UNIVERSIDADE DA CORUÑA

TRABAJO FIN DE MÁSTER

MÁSTER DE LA ABOGACÍA

CURSO 2018 - 2020

Poder de control empresarial, novas tecnoloxías e dereitos fundamentais dos traballadores

Poder de control empresarial, nuevas tecnologías y derechos fundamentales de los trabajadores

Power of business control, new technologies and fundamental rights of workers

MARÍA MEIZOSO SECO

Tutor: Prof. Cat. ALBERTO ARUFE VARELA

ÍNDICE

Capítulo III

El CONTROL DE LA PRESTACIÓN LABORAL A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS (2): LA VIDEOVIGILANCIA EMPRESARIAL

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
Art(s).	Artículo(s)
BOE	*Boletín Oficial del Estado*
CE	Constitución Española
CEDH	Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales
DOUE	*Diario Oficial de la Unión Europea*
ET	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
FD	Fundamento(s) de Derecho
IT	Incapacidad Temporal
JS	Juzgado de lo Social
LISOS	Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social
LOPD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
LRJS	Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social
Párr.	Párrafo(s)
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección civil 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
S	Sentencia(s)
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia

INTRODUCCIÓN

En el presente trabajo se estudiarán los aspectos jurídicos más relevantes en relación con el poder de control empresarial ejercido a través de las nuevas tecnologías. Para ello, se indagará en la realidad de este tipo de controles, a fin de dilucidar hasta donde pueden llegar las partes implicadas en la relación laboral –empresario y trabajador– y, por ende, cuáles serán las líneas de defensa más acertadas de cada una de ellas en caso de controversia judicial.

Las facultades de control y vigilancia empresarial, en su configuración tradicional, se han visto perturbadas por las nuevas tecnologías, pues igual que sucede en otras ramas del derecho, los avances tecnológicos han irrumpido de lleno en el mundo laboral y, por consiguiente, en el Derecho del Trabajo. La fiscalización de los ordenadores utilizados para el desempeño del trabajo, la instalación de sistemas de videovigilancia o el almacenamiento de datos de carácter personal en el ámbito laboral, son temas que han ido adquiriendo un notable protagonismo y han pasado a ser una de las principales preocupaciones de los trabajadores. La demanda de asesoramiento legal en esta materia es un fiel reflejo de la realidad, ya que los trabajadores se cuestionan, cada vez más, hasta qué punto el empresario puede registrar el contenido del ordenador de empresa o si este puede instalar cámaras de videovigilancia en el centro de trabajo.

El eje fundamental sobre el que gira el presente trabajo es el choque entre el poder de control empresarial y los derechos fundamentales de los trabajadores, por lo que se analizará si es posible modular tales derechos en el ámbito laboral o si, por el contrario, estos quedan completamente mermados por el poder de control del empresario. Con respecto a esta cuestión, tanto la regulación legal como la negociación colectiva se encuentran un paso por detrás de la realidad, lo cual provoca que en la actualidad no existan soluciones precisas y concluyentes. Además, tampoco parece que un futuro cercano vaya a existir una regulación legal decisiva, sin perjuicio de la promulgación esporádica de leyes que resulten de aplicación al tema objeto de estudio. Todo lo anterior, propicia la judicialización de las controversias e incrementa las decisiones de los tribunales, las cuales ayudan, aunque sea mínimamente, a establecer un marco al que atenerse.

La información será estructurada en tres capítulos principales. El Capítulo I, se dedicará a analizar de forma genérica las facultades de control y vigilancia empresarial, como facultades integrantes del poder directivo. A continuación, el Capítulo II tratará sobre el control del uso de los medios informáticos puestos a disposición del trabajador y la colisión de este tipo de control con el derecho fundamental a la intimidad y al secreto de las comunicaciones. El Capítulo III, sitúa su análisis en la videovigilancia empresarial y la colisión de esta con el derecho fundamental a la protección de datos de carácter personal. Para ello, se examinarán las grandes tendencias jurisprudenciales recaídas al interpretar la escasa normativa sobre el objeto de estudio.

A pesar del intento por delimitar cada una de las cuestiones planteadas y debido al ámbito tan específico sobre el que recae el presente trabajo, resulta complicado tratar ciertos aspectos de forma independiente –como son las cuestiones relativas a los derechos fundamentales de los trabajadores– por lo que estos aspectos serán tratados de forma transversal a lo largo de los tres capítulos.

Capítulo I

FACULTADES EMPRESARIALES DE VIGILANCIA Y CONTROL EN LAS RELACIONES DE TRABAJO

1. PODER DE DIRECCIÓN EMPRESARIAL Y FACULTADES DE CONTROL Y VIGILANCIA

1.1. Concepto y alcance de las facultades de control y vigilancia en la relación laboral

Antes de nada, es importante tener en cuenta que el fundamento del poder de dirección empresarial se encuentra recogido en el artículo (en adelante art.) 38 de la Constitución Española[1] (en adelante CE), el cual reconoce la libertad de empresa en el marco de la economía de mercado. Así, la CE, contempla la posibilidad de que tanto las personas físicas como jurídicas desarrollen iniciativas económicas, lo que se materializa, en su vertiente laboral, a través del poder de dirección y organización que el empresario despliega sobre sus trabajadores y sobre el desarrollo de la prestación laboral[2]. Por tanto, con base en el citado art. 38 CE, el derecho laboral ha reconocido al empresario el poder de organizar y dirigir su empresa[3].

En cuanto a la legislación laboral, el poder de dirección empresarial está reconocido en numerosos artículos (en adelante arts.) del 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[4] (en adelante ET), concretamente, en los arts. 1.1, 5 c), 20.1 y 20.2 del mencionado texto legal.

Tradicionalmente, la doctrina ha definido el poder de dirección empresarial como un abanico de facultades jurídicas por las que el empresario dispone del trabajo realizado, ordena las prestaciones laborales y organiza el trabajo en la empresa[5]. En este punto es preciso cuestionarse si dentro de las facultades jurídicas que engloba el poder de dirección se encuentran las de control y vigilancia empresarial.

El art. 20 ET, que lleva por rúbrica «*dirección y control de la actividad laboral*», preceptúa, en su apartado tercero, que «*el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el*

---

[1] *Boletín Oficial del Estado* (en adelante *BOE*) n.º 311, de 29 de diciembre de 1978.

[2] FERNÁNDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, Aranzadi, Cizur Menor (Navarra), 2003, p. 20.

[3] FABREGAT MONFORT, G.: *Vademécum de Derecho Laboral (5ª Edición)*, Tirant Lo Blanch, Valencia, 2017, p. 69.

[4] *BOE* n.º 255, de 24 de octubre de 2015.

[5] MONTOYA MELGAR, A.: «Dirección y control de la actividad laboral», BORRAJO DACRUZ, E. (Dir.), *Comentarios a las leyes laborales. El Estatuto de los Trabajadores*, tomo V, Edersa, Madrid, 1985, p. 132.

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». Así las cosas, todo parece indicar que las facultades de control y vigilancia se encuentran incardinadas en el poder directivo empresarial, y son las que permiten al empresario adoptar medidas de supervisión de la actividad laboral[6].

En línea con lo anterior, cabe señalar que las facultades de control y vigilancia, estrechamente relacionadas con el poder directivo, tienen su razón de ser en la particularidad de la relación laboral, la cual implica que el trabajador no se obliga únicamente a desempeñar una determinada actividad, sino a desempeñarla conforme a las órdenes e indicaciones empresariales[7]. Por tanto, si el empresario no tuviese potestad para supervisar el cumplimiento de las instrucciones dadas, las mismas perderían, en gran medida, su virtualidad. No obstante, en la práctica, el control no conlleva únicamente la comprobación de que las órdenes empresariales se cumplen, sino que la vigilancia se despliega sobre el conjunto de la prestación laboral, como se expondrá a lo largo del presente trabajo.

En lo tocante al alcance de las facultades de control y vigilancia empresarial, el art. 20.3 ET delimita tímidamente tanto el ámbito sobre el que debe recaer la vigilancia empresarial, como el tipo de medidas de control que el empresario puede adoptar.

En primer lugar, y según lo dispuesto en el art. 20.3 ET, el control empresarial únicamente podrá estar orientado a comprobar que el trabajador cumple con sus obligaciones y deberes laborales, lo que implica que el ámbito objeto de control debe ser, como regla general, el ámbito laboral y nunca las conductas extralaborales del trabajador. No obstante, la progresiva evolución de las formas de prestación del trabajo ha desdibujado la frontera entre la vida personal y profesional de los trabajadores, por lo que en algunos casos resulta complicado distinguir entre el ámbito estrictamente laboral y ámbito el extralaboral. Además, existen casos donde el control empresarial desplegado sobre conductas extralaborales ha sido considerado válido por nuestros tribunales, al entender que la conducta del trabajador perjudicaba los legítimos intereses empresariales[8].

En segundo y último lugar, el ET permite al empresario adoptar las medidas de control y vigilancia que considere más oportunas, siempre y cuando estas guarden el debido

[6] DE VICENTE PACHÉS, F.: «Las facultades empresariales de vigilancia y control en las relaciones de trabajo: concepto y fundamento. Una primera aproximación a las diversas formas de control empresarial», GARCÍA NINET, J. I. (Dir.), *El control empresarial en el ámbito laboral*, CISS, 2005, p. 22.

[7] FERNÁNDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral, op. cit.*, p. 22.

[8] En este sentido la Sentencia (en adelante S) de la Sala de lo Social de Granada, del Tribunal Superior de Justicia (en adelante TSJ) de Andalucía 2459/2018, de 25 de octubre (*Aranzadi Westlaw*, referencia JUR 2019\26436) consideró legítimo el hecho de que un empresario, a través de un detective privado, controlase a una trabajadora que se encontraba de baja por Incapacidad Temporal (en adelante IT) y realizaba, en su vida privada, actividades incompatibles con su situación de IT.

respeto a la dignidad del trabajador. Si bien el ET ofrece un amplio margen de posibilidades, dejando a elección del empresario la medida de control a aplicar, también impone un límite infranqueable: el respeto a la dignidad de los trabajadores.

1.2. Delimitación frente a otras facultades empresariales

Una vez analizado el concepto y el alcance del poder de control y vigilancia empresarial, resulta necesario reparar en la relación existente entre dicho poder y otras facultades empresariales, como son, por ejemplo, las facultades disciplinarias y las facultades recogidas en el art. 18 ET, conocidas como facultades de «*policía empresarial*».

Como ya se ha visto, el poder de dirección empresarial engloba todo un conjunto de facultades, entre las que se encuentran, la facultad de dictar órdenes, la facultad de control y vigilancia y la facultad disciplinaria. Ello implica que el poder disciplinario sea entendido como un complemento necesario al poder de control y vigilancia, ya que, de lo contrario, este último se convertiría en un poder vacío de contenido[9]. Así, si la vigilancia no estuviera acompañada de la facultad de sancionar los incumplimientos observados, carecería por completo de sentido.

Parece que la relación entre ambos poderes es recíproca, ya que, por un lado, el poder de control es un instrumento necesario del que se aprovecha el poder disciplinario, siendo habitual en la práctica que las medidas de control y vigilancia desplegadas por el empresario se utilicen, *a posteriori*, para justificar la procedencia de la sanción impuesta[10]. Por otro lado, el poder disciplinario sirve a su vez a las facultades de control y vigilancia, debido a su gran efecto disuasorio.

Distintas consideraciones pueden hacerse respecto de la delimitación de las facultades de control frente al denominado poder de «*policía empresarial*». Para abordar esta cuestión es importante partir del art. 18 ET, el cual faculta al empresario a realizar registros sobre la persona del trabajador, en sus taquillas y efectos particulares, siempre y cuando sean necesarios para proteger el patrimonio empresarial y el de los demás trabajadores de la empresa[11]. Además, según lo dispuesto en el mencionado precepto, el registro deberá efectuarse dentro del centro de trabajo, durante la jornada laboral, y contando, en el momento de su realización, con la presencia de un representante legal de

[9] POQUET CATALÁ, R.: *La actual configuración del poder disciplinario empresarial*, Tirant Lo Blanch, Valencia, 2011, p. 29 y 30.

[10] V. la S de la Sala de lo Social del TSJ de Madrid 75/2019, de 25 de enero (*Aranzadi Westlaw*, referencia AS 2019\1174), en la que se ha declarado procedente un despido tras comprobar el empresario, mediante cámaras de videovigilancia, que un trabajador se apropiaba productos de la empresa sin abonar su importe, o la S de la Sala de lo Social del TSJ de la Comunidad Valenciana 1483/2019, de 16 de mayo (*Aranzadi Westlaw*, referencia JUR 2019\271326), que avala la sanción de suspensión de empleo y sueldo, tras observar la empresa, a través de los historiales de navegación, que el trabajador destinaba gran parte de su jornada a navegar por internet, desatendiendo sus obligaciones laborales.

[11] Fundamento de derecho (en adelante FD) 4.º de la S de la Sala de lo Social del TSJ de Castilla La Mancha 670/2018, de 11 de mayo (*Aranzadi Westlaw*, referencia JUR 2018\183155).

los trabajadores, y en defecto de representación legal, con la presencia de otro trabajador de la empresa. Por tanto, el art. 18 ET permite al empresario el ejercicio de una verdadera actividad de policía privada en la empresa, que excede del mero control de la actividad laboral[12].

En este caso, no existe una relación íntima entre ambos poderes, sino que estos están claramente diferenciados. Sobre esta relación de poderes existe algún pronunciamiento judicial interesante. Así, por ejemplo, el FD 3.º de la S de la Sala Cuarta del Tribunal Supremo (en adelante TS), de 26 de septiembre de 2007 (*Aranzadi Westlaw*, referencia RJ 2007\7514) señala que el art. 18 ET le atribuye al empresario un control «*que excede del que deriva de su posición en el contrato de trabajo y que, por tanto, queda fuera del marco del artículo 20 del Estatuto de los Trabajadores. En los registros el empresario actúa, de forma exorbitante y excepcional, fuera del marco contractual de los poderes que le concede el artículo 20 del Estatuto de los Trabajadores y, en realidad, como ha señalado la doctrina científica, desempeña –no sin problemas de cobertura– una función de policía privada o de policía empresarial que la Ley vincula a la defensa de su patrimonio o del patrimonio de otros trabajadores de la empresa [...] Tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores*».

En definitiva, mientras que existen poderes empresariales estrechamente relacionados con las facultades de control y vigilancia –como ocurre en el caso del poder disciplinario–, existen otros –como es el poder de *«policía empresarial»*–, que se encuentran completamente desvinculados del concepto de control y vigilancia recogido en el art. 20.3 ET.

1.3. Cuadro normativo actual de las facultades de control y vigilancia

El eje normativo sobre el que se articula el poder de control y vigilancia empresarial es el ET y algunos otros textos normativos que, a pesar de no estar específicamente pensados para el ámbito laboral, contienen reglas y principios operativos en dicho ámbito[13].

Por lo que respecta al ET, en él se contienen las referencias más básicas al poder de control y vigilancia. Como ya se ha visto, el art. 20.3 del citado texto legal, recoge con cierta ambigüedad el concepto y el alcance de las facultades de control y vigilancia. Si bien, el art. 20.4 ET se centra específicamente en un tipo de control empresarial, que es aquel que lleva a cabo el empresario sobre el estado de salud del trabajador. Este art. dispone que «*el empresario podrá verificar el estado de salud del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante*

[12] GOÑI SEIN, J. L.: *El respeto a la esfera privada del trabajador*, Civitas, Madrid, 1988, p. 161.
[13] FERNÁNDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, *op. cit.*, p. 31.

reconocimiento a cargo de personal médico». Así, se permite a la empresa comprobar el estado de salud de los trabajadores, contratando la gestión de la prestación de IT por contingencias comunes con una Mutua.

A través de la Disposición Final Decimotercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[14] (en adelante LOPD), se incorporó en el ET un nuevo art. 20 bis que recoge el derecho de los trabajadores a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empresario, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización. Sin embargo, parte de la doctrina ha cuestionado la ubicación de esta previsión normativa en el art. destinado al control y vigilancia de la actividad laboral, entendiendo que no es el lugar natural, sino que esta norma debería haberse incluido en el art. 4.2 ET, dedicado a los derechos de los trabajadores, o, en todo caso, en el art. 18 ET, sobre inviolabilidad de la persona del trabajador[15].

Ahora bien, lo que es evidente es que, mediante este nuevo precepto, la legislación laboral asume y se adapta a las nuevas formas de control y vigilancia empresarial, como más tarde se tendrá la oportunidad de analizar.

A mayor abundamiento, la LOPD se complementa con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección civil 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[16] (en adelante RGPD). Por tanto, el empresario también deberá acomodar la organización empresarial y, concretamente, las facultades de control y vigilancia, a las exigencias fijadas por el RGPD.

Por último, el prototipo de norma que despliega sus efectos sobre las relaciones laborales, es 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[17] (en adelante Ley 1/1982), articulando dos derechos fundamentales actualmente implicados en el control y vigilancia empresarial. Por una parte, el derecho a la intimidad del trabajador y, por otra parte, el derecho a la libertad informática, el cual se ve claramente afectado con la aparición de nuevos mecanismos de control empresarial[18].

---

[14] *BOE* n.º 294, de 6 de diciembre de 2018.

[15] FERNÁNDEZ ORRICO, F. J.: «Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre», *Revista Española de Derecho del Trabajo*, n.º 222, 2019. Versión electrónica: www.westlaw.es (BIB 2019\7744).

[16] *Diario Oficial de la Unión Europea* (en adelante *DOUE*) n.º 119, de 4 de mayo de 2016.

[17] *BOE* n.º 115, de 14 de mayo de 1982.

