuevas tecnologías de la información y las comunicaciones”. Revista de Relaciones Laborales. Nº 1. Págs. 1413-1436.
- MARTINEZ PEÑA, L. (2011) “Los inicios de la legislación laboral española: La Ley Benot”. Revista Aequitas Volumen 1 Págs. 25-70.
- MARX, K. y ENGELS, F. (1848) El Manifiesto del Partido Comunista (2012). Madrid, España: Nordicalibros.
- MIRÓ MORROS, D. Y CRUZ DE PABLO, M. (2014) “El uso de la video vigilancia en el ámbito laboral”. Revista Actualidad Jurídica Aranzadi. Nº 891/2014.
- MOLERO, C. (2003) Manual de Derecho del Trabajo. 3ª. Ed. Madrid, España: Civitas.
- PÉREZ PORTO, J., MERINO, M. (2008). “Correo electrónico - Qué es, definición, cómo funciona y estructura”. www.definicion.de. Última actualización el 7 de mayo de 2021. Recuperado el 19 de mayo de 2023 de https://definicion.de/correo-electronico/
- PICO I JUNOY, J. (2006) Aspectos prácticos de la prueba civil. Barcelona, España: BOSCH.
- REBOLLO DELGADO, L. (2005), “El Derecho Fundamental a la intimidad”, Madrid, España: Dykinson, 2ª edición.
- ROATTA, S., CASCO, M.E., y FOGLIATO, M. “El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012”, publicado en https://core.ac.uk/download/pdf/296383939.pdf,http://sedici.unlp.edu.ar/bitstream/handle/10915/46243/Documento_completo.pdf?sequence=1&isAllowed=y
- RODOTÀ S. (2003) "Democracia y protección de datos", Cuadernos de Derecho Público, Núms. 19-20.

- RODRÍGUEZ ESCANCIANO, S. (2009) El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas. Albacete, España: Bomarzo.
- ROIG, A. (2010) Derechos fundamentales y tecnologías de la información y de las comunicaciones (TICs). Barcelona, España: BOSCH.
- RUIZ RESA, J.D. (2015) Los Derechos de los Trabajadores en el franquismo. Madrid, España: Dykinson.
- SAN MARTIN MAZZUCCONI, C. (2002) Nuevas Tecnologías y Relaciones Laborales. Aranzadi, Cizur Menor.
- SAN MARTIN MAZZUCCONI, C. (2007) "El uso y control empresarial de las nuevas tecnologías en el ámbito laboral". Revista Doctrinal Aranzadi nº 2. Págs. 2666-2677.
- SANZ MARTIN, L., (1996) Sociedad y derecho en la Hispania Romana. Madrid, España: Dykinson.
- SANZ MARTIN, L., (2021) El teletrabajo. Tecnoretos del Derecho; Coordinado por SANTAMARIA RAMOS F.J. Valencia, España: Tirant lo Blanch. Págs. 184-214.
- SELMA PEÑALVA, A. (2009) "Las peculiaridades prácticas del control en la empresa". Revista Actualidad Laboral. Nº 14. Págs. 92-130.
- SEMPERE NAVARRO A.V. (2000) Nuevas tecnologías y Relaciones Laborales. Madrid, España: Francis Lefevre.
- SEMPERE NAVARRO A.V. (2015) Las TICs en el ámbito laboral. Madrid, España: Francis Lefevre.
- SEMPERE NAVARRO, A.V. Y SAN MARTÍN MAZZUCCONI, C. (2012) "Sobre el control empresarial de los ordenadores". Revista Doctrinal Aranzadi Social. Nº 3/2012.
- SEMPERE NAVARRO, A.V. Y SAN MARTÍN MAZZUCCONI, C. (2005) "El uso sindical del correo electrónico a la luz de la STC 281/2005, de 7 noviembre". Revista Doctrinal Aranzadi Social. Nº 5/2005, págs. 535-546.
- SEMPERE NAVARRO, A.V. Y SAN MARTÍN MAZZUCCONI, C. (2010) "Nuevas Tecnologías y Relaciones Laborales". Revista Doctrinal Aranzadi Social Vol. 11 nº 11, págs. 259-287.