[18] La S del Tribunal Constitucional (en adelante TC) 245/1993, de 20 de julio (*Aranzadi Westlaw*, referencia RTC 1993\254), definió el derecho a la libertad informática como el derecho a controlar el uso de los datos insertos en un programa informático, que comprende, entre otras cosas, la oposición del ciudadano a que determinados datos personales sean usados para fines distintos de aquel legítimo que justificó su obtención. En este sentido, V. también la STC 94/1998, de 4 de mayo (*Aranzadi Westlaw*, referencia RTC 1998\94).

2. EL LÍMITE A LAS FACULTADES DE CONTROL Y VIGILANCIA: LOS DERECHOS FUNDAMENTALES DE LOS TRABAJADORES

Según lo dispuesto en el art. 1.1 ET, los trabajadores desempeñan su actividad laboral dentro del ámbito de organización y dirección del empresario, realizando las funciones que tienen encomendadas bajo la dependencia de la empresa y por cuenta de la misma. Por tanto, los trabajadores adoptan una clara posición de subordinación, lo que genera, a su vez, una importante situación de desigualdad. Esta situación de desigualdad queda indiscutiblemente clara en la STC 129/1989[19]:

> Esta garantía por parte de los poderes públicos, y en particular por parte del legislador de la vigencia de los derechos fundamentales puede resultar singularmente apremiante en el ámbito laboral, en el que la desigual distribución de poder social entre trabajador y empresario y la distinta posición que estos ocupan en las relaciones laborales elevan en cierto modo el riesgo de eventuales menoscabos de los derechos fundamentales del trabajador. Por ello, este Tribunal se ha cuidado de advertir que nada legitima que quienes presten servicios en organizaciones empresariales 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, de suerte que la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano.

Los trabajadores se integran en una organización en la que están sometidos a diversos poderes empresariales, y es por ello por lo que resulta necesario limitar y restringir dichos poderes, garantizando así el ejercicio por los trabajadores de sus derechos fundamentales. Es decir, el hecho de que el poder de dirección empresarial tenga como fundamento la libertad de empresa no implica que las facultades empresariales sean absolutas o que el empresario pueda desplegar las mismas sin ningún tipo de límite, amparándose para ello en su posición de superioridad con respecto a los trabajadores.

En lo tocante a los derechos fundamentales afectados frente al ejercicio de la actividad de control empresarial, señalar que son todos aquellos que posee el trabajador, inherentes a su condición de ciudadano. Si bien, en la práctica, los derechos fundamentales más directamente afectados por las medidas de vigilancia y control son los recogidos en el art. 18 CE, particularmente, el derecho a la intimidad personal y familiar, el derecho al secreto de las comunicaciones y el derecho a la libertad informática[20].

Además, sobre la limitación del poder de control y vigilancia se ha manifestado el TC a través de dos pronunciamientos emblemáticos que han supuesto un hito y han condicionado toda la jurisprudencia posterior en relación con este tema. Por una parte, la

[19] FD 3.º de la STC 129/1989, de 17 de julio (*Aranzadi Westlaw*, referencia RTC 1989\129).

[20] DE VICENTE PACHÉS, F.: «Las facultades empresariales de vigilancia y control en las relaciones de trabajo: concepto y fundamento. Una primera aproximación a las diversas formas de control empresarial», *op. cit.*, p. 29.

STC 98/2000 ha señalado que las limitaciones o modulaciones al poder de control tienen que ser las indispensables y estrictamente necesarias para satisfacer un interés empresarial merecedor de tutela y protección, de manera que si existen otras posibilidades de satisfacer dicho interés, menos agresivas y afectantes de derechos fundamentales, habrá que emplear estas últimas[21]. Por otra parte, la STC 186/2000 ha puesto de manifiesto la necesidad de comprobar si una medida de control empresarial, restrictiva de un derecho fundamental, supera el juicio de proporcionalidad. Para ello, habrá que observar si tal medida es susceptible de conseguir el objetivo propuesto –juicio de idoneidad–, si es necesaria, en el sentido de que no exista otra medida más moderada para la consecución del propósito de control –juicio de necesidad– y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto –juicio de proporcionalidad en sentido estricto–[22].

Tomando como base los anteriores pronunciamientos, está claro que la práctica obliga a ponderar el ejercicio del poder de control y vigilancia empresarial, evitando que las medidas de vigilancia empleadas por el empresario atenten contra los derechos fundamentales de los trabajadores. Ahora bien, los derechos fundamentales tampoco son absolutos, siendo especialmente conflictiva la limitación del derecho a la intimidad en relación con ejercicio de la facultad de control regulada en el art. 20.3 ET.

En cuanto al derecho a la intimidad en el lugar de trabajo, el art. 4.2 e) ET garantiza que los trabajadores tienen derecho a la intimidad y a la consideración debida a su dignidad. También, y como ya se ha visto, el art. 20.3 ET menciona que, a la hora de adoptar las medidas de control, el empresario deberá guardar la consideración debida a la dignidad del trabajador. Del mismo modo, el art. 20 bis ET regula el derecho a la intimidad del trabajador cuando este es controlado a través de dispositivos digitales. Así las cosas, el derecho a la intimidad es una pieza clave en la legislación laboral, sobre todo a la hora de controlar la actividad laboral, pues, se trata de uno de los límites más importantes que el empresario debe tener en cuenta.

El TC ha dejado claro en su STC 98/2000 que «*el derecho a la intimidad, en cuanto derivación de la dignidad de la persona [...] 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 [...] el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho*»[23]. Es decir, independientemente de que exista el derecho a la intimidad en el lugar de trabajo, no cabe defender un derecho absoluto del trabajador a desarrollar esta vida privada en el marco de la relación laboral.

[21] FD 7.º de la STC 98/2000, de 10 de abril (*Aranzadi Westlaw*, referencia RTC 2000\98).
[22] FD 6.º de la STC 186/2000, de 10 de julio (*Aranzadi Westlaw*, referencia RTC 2000\186).
[23] FD 5.º de la STC 98/2000, de 10 de abril (*Aranzadi Westlaw*, referencia RTC 2000\98).

Asimismo, el Tribunal Europeo de Derechos Humanos (en adelante TEDH) entendió que era demasiado restrictivo limitar el concepto de vida privada a un círculo íntimo, sino que el respeto a la vida privada debe incluir el derecho de los individuos para establecer y desarrollar relaciones con sus semejantes, entre las que se incluyen, las relaciones laborales, ya que es en el trabajo donde la mayoría de las personas tienen múltiples oportunidades para fortalecer sus vínculos con el mundo exterior[24].

En este punto, es oportuno reparar en otro de los límites a la adopción de las medidas de control, recogido en el art. 64.5 f) ET. Este precepto dispone que el Comité de Empresa tendrá derecho a emitir informe, con carácter previo a la ejecución por el empresario, sobre la implantación y revisión de sistemas de organización y control del trabajo. Así, y a pesar de que el informe emitido por el Comité de Empresa no es vinculante, los representantes legales de los trabajadores ejercen una función de garantía adicional de los derechos fundamentales frente a las medidas de control y vigilancia empresarial.

Por último, para el caso de que el empresario lleve a cabo un control lesivo y no respete los derechos fundamentales, el ordenamiento jurídico contempla una respuesta en su art. 50.1 c) ET. Este precepto permite al trabajador extinguir unilateralmente el contrato de trabajo cuando el empresario incumpla gravemente sus obligaciones, percibiendo la indemnización fijada para el despido improcedente[25]. Todo ello, sin perjuicio de la indemnización por vulneración de derechos fundamentales que prevén los arts. 8.11 y 40.1 c) del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social[26] (en adelante LISOS).

En los capítulos posteriores se tratarán supuestos concretos de lo afirmado anteriormente, situaciones conflictivas entre el poder de control empresarial y los derechos fundamentales de los trabajadores, donde las soluciones ofrecidas por nuestros tribunales son variadas y heterogéneas. Uno de los supuestos que suele generar mayores controversias es el control empresarial llevado a cabo a través de los medios informáticos facilitados por la empresa y el control efectuado mediante la videovigilancia, ya que, como se tendrá oportunidad de ver, la evolución tecnológica ha intensificado la capacidad de control empresarial, a la par que ha incrementado las posibilidades de lesionar los derechos fundamentales de los trabajadores.

[24] Párrafo (en adelante párr.) 29 de la STEDH caso Niemietz contra Alemania, de 16 de diciembre de 1992 (*Aranzadi Westlaw*, referencia TEDH 1992\77).
[25] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant Lo Blanch, Valencia, 2015, p. 129.
[26] *BOE* n.º 189, de 8 de agosto de 2008.

3. EVOLUCIÓN DE LAS FACULTADES DE CONTROL Y VIGILANCIA EMPRESARIAL ANTE LA NUEVA COYUNTURA TECNOLÓGICA

Desde finales del siglo pasado y principios del actual, las nuevas tecnologías han entrado a un ritmo imparable en el mundo laboral para revolucionar los sistemas de producción, modificar la estructura ocupacional y alterar las relaciones entre empresarios y trabajadores[27]. Por tanto, igual que ocurre en los demás ámbitos de la vida, la evolución tecnológica ha impactado de lleno en el entorno laboral, marcando un punto de inflexión en las relaciones de trabajo y configurando una realidad distinta a la conocida en tiempos anteriores[28].

Las innovaciones tecnológicas se han implantado en las empresas, mejorando la organización, la productividad y la gestión empresarial. Sin embargo, dichas innovaciones no solo han influido en los campos anteriormente reseñados, sino que también han transformado los tradicionales mecanismos de control y vigilancia empresarial. De esta forma, el empresario recurre a los adelantos tecnológicos –como es la informática, la videovigilancia, el GPS, e incluso los controles biométricos– para supervisar a los trabajadores, pasando a efectuar un control impersonal y centralizado, en contraste con el ejercido tradicionalmente, que era personal, periférico y discontinuo[29].

La tecnificación de las facultades de control empresarial como consecuencia de las innovaciones tecnológicas gira en torno a dos cuestiones fundamentales. En primer lugar, el control que el empresario puede desplegar respecto al uso que los trabajadores hacen de las herramientas informáticas puestas a su disposición. Y, en segundo lugar, el control llevado a cabo por el empresario a través de medios electrónicos y nuevas tecnologías.

Cuando el trabajador ejecuta su trabajo sirviéndose de los medios informáticos propiedad de la empresa –como es el ordenador–, cabe la posibilidad de que el empresario decida fiscalizar el uso que el trabajador hace de los mismos, trascendiendo así su mera función instrumental[30]. Las fórmulas que el empresario utiliza para controlar el uso del ordenador de empresa son variadas y dispares, pues oscilan desde el registro del ordenador aprovechando la ausencia del trabajador[31], hasta la monitorización[32] –mediante *softwares* especializados– pasando por la instalación de programas espía que registran

[27] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, p. 11.

[28] CALVO MORALES, D., TOSCANI GIMENEZ, D.: «El uso de internet y el correo electrónico en la empresa. Límites y garantías», *Revista Española de Derecho del Trabajo*, n.º 165, 2014. Versión electrónica: www.westlaw.es (BIB 2014\1659).

[29] MARÍN ALONSO, I.: *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Tirant Lo Blanch, Valencia, 2005, p. 50.

[30] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op. cit.*, p. 11.

[31] S de la Sala de lo Social del TSJ de Madrid 685/2009, de 5 de noviembre (*Aranzadi Westlaw*, referencia AS 2009\133).

[32] V., entre otras, la S de la Sala de lo Social del TSJ de Madrid 591/2018, de 13 de septiembre (*Aranzadi Westlaw*, referencia AS 2019\923) y la S de la Sala de lo Social del TSJ de la Comunidad Valenciana 3390/2018, de 19 de noviembre (*Aranzadi Westlaw*, referencia AS 2019\1207).

pulsaciones de teclas en tiempo, rutas de aplicaciones, nombres de páginas web visitadas, correos electrónicos, mensajes instantáneos, e incluso, contraseñas[33].

La razón de ser de este tipo de control tiene dos dimensiones íntimamente relacionadas. La dimensión disciplinaria, que permite al empresario sancionar a aquel trabajador que lleve a cabo un uso inadecuado de las herramientas informáticas, lo que en la práctica ocurre frecuentemente cuando el trabajador hace un uso abusivo de la navegación por internet o se excede en la comunicación personal a través del correo electrónico y aplicaciones de mensajería instantánea. Y, la dimensión de prevención, que tiene como finalidad evitar actitudes desviadas, al ser conocedores los trabajadores de que el uso de los medios informáticos puede ser inspeccionado por el empleador.

En lo tocante al control llevado a cabo a través de medios electrónicos y nuevas tecnologías, cabe afirmar que la videovigilancia empresarial es el medio de supervisión de la actividad laboral por excelencia, sin perjuicio de otras innovaciones tecnológicas empleadas con idéntico fin, tales como el GPS[34] o el control biométrico[35]. Si bien es cierto que la finalidad de estos controles es vigilar el cumplimiento por los trabajadores de sus obligaciones laborales, en algunas ocasiones, se despliegan de forma invasiva sobre toda la actividad laboral, poniendo en riesgo los derechos más vulnerables de los trabajadores.

Es importante saber hasta qué punto el empresario puede controlar el uso que el trabajador hace de los medios informáticos y, por otra parte, conocer con que límites cuenta a la hora de recurrir a medios electrónicos para optimizar la vigilancia empresarial. Pues, en caso contrario, estaría lesionando los derechos fundamentales previstos en el art. 18 CE, especialmente el derecho a la intimidad, a la propia imagen, al secreto de las comunicaciones y, una vez que la información es almacenada y tratada, el derecho a la protección de datos[36].

En cualquier caso, lo que es evidente es que el avance de la tecnología ha repercutido notablemente en las formas tradicionales de ejercer el control y la vigilancia empresarial. Esto tiene inevitables consecuencias, sobre todo, con respecto a los límites del poder directivo y al alcance que poseen los derechos constitucionales en el ámbito laboral[37]. Además, la utilización de medios tecnológicos por parte del empresario genera un debate que no puede ser zanjado por el ordenamiento legal, ya que, el marco de regulación legal

[33] S de la Sala de lo Social del TSJ de País Vasco 1072/2012, de 17 de abril (*Aranzadi Westlaw*, referencia AS 2012\1676).

[34] V. la S de la Sala de lo Social de Las Palmas, del TSJ de Islas Canarias 53/2018, de 26 de enero (*Aranzadi Westlaw*, referencia AS 2019\822), sobre la instalación por la empresa de un sistema de GPS en el Smartphone entregado al trabajador para el desempeño de sus funciones.

[35] V., a modo de ejemplo, la S de la Sala de lo Social del TSJ de Madrid 783/2019, de 12 julio (*Aranzadi Westlaw*, referencia JUR 2019\252146) o la S de la Sala de lo Social del TSJ de Murcia 47/2010, de 25 de enero (*Aranzadi Westlaw*, referencia AS 2010\165).

[36] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op. cit.*, p. 16.

[37] SAN MARTÍN MAZZUCCONI, C., SEMPERE NAVARRO, A. V.: «Sobre Nuevas Tecnologías y Relaciones Laborales», *Revista Doctrinal Aranzadi Social*, n.º 15, 2002. Versión electrónica: www.westlaw.es (BIB 2002\2021).

en relación con esta materia es escaso y no aporta soluciones claras, lo que provoca que sean los tribunales los encargados de suplir las carencias de regulación a través de un nutrido grupo de pronunciamientos, en muchos casos, contradictorios.

4. RECAPITULACIÓN

Después de haber expuesto las cuestiones relativas a las facultades empresariales de vigilancia y control en las relaciones de trabajo, se está en disposición de indicar los resultados extraídos de este capítulo.

Primero, que el poder directivo del empresario abarca un conjunto de facultades, como es la de organización, la disciplinaria o la de control y vigilancia. Por tanto, la facultad de control y vigilancia se encuentra integrada en el poder de dirección empresarial, y se relaciona, a su vez, con otras facultades como es la disciplinaria, la cual actúa en muchos casos como una extensión de la vigilancia empresarial. No obstante, existe alguna que otra facultad, como la de «*policía empresarial*», que, contrariamente a lo que pueda parecer, queda al margen del art. 20.3 ET, puesto que no tiene como objetivo controlar al trabajador, sino defender el patrimonio empresarial.

Segundo, por lo que respecta al cuadro normativo actual del poder de control y vigilancia, el ET contiene las alusiones más básicas, sin perjuicio de la existencia de otras normas que, a pesar de no haber sido elaboradas específicamente para esta materia, resultan de aplicación, como sucede con la LOPD o la Ley 1/1982.

Tercero, que a pesar de que el art. 20.3 ET no detalla el tipo de mecanismos de control que el empresario puede desplegar, es evidente es que estos deben respetar los derechos fundamentales de los trabajadores, concretamente el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la libertad informática, articulados en la CE y en las demás leyes.

Por último, como conclusión final de este capítulo cabe señalar que el hecho de que en las últimas décadas la evolución tecnológica se haya adentrado en las relaciones laborales, ha alterado la forma de ejercer el poder de control empresarial, cuyo concepto y alcance se ha visto sustancialmente modificado. En primer lugar, se ha abierto la posibilidad al empresario de controlar el uso que los trabajadores hacen de los medios informáticos puestos a su disposición. Y, en segundo lugar, las innovaciones tecnológicas han permitido al empresario servirse de las mismas para ejercer la vigilancia y supervisión, que hasta entonces se llevaba a cabo a través de métodos más tradicionales.

Capítulo II

EL CONTROL DE LA PRESTACIÓN LABORAL A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS (1): EL CONTROL INFORMÁTICO

1. EL ORDENADOR COMO OBJETO DE CONTROL Y COMO INSTRUMENTO DE CONTROL

El uso del ordenador de empresa para fines distintos de la actividad laboral, como es el acceso a páginas web de ocio, el acceso a redes sociales, la realización de gestiones personales, el envío y recepción de mensajes personales a través del correo electrónico de empresa, e incluso la realización de actos de competencia desleal a través del correo electrónico, genera un gran número de conflictos a los que necesariamente el Derecho del Trabajo se tiene que adaptar[38].

Así las cosas, el control del uso que el trabajador hace del ordenador de empresa se despliega, principalmente, a través de dos vías. Bien, mediante el registro directo del servidor o terminal, bien mediante la monitorización del ordenador utilizando para ello programas y aplicaciones que permiten al empresario conocer la actividad del trabajador y los movimientos efectuados por este, lo cual puede desembocar, como se verá, en una fiscalización total y absoluta de la actividad laboral.

1.1. Registro del ordenador

Tradicionalmente, multitud de resoluciones judiciales consideraron que el empresario podía registrar libremente el contenido de los ordenadores de empresa, ya que se trataba de útiles empleados para el desarrollo de la prestación laboral por los trabajadores, cuya propiedad le pertenecía al empresario[39]. Por tanto, tomando como base estos pronunciamientos, nada diferenciaría al ordenador de cualquier otra herramienta o utensilio de trabajo.

En contraposición con lo anterior, existen resoluciones judiciales posteriores que asimilan el ordenador de empresa utilizado por el trabajador a los efectos particulares de este, estableciendo que, a la hora de proceder al registro del contenido del ordenador, es obligatorio respetar las garantías previstas en el art. 18 ET, concretamente, contar con la asistencia de un representante legal de los trabajadores, o, en su ausencia, con la asistencia de otro trabajador de la empresa. En este sentido, se manifestó la STSJ de País Vasco, de

[38] CALVO MORALES, D., TOSCANI GIMENEZ, D.: «El uso de internet y el correo electrónico en la empresa. Límites y garantías», *op. cit.*, n.º 165, 2014.

[39] S de la Sala de lo Social de Sevilla, del TSJ de Andalucía 1619/2003, de 9 de mayo (*Aranzadi Westlaw*, referencia AS 2003\2840).

12 de septiembre de 2006[40], declarando la nulidad, por discriminatorio, del despido del actor. La STSJ versa sobre una empresa que despidió disciplinariamente al trabajador, tras comprobar, a través de un registro en el ordenador de empresa, la existencia de una gran cantidad de archivos personales e información muy sensible de la compañía, relativa a diversos programas informáticos que se estaban desarrollando en ese momento. El TSJ declaró el despido nulo por atentar contra el derecho a la intimidad del actor, ya que el registro había sido efectuado sin respetar las garantías del art. 18 ET, previstas para el registro de efectos personales de los trabajadores.

Esta línea jurisprudencial quedó superada con la STS de 26 de septiembre de 2007, que condicionó toda la jurisprudencia posterior en relación con los registros informáticos, al establecer que «*el artículo 18 del ET 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*»[41]. Esta afirmación parte de la premisa de que los registros informáticos forman parte del poder directivo ordinario, y que por lo tanto, no es lo mismo registrar la taquilla o el bolso de un trabajador que su ordenador, ya que, aunque en ambos casos se pueden encontrar elementos personales, la finalidad del registro es diferente[42]. Así, y a pesar de que puede resultar conveniente la presencia garantista de terceros en el registro –notario, representante legal de los trabajadores, otro trabajador o incluso el propio interesado–, su ausencia en absoluto condiciona la validez del acto de control, a cuya prueba se le dará la fehaciencia que en su caso corresponda[43].

Por último, aunque no se apliquen las garantías del art. 18 ET al registro informático, el mismo no puede suponer, en ningún caso, un volcado masivo de todos los datos que el empresario descubra en el ordenador empleado por el trabajador, sino solo de aquellos que sean plenamente relevantes. Es decir, el registro no puede efectuarse sobre la totalidad del contenido, ni conllevar un estudio individual y detallado de toda la información encontrada[44].

1.2. Monitorización del uso laboral del ordenador

La monitorización del uso que un empleado hace del ordenador de empresa, se lleva a cabo, fundamentalmente, a través de distintas aplicaciones instaladas en el ordenador objeto de control, las cuales permiten conocer en tiempo real las páginas web visitadas, la duración de las visitas y el número de ocasiones en las que se ha accedido a dichas

[40] S de la Sala de lo Social del TSJ de País Vasco, de 12 de septiembre (*Aranzadi Westlaw*, referencia AS 2006\2602).
[41] FD 3.º de la S de la Sala Cuarta del TS de 26 de septiembre de 2007 (*Aranzadi Westlaw*, referencia RJ 2007\7514).
[42] FD 5.º de la S de la Sala de lo Social del TSJ de Madrid 775/2009, de 30 de octubre (*Aranzadi Westlaw*, referencia JUR 2010\27623).
[43] FD 3.º de la S de la Sala Cuarta del TS 119/2018, de 8 de febrero (*Aranzadi Westlaw*, referencia RJ 2018\666).
[44] V. la S de la Sala de lo Social del TSJ de Madrid 531/2017, de 19 de julio (*Aranzadi Westlaw*, referencia JUR 2017\249682).

páginas, sin que el usuario del ordenador tenga conocimiento de ello[45]. Además de los programas de monitorización, existen otros muchos, como es el caso de los denominados «*sniffers*»[46], que se instalan en el servidor de empresa y permiten conocer absolutamente todo lo que realiza el trabajador durante la jornada laboral.

Además, la monitorización se trata de un control interno, puesto que es el propio medio informático el encargado de registrar la información necesaria, que luego será tenida en cuenta por el empresario, a la hora de tomar, si concurren los supuestos para ello, las medidas disciplinarias oportunas[47]. Cabe señalar que, en la mayoría de los casos, estos controles son completamente indiscriminados, ya que almacenan todo tipo de información, sin filtro alguno y en tiempo real.

En algunas ocasiones se ha entendido que el acopio de datos efectuado por los programas de monitorización permite al empresario reconstruir aspectos subjetivos relativos a la intimidad del trabajador, lo cual excede, sin ningún género de duda, a la finalidad del control, que es conocer el uso que el trabajador hace del medio informático durante la jornada laboral, y si dicho uso es abusivo o no[48]. Es decir, no resulta necesario monitorizar indiscriminadamente el uso que se hace del ordenador para conocer si el trabajador dedica una parte relevante de su tiempo de trabajo a asuntos ajenos a su actividad laboral.

Existen pronunciamientos judiciales actuales que han establecido que no será válida aquella monitorización dedicada a recopilar toda la navegación en internet, así como el contenido de todos los correos electrónicos enviados y recibidos por el trabajador[49]. En este sentido, la STSJ de Madrid 591/2018, anteriormente citada, declaró improcedente el despido disciplinario de una trabajadora, tras entender que la monitorización llevada a cabo durante tres días por la empresa, mediante un sistema que visualizaba y grababa todo lo que aparecía en la pantalla del ordenador, vulneraba su derecho a la intimidad, pues la empresa había accedido incluso a correos electrónicos que la trabajadora enviaba a sus familiares.

En efecto, aunque la monitorización de los ordenadores haya supuesto un gran avance, toda vez que permite llevar a cabo un control más exhaustivo del uso que los trabajadores realizan de los medios informáticos, no se debe obviar que se trata de un sistema que, si es empleado de forma inadecuada, puede vulnerar el derecho a la intimidad de los

[45] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op. cit.*, p. 86.

[46] S de la Sala de lo Social del TJS de Madrid 452/2004, de 11 de mayo (*Aranzadi Westlaw*, referencia JUR 2004\241595).

[47] FERNÁNDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, *op. cit.*, p. 117.

[48] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, p. 184.

[49] S de la Sala de lo Social del TSJ de la Comunidad Valenciana 3390/2018, de 19 de noviembre (*Westlaw Aranzadi*, referencia AS 2019\1207).

trabajadores y, en caso de que se acceda al contenido de los correos electrónicos, el derecho al secreto de las comunicaciones.

2. EL CONTROL DEL ACCESO INDEBIDO A INTERNET Y DEL CORREO ELECTRÓNICO DE EMPRESA

2.1. Requisitos del control

Los criterios que guían el ejercicio de las facultades de control empresarial en relación con los medios informáticos han ido evolucionando durante los últimos años, propiciando numerosos e importantes cambios.

Con la aparición de estos nuevos mecanismos de control, los tribunales optaban por una posición más restrictiva, ofreciendo mayor protección a los intereses empresariales frente a los derechos fundamentales de los trabajadores, pero progresivamente se han ido estableciendo un mayor número de requisitos, cuya observancia es obligatoria. Es decir, el empresario no puede fiscalizar de forma arbitraria y caprichosa el uso de los medios informáticos dispuestos con fines productivos, sino que a la hora de ejercer el control deberá observar una serie de criterios.

Por ello, y antes de profundizar en el análisis de la doctrina judicial, resulta imprescindible introducir importantes consideraciones con respecto a este tema, sin obviar la enorme variedad de casuística que enmarca la actividad de control empresarial[50].

2.1.1. El principio de proporcionalidad

El primer requisito relevante al que debe estar sujeto el control del uso que el trabajador hace del ordenador es el principio de proporcionalidad. Como ya se ha manifestado en el capítulo anterior, se trata de un principio trascendente para determinar si los límites impuestos a los derechos fundamentales de los trabajadores, con el ejercicio del mencionado control, son legítimos o no.

De entrada, cabe recordar que el trabajador no es el sujeto activo del conflicto, sino el sujeto pasivo que sufre las consecuencias de la medida de vigilancia, por lo que estamos ante un proceso donde se opone un derecho fundamental –el derecho a la intimidad o el derecho al secreto de las comunicaciones– frente a las injerencias de la empresa sobre el trabajador[51].

---

[50] MARTÍNEZ FONS, D.: «El uso y control del correo electrónico e internet en la empresa: aspectos laborales», ROIG BATALLA, E. (Coord.), *El uso laboral y sindical del correo electrónico e internet en la empresa*, Tirant Lo Blanch, Valencia, 2007, p. 203.

[51] GOÑI SEIN, J. L.: «Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?», *Comunicación presentada al XXIX Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Pamplona, 2014, p. 59.

Tradicionalmente, el parámetro para valorar si el control vulneraba algún derecho fundamental era si el trabajador había actuado conforme a las pautas buena fe en el uso del ordenador de empresa puesto a su disposición y, en el caso de que no lo hubiera hecho, la medida de control no se consideraba ni intrusiva, ni vulneradora de derechos fundamentales. Sin embargo, el modo de interpretar la noción de buena fe, llevaba aparejado un sacrificio excesivo de los mencionados derechos[52]. Por ello, la resolución de controversias entorno a este tema se ha ido distanciando del requisito de la buena fe, optando por una ponderación equilibrada entre los derechos de los trabajadores y los intereses del empresario. Ponderación que es llevada a cabo mediante el principio de proporcionalidad, también denominado «*test de proporcionalidad*».

A tenor de este principio, los tribunales deberán valorar si el límite impuesto al derecho fundamental en cuestión, resulta oportuno a fin de preservar el correcto desempeño de la actividad laboral, la disciplina en el trabajo o la imagen empresarial, imagen que se altera, por ejemplo, si el trabajador efectúa conductas de competencia desleal aprovechándose para ello de los medios informáticos propiedad de la empresa.

Así las cosas, la legitimidad de la medida de control se valorará atendiendo a cuatro factores. En primer lugar, la justificación de la medida impuesta, por existir motivos suficientes para su adopción. En segundo lugar, la idoneidad, esto es, que la misma sea susceptible de conseguir el objetivo propuesto. En tercer lugar, la necesidad, en el sentido de que no exista otra medida menos gravosa para conseguir el mismo propósito con idéntica eficacia. Por último, la proporcionalidad en sentido estricto, que exige averiguar si la limitación del derecho fundamental es equilibrada en relación al bien empresarial que se trata de proteger, por derivarse de ella más beneficios o ventajas para el interés general, que perjuicios sobre otros bienes o valores en conflicto. Por consiguiente, solo la superación de estas cuatro condiciones otorga validez a la medida restrictiva de los derechos fundamentales del trabajador.

El principio de proporcionalidad ha sido consolidado por nuestros tribunales. Así, y como ya se ha manifestado con anterioridad, fueron las SSTC 98/2000 y 186/2000 quienes hicieron referencia, por primera vez, al mentado principio, siendo los razonamientos contenidos en ellas, corroborados con posterioridad por dicho tribunal en incontables ocasiones. Además, se trata de un principio plenamente asentado en la jurisprudencia ordinaria. Como confirmación de la aplicación por los tribunales ordinarios de este principio, se encuentra la actual STSJ de la Comunidad Valenciana 3390/2018, la cual declara «*que la prueba obtenida por la empresa demandada para justificar el despido disciplinario de la actora es ilícita, toda vez que la monitorización de la utilización de los medios informáticos puestos a disposición de la misma por la demandada, no superan los juicios de idoneidad, necesidad y proporcionalidad*»[53],

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

[53] FD 2.º de la S de la Sala de lo Social del TSJ de la Comunidad Valenciana 3390/2018, de 19 de noviembre (*Aranzadi Westlaw*, referencia AS 2019\1207).

En este caso, la mercantil demandada procedió a la instalación de un programa en el ordenador utilizado por la actora, con la finalidad de monitorizar y registrar la navegación por internet y los correos electrónicos, así como capturar todo lo encontrado en el dispositivo informático. El TSJ de la Comunidad Valenciana entiende que no concurre ninguna de condiciones exigidas por el principio de proporcionalidad, ya que, en primer lugar, la empresa no ha probado la existencia de un motivo legítimo que justifique la monitorización, con lo cual, si no existe motivo alguno que justifique el control, tampoco existirá un objetivo a conseguir. En segundo lugar, la medida de vigilancia fue adoptada por el empresario sin tener en cuenta las garantías previstas en el protocolo firmado por las partes, en el que se plasmaba que la empresa demandada se reservaba el derecho a revisar cualquier acceso a internet, así como los mensajes de correo electrónico, siempre en presencia del usuario del ordenador, del representante legal de los trabajadores, o de otro trabajador de la empresa. Por último, el tribunal entiende que la medida de vigilancia tampoco es proporcional, pues el objetivo contenido en el citado protocolo –defensa del patrimonio de la empresa y el derecho de otros trabajadores– puede alcanzarse con métodos menos intrusivos que el acceso al contenido de las comunicaciones y archivos de la trabajadora demandante.

Sin perjuicio de lo manifestado anteriormente, el principio de proporcionalidad no basta por sí solo para enjuiciar si las medidas de control adoptadas por el empresario, limitativas de derechos fundamentales, son legítimas o no. Es decir, no resulta posible que la decisión empresarial quede subordinada únicamente a la superación del «*test de proporcionalidad*», omitiendo la información previa que el empresario proporciona a los trabajadores.

Además, aunque en este epígrafe se contempla el principio de proporcionalidad en relación con el control del uso de los medios informáticos, el mismo es extensible en caso que el empresario decida controlar la actividad del trabajador a través de cámaras de videovigilancia, como se verá en el último capítulo del presente trabajo.

2.1.2. El principio de información previa

Otro requisito destacado es el principio de información previa, el cual engloba, por una parte, el establecimiento de las condiciones de uso que el trabajador puede hacer de los medios informáticos y, por otra parte, la advertencia empresarial de que dicho uso puede ser objeto de control.

Tradicionalmente, los tribunales no exigían más que la superación del principio de proporcionalidad para legitimar la medida de vigilancia empresarial. En cambio, en la actualidad, tanto el principio de información previa como el principio de proporcionalidad son aplicados de forma simultánea y conjunta en la resolución de controversias. Es decir, el hecho de que la medida de control empresarial sea justificada, idónea, necesaria y proporcionada, no es suficiente para validar el control, sino que el empresario debe fijar unas normas de uso de los ordenadores de empresa, así como advertir al trabajador de la posibilidad de efectuar controles sobre el uso de los mencionados dispositivos.

En lo tocante al establecimiento empresarial de las condiciones de uso de los medios informáticos, no existe ninguna norma en la legislación laboral que contemple dicho establecimiento, si bien, el art. 87.3 LOPD dispone que «*los empleadores deberán establecer criterios de 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 constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores*». Además, el mencionado precepto exige que los trabajadores sean informados de los criterios de uso adoptados.

Tomando como base lo anterior, y al no existir norma alguna que reconozca o prohíba el derecho del trabajador al uso personal del ordenador de empresa, tendrán que ser los contratos de trabajo, los convenios colectivos, los protocolos de empresa o las instrucciones empresariales, quienes se encarguen de establecer qué tipo de uso puede hacer el trabajador de las herramientas informáticas[54].

En cuanto a la participación de los representantes de los trabajadores en la elaboración de los criterios de uso, el art. 87.3 LOPD dispone que la misma será preceptiva, pero no aclara que ocurre si no existe acuerdo. Ahora bien, todo parece indicar que la facultad dirección y control empresarial no puede quedar mermada en caso de que no exista consenso con los representantes de los trabajadores[55].

De acuerdo con lo expuesto, conviene distinguir tres posibilidades. Primero, que el empresario prohíba todo tipo de uso personal. Segundo, que el empresario permita dicho uso, ya sea con limitaciones o sin ellas. Tercero, que el empresario no se pronuncie acerca del uso que deben hacer los empleados de los medios informáticos. Así, y en función de la opción elegida, el control desplegado con posterioridad, será considerado lícito o no.

Por lo que respecta a la prohibición de uso, la STS de 6 de octubre de 2011[56] reconoce la facultad del empresario para prohibir de forma absoluta los usos personales del ordenador de empresa. El TS señala que, si no existe derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, puesto que, al no existir una situación de tolerancia de uso personal, tampoco puede reconocerse una «*expectativa razonable de confidencialidad*».