- SERRANO GARCIA, J. Mª. (2019) “El Derecho a la libertad de expresión del trabajador a través de las nuevas tecnologías y el derecho a la reputación de la empresa”. Revista Española de Derecho del Trabajo nº 217, Págs. 101-127.
- SERRANO GARCIA, J. Mª. (2021) “La Protección de datos y la regulación de los derechos digitales en la negociación colectiva y en la jurisprudencia”. Publicada en la Revista de derecho social nº 94, págs. 167-192
- SEVERÍN FUSTER, G. (2015). “Sobre el modelo de contratación de servicios remunerados en el derecho romano. Algunos aspectos relevantes de la *locatio conductio*”. Revista de Derecho Universidad Católica del Norte, vol. 22, nº2. Coquimbo 2015, Págs. 357-389.
- TASCÓN LÓPEZ, R. (2007) “El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica”. Madrid. Revista Doctrinal Aranzadi Social, Nº 5, 2007, págs. 1985-2006.
- WARREN, S.D. y BRANDEIS, L.D. (1890) “The Right to Privacy”. Harvard Law Review, Vol. 4, No. 5, pp. 193-220. Obtenido en la web https://www.jstor.org/stable/1321160?seq=1.

13.- Webgrafía

https://www.cielolaboral.com

https://core.ac.uk/download/pdf/296383939.pdf

https://definicion.de/correo-electronico/

https://www.diariolaley.laleynext.es

https://dpej.rae.es/lema/direccion-ip

https://www.dpglegal.es/es/noticia/la-monitorizacion-empresarial/

https://dx.doi.org/10.4067/S0718-97532015000200012

https://www.economistjurist.es/premium/la-firma/tome-vd-asiento-acerca-de-la-ley-de-la-silla/

https://www.eduardorojotorrecilla.es

http://www.eduardorojotorrecilla.es/2020/10/geolocalizacion-y-utilizacion-de.html

https://www.elderecho.com

https://elderecho.com/origen-juridico-historico-la-proteccion-datos-evolucion-las-diferentes-teorias-juridicas-la-protegido

http://www.elderecho.com/tribuna/laboral/Comunicaciones-empresa-control-correo-electronicotrabajador_11_1045180003.html;

https://www.gps.gov/spanish.php

https://www.iberley.es

https://www.jstor.org/stable/1321160?seq=1

https://www.losojosdehipatia.com.es

https://www.leyderecho.org

https://www.noticiasjuridicas.com

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1›

https://polaridad.es/historia-del-circuito-integrado-quien-lo-invento/

https://www.secpho.org/microelectronica

http://sedici.unlp.edu.ar/bitstream/handle/10915/46243/Documento_completo.pdf?sequence=1&isAllowed=y

https://www.vlex.es

https://www.wikipedia.com

https://es.wikipedia.org/wiki/Inform%C3%A1tica

https://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n

https://es.wikipedia.org/wiki/Internet

https://es.wikipedia.org/wiki/World_Wide_Web

https://es.wikipedia.org/wiki/Protocolo_para_transferencia_simple_de_correo

https://es.wikipedia.org/wiki/Protocolo_de_transferencia_de_archivos

https://es.wikipedia.org/wiki/Phishing

https://es.wikipedia.org/wiki/Ataque_de_intermediario

https://es.wikipedia.org/wiki/Hardware

https://es.wikipedia.org/wiki/Software

14.- ANEXO DE JURISPRUDENCIA Y DOCTRINA JURISPRUDENCIAL

14.1. SENTENCIAS TRIBUNAL EUROPEO DE DERECHOS HUMANOS

- Sentencia de la Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford vs Reino Unido).
- Sentencia de la Tribunal Europeo de Derechos Humanos de 3 de abril de 2007 (caso Copland vs Reino Unido).
- Sentencia del Tribunal Europeo de Derechos Humanos, de 5 de octubre de 2010 (Caso Köpke contra Alemania).
- Sentencia del Tribunal de Derechos Humanos de 12 de enero de 2016, (Caso Barbulescu vs Rumanía), Barbulescu I.
- Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos 61/2017 de 5 de septiembre de 2017 (Caso Barbulescu vs Rumanía). Barbulescu II.
- Sentencia del Tribunal Europeo de Derechos Humanos, de 9 de enero de 2018 (Caso López Ribalda vs España).
- Sentencia de la Gran Sala del Tribunal Europeo de Derechos Humanos, de 17 de octubre de 2019 (Caso López Ribalda vs España).

14.2. SENTENCIAS TRIBUNAL CONSTITUCIONAL

- Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre de 1984.
- Sentencia del Tribunal Constitucional 99/1994, de 11 de abril de 1994.
- Sentencia del Tribunal Constitucional 6/1995, de 10 de enero de 1995.
- Sentencia del Tribunal Constitucional 136/1996, de 23 de julio de 1996.
- Sentencia del Tribunal Constitucional 94/1984, de 16 de octubre de 1984.
- Sentencia del Tribunal Constitucional 171/1989, de 19 de octubre de 1989.
- Sentencia del Tribunal Constitucional 123/1992, de 28 de septiembre de 1992.
- Sentencia del Tribunal Constitucional 173/1994, de 7 de junio de 1994.
- Sentencia del Tribunal Constitucional 11/1981, de 8 de abril de 1981.
- Sentencia del Tribunal Constitucional 66/1995, de 8 de mayo de 1995.
- Sentencia del Tribunal Constitucional 55/1996, de 28 de marzo de 1996.
- Sentencia del Tribunal Constitucional 207/1996, de 16 de diciembre de 1996.