Conviene puntualizar que, la prohibición de uso personal de los medios informáticos debe ser expresa y suficientemente clara, pues solo en ese caso el empresario podrá controlar legítimamente dicho uso. Ahora bien, ello no implica que cualquier control sea válido, sino que estará sometido a los demás requisitos adicionales y limitado por el respeto a la dignidad, contenido en el art. 10 CE.

---

[54] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, p. 174.

[55] QUÍLEZ MORENO, J. M.: «La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores», *Revista Española de Derecho del Trabajo*, n.º 217, 2019. Versión electrónica: www.westlaw.es (BIB 2019\1558).

[56] S de la Sala Cuarta del TS de 6 de octubre de 2011 (*Aranzadi Westlaw*, referencia RJ 2011\7699).

Otro ejemplo destacado lo ofrece la STSJ de Andalucía 1730/2017[57], que declaró la procedencia del despido disciplinario del trabajador, tras un uso personal abusivo y continuado del ordenador puesto a su disposición, en contra del protocolo firmado por el propio empleado, en el cual se recogía la prohibición flagrante de utilizar los medios informáticos para fines particulares, no relacionados con los cometidos laborales.

En sentido contrario, es posible que el empresario permita el uso del ordenador de empresa con fines privados, en cuyo caso el art. 87.3 LOPD exige especificar que usos están autorizados y cuáles no, así como los períodos de tiempo en que los dispositivos pueden utilizarse para fines privados. Además, es posible que el empresario permita el uso, sin establecer límite alguno, lo cual no implica que se consienta un uso privado desmesurado y descontrolado. Sin embargo, en este caso, únicamente será posible efectuar los denominados «*controles extraordinarios*», que tienen su fundamento en la protección de intereses empresariales de gran relevancia, lo que ocurre en casos de competencia desleal, de apropiación indebida de información empresarial sensible, de acoso laboral, etc.

Además, puede ser que el empresario no se pronuncie acerca del uso que deben hacer los empleados de los medios informáticos, en cuyo caso se entenderá que tolera los usos personales moderados, creando así, una «*expectativa razonable de confidencialidad*»[58]. Todo ello sin perjuicio, como ya se ha dicho, de los «*controles extraordinarios*», en caso de que sea necesario prevenir riesgos o infracciones graves. En relación con este extremo, cabe manifestar que, aunque el empresario no fije normas de utilización personal de los medios informáticos, el trabajador no debe abusar de la tolerancia empresarial, ni alejarse de los criterios que representan el buen juicio y la moderación, ni tampoco infringir los deberes de fidelidad, lealtad, probidad y confianza, implícitos en toda relación laboral[59].

Finalmente, la empresa también deberá advertir expresamente a los trabajadores de la posibilidad de control y vigilancia, así como de la existencia de medidas tendentes a garantizar la utilización laboral del medio informático. Sobre la pertinencia de este requisito se pronunció el TEDH[60], fijando la obligación de que la injerencia empresarial esté prevista a través de una norma, en la cual se contemplen los distintos supuestos en que se puede producir el control, la finalidad perseguida con el mismo y los medios utilizados para ello.

---

[57] S de la Sala de lo Social de Granada, del TSJ de Andalucía 1730/2017, de 12 de julio (*Aranzadi Westlaw*, referencia AS 2017\2114).

[58] V. la S de la Sala de lo Social del TSJ de Madrid 715/2012, de 29 de octubre (*Aranzadi Westlaw*, referencia AS 2012\380458).

[59] FD 7.º de la S de la Sala de lo Social del TSJ de Madrid 432/2003, de 13 mayo (*Aranzadi Westlaw*, referencia AS 2003\3649).

[60] S de la Sección Cuarta del TEDH caso Copland contra Reino Unido, de 3 de abril de 2007 (*Aranzadi Westlaw*, referencia TEDH 2007\23).

2.2. Límites del control: los derechos fundamentales de los trabajadores

Antes de nada, es importante tener en cuenta el ámbito de proyección del derecho a la intimidad y del derecho al secreto de las comunicaciones, puesto que son los derechos fundamentales directamente afectados cuando la empresa despliega las medidas de control sobre el uso de los medios informáticos.

Por un lado, el derecho a la intimidad se proyecta sobre el uso privado del correo electrónico de empresa, sobre los archivos personales del trabajador que se encuentran en el ordenador y sobre la información derivada de la navegación en internet, ya que, esta información puede contener datos sensibles en relación con la intimidad personal, en la medida en que pueden incluir informaciones reveladoras sobre determinados aspectos de la vida privada del trabajador, tales como ideología, orientación sexual, aficiones personales, etc.[61]. Por otro lado, el derecho constitucional al secreto de las comunicaciones, recogido en el art. 18.3 ET, únicamente afecta al correo electrónico y a los programas de mensajería instantánea instalados en el ordenador de empresa.

En la práctica, con cierta frecuencia, la vigilancia desplegada vulnera alguno de estos derechos fundamentales, por ello es necesario reparar en las consecuencias de dicha vulneración. Concretamente, en las consecuencias procesales en cuanto a la ilicitud de la prueba obtenida y en las consecuencias jurídicas de la sanción disciplinaria impuesta por el empresario tras comprobar, a través de cauces vulneradores de derechos constitucionales, un uso desviado del ordenador de empresa.

2.2.1. Derecho a la intimidad y esfera privada

El derecho a la intimidad dimana de la dignidad de la persona, y a tenor de la doctrina constitucional recogida en el primer capítulo del presente trabajo, supone la existencia de un ámbito reservado al conocimiento de los demás, necesario para mantener una calidad mínima de vida humana.

El mencionado derecho se encuentra recogido en preceptos generalistas, como es el art. 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales[62] (en adelante CEDH), que dispone que «*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*». Asimismo, el art. 18.1 CE recoge como derecho fundamental la intimidad personal, mientras que el art. 4.2 ET, dentro del amplio abanico de derechos básicos de los trabajadores, reconoce el derecho a la intimidad.

Con respecto al derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral, que es lo que ahora interesa, cabe señalar que no ha sido hasta la promulgación de la nueva LOPD cuando se ha concretado dicho derecho. Así, el art. 87.1 LOPD

[61] FD 6.º de la S de la Sala de lo Social del TSJ de País Vasco 1757/2015, de 29 de septiembre (*Aranzadi Westlaw*, referencia AS 2015\1922).
[62] *BOE* n.º 243, de 10 de octubre de 1979.

reconoce que los trabajadores tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por el empresario. Además, el art 87.2 de la citada norma dispone que el empresario podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores, únicamente a los efectos de controlar el cumplimiento de las obligaciones laborales y de garantizar la integridad de dichos dispositivos.

Con todo, el derecho a la intimidad del trabajador está sujeto a una modulación importante, que dependerá del caso concreto, así como de los criterios de uso fijados por el empresario y de las advertencias de control, siempre teniendo en cuenta la posición preeminente del derecho a la intimidad. El problema surge cuando la modulación suprime la seguridad jurídica y conduce a un aumento de decisiones contradictorias fundadas en criterios subjetivos de valoración de cada tribunal, como se tendrá la oportunidad de examinar más adelante[63].

2.2.2. Derecho al secreto de las comunicaciones como derecho autónomo respecto a otros derechos fundamentales

Especial atención merece el uso personal del correo electrónico empresarial por parte del trabajador y, particularmente, la facultad empresarial de acceder a los correos electrónicos de los trabajadores que desempeñan sus servicios en la empresa.

El art. 18.3 CE garantiza el secreto de las comunicaciones, salvo resolución judicial. Así, a través del mencionado precepto, se garantiza la confidencialidad de lo comunicado, salvo que una resolución judicial disponga lo contrario. Conviene señalar que, el derecho al secreto de las comunicaciones se trata de un derecho autónomo e independiente del derecho a la intimidad, pues es indiferente si el contenido de lo comunicado pertenece al ámbito de lo personal o lo íntimo[64].

Conforme a lo señalado por el TC en multitud de ocasiones[65], el art. 18.3 CE protege las comunicaciones, independientemente de cual haya sido el sistema empleado para realizarlas. Por tanto, como regla general, las comunicaciones llevadas a cabo por el trabajador mediante el correo electrónico de empresa o cualquier otro programa de mensajería instantánea, quedan protegidas por dicho precepto. Eso sí, ha de tenerse en cuenta que, igual que sucede con el derecho a la intimidad, el empresario puede limitar el derecho al secreto de las comunicaciones a través de la fijación de normas de uso del correo electrónico de empresa y de las advertencias de control.

---

[63] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, p. 179.

[64] MARÍN ALONSO, I.: *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, *op cit*., pp. 115-126.

[65] V., entre otras, las SSTC 70/2002, de 3 de abril *(Aranzadi Westlaw*, referencia RTC 2002\70) y 230/2007, de 5 de noviembre (*Aranzadi Westlaw*, referencia RTC 2007\230).

Así, y ante un supuesto donde la empresa procede a examinar el correo electrónico del trabajador, tras el hallazgo casual de fotocopias de transferencias efectuadas por un proveedor a su favor, el TS declara que no ha existido vulneración del derecho al secreto de las comunicaciones ni del derecho a la intimidad, toda vez que la empresa ha examinado de forma limitada y controlada los correos electrónicos relativos a las transferencias, utilizando para ello parámetros de búsqueda informática orientados a limitar la injerencia empresarial[66]. A mayor abundamiento, la empresa había prohibido expresamente el uso extralaboral de los medios informáticos y había advertido a los empleados de las posibilidades de control.

Con respecto a la necesidad de resolución judicial para intervenir las comunicaciones del correo electrónico de empresa, cabe manifestar que, en el ámbito laboral, tal injerencia es posible sin autorización judicial, toda vez que la propiedad de las herramientas que canalizan las comunicaciones intervenidas pertenece al empresario. Sin embargo, resulta cuanto menos sorprendente, el hecho de que la empresa esté facultada para limitar el derecho al secreto de las comunicaciones, protegido férreamente por la CE, mediante previsiones de uso contenidas en un convenio colectivo, o incluso, en protocolos e instrucciones empresariales[67].

De todas formas, serán los tribunales del orden social, como se verá, los encargados de equilibrar el derecho al secreto de las comunicaciones y la facultad empresarial de vigilancia y control.

2.2.3. Consideración de prueba ilícita

Puede ser que el empresario, a fin de comprobar un uso inadecuado del ordenador, despliegue una medida de control vulneradora de derechos fundamentales, y proponga en juicio dicha medida como medio de prueba para acreditar la sanción impuesta, ya sea un despido u otro tipo de sanción. En este caso, es necesario conocer cuál será la consideración procesal de la medida de control y la calificación jurídica de la sanción impuesta.

El art. 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial[68] (en adelante LOPJ), establece que no surtirán efecto las pruebas obtenidas, directa o indirectamente, vulnerando derechos fundamentales. Por su parte, el art. 90.2 de la Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social[69] (en adelante LRJS), dispone que no se admitirán pruebas que tengan su origen o se hayan obtenido, de forma directa o indirecta, a través de procedimientos que supongan violación de derechos fundamentales.

---

[66] FD 5.º de la S de la Sala Cuarta del TS 119/2018, de 8 de febrero (*Aranzadi Westlaw*, referencia RJ 2018\666).

[67] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, *op. cit.*, p. 64.

[68] *BOE* n.º 157, de 2 de julio de 1985.

[69] *BOE* n.º 245, de 11 de octubre de 2011.

Habida cuenta de lo anterior, los resultados de la medida de control empresarial vulneradora de derechos fundamentales, aunque logren probar un uso desviado del ordenador de empresa, no podrán ser tenidos en cuenta, pues tendrán la consideración de prueba ilícita, y, por consiguiente, nula. Por tanto, aunque la prueba ilícita haya servido para acreditar un hecho, este se tendrá por no probado, salvo que de otras pruebas practicadas se pueda acreditar dicho hecho –por ejemplo, a través de testigos–.

Con respecto a la calificación jurídica de la sanción empresarial impuesta, hay que partir de la base de que la ilicitud o nulidad de la medida de control no se extiende a la sanción, cuya calificación final dependerá de si se han acreditado las causas que han motivado la decisión empresarial, pero no de la forma en como se ha intentado investigar la conducta irregular del trabajador[70]. Así pues, la calificación jurídica de la sanción dependerá de lo acreditado por la prueba que finalmente se considere lícita, y se ajustará a lo dispuesto en los arts. 55 ET y 108 LRJS.

En este sentido se ha pronunciado la STSJ de Madrid 591/2018, señalando que «*no procede la calificación de despido nulo, 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, cuestión distinta de la sucedida en este supuesto en 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*»[71].

En definitiva, el hecho de que una medida de control empresarial sea considerada nula a efectos probatorios, no implica automáticamente la nulidad de la sanción impuesta, sino que la misma puede ser calificada como improcedente –si no se logran probar los hechos constitutivos de la sanción–, o como procedente –si los hechos constitutivos de la sanción son acreditados mediante otras pruebas válidas–.

3. EL CONTROL INFORMÁTICO EN LA DOCTRINA JUDICIAL

Teniendo en cuenta las consideraciones vertidas con anterioridad, se pasará a analizar la evolución de la doctrina judicial sobre el control de las herramientas informáticas y de comunicación de la empresa, tomando como referencia las SSTEDH de 12 de enero de

[70] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, p. 146.

[71] FD 2.º de la S de la Sala de lo Social del TSJ de Madrid 591/2018, de 13 de septiembre (*Aranzadi Westlaw*, referencia AS 2019\923).

2016, caso Barbulescu contra Rumanía[72] (en adelante *Barbulescu I*) y de 5 de septiembre de 2017, caso Barbulescu contra Rumanía[73] (en adelante *Barbulescu II*).

A continuación, se expondrán las resoluciones anteriores al caso Barbulescu más destacadas, para después examinar las dos sentencias dictadas por el TEDH y la influencia de las mismas en el sistema español.

3.1. Doctrina del Tribunal Supremo y del Tribunal Constitucional anterior al caso «*Barbulescu contra Rumanía*»

De entrada, debe recordarse que previamente al año 2007 no existía un criterio homogéneo sobre este tema, sino que los tribunales de suplicación emitían pronunciamientos contradictorios y vacilantes. Así, mientras que algunos tribunales entendían que el control empresarial era en todo caso legítimo, al ser el ordenador una herramienta productiva cuya titularidad correspondía al empresario[74], otros consideraban que no podía existir en ningún caso una prohibición absoluta de uso personal del ordenador de empresa –concretamente del correo electrónico–, ya que el art. 18.3 CE reconoce de forma indirecta el derecho fundamental de los trabajadores a comunicarse libremente en el ámbito laboral[75].

A partir del año 2007, el TS unificó doctrina mediante tres pronunciamientos de 26 de septiembre de 2007 (caso *Etiquetas de Galicia*), de 8 de marzo de 2011[76] (caso *Font Salem*) y de 6 de octubre de 2011 (caso *Annaligia*), que han supuesto un punto de inflexión y han condicionado toda la doctrina de suplicación posterior. El principio general que rige en las tres sentencias es que el ordenador es una herramienta propiedad del empresario, y este, como propietario, puede reglamentar su utilización, prohibiendo los usos personales y procediendo a la supervisión y vigilancia[77].

El TS mantiene que, si existe tolerancia empresarial, existirá una «*expectativa razonable de confidencialidad*» y, por consiguiente, primará el derecho fundamental a la

---

[72] S de la Sección Cuarta del TEDH caso Barbulescu contra Rumanía, de 12 de enero de 2016 (*Aranzadi Westlaw*, referencia TEDH 2016\1).

[73] S de la Gran Sala del TEDH caso Barbulescu contra Rumanía, de 5 de septiembre de 2017 (*Aranzadi Westlaw*, referencia TEDH 2017\61).

[74] V., entre otras, la S de la Sala de lo Social del TSJ de Galicia, de 4 de octubre de 2001 (*Aranzadi Westlaw*, referencia AS 2001\3366) y la S de la Sala de lo Social de Sevilla, del TSJ de Andalucía 1619/2003, de 9 de mayo (*Aranzadi Westlaw*, referencia AS 2003\2840).

[75] En este sentido, la S de la Sala de lo Social del TSJ de País Vasco de 6 de noviembre de 2007 (*Aranzadi Westlaw*, referencia AS 2008\1556), estableció que la decisión sobre si el trabajador puede proyectar su autonomía y libertad sobre un elemento propiedad de la empresa depende de un debate constitucional, y no puede ser resuelto con la prohibición de uso personal, ni con una advertencia empresarial de control.

[76] S de la Sala Cuarta del TS de 8 de marzo de 2011 (*Aranzadi Westlaw*, referencia RJ 2011\932).

[77] DESDENTADO BONETE, A., DESDENTADO DAROCA, E.: «La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador», *Revista de Información Laboral*, n.º 1, 2018. Versión electrónica: www.westlaw.es (BIB 2018\6059).

intimidad y al secreto de las comunicaciones. Ahora bien, si no existe tolerancia empresarial, tras haber prohibido el empresario el uso privado del ordenador de empresa, tampoco existirá expectativa de confidencialidad alguna y tanto el derecho a la intimidad, como el derecho al secreto de las comunicaciones, tendrán una protección mucho menor. Con lo cual, atendiendo a la doctrina del TS, basta con una prohibición de uso personal, junto con la superación del principio de proporcionalidad, para que el control empresarial sea legítimo y válido.

A la doctrina mantenida por el referido tribunal, se suma la comprendida en la STS de 13 de septiembre de 2016[78] (caso *Radio Televisión de Galicia*). Esta STS resuelve un recurso de casación para la unificación de doctrina y asienta nuevamente las bases sobre las que se sustentará la línea jurisprudencial seguida en multitud de sentencias posteriores.

En este caso, mediante demanda de conflicto colectivo, se pretende dejar sin efecto una resolución empresarial que fija la normativa de uso de los sistemas informáticos. A través de esta resolución, la empresa impone a los trabajadores un uso estrictamente laboral del equipo informático, prohibiendo destinar el mismo a un uso privado. Además, en la resolución, la mercantil hace constar que se reserva el derecho a monitorizar y a comprobar cualquier sesión de acceso a internet, así como revisar los mensajes de correo electrónico de los usuarios de la red corporativa, siempre respetando la regulación vigente en cada momento. El TS comienza señalando que «*no cabe duda de que es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial por parte del trabajador, así como la facultad empresarial de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales*». El TS prosigue señalando que, si existe un régimen previo de limitación –con prohibición de uso extralaboral y advertencia de control– la facultad de vigilancia puede ser ejercida legítimamente. La STS concluye que, en este caso, la resolución impugnada cumple el juicio de proporcionalidad, ya que con ella se satisface el legítimo objetivo propuesto –exclusión del uso privado de los instrumentos informáticos–, no existe otra medida más benévola de control, y la ponderación de los intereses en juego es equilibrada.

El TC también se ha manifestado al respecto, consolidando la doctrina unificada del TS y estableciendo notables precisiones en el ámbito del derecho al secreto de las comunicaciones.

La STC 241/2012[79] (caso *Global Sales*), versa sobre una trabajadora, la ahora recurrente, que en connivencia con otra de sus compañeras, instaló un programa de mensajería instantánea –*Trillian*– en el ordenador de empresa, el cual era de uso común y no contaba con clave de acceso. Además, la empresa había prohibido expresamente la instalación de programas informáticos distintos a los existentes en el sistema.

Las conversaciones mantenidas por las trabajadoras fueron descubiertas casualmente por otro de sus compañeros, el cual lo puso en conocimiento de la empresa, que tras la

[78] S de la Sala Cuarta del TS 723/2016, de 13 de septiembre (*Aranzadi Westlaw*, referencia RJ 2016\4843).
[79] STC 241/2012, de 17 de diciembre (*Westlaw Aranzadi*, referencia RTC 2012\241).

lectura de los mensajes que contenía el programa de mensajería procedió a amonestar a las trabajadoras. En las conversaciones intervenidas por la empresa, las trabajadoras criticaban duramente a sus compañeros, superiores y clientes.

Por un lado, la recurrente en amparo alega que la empresa ha vulnerado el derecho a la intimidad, ya que no hay duda del carácter íntimo de las conversaciones afectadas, tratándose de opiniones sobre compañeros de trabajo o clientes que lógicamente sus autoras deseaban mantener en un ámbito propio y reservado. Por otro lado, alega la vulneración del derecho al secreto de las comunicaciones, ya que el programa informático instalado se trata de un programa que permite la comunicación entre dos o más personas, quedando archivadas en una carpeta del ordenador las comunicaciones efectuadas, las cuales deben estar protegidas por el mandato constitucional del art. 18.3 CE. Destaca la recurrente que el hecho de que el ordenador no tuviese clave de acceso, no implica que no se haya vulnerado el secreto de las comunicaciones, ya que «*la posibilidad de acceso no convierte al mismo el legítimo*».

La STC considera que no ha existido vulneración del derecho a la intimidad, ya que fue la propia recurrente quien eliminó la barrera de la confidencialidad, al mantener las conversaciones a través de un ordenador de uso común y sin clave de acceso. Del mismo modo, y con respecto al secreto de las comunicaciones, el TC manifiesta que, en primer lugar, las comunicaciones mantenidas por las trabajadoras quedan al margen de la protección dispensada por el art. 18.3 CE, «*por tratarse de formas de envío que se configuran legalmente como comunicación abierta, esto es, no secreta*». En segundo lugar, la injerencia en las comunicaciones se produce tras un hallazgo casual por un compañero de las trabajadoras. Y, en tercer lugar y último lugar, el TC entiende que la actuación de control empresarial supera el juicio de proporcionalidad.

El voto particular formulado en la STC objeto de análisis pone nuevamente de manifiesto la existencia de criterios contradictorios a la hora de resolver las controversias. El magistrado disidente, Don Fernando Valdés Dal-Ré, entiende que, con independencia del establecimiento de criterios de uso, el empresario no está autorizado a la apertura deliberada de archivos de correo electrónico o de mensajería de los trabajadores, siempre que puedan ser identificados como tales –como ocurre en este caso–, siendo totalmente indiferente que para acceder a los archivos no existan claves de acceso o que el ordenador sea de uso común. A mayor abundamiento, el magistrado considera que el acceso fue excesivo y dilatado en el tiempo, ya que la empresa procedió a la lectura completa y al resumen de las conversaciones mantenidas por las trabajadoras, lo cual desvela una clara intención lesiva.

En un asunto similar, la STC 170/2013[80] (caso *Alcaliber*), enjuicia un supuesto en el que la empresa intercepta los correos electrónicos de un trabajador, enviados desde la dirección electrónica proporcionada por la empresa y cuyo contenido permitió confirmar las sospechas previas de que el empleado transmitía información confidencial a terceros. Ante esta situación, la mercantil procede al despido disciplinario del trabajador por

[80] STC 170/2013, de 7 de octubre (*Aranzadi Westlaw*, referencia RTC 2013\170).

transgresión de la buena fe contractual. Además, el convenio colectivo de aplicación en la empresa tipificaba como falta leve el uso de los medios informáticos para fines distintos de los relacionados con la prestación laboral.

En el caso *Alcaliber* el recurrente alega la vulneración del derecho a la intimidad y al secreto de las comunicaciones. Asimismo, considera que el hecho de que el convenio colectivo prevea como infracción leve el uso privado de los medios informáticos es, a todas luces, insuficiente para controlar el contenido de los correos electrónicos.

Lo destacable de este pronunciamiento es que el TC considera que el contenido del convenio colectivo obliga a ambas partes, por lo que el hecho de tipificar como infracción el uso extralaboral de los medios informáticos debe entenderse como una prohibición suficiente, la cual habilita a la empresa a efectuar futuros controles. Además, la STC entiende que, en este caso, no ha existido una interceptación de comunicaciones ajenas realizadas en canal cerrado, y descarta por ello la lesión del derecho al secreto de las comunicaciones. Igualmente, señala que el derecho a la intimidad ha quedado debidamente protegido, ya que el acceso al contenido de los correos electrónicos no ha resultado excesivo o desproporcionado, máxime si se tiene en cuenta que el régimen jurídico aplicable en la empresa hacía previsible que el empresario ejerciera la facultad de vigilancia sobre los correos electrónicos del trabajador, sin necesidad de advertir previamente de ello.

En definitiva, los pronunciamientos del TS y del TC anteriores a *Barbulescu I* y *Barbulescu II* confirman que la prohibición de uso personal, aunque no vaya acompañada de una advertencia de control, es suficiente para eliminar la «*expectativa razonable de confidencialidad*». No obstante, llama la atención el hecho de que los tribunales, en ninguno de sus pronunciamientos clave, hayan fijado como requisito obligatorio la advertencia de la posibilidad de fiscalización, tendente a evitar controles sorpresivos y vulneradores del principio de buena fe contractual inherente a toda relación laboral[81].

3.2. Debate en el Tribunal Europeo de Derechos Humanos. Cambio de criterio en el caso «*Barbulescu contra Rumanía*»

3.2.1. Los hechos enjuiciados

Barbulescu I y *Barbulescu II* tratan sobre un trabajador –ingeniero rumano– que fue despedido tras ser sorprendido utilizando el programa de mensajería instantánea –*Yahoo! Messenger*– para fines personales. El programa había sido instalado por petición de la compañía para la comunicación exclusiva con los clientes, y en la empresa existía un reglamento que prohibía expresamente cualquier uso privado de los terminales

[81] DEL PINO PADRÓN, M. C.: «El impacto de las tecnologías de la información en el Derecho laboral, especial referencia a la intimidad del trabajador y el secreto de sus comunicaciones», *Cadernos de Dereito Actual*, n.º 8, 2018, p. 161.

informáticos. No obstante, el reglamento interno, no incluía mención alguna sobre la posibilidad de que la compañía vigilase las comunicaciones efectuadas por los empleados.

Previamente a efectuar el control, la empresa remitió un comunicado a todos sus empleados, en el que indicaba que la compañía se veía en la obligación de verificar, controlar y, en su caso, sancionar el uso de internet, los teléfonos y las fotocopiadoras. Tan solo dos días después de emitir el comunicado, la empresa procedió a registrar, durante siete días y en tiempo real, las comunicaciones del trabajador en el programa de mensajería instantánea. Además, no consta acreditado que el trabajador conociese el contenido de la comunicación con anterioridad a que la empresa desplegase la vigilancia.

La compañía tuvo una primera reunión con el trabajador, y tras ser cuestionado por el uso del ordenador con fines personales en horario laboral, este negó haber utilizado los recursos de la empresa para fines distintos de los profesionales. En una segunda reunión, horas después de haber tenido lugar la primera, la empresa le mostró al trabajador cuarenta y cinco folios de transcripciones de conversaciones entre este y su familia, la mayoría de contenido íntimo, las cuales habían sido llevadas a cabo a través de la cuenta corporativa del trabajador en *Yahoo! Messenger*.

Tras ser despedido disciplinariamente, el trabajador interpuso la correspondiente demanda, pero los tribunales rumanos, en todas sus instancias, desestimaron su pretensión, siendo la decisión judicial interna la que constituye objeto de valoración por el TEDH.

3.2.2. El razonamiento del Tribunal Europeo de Derechos Humanos en *Barbulescu I*

Partiendo de los hechos reseñados anteriormente, el trabajador acude ante el TEDH y plantea una queja vinculada a que la decisión empresarial de extinguir la relación laboral se apoyó en una vulneración de su derecho a la intimidad y a la correspondencia, y que los tribunales nacionales rumanos no protegieron este derecho contenido en el art. 8 CEDH, el cual dispone, como ya se ha visto, que «*toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*».

En *Barbulescu I*, la Sección Cuarta del TEDH, comienza señalando que la empresa accedió a la cuenta profesional de *Yahoo! Messenger* tras mantener la primera reunión con el trabajador, y bajo la creencia de que contenía mensajes de carácter profesional, ya que trabajador había afirmado en dicha reunión que únicamente había usado la cuenta con fines profesionales (párr. 57). El TEDH entiende que los tribunales nacionales únicamente se apoyaron en las transcripciones en la medida en que estas demuestran la infracción disciplinaria cometida por el demandante (párr. 58), y que, si bien es cierto que se examinaron las comunicaciones de la cuenta de *Yahoo! Messenger*, en ningún momento se accedió a ninguna otra información guardada en su ordenador (párr. 60). Concluye el tribunal, manifestando que «*no hay elemento alguno en el presente asunto que indique que las autoridades nacionales incumplieran su obligación de establecer un*

equilibrio adecuado, dentro de su margen de apreciación, entre los intereses del empleador y el derecho del demandante al respeto de su vida privada en virtud del art. 8».

A pesar de que el TEDH no aprecia la vulneración de los derechos protegidos en el art. 8 CEDH, sí pone de manifiesto la necesidad de garantizar una protección a la intimidad personal y de regular de forma exhaustiva esta cuestión, concretamente con respecto a las comunicaciones electrónicas privadas en el ámbito laboral[82].

Llama poderosamente la atención que el pronunciamiento objeto de análisis no haga alusión a los medios empleados por la mercantil para examinar las comunicaciones y únicamente se limite a señalar que las mismas fueron intervenidas en tiempo real. Tampoco recoge si la transcripción de las comunicaciones era necesaria por algún motivo, o si la duración de la injerencia empresarial –nada menos que siete días– fue excesiva o no. Además, el TEDH en ningún momento contempla si el hecho de que exista un reglamento interno prohibiendo el uso personal basta para descartar la «*expectativa razonable de confidencialidad*», o si es necesaria, a mayores, una advertencia previa de control.

En este sentido, se pronuncia el contundente voto particular, formulado por el magistrado Don Paulo Pinto de Albuquerque, el cual difiere de la decisión mayoritaria y parte de la base de que para que el control empresarial pueda ser considerado legítimo, es obligatoria la previa comunicación a los trabajadores de la política que rige en la empresa. Es decir, la empresa deberá comunicar los criterios de uso, el propósito de control, la extensión del mismo, los medios técnicos utilizados para llevarlo a cabo y el horario en el que se va a producir. Además, el magistrado discordante señala que la advertencia de control debe ser de carácter individualizado, y que el trabajador deberá dar su consentimiento expreso para que la empresa pueda acceder a sus comunicaciones, puesto que de lo contrario únicamente podrán ser intervenidas mediante autorización judicial.

En cualquier caso, y a pesar de la existencia de criterios discordantes en el seno del TEDH, la fundamentación y el fallo de *Barbulescu I* se encuentra en clara convergencia con la doctrina del TC en los casos *Global Sales* y *Alcaliber*[83].

3.2.3. El razonamiento del Tribunal Europeo de Derechos Humanos en *Barbulescu II*

El trabajador, al amparo del art. 43 CEDH, solicitó la remisión del asunto ante la Gran Sala del TEDH. La solicitud fue aceptada, al entender que el caso planteaba una cuestión

[82] MARTÍNEZ LÓPEZ-SAEZ, M.: «Nuevos perfiles del derecho al olvido en Europa y España», en AA. VV, *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, Dykinson, Madrid, 2017, p. 249.

[83] GARCÍA RUBIO, M. A, PÉREZ DE LOS COBOS ORIHUEL, F.: «El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos», *Nueva Revista Española de Derecho del Trabajo*, n.º 196, 2017, pp. 41-54.

grave relativa a la interpretación o a la aplicación del CEDH, y la Gran Sala se pronunció a través de *Barbulescu II*, que cambia radicalmente el criterio sostenido en *Barbulescu I*.

Barbulescu II parte de la idea de que el establecimiento de criterios de uso de los terminales informáticos no puede anular el ejercicio de la privacidad social en el puesto de trabajo, sino que el derecho a la intimidad y al secreto de las comunicaciones sigue siendo necesario, sin perjuicio, eso sí, de que dichos derechos puedan ser acotados (párr. 80). Además, el TEDH manifiesta que las comunicaciones que el trabajador realizó en su lugar de trabajo están comprendidas en los conceptos de «*vida privada*» y «*correspondencia*», por lo que, el art. 8 CEDH es plenamente aplicable a este asunto (párr. 81).

Partiendo de las anteriores premisas, la Gran Sala del TEDH impone seis condiciones que deben cumplir los controles empresariales –en particular los controles sobre el uso del correo electrónico u otro programa de mensajería– para ser considerados legítimos por los tribunales (párr. 120).

En primer lugar, es obligatorio comunicar al trabajador la posibilidad de control, así como el tipo de medidas de control que se van a desplegar. El TEDH señala que la comunicación debe ser clara y anterior a la puesta en marcha de la actividad de vigilancia.

En segundo lugar, se debe tener en cuenta el alcance de la supervisión y el grado de intrusión en la vida privada del trabajador. Es trascendente para determinar el alcance del control, conocer si la vigilancia de las comunicaciones se ha efectuado sobre el flujo de las mismas o si, por el contrario, se ha accedido a su contenido. Asimismo, se deberá valorar si la supervisión se ha realizado sobre la totalidad de las comunicaciones o únicamente sobre una parte de ellas. Del mismo modo, es necesario averiguar si la intervención empresarial ha sido limitada o extensa en el tiempo, así como el número de personas que han accedido a los resultados de la misma.

En tercer lugar, y dado que la vigilancia del contenido de las comunicaciones es un método absolutamente invasivo, se requerirá una explicación fundamentada de los motivos que llevan a efectuar dicha vigilancia.

En cuarto lugar, se ha de valorar si es factible alcanzar el objetivo empresarial con medidas menos intrusivas que el acceso al contenido de las comunicaciones. Por ejemplo, supervisando los datos externos de la comunicación, tales como destinatario, asunto, etc.

En quinto lugar, se deben valorar tanto las consecuencias de la medida de control, como el uso que el empresario hace de los resultados obtenidos con el control, y más concretamente, si el uso realizado de los datos obtenidos es abusivo o no.

En sexto y último lugar, habrá que tener en cuenta si las garantías ofrecidas al trabajador son suficientes, es decir, si la empresa que accedió al contenido de las comunicaciones notificó previamente al empleado de tal circunstancia.

Como es evidente, los tribunales nacionales deberán tener en cuenta la superación de estas seis condiciones, también denominado «*test Barbulescu*», a la hora de determinar si

un control empresarial afecta al derecho a la intimidad y al secreto de las comunicaciones. Aplicando lo anteriormente dispuesto a este asunto, la Gran Sala del TEDH declara que los tribunales rumanos no protegieron adecuadamente los derechos contenidos en el art. 8 CEDH.

Así las cosas, el TEDH sostiene que en ningún momento los órganos jurisdiccionales rumanos determinaron si el trabajador había sido notificado, de forma clara y previa, sobre la posibilidad de control y sobre la naturaleza del mismo. En cuanto al alcance de la supervisión, la Gran Sala considera que esta cuestión tampoco fue examinada por los tribunales rumanos, a pesar de que el empleador registró en tiempo real las comunicaciones y transcribió su contenido. Además, los órganos internos no comprobaron si existían motivos suficientes para acceder a las comunicaciones, ni tampoco verificaron si el objetivo empresarial podía haberse alcanzado con métodos menos invasivos. Finalmente, el tribunal señala que los órganos nacionales no constataron la gravedad de las consecuencias de la medida de control y del procedimiento disciplinario seguido, máxime cuando el trabajador fue sometido a la medida disciplinaria más grave.