- Sentencia del Tribunal Constitucional 37/1998, de 17 de febrero de 1998.
- Sentencia del Tribunal Constitucional 6/1998, de 13 de enero de 1998.
- Sentencia del Tribunal Constitucional 186/2000, de 10 de julio de 2000.
- Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000.
- Sentencia del Tribunal Constitucional 29/2013 de 11 de febrero de 2013.
- Sentencia del Tribunal Constitucional 39/2016**,** de 3 de marzo de 2016.
- Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre de 1984.
- Sentencia del Tribunal Constitucional 70/2002, de 3 de abril de 2002.
- Sentencia del Tribunal Constitucional 123/2002, de 20 de mayo de 2002.
- Sentencia del Tribunal Constitucional 170/2013, de 7 de octubre 2013.
- Sentencia del Tribunal Constitucional 98/2003, de 10 de abril de 2003.
- Sentencia del Tribunal Constitucional 186/2000, de 10 de julio de 2000.
- Sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre de 2012.
- Sentencia del Tribunal Constitucional 88/1985, de 19 de julio de 1985.
- Sentencia del Tribunal Constitucional 99/1994, de 11 de abril de 1994.
- Sentencia del Tribunal Constitucional 126/2003, de 30 de junio de 2003.
- Sentencia del Tribunal Constitucional 99/1994, de 11 de abril de 1994.
- Sentencia del Tribunal Constitucional 213/2002, de 11 de noviembre de 2002.
- Sentencia del Tribunal Constitucional 20/2002, de 28 de enero de 2002.
- Sentencia del Tribunal Constitucional 151/2004, de 20 de septiembre de 2004.
- Sentencia del Tribunal Constitucional 70/2002, de 3 de abril de 2002.
- Sentencia del Tribunal Constitucional 39/2016 de 3 de marzo de 2016.
- Sentencia del Tribunal Constitucional 281/2005 de 7 de noviembre de 2005.
- Sentencia del Tribunal Constitucional 94/1995 de 19 de junio de 1995.
- Sentencia del Tribunal Constitucional 308/2000, de 18 de diciembre de 2000.
- Sentencia del Tribunal Constitucional 185/2003, de 27 de octubre de 2003.
- Sentencia del Tribunal Constitucional 198/2004, de 15 de noviembre de 2004.
- Sentencia del Tribunal Constitucional 173/1992, de 29 de octubre de 1992.
- Sentencia del Tribunal Constitucional 164/1993, de 18 de mayo de 1993.
- Sentencia del Tribunal Constitucional 13/1997, de 27 de enero de 1997.
- Sentencia del Tribunal Constitucional 36/2004, de 8 de marzo de 2004.
- Sentencia del Tribunal Constitucional 132/2000, de 16 de mayo de 2000.
- Sentencia del Tribunal Constitucional 269/2000, de 13 de noviembre de 2000.

- Sentencia del Tribunal Constitucional 281/2005, de 7 de noviembre de 2005.
- Sentencia del Tribunal Constitucional 173/1992, de 29 de octubre de 1992.
- Sentencia del Tribunal Constitucional 98/2000, de 10 de abril de 2000.
- Sentencia del Tribunal Constitucional 186/2000, de 10 de julio de 2000.
- Sentencia del Tribunal Constitucional 196/2004, de 15 de noviembre de 2004.

14.3. SENTENCIAS TRIBUNAL SUPREMO

- Sentencia del Tribunal Supremo 119/2018, de 8 de febrero de 2018.
- Sentencia del Tribunal Supremo de 26 de septiembre de 2007.
- Sentencia del Tribunal Supremo de 5 de diciembre de 2003.
- Sentencia del Tribunal Supremo de fecha 19 de julio de 1989.
- Sentencia del Tribunal Supremo de 8 marzo 2011.
- Sentencia del Tribunal Supremo de 7 de febrero de 2018.
- Sentencia del Tribunal Supremo de 8 de febrero de 2021.
- Sentencia del Tribunal Supremo de 15 de septiembre de 2021.
- Sentencia del Tribunal Supremo de fecha 13 de mayo de 2014.
- Sentencia del Tribunal Supremo de 15 de enero de 2009.
- Sentencia del Tribunal Supremo 24 de mayo de 2005.
- Sentencia del Tribunal Supremo de 16 de octubre de 1986.
- Sentencia del Tribunal Supremo de 26 de enero de 1987.
- Sentencia del Tribunal Supremo de 19 de diciembre de 1990.
- Sentencia del Tribunal Supremo de 4 de febrero de 1991.
- Sentencia del Tribunal Supremo de 21 de enero de 1991.
- Sentencia del Tribunal Supremo de 27 de enero de 2004.
- Sentencia del Tribunal Supremo de 15 septiembre de 2020.
- Sentencia del Tribunal Supremo de 20 de mayo de 2012.
- Sentencia del Tribunal Supremo de 16 de julio de 2012.
- Sentencia del Tribunal Supremo de 3 de diciembre de 2013.
- Sentencia del Tribunal Supremo de 25 de febrero de 2013.
- Sentencia del Tribunal Supremo de 9 de diciembre de 2016.
- Sentencia del Tribunal Supremo de 10 de junio de 2009.
- Sentencia del Tribunal Supremo de 9 de diciembre de 2010.