Habida cuenta de todo lo anterior, es evidente que *Barbulescu II* revoca el criterio sostenido en *Barbulescu I* y afecta de lleno a la doctrina mantenida por el TS y por el TC, la cual deberá ser profundamente revisada[84] .

Son claras las diferencias entre ambos pronunciamientos, puesto que mientras que *Barbulescu I* únicamente exige la prohibición de uso personal para destruir la «*expectativa razonable de confidencialidad*», *Barbulescu II* entiende que habrá vulneración del derecho a la intimidad y al secreto de las comunicaciones si el trabajador no ha sido previamente informado de la posibilidad de control, incluso aunque existan normas en la empresa que prohíban la utilización de los medios informáticos con fines personales. A mayor abundamiento, *Barbulescu II* fija una serie de estándares mínimos que deberán ser observados por los órganos jurisdiccionales internos en la resolución de controversias.

En definitiva, el cambio de criterio del TEDH ha supuesto un punto de inflexión, no se sabe si definitivo, en las relaciones laborales y, concretamente, en el modo en que el empresario ejerce la vigilancia de las comunicaciones que sus empleados realizan a través del ordenador de empresa.

3.3. Consecuencias de la nueva doctrina del Tribunal Europeo de Derechos Humanos en el sistema español

Es indudable que *Barbulescu II* va a suponer un giro importante de la doctrina constitucional y jurisprudencial. Ahora bien, las consecuencias de este cambio pueden ser

[84] PRECIADO DOMÈNECH, C. H.: «Comentario de urgencia a la STEDH de 5 de septiembre 2017. Caso Barbulescu contra Rumanía (Gran Sala). Recuperando la dignidad en el trabajo», *Revista de Información Laboral*, n.º 10, 2017. Versión electrónica: www.westlaw.es (BIB 2017\13278).

incluso problemáticas, aumentando el arbitrio judicial y generando, si cabe, más interrogantes. En este sentido, la nueva doctrina del TEDH, establece que la empresa tiene que advertir previamente al trabajador del control que se va a efectuar, pero no aclara que tipo de información debe facilitar, ni si esta información debe ser individualizada, ni tampoco a través de qué medios se debe proporcionar la misma. Por tanto, tendrán que ser nuevamente los tribunales los que vayan matizando y delimitando estas cuestiones, con el riesgo de emitir resoluciones judiciales discordantes.

En cuanto a la vinculación de los tribunales españoles a la doctrina del TEDH, cabe señalar que el TC ha puesto de manifiesto en numerosas ocasiones que «*si bien el derecho de la Unión Europea no integra el canon de constitucionalidad [...] tanto los tratados y acuerdos internacionales como el Derecho comunitario derivado pueden constituir valiosos criterios hermenéuticos del sentido y alcance de los derechos y libertades que la Constitución reconoce, valor que se atribuye con fundamento en el art. 10.2 CE […] interpretación que no puede prescindir de la que, a su vez, llevan a cabo los órganos de garantía establecidos por esos mismos tratados y acuerdos internacionales*»[85]. Así las cosas, y a pesar de no ser un tema pacífico, el TC ha admitido la vinculación jurídica de las autoridades nacionales de los Estados parte del CEDH a la interpretación que del mismo realiza el TEDH[86].

Por tanto, parece claro que a partir de *Barbulescu II*, ya no podrá considerarse que la mera prohibición empresarial –ya sea a través de un convenio colectivo o de un reglamento interno– es adecuada para eliminar la expectativa de intimidad del trabajador, sino que, será necesario que el trabajador en cuestión tenga un conocimiento previo y claro del control que va a llevar a cabo el empresario, máxime cuando este va a acceder al contenido de las comunicaciones efectuadas por el trabajador.

En cualquier caso, ya existen pronunciamientos judiciales posteriores a *Barbulescu II* que se han hecho eco de esta nueva doctrina. Es destacable la STS de 8 de febrero de 2018, mencionada anteriormente, y que trata sobre una empresa que, ante un hallazgo casual de fotocopias de transferencias bancarias efectuadas por un proveedor a favor de un empleado, decide examinar, mediante una prueba pericial, la cuenta profesional del correo electrónico del trabajador. El TS entiende que, en este caso, la conducta empresarial supera sobradamente el filtro de los seis requisitos que el TEDH exige para atribuir legitimidad a la actividad de control empresarial[87].

De igual modo, algún tribunal de suplicación ha declarado la improcedencia del despido disciplinario, tras entender que la medida de control aplicada por el empresario contravenía la doctrina establecida en *Barbulescu II*, al no haber transmitido al trabajador

[85] V., por ejemplo, el FD 5.º de la STC 61/2013, de 14 de marzo (*Aranzadi Westlaw*, referencia RTC 2013\61) y el FD 5.º de la STC 13/2017, de 30 de enero (*Aranzadi Westlaw*, referencia RTC 2017\13).

[86] FOSSAS ESPALADER, E.: «Cosa interpretada en derechos fundamentales: jurisprudencia del TEDH y jurisprudencia constitucional», *Revista Vasca de Administración Pública*, n.º 82, 2, 2008, pp. 165-180.

[87] FD 6.º de la S de la Sala Cuarta del TS 119/2018, de 8 de febrero (*Aranzadi Westlaw*, referencia RJ 2018\666).

una información clara en cuanto a la naturaleza y alcance de la supervisión[88]. Por añadidura, el «*test Barbulescu*» también se ha tenido en cuenta por los tribunales del orden social a la hora de valorar si una aplicación informática instalada en los teléfonos móviles de los empleados vulneraba el derecho a la intimidad de los mismos[89].

4. RECAPITULACIÓN

Una vez analizadas las cuestiones relativas al control empresarial desplegado sobre el uso de dispositivos informáticos y su evolución en la doctrina judicial, se pueden exponer los resultados de este capítulo.

En primer término, los requisitos que debe cumplir todo control para ser considerado válido han sido objeto de matización por los tribunales, estando sujetos a una casuística muy amplia, pues mientras que tradicionalmente algunos órganos judiciales exigían únicamente la superación del juicio de proporcionalidad, otros requerían, a mayores, la existencia de información empresarial previa.

En segundo término, lo que es diáfano es que la vigilancia sobre el uso de dispositivos digitales debe respetar, por un lado, el derecho a la intimidad del trabajador, el cual ha sido concretado recientemente a través del art. 87 LOPD y, por otro lado, el derecho al secreto de las comunicaciones, protegido en el art. 18.3 CE.

En tercer término, la medida de control empresarial que no respete los mencionados derechos constitucionales tendrá la consideración de prueba ilícita, en caso de que el empresario se intente valer de la misma en juicio para acreditar un incumplimiento laboral.

En cuarto y último término, la situación de desprotección causada tradicionalmente al trabajador ha ido mejorando paulatinamente, y parece que los tribunales están más cerca de lograr el equilibrio entre el interés empresarial de garantizar el buen funcionamiento de la empresa y los derechos fundamentales de los trabajadores. Concretamente, *Barbulescu II* ha supuesto un punto de inflexión en esta materia, cambiando el criterio mantenido hasta entonces por el TEDH y cuestionando la doctrina asentada por el TS y el TC.

[88] FD 2.º de la S de Sala de lo Social del TSJ de la Comunidad Valenciana 3390/2018, de 19 de noviembre (*Aranzadi Westlaw*, referencia AS 2019\1207).

[89] S de la Sala de lo Social de Santa Cruz de Tenerife, del TSJ de Islas Canarias 1002/2018, de 16 de octubre (*Aranzadi Westlaw*, referencia AS 2019\1522).

Capítulo III

EL CONTROL DE LA PRESTACIÓN LABORAL A TRAVÉS DE LAS NUEVAS TECNOLOGÍAS (2): LA VIDEOVIGILANCIA EMPRESARIAL

1. CONTROL MEDIANTE LA CAPTACIÓN O GRABACIÓN DE LA IMAGEN DURANTE LA PRESTACIÓN LABORAL

El establecimiento de dispositivos de captación o grabación de la imagen a fin de controlar el desarrollo de la prestación laboral, genera las mismas incógnitas que se suscitaban en el capítulo anterior. La primera cuestión que se plantea es si el empresario puede utilizar cámaras de videovigilancia para controlar a los empleados y, en caso afirmativo, surgen la dudas sobre el modo en que se debe llevar a cabo el control y las limitaciones al mismo.

Hay que comenzar señalando que, aunque la videovigilancia empresarial modernice las facultades de control, existe un límite infranqueable, que es la finalidad estrictamente laboral del control efectuado, evitando con ello la vulneración de los derechos fundamentales de los trabajadores[90]. En este sentido, cabe destacar la STSJ de Asturias 1482/2004[91], en la cual queda probado que el gerente de la empresa, bajo la tolerancia y pasividad de la mercantil, procedió a instalar dos cámaras ocultas en las mesas de las empleadas, y una tercera cámara en el interior del marco del aseo utilizado por estas. Como es lógico, el tribunal de suplicación entiende que, la actitud de permisividad de la empresa atenta frontalmente contra el derecho a la intimidad y a la dignidad de las trabajadoras afectadas por las grabaciones, por lo que condena a la mercantil a una indemnización por vulneración de derechos fundamentales, a fin de resarcir el daño moral causado.

Además, llama la atención, que los derechos de los trabajadores que pueden quedar afectados por las medidas de videovigilancia son más numerosos que los vistos en el capítulo anterior, pues, además de la dignidad y de la intimidad, han de tenerse en consideración otros derechos como es el derecho a la propia imagen, contenido en el art. 18.1 CE, y aquellos derechos derivados de la normativa de protección de datos personales[92].

---

[90] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, p. 20.

[91] S de la Sala de lo Social del TSJ de Asturias 1482/2004, de 30 de abril (*Aranzadi Westlaw*, referencia AS 2004\2112).

[92] FERNÁNDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, *op. cit.*, pp. 72-75.

En cuanto a los requisitos exigidos para considerar legítimo este tipo de control, se debe reparar, por un lado, en el principio de proporcionalidad, y, por otro lado, en el deber de información previa.

En lo tocante al principio de proporcionalidad, y como se ha tenido la oportunidad de examinar, este requisito es inherente a toda medida de control, independientemente de su naturaleza. Así pues, para que la medida videovigilancia sea considerada válida tendrá que ser, como mínimo, justificada, idónea, necesaria y proporcionada.

Por lo que respecta al deber de información previa, el art. 89.1 LOPD ha establecido, con respecto al uso de medidas de videovigilancia, que «*los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida*». Si bien este precepto fue incluido en la nueva LOPD, en aras de adecuar el RGPD y clarificar la situación, lo cierto es que ha generado una mayor controversia y arbitrio judicial, pues mientras que algunos órganos judiciales entienden que el deber de información se satisface mediante la colocación de un distintivo informativo en un lugar suficientemente visible –como exige el art. 3 de la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos (en adelante AEPD), sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras[93] (en adelante Instrucción 1/2006)–, otras resoluciones judiciales han puesto de manifiesto que es necesario proporcionar información previa, concreta y precisa, que incluya la finalidad buscada con el sistema de videovigilancia implantado –incluida la finalidad sancionadora para el caso de que se capten incumplimientos laborales–, sin que sea posible atenuar el deber informativo con la mera colocación de un distintivo.

A mayor abundamiento, el segundo apartado del art. 89.1 LOPD dispone que en el caso de que el empresario haya captado la comisión flagrante de un acto ilícito por los trabajadores, se entenderá cumplido el deber de informar cuando existiese, al menos, el mencionado cartel informativo. No obstante, este precepto no aclara que se debe entender por acto ilícito, lo que ha obligado nuevamente a los tribunales a interpretar dicho concepto, como se tendrá la oportunidad de ver.

Lo que está meridianamente claro es que no se admitirá, en ningún caso, la instalación de sistemas de videovigilancia «*en lugares destinados al descanso o esparcimiento de los trabajadores o empleados públicos, tales como vestuarios, aseos, comedores y análogos*»[94]. Así lo ha recogido el art. 89.2 LOPD y también el TC en la STC 98/2000 antedicha, al manifestar que «*ciertamente la instalación de tales medios en lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos resulta, a fortiori, lesiva en todo caso del derecho a la intimidad de los trabajadores, sin más*

[93] *BOE* n.º 296, de 12 de diciembre de 2006.

[94] En relación con este tema, es interesante la S de la Sala de lo Social de Sevilla, del TSJ de Andalucía 899/2017, de 22 de marzo (*Aranzadi Westlaw*, referencia AS 2017\1052), que considera válida la colocación de cámaras en un cuarto de baño utilizado por los auxiliares para bañar a los pacientes discapacitados, ante la sospecha de malos tratos a estos y entendiendo que primaba el derecho de los pacientes, gravemente discapacitados, física y mentalmente.

consideraciones, por razones obvias»[95]. Además, los tribunales de suplicación han sido contundentes al declarar que las cámaras instaladas en este tipo de lugares determinan, la intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE[96].

Con todo, a pesar de que el art. 89 LOPD ha intentado imponer el deber informativo, lo cierto es que la materia está sujeta a una amplia casuística, como ocurría con el control desplegado sobre el uso de los medios informáticos puestos a disposición del trabajador.

2. CONTROL MEDIANTE LA ESCUCHA O GRABACIÓN DE SONIDOS DURANTE LA PRESTACIÓN LABORAL

Brevemente señalar que, con respecto a la utilización de sistemas de escucha o grabación de sonidos en el centro de trabajo, no existe ninguna norma específica en la legislación laboral que habilite o prohíba al empresario la implantación de dichos sistemas. Nuevamente, es el art. 89 LOPD, en su tercer apartado, el que dispone que los sistemas de grabación de sonido se admitirán únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas, derivados de la actividad desarrollada en el centro de trabajo.

Además, será necesario cumplir los mismos requisitos exigidos para el caso de la instalación de videocámaras, es decir, la superación del principio de proporcionalidad y el deber de información previa.

Respecto a la supresión de los sonidos grabados, el art. 22.3 LOPD señala que deberán ser eliminados 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.

A diferencia de lo que ocurre con los sistemas de videovigilancia, los sistemas de grabación de sonidos requieren la existencia de riesgos relevantes derivados de la actividad laboral para justificar su instalación. Ello es así porque la grabación de sonidos y, particularmente, de conversaciones, es mucho más sensible para la intimidad que la grabación de una imagen, puesto que, la conversación puede desvelar pensamientos y sentimientos internos que la imagen no proporciona, o lo hace muy limitadamente[97].

Un ejemplo reciente es la STSJ de Castilla y León, de 11 de abril de 2018[98], donde la empresa instala cámaras de videovigilancia sin informar previamente sobre ello al trabajador afectado y, a mayores, procede a grabar las conversaciones mantenidas por el

[95] FD 6.º de la STC 98/2000, de 10 de abril (*Aranzadi Westlaw*, referencia RTC 2000\98).

[96] V., por ejemplo, la S de la Sala de lo Social de las Palmas, del TSJ de Islas Canarias 628/2001, de 25 de julio (*Aranzadi Westlaw*, referencia AS 2001\4603) o la S de la Sala de lo Social del TSJ de Cantabria 583/2002, de 29 de abril (*Aranzadi Westlaw*, referencia JUR 2002\157929).

[97] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, p. 28.

[98] S de la Sala de lo Social de Valladolid, del TSJ de Castilla y León, de 11 de abril de 2018 (*Aranzadi Westlaw*, referencia AS 2018\1211).

empleado. El TSJ manifiesta que, en este caso, no solo se ha procedido a grabar la imagen, sino también el sonido y, por consiguiente, las conversaciones mantenidas por el trabajador con los clientes, lo cual agrava la situación, máxime cuando la instalación de aparatos de captación y grabación del sonido no era necesaria para la seguridad de las instalaciones, bienes o personas. En definitiva, el TSJ declara que la actuación empresarial rebasa las facultades que al empresario le otorga el art. 20.3 ET y supone una intromisión ilegítima en el derecho a la intimidad.

3. LÍMITES A LA VIDEOVIGILANCIA EMPRESARIAL

La instalación de cámaras de videovigilancia en el centro de trabajo, permite la captación, transmisión, almacenamiento y reproducción de las imágenes obtenidas, por lo que, los derechos potencialmente afectados serán aquellos que derivan del art. 18 CE.

Por tanto, una vez reconocida la posibilidad de instalar cámaras de vigilancia a efectos de controlar el desarrollo de la prestación laboral por los empleados, se debe proceder a examinar los límites a la videovigilancia empresarial, reparando específicamente en el derecho fundamental a la intimidad y a la protección de datos de carácter personal, y realizando una breve referencia al derecho fundamental a la propia imagen.

3.1. Derecho a la intimidad y a la protección de datos

En cuanto al derecho a la intimidad en el ámbito de la videovigilancia, y como ocurría en el uso de dispositivos digitales, el mismo se incorporó a la legislación laboral a través del art. 20 bis ET que lleva por rúbrica «*derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión*» y que reconoce «*el derecho a la intimidad frente al uso de dispositivos de videovigilancia, en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales*». Así las cosas, ha sido el actual art. 20 bis ET el encargado de armonizar la normativa de la LOPD en la legislación laboral.

Sorprende que, tanto el ET como la LOPD, reconozcan el derecho a la intimidad, pero no lo regulen detalladamente, lo cual genera, como es lógico, un incremento de controversias en las relaciones laborales. De la lectura del art. 89 LOPD parece que es suficiente con la superación del principio de proporcionalidad y con el cumplimiento del deber informativo para considerar que la videovigilancia efectuada no vulnera el derecho a la intimidad del trabajador, pero esto no es así necesariamente, sino que habrá que atender a las distintas circunstancias y eventualidades del caso en cuestión.

A pesar de encontrarse protegidos por el mismo precepto constitucional, el contenido del derecho a la intimidad personal y del derecho a la protección de datos es completamente distinto. Así lo ha puesto de manifiesto el TC al establecer que «*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 de intromisiones de terceros en contra de su voluntad […] en cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno […] el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos […] pero ese poder de disposición sobre los propios datos personales de nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin»[99].

De esta forma, e igual que ocurría con el derecho al secreto de las comunicaciones, el derecho a la protección de datos no se reduce a datos íntimos o privados, sino a cualquier tipo de información de carácter personal cuyo conocimiento o tratamiento por un tercero –el empresario– pueda afectar a otros derechos del trabajador, sean o no fundamentales[100].

Si el trabajador controlado mediante videocámaras invoca la vulneración del derecho a la protección de datos de carácter personal, el conflicto adquiere otra dimensión, precisamente por la exigencia de que se cumpla obligatoriamente con el deber informativo impuesto en el art. 89 LOPD, a fin de lograr una protección eficaz del derecho de autodeterminación informativa, inherente al derecho a la libertad informática del art. 18.4 CE[101]. El citado precepto de la LOPD no exige que el trabajador otorgue su consentimiento a ser grabado, pero ello no exime a la empresa del deber de informarlo, dado que, como ya se ha expuesto, este deber es un complemento imprescindible del derecho a la libertad informática[102].

En definitiva, el trabajador que va a ser controlado mediante sistemas de videovigilancia, deberá conocer de forma previa, expresa e inequívoca, la intención empresarial de controlar su actividad laboral a través de cámaras de videovigilancia, así como, la existencia de un fichero de datos de carácter personal. Es decir, el empleado debe ser informado de quien dispone de sus datos personales y del propósito de su tratamiento. Con todo, si el empresario cumple estas exigencias, junto con el principio de proporcionalidad, será menos probable que el derecho a la protección de datos personales se vea conculcado.

---

[99] FD 6.º de la STC 292/2000, de 30 de noviembre (*Aranzadi Westlaw*, referencia RTC 2000\292).

[100] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores, op. cit.*, p. 149.

[101] FERNÁNDEZ ORRICO, F. J.: «Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre», *op. cit.*, n.º 222, 2019.

[102] En este sentido, el FD 3.º de la S de la Sala Social de Málaga, del TSJ de Andalucía 670/2017, de 5 de abril (*Aranzadi Westlaw*, referencia JUR 2017\163007) establece que, en el ámbito laboral, el consentimiento del trabajador pasa, como regla general, a un segundo plano, ya que se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el cumplimiento del contrato firmado por las partes.

3.2. Derecho a la propia imagen

El derecho a la propia imagen se encuentra recogido en el art. 18.1 CE, y se trata de un derecho íntimamente vinculado a la dignidad personal, como sucede con el derecho a la intimidad. El TC ha matizado este derecho, señalando que su ámbito de protección comprende, entre otras facultades, la de poder impedir la obtención, reproducción o publicación de la propia imagen por parte un tercero no autorizado, independientemente de la finalidad perseguida por quien la capta o difunde[103].

A mayor abundamiento, el art. 7.5 de la Ley 1/1982 establece que tendrá consideración de intromisión ilegítima la captación de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos.

Habida cuenta de lo anterior, todo parece indicar que el hecho de grabar a un trabajador en el centro de trabajo, a fin de controlar el desempeño de su actividad laboral, supone un quebranto del derecho a la propia imagen. Sin embargo, el art. 2.2 de la Ley 1/1982 dispone que «*no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por ley o cuando el titular del derecho hubiese otorgado a tal efecto su consentimiento expreso*». Así las cosas, y dada la peculiaridad de la relación laboral, la norma que permite al empresario grabar la imagen del empleado en el centro de trabajo es el art. 20.3 ET. Conforme a este precepto, el empresario podrá captar la imagen de trabajador en el lugar y en tiempo de trabajo mediante sistemas de videovigilancia, siempre y cuando respete los requisitos antedichos.

Concluyendo, el derecho a la propia imagen en el ámbito laboral queda desplazado a un segundo plano desde el momento en que el trabajador se somete, en virtud de un contrato de trabajo, al poder de control y vigilancia empresarial del art. 20.3 ET[104].

4. LA VIDEOVIGILANCIA EMPRESARIAL EN LA DOCTRINA JUDICIAL

Si en el control empresarial del uso de los medios informáticos, la doctrina judicial –ahora afectada por *Barbulescu II*– se muestra vacilante, algo semejante sucede cuando el control se despliega mediante sistemas de videovigilancia. La austera regulación legal sobre esta materia no ha permitido, hasta el momento, obtener respuestas claras y concretas, sino que, por el contrario, ha generado la adopción de criterios contradictorios en el seno del TC y del TEDH, los cuales serán tratados a continuación.

Primero, se estudiarán los pronunciamientos previos a las SSTC 29/2013[105] y 39/2016[106], para posteriormente pasar a analizar la doctrina constitucional emanada de estas dos resoluciones que han marcado un hito importante en el ámbito de la

[103] FD 4.º de la STC 23/2010, de 27 de abril (*Aranzadi Westlaw*, referencia RTC 2010\23).

[104] DESDENTADO BONETE, A., MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, *op. cit.*, p. 61.

[105] STC 29/2013, de 11 de febrero (*Aranzadi Westlaw*, referencia RTC 2013\29).

[106] STC 39/2016, de 3 de marzo (*Aranzadi Westlaw*, referencia RTC 2016\39).

videovigilancia laboral. Por último, se examinarán las recientes SSTEDH de 9 de enero de 2018, caso López Ribalda y otros contra España[107] (en adelante *López Ribalda I*) y de 17 de octubre de 2019, caso López Ribalda y otros contra España[108] (en adelante *López Ribalda II*), pues, como sucede en el caso Barbulescu, un mismo tribunal, ante los mismos hechos, dicta fallos opuestos, generando un alto nivel de imprevisibilidad e inseguridad jurídica.

4.1. La doctrina constitucional previa a las SSTC 29/2013 y 39/2016. Solución mediante la ponderación

En las SSTC 98/2000 y 186/2000, ya citadas, se contempla exclusivamente el derecho a la intimidad y a la propia imagen, pero en ningún momento se hace referencia al derecho a la protección de datos, ni a la autodeterminación informativa dimanante del art. 18.4 CE, como sí lo hicieron, de forma acertada, las sentencias dictadas ulteriormente por el TC[109].

Por un lado, la STC 98/2000, que versa sobre la instalación de micrófonos en el centro de trabajo, establece una serie de pautas que los tribunales deben seguir a la hora de valorar la legitimidad de la medida de control. Especialmente, el TC hace referencia al principio de proporcionalidad, y entiende que la superación del mismo es suficiente para declarar la validez de los dispositivos de control instalados. Siguiendo este razonamiento, la STC determina que en el supuesto de autos la instalación de micrófonos no se ajusta a las exigencias indispensables del derecho a la intimidad y tampoco cumple el principio de proporcionalidad, ya que la empresa procedió a grabar de manera indiscriminada las conversaciones de los trabajadores[110].

Por otro lado, la STC 186/2000 recoge un supuesto donde la empresa –un supermercado– despide disciplinariamente a uno de sus trabajadores, después de comprobar, mediante la instalación de cámaras de videovigilancia orientadas a las cajas registradoras, que este sustraía dinero de la caja. La mercantil instaló las cámaras tras advertir irregularidades y desajustes en la contabilidad, y sin informar al trabajador de ello. El TC considera que, en este caso, la medida de control supera el principio de proporcionalidad y afirma que no existe necesidad alguna de informar, ni a los

[107] S de la Sección Tercera del TEDH caso López Ribalda y otros contra España, de 9 de enero de 2018 (*Aranzadi Westlaw*, referencia TEDH 2018\1).

[108] S de la Gran Sala del TEDH caso López Ribalda y otros contra España, de 17 de octubre de 2019 (*Aranzadi Westlaw*, referencia TEDH 2019\144).

[109] GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales», *Comunicación presentada al XIX Congreso de ASNALA,* Málaga, 2018, p. 4.

[110] FD 9.º de la STC 98/2000, de 10 de abril (*Aranzadi Westlaw*, referencia RTC 2000\98).

trabajadores afectados, ni al Comité de Empresa, sobre la instalación de cámaras de videovigilancia[111].

En suma, ambas resoluciones exigen ponderar si la instalación de cámaras ha respetado el derecho a la intimidad personal de los trabajadores, de conformidad con el «*test de proporcionalidad*». Cabe destacar que este ha sido el único criterio tenido en cuenta durante mucho tiempo por los tribunales del orden social, los cuales seguían la estela de las mencionadas resoluciones constitucionales.

4.2. El deber informativo en la doctrina de las SSTC 29/2013 y 39/2016. Cambio de criterio en el Tribunal Constitucional

Hasta las SSTC 29/2013 y 39/2016, el TC únicamente tenía en cuenta el derecho a la intimidad y a la propia imagen, sin embargo, en estos dos pronunciamientos introduce el derecho a la protección de datos de carácter personal en el ámbito de la videovigilancia empresarial.

Previamente, señalar que en el momento temporal en el que se dictaron ambas resoluciones, no se encontraba en vigor la actual LOPD, que exige al empresario proporcionar al trabajador afectado por la instalación de videocámaras información previa, expresa, clara y concisa, sino que la única norma en el ordenamiento jurídico que hacía vagamente referencia al deber de información era el art. 5 de la antigua Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[112] (en adelante Ley 15/1999). Este precepto, era un precepto generalista que no estaba destinado específicamente a la videovigilancia en el ámbito laboral, a diferencia del vigente art. 89 LOPD.

La doctrina constitucional examinada en el epígrafe anterior fue modificada de forma drástica a través de la STC 29/2013 que establece como condición adicional al principio de proporcionalidad el cumplimiento del deber informativo previo a los trabajadores. Así, esta resolución reconoce la dimensión laboral del derecho a la libertad informática consagrado en el art. 18.4 CE y, a mayores, delimita el contenido esencial del mencionado derecho[113].

Los hechos enjuiciados en la STC 29/2013 versan sobre un trabajador de la Universidad de Sevilla –con categoría profesional de «*director de servicio habilitado*»– que es sancionado con suspensión de empleo y sueldo por incumplir su horario laboral. La Universidad, recurre a las cámaras de videovigilancia instaladas en los accesos a las dependencias, para constatar las sospechas previas y así poder justificar futuras sanciones. El Comité de Empresa era conocedor de la instalación de sistemas de grabación y existían

[111] FD 7.º de la STC 186/2000, de 10 de julio (*Aranzadi Westlaw*, referencia 2000\186).

[112] *BOE* n.º 298, de 14 de diciembre de 1999.

[113] GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016», *Revista Aranzadi Doctrinal*, n.º 5, 2016. Versión electrónica: www.westlaw.es (BIB 2016\21165).

carteles anunciadores de las cámaras de seguridad. No obstante, los trabajadores de la Universidad de Sevilla no habían sido informados previamente de que los datos personales recabados de las grabaciones podían ser utilizados con fines sancionadores.

El TC, tras pronunciarse sobre el concepto de «*dato de carácter personal*», manifiesta que el derecho a la protección de datos se encuentra íntimamente vinculado a la videovigilancia en el ámbito laboral[114]. Además, alude a la ya citada STC 292/2000, que fue una de las pioneras en establecer el derecho a la libertad informática, para aclarar que es en ella donde se encuentra la solución al recurso de amparo presentado por el trabajador y no en otros precedentes del TC, como es la doctrina emanada de las SSTC 98/2000 y 186/2000[115].

Para la STC objeto de análisis es necesario, siempre y en todo caso, que el empresario proporcione una información previa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral. Además, el TC considera que la información debe concretar las características y el alcance del tratamiento de datos, es decir, en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando la posibilidad de que las grabaciones se utilicen para la imposición de sanciones disciplinarias. El TC es manifiestamente claro al afirmar que no basta para entender cumplido el deber informativo con la existencia de distintivos anunciando la instalación de cámaras en el recinto universitario.

En definitiva, la STC 29/2013 estima el recurso de amparo planteado por el trabajador de la Universidad de Sevilla y declara la lesión del art. 18.4 CE, al entender que la empresa llevó a cabo la videovigilancia a través de medios encubiertos, negando al trabajador la información exigible.

La doctrina establecida por el TC en el año 2013, lejos de consolidarse definitivamente ha sido modificada de forma inesperada por el Pleno del TC a través de la STC 39/2016, la cual considera, en pos de los intereses empresariales, que el deber informativo se cumple cuando el empresario coloca los distintivos informativos a los que se refiere la Instrucción 1/2006 de la AEPD, sin que resulte necesario especificar a los trabajadores afectados por la medida, la finalidad exacta asignada al control.

Este cambio de doctrina ha sido duramente criticado en la propia STC 39/2016 por el magistrado Don Fernando Valdés Dal-Ré, autor de uno de los votos particulares emitidos. El magistrado hace hincapié en la insólita forma con la que la resolución se separa de la jurisprudencia ya elaborada por el TC sobre el derecho a la protección de datos de carácter personal en supuestos de videovigilancia laboral. Además, censura el hecho de que el TC no haya detallado los motivos que permitan entender el porqué del abandono a una jurisprudencia cuyo objetivo, primero y esencial, fue el fijar los límites del contenido del derecho fundamental que el art. 18.4 CE confiere a los trabajadores. A mayor abundamiento, el magistrado disidente, entiende que la doctrina ahora defendida por el TC «*se sitúa en esa senda [...] de retroceso en la protección de los derechos*

[114] FD 5.º de la STC 29/2013, de 11 de febrero (*Aranzadi Westlaw*, referencia RTC 2013\29).
[115] FD 6.º de la STC 29/2013, de 11 de febrero (*Aranzadi Westlaw*, referencia RTC 2013\29).

fundamentales de las personas que prestan un trabajo asalariado [...] una senda que tiende a vaciar de contenido sustantivo un modelo constitucional de relaciones laborales acorde con el Estado social y democrático de Derecho».

Los hechos enjuiciados en este caso, coinciden sustancialmente con los de la STC 29/2013. La empresa procedió a despedir a la trabajadora, después de comprobar a través de una cámara de videovigilancia que esta se apropiaba de efectivo de la caja, en diferentes fechas y de forma habitual. La cámara fue instalada a raíz de las irregularidades percibidas en la caja donde prestaba sus servicios la trabajadora y en ningún momento previo a la instalación se le comunicó a la empleada afectada que iba a ser grabada, si bien el distintivo informativo se colocó en un lugar visible del escaparate del local.

En relación con el derecho a la protección de datos de carácter personal, el TC comienza reconociendo que el deber de información previa al trabajador forma parte del contenido esencial del derecho a la protección de datos. En este caso, el tribunal entiende cumplido dicho deber, pues la empresa colocó el correspondiente distintivo en el escaparate del establecimiento, con lo cual, la trabajadora podía conocer sobradamente la existencia de las cámaras y la finalidad para la que habían sido instaladas.

En lo tocante al derecho a la intimidad personal, la STC se remite al principio de proporcionalidad y manifiesta que la videovigilancia llevada a cabo por la mercantil es justificada –pues existían sospechas previas–, idónea, necesaria y equilibrada.

Otro de votos particulares a la STC 39/2016 es el formulado por el magistrado Don Juan Antonio Xiol Ríos, que considera inaceptable que la información dirigida al público a través de un cartel informativo sea suficiente para cumplir el requisito de información previa. El magistrado expone que la opinión mayoritaria «*dinamita el contenido esencial del derecho fundamental a la protección de datos*», pues la misma conduce a admitir que el empresario, ante cualquier sospecha –fundada o infundada– está autorizado para instalar libremente –siempre que en el centro de trabajo haya un aviso al público– cámaras, a fin de controlar la actividad laboral de sus trabajadores.

En línea con lo anterior, el TS, haciéndose eco de la STC 39/2016, también ha refrendado la utilización por la empresa de cámaras de videovigilancia al conocer el trabajador su mera existencia, aun cuando no hubiese sido informado expresamente sobre el uso y destino de las grabaciones obtenidas[116].

4.3. Debate en el Tribunal Europeo de Derechos Humanos. Caso «*López Ribalda y otros contra España*»

No es posible analizar la evolución de la videovigilancia empresarial en la doctrina judicial, sin reparar en los últimos pronunciamientos del TEDH en *López Ribalda I* y *López Ribalda II*. La interpretación llevada a cabo en ambos pronunciamientos sobre el

[116] V. las SSTS 630/2016, de 7 de julio (*Aranzadi Westlaw*, referencia RJ 2016\4434) y 96/2017, de 2 de febrero (*Aranzadi Westlaw*, referencia RJ 2017\1628).

derecho a la intimidad y a la protección de datos, se ha vuelto imprescindible a efectos de ejercer el poder de dirección en un justo equilibrio con los derechos fundamentales de los trabajadores.

En *López Ribalda I* se impone el carácter absoluto del deber informativo, lo que supone una llamada de atención a los tribunales españoles, pues obliga a los mismos a regresar al origen de su doctrina más garantista para con los trabajadores, que es la contenida en la STC 29/2013[117].

El asunto trata, *grosso modo*, sobre la videovigilancia encubierta a varios trabajadores de una cadena española de supermercados, a fin de confirmar las sospechas de hurto, pues la empresa había reparado tiempo atrás en los importantes desajustes existentes entre las ventas diarias y el inventario del supermercado. En el establecimiento se instalaron cámaras visibles –orientadas a la entrada y salida– y cámaras ocultas, enfocando a las cajas. Además, se colocó una señal advirtiendo de la existencia de las cámaras visibles, pero nada se dijo acerca de las cámaras ocultas, ni a los trabajadores, ni a los delegados de personal. En las grabaciones se observa como algunos trabajadores –entre ellos las demandantes– se apropian de productos del supermercado sin pagar. Como consecuencia de lo anterior, la empresa procedió a despedir disciplinariamente a los trabajadores implicados en los hurtos, por incumplimiento grave de las obligaciones de buena fe y lealtad exigidas en toda relación laboral.