- Sentencia del Tribunal Supremo de 20 de mayo de 2013.
- Sentencia del Tribunal Supremo de 19 de noviembre de 2013.
- Sentencia del Tribunal Supremo de 19 de diciembre de 2019.
- Sentencia del Tribunal Supremo de 10 de enero de 2023.

14.4. SENTENCIAS TRIBUNALES SUPERIORES DE JUSTICIA

- Sentencia del Tribunal Superior de Justicia de Castilla-La Mancha de 28 de mayo de 2009.
- Sentencia del Tribunal Superior de Justicia de Castilla-La Mancha de 23 de marzo de 2015.
- Sentencia del Tribunal Superior de Justicia de Cataluña de fecha 9 de septiembre de 2019.
- Sentencia del Tribunal Superior de Justicia de las Palmas de Gran Canaria de fecha 22 de enero de 2016.
- Sentencia del Tribunal Superior de Justicia de Madrid de 18 de mayo de 2004.
- Sentencia del Tribunal Superior de Justicia de Madrid 739/2014, de 29 septiembre de 2014.
- Sentencia del Tribunal Superior de Justicia de Madrid, de 13 de mayo de 2016.
- Sentencia del Tribunal Superior de Justicia de Madrid de 21 de marzo de 2014.
- Sentencia del Tribunal Superior de Justicia de Madrid de 12 de junio de 2017.
- Sentencia del Tribunal Superior de Justicia de Andalucía (Málaga) 63/2020, de 20 de mayo de 2020.
- Sentencia del Tribunal Superior de Justicia de Madrid de 28 de octubre de 2011.
- Sentencia del Tribunal Superior de Justicia de Castilla y León en fecha 15 de marzo de 2021.
- Sentencia del Tribunal Superior de Justicia de Castilla y León (Valladolid) de 30 de diciembre de 2021.
- Sentencia del Tribunal Superior de Justicia de Cataluña de fecha 22 de mayo de 2015.
- Sentencia del Tribunal Superior de Justicia de la Comunidad Valenciana de fecha 21 de marzo de 2017.

- Sentencia del Tribunal Superior de Justicia de Andalucía (Sevilla) de 9 de marzo de 2001.
- Sentencia del Tribunal Superior de Justicia de Madrid, de 7 de marzo de 2014.
- Sentencia del Tribunal Superior de Justicia de Madrid en fecha 20 de enero de 2020.
- Sentencia del Tribunal Superior de Justicia de Cataluña de fecha 22 de mayo de 2015.
- Sentencia del Tribunal Superior de Justicia del País Vasco en su sentencia de fecha 10 de mayo de 2011.
- Sentencia del Tribunal Superior de Justicia de Castilla-La Mancha de 18 de mayo de 2004.
- Sentencia del Tribunal Superior de Justicia de Asturias de 30 de noviembre de 2013.
- Sentencia del Tribunal Superior de Justicia de Andalucía (Málaga), de fecha 5 de abril de 2017.
- Sentencia del Tribunal Superior de Justicia de Valladolid de 30 de diciembre de 2021.
- Sentencia del Tribunal Superior de Justicia de Madrid de 2 de junio de 2022.
- Sentencia del Tribunal Superior de Justicia de Madrid de 18 de julio de 2022.
- Sentencia del Tribunal Superior de Justicia de Madrid de Madrid de 24 enero de 2022.
- Sentencia del Tribunal Superior de Justicia de Galicia de 28 de enero de 2016.
- Sentencia del Tribunal Superior de Justicia de Cataluña de 16 de octubre de 2015.
- Sentencia del Tribunal Superior de Justicia de Asturias de 18 de octubre de 2022.
- Sentencia del Tribunal Superior de Justicia de Andalucía (Sevilla), de 28 de marzo 2019.
- Sentencia del Tribunal Superior de Justicia de Madrid de 26 de abril de 2023.
- Sentencia del Tribunal Superior de Justicia de Madrid de 8 de junio de 2023.