Así las cosas, cinco de las trabajadoras despedidas interponen la correspondiente demanda ante la jurisdicción social, pero el TSJ de Cataluña admite como prueba las grabaciones y confirma la decisión de despido, al entender que la falta de información a los trabajadores y a los delegados de personal se debe al temor empresarial de que el conocimiento, por los trabajadores, del sistema de filmación frustre la finalidad del control. No obstante, el TEDH no comparte el criterio de los tribunales españoles y declara la vulneración del art. 8 CEDH, al determinar que la videovigilancia efectuada por la compañía fue desarrollada durante un período excesivamente prolongado –diez días– y no cumplió con las exigencias derivadas del art. 5 de la Ley 15/1999, en particular, con la obligación de informar previa, explícita e inequívocamente a los afectados por el sistema de captación de datos personales[118].

El TEDH resuelve que informar acerca del alcance de la medida implica proporcionar información de la finalidad del sistema instalado, incluida la sancionadora para el caso de que se capten incumplimientos laborales. Con lo cual, quedan absolutamente prohibidas las grabaciones secretas, que es sinónimo de no informadas, pues las sospechas de conductas desviadas en el puesto de trabajo no legitiman la excepción del deber informativo.

[117] GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales», *op cit.*, p. 26 y 27.
[118] COSTA HERNANDIS, R.: «Protección de datos en el ámbito laboral», RALLO LOMBARTE, A. (Dir.), *Tratado de Protección de Datos,* Tirant Lo Blanch, Valencia, 2019, pp. 655-671.

Según lo anteriormente manifestado, parece claro que la doctrina contenida en *Barbulescu II* y la contenida en *López Ribalda I*, plantean un nuevo enfoque, mucho más estricto, del poder del control del empresario en materia de uso de correo electrónico y dispositivos de videovigilancia, respectivamente[119]. Sin embargo, esto queda en entredicho con la reciente aparición de *López Ribalda II*, pronunciamiento que trae causa de *López Ribalda I* y que surge, tras la remisión a la Gran Sala del TEDH del asunto objeto de debate.

Es menester señalar que, si bien *López Ribalda II* data de fecha 17 de octubre de 2019, en la época de los hechos enjuiciados la legislación interna a aplicar era otra, pues, en la actualidad, la regulación legal –aunque escasa– es más garantista. Sin perjuicio de lo anterior, el RGPD, en vigor en el momento de la resolución, es diáfano en sus arts. 12 a 15 con respecto al deber informativo, con lo cual, la decisión del TEDH, aunque no contemple la legislación nacional actual en materia de protección de datos, sí debe ajustarse a la normativa comunitaria.

La actual STEDH estima, en primer lugar, que los órganos jurisdiccionales internos constataron que la instalación de cámaras estaba justificada, debido a las pérdidas significativas –aproximadamente 25.000 euros– que venía sufriendo la tienda en la que prestaban sus servicios las demandantes (párr. 123). En segundo lugar, considera que los tribunales españoles comprobaron que la medida de control estaba limitada, en cuanto a los espacios y al personal vigilado, pues las cámaras enfocaban exclusivamente la zona de cajas, que eran los únicos lugares donde se podían cometer los hurtos (párr. 124). En tercer lugar, el TEDH destaca que las funciones de caja se cumplían en un lugar abierto al público, lo que indudablemente influye en la expectativa de privacidad que razonablemente puede tener todo empleado (párr. 125). En cuarto lugar y último lugar, el tribunal entiende que la videovigilancia no fue excesiva, sobre todo, si se compara con asuntos donde las grabaciones se extendieron durante meses. Por todo ello, la STEDH resuelve que los órganos judiciales españoles verificaron debidamente el cumplimiento de los criterios de proporcionalidad establecidos por el TC (párr. 132).

En cuanto al requisito informativo, el TEDH reconoce la obligación empresarial de informar, con claridad y carácter previo, a los trabajadores implicados en la videovigilancia. El tribunal admite que, si bien es cierto que los órganos jurisdiccionales internos no tuvieron en cuenta la falta de información previa, no son menos ciertas las particulares circunstancias que motivaron la instalación de cámaras ocultas. Estas circunstancias se ciñen a la existencia de sospechas razonables de que se estaban cometiendo graves irregularidades, dado el alcance de los hurtos constatados. Para el TEDH se trata de una justificación seria y fundada, máxime cuando no era un solo empleado quien hurtaba, sino que los hurtos se efectuaban mediante una acción conjunta de varios trabajadores. Por ello, entiende que el deber de información previa consagrado

[119] PRECIADO DOMÈNECH, C. H.: «Comentario de urgencia a la STEDH de 9 de enero. Caso López Ribalda y otras c. España», *Revista de Información Laboral*, n.º 1, 2018. Versión electrónica: www.westlaw.es (BIB 2018\6060).

en la LOPD y en el RGPD queda dispensado, debido a la gravedad de las conductas cometidas por los empleados.

En suma, la STEDH declara que los órganos internos cumplieron sus obligaciones en virtud del art. 8 CEDH, por lo que no ha existido lesión alguna del citado precepto.

Nuevamente, resulta inaudito el giro doctrinal acaecido en el TEDH, ya que los criterios fijados en *López Ribalda I*, tendentes a proteger los derechos fundamentales de los trabajadores, ahora son omitidos, fortaleciendo con ello las facultades de control y vigilancia empresarial.

4.4. Consecuencias de la nueva doctrina contenida en la STEDH «*López Ribalda y otros contra España*», de 17 de octubre de 2019

La doctrina contenida en *López Ribalda II* supone un importante retroceso y provoca la aparición de nuevos problemas, que parecían superados después de *López Ribalda I*[120]. Así, y después de todos los cambios sufridos en la doctrina judicial, parece que la materia de la videovigilancia laboral se encuentra de nuevo en el punto de partida.

Como ya se ha anunciado, en el momento de los hechos enjuiciados, la legislación a aplicar era otra, puesto que en el ordenamiento jurídico español todavía no existía ningún precepto que regulase propiamente la videovigilancia en el lugar de trabajo. En el año 2018 entra en vigor la actual LOPD, que a través de su art. 89 intenta dilucidar la situación, imponiendo al empresario la obligación de informar de forma expresa, clara y concisa a los trabajadores sobre la instalación de cámaras tendentes a controlar su actividad laboral. No obstante, habrá que esperar un tiempo prudencial para observar si la LOPD clarifica la situación o si, por el contrario, se continúan emitiendo un sinfín de resoluciones judiciales en sentidos opuestos.

Por el momento, lo único seguro es que el sistema de videovigilancia deberá cumplir el principio de proporcionalidad y el deber de información previa. Ahora bien, el tema conflictivo está en determinar si el deber de proporcionar información expresa, clara y concisa se entiende cumplido al colocar un cartel informativo o es necesario llevar a cabo una información individualizada a los trabajadores afectados.

A mayor abundamiento, el art. 89.1 LOPD contempla una excepción en su segundo apartado, al disponer que, si se capta la comisión flagrante de un acto ilícito por los trabajadores, se entenderá cumplido el deber de informar con la mera colocación de un cartel de «*zona videovigilada*». Esto suscita nuevamente una serie de incógnitas.

[120] De hecho, algunos pronunciamientos judiciales comenzaban a reproducir los criterios fijados en *López Ribalda I*. Por ejemplo, la S de la Sala de lo Social del TSJ de Madrid 388/2019, de 24 de abril (*Aranzadi Westlaw*, referencia 2019\2359), que declara válida la utilización por la empresa de cámaras de videovigilancia, al ser informados los trabajadores su existencia y finalidad disciplinaria. En idéntico sentido, la S de la Sala de lo Social de Burgos, del TSJ de Castilla y León 319/2019, de 15 de mayo (*Aranzadi Westlaw*, referencia 2019\1751).

Primero, todo parece indicar que más que una excepción, este precepto contiene una regla general. Es decir, si el trabajador que está siendo grabado de forma secreta, comete un acto ilícito, puede ser despedido disciplinariamente y la empresa no habrá vulnerado su derecho a la protección de datos, siempre y cuando figure el distintivo informativo en un lugar visible. Por tanto, se trata de una previsión inútil, pues en todo caso tendrá valor probatorio la grabación, aunque se omitan las exigencias informativas del apartado primero del art. 89.1 LOPD[121].

Segundo, surgen dudas en relación con el concepto de «*acto ilícito*». En este sentido, por acto ilícito sólo cabe entender lo que la propia expresión indica, es decir, cualquier acto contrario al ordenamiento jurídico, lo que incluye delitos, infracciones administrativas e incumplimiento de las obligaciones laborales[122]. Sin embargo, el TEDH no plasma en sus pronunciamientos el concepto de «*acto ilícito*», sino que se refiere a actos o comportamientos delictivos, lo cual genera una nueva problemática.

Tercero, se pone de manifiesto el desajuste existente entre la legislación nacional y la legislación comunitaria, concretamente, entre la LOPD y el RGPD. Es decir, se suscita la duda de si una ley nacional puede contemplar excepciones que la ley comunitaria de la que trae causa, esto es, el RGPD, no contempla.

Es conveniente señalar que la norma española no puede rebajar la exigencia del deber informativo, con lo cual, si no es por aplicación directa de la doctrina del TEDH los tribunales españoles deberán aplicar las exigencias informativas del RGPD. En otras palabras, la norma española únicamente puede complementar la norma comunitaria en aquello que esta permite, y sin contradecir la regulación esencial del propio RGPD, el cual se aplica de forma directa y con eficaz primacía frente a las normas nacionales[123]. En definitiva, si la LOPD rebaja la exigencia del deber informativo –regulando excepciones para el caso de la comisión flagrante de actos ilícitos– el juez español deberá inaplicar la norma española contradictoria como consecuencia de la primacía del RGPD.

5. RECAPITULACIÓN

Tras haber estudiado las cuestiones relativas a la videovigilancia empresarial y su evolución en la doctrina judicial, se pueden puntualizar las siguientes conclusiones.

En primer lugar, la videovigilancia es un sistema muy utilizado en la práctica por las empresas para controlar la actividad laboral de los trabajadores y para poder probar en juicio los eventuales incumplimientos laborales. Si bien la captación o grabación de imágenes está permitida, siempre y cuando se cumplan una serie de requisitos, no puede

[121] FERNÁNDEZ ORRICO, F. J.: «Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre», *op. cit.*, n.º 222, 2019.

[122] FD 2.º de la S del Juzgado de lo Social (en adelante JS) n.º 3 de Pamplona 52/2019, de 18 de febrero (*Aranzadi Westlaw*, referencia AS 2019\1014).

[123] FD 2.º de la SJS n.º 3 de Pamplona 52/2019, de 18 de febrero (*Aranzadi Westlaw*, referencia AS 2019\1014).

afirmarse lo mismo de la escucha o grabación de conversaciones, y esto es así porque las conversaciones mantenidas entre los trabajadores en su puesto de trabajo revelan aspectos mucho más íntimos y privados que las meras imágenes.

En segundo lugar, uno de los derechos fundamentales implicados en la videovigilancia, además del derecho a la intimidad y a la propia imagen, es el derecho a la protección de datos de carácter personal. La regulación de este derecho, en su dimensión laboral, se ha llevado a cabo recientemente a través de la LOPD, que trata de adecuar las exigencias del RGPD.

En tercer y último lugar, la doctrina del TC ha ido cambiando trascendentalmente durante estos últimos años, pasando de valorar únicamente el principio de proporcionalidad a fijar el deber informativo previo e individualizado al trabajador. Por su parte, el TEDH también ha cambiado de orientación recientemente, dando respuesta, no se sabe si definitiva, a una de las cuestiones más controvertidas en materia de videovigilancia de los últimos años. Así, la Gran Sala valida los controles encubiertos a los trabajadores, pero nunca ante la más mínima sospecha de hurto o de cualquier otro incumplimiento, sino solo cuando existan sospechas razonables y fundadas de que los trabajadores están cometiendo conductas susceptibles de generar un grave perjuicio empresarial.

CONCLUSIONES GENERALES

Después de haber examinado el poder de control empresarial ejercido a través de las nuevas tecnologías, el contenido del trabajo puede ser recopilado mediante algunas conclusiones de cierre, que pretenden poner de relevancia los aspectos clave aquí expuestos, sin olvidar que se trata de una materia donde existen multitud de preguntas y escasas respuestas.

Si bien en el presente trabajo se ha analizado el control del uso del ordenador de empresa y el control mediante videocámaras –al ser estos los controles más frecuentes en la práctica empresarial– no se puede obviar la existencia de otras formas de vigilancia, tales como el GPS o los controles biométricos. Además, el futuro en esta materia no parece en absoluto alentador, y un ejemplo de ello es la noticia publicada recientemente en la prensa, en la que se recoge que *Biohax*, una compañía sueca de microchips, se encuentra en conversaciones con varias firmas británicas para la implantación de microchips a sus empleados, a fin de mejorar la seguridad en las empresas e incrementar, hasta el extremo más absoluto, el poder y control sobre los trabajadores[124].

Como primera conclusión, el control del uso que el trabajador hace del ordenador de empresa está plenamente influenciado por la doctrina de la proporcionalidad, que requiere que dicho control sea justificado, idóneo, necesario y proporcionado. En una primera etapa, tanto los tribunales nacionales como comunitarios, entendieron que además de la doctrina de la proporcionalidad era necesario fijar criterios de uso, hasta el punto de que la mera tipificación en el convenio colectivo de aplicación, debía entenderse como una prohibición absoluta de uso personal del ordenador de empresa. A mayor abundamiento, en una segunda etapa, representada principalmente por *Barbulescu II*, se exigió, además de la doctrina de la proporcionalidad y del establecimiento de criterios de uso, advertir al trabajador acerca de que dicho uso podía ser objeto de control.

Como segunda conclusión, la instalación de cámaras de videovigilancia provoca que adquiera importancia el derecho fundamental a la protección de datos de carácter personal, sin perder de vista el derecho fundamental a la intimidad. Ante los últimos pronunciamientos judiciales surge nuevamente la duda de si es suficiente con la colocación de un cartel informativo en el que se recoja la existencia de cámaras de videovigilancia o si, además, es obligatorio informar previamente a los trabajadores afectados por las grabaciones de la finalidad sancionadora para el caso de que se capten incumplimientos laborales.

Como tercera conclusión, la doctrina de la proporcionalidad nunca se ha olvidado, sino que está presente en todos los pronunciamientos judiciales más importantes sobre esta materia, tanto en el caso del control del uso del ordenador como en el caso de la

[124]https://www.telegraph.co.uk/technology/2018/11/10/major-uk-companies-preparing-microchip-employees/ (última consulta, 8 de enero de 2020).

videovigilancia empresarial. Así, aunque a mayores tenga que ser completada con otra serie de requisitos, debe tenerse siempre en cuenta como punto de partida.

Como cuarta conclusión, el hecho de proporcionar al trabajador información previa, puede llegar a frustrar la finalidad sancionadora del control, pues todo indica a pensar que, si el trabajador que está cometiendo alguna irregularidad es conocedor del control desplegado y de la finalidad del mismo, cesará en su conducta desviada. Por tanto, la finalidad sancionadora deja de ser el objetivo primordial, ganando peso la finalidad preventiva o disuasoria.

Como quinta y última conclusión, surge la duda de si es posible trasladar a la ley la doctrina de la proporcionalidad, o si, por el contrario, hay que atender a cada caso en concreto. A mi juicio, se debería producir una intensa actividad legislativa orientada a ofrecer respuestas claras y a buscar un justo equilibrio entre la libertad del empresario en sus poderes de dirección y la protección de los derechos fundamentales de los trabajadores, sin perjuicio de las particularidades que en la práctica puedan surgir.

BIBLIOGRAFÍA

CALVO MORALES, D. y TOSCANI GIMENEZ, D.: «El uso de internet y el correo electrónico en la empresa. Límites y garantías», *Revista Española de Derecho del Trabajo*, n.º 165, 2014. Versión electrónica: www.westlaw.es (BIB 2014\1659).

COSTA HERNANDIS, R.: «Protección de datos en el ámbito laboral», RALLO LOMBARTE, A. (Dir.), *Tratado de Protección de Datos*, Tirant Lo Blanch, Valencia, 2019, pp. 655-671.

DE VICENTE PACHÉS, F.: «Las facultades empresariales de vigilancia y control en las relaciones de trabajo: concepto y fundamento. Una primera aproximación a las diversas formas de control empresarial», GARCÍA NINET, J. I. (Dir.), *El control empresarial en el ámbito laboral*, CISS, 2005, pp. 17-35.

DEL PINO PADRÓN, M. C.: «El impacto de las tecnologías de la información en el Derecho laboral, especial referencia a la intimidad del trabajador y el secreto de sus comunicaciones», *Cadernos de Dereito Actual*, n.º 8, 2018, pp. 153-164.

DESDENTADO BONETE, A. y MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012.

DESDENTADO BONETE, A. y DESDENTADO DAROCA, E.: «La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador», *Revista de Información Laboral*, n.º 1, 2018. Versión electrónica: www.westlaw.es (BIB 2018\6059).

FABREGAT MONFORT, G.: *Vademécum de Derecho Laboral (5ª Edición)*, Tirant Lo Blanch, Valencia, 2017.

FERNÁNDEZ ORRICO, F. J.: «Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre», *Revista Española de Derecho del Trabajo*, n.º 222, 2019. Versión electrónica: www.westlaw.es (BIB 2019\7744).

FERNÁNDEZ VILLAZÓN, L. A.: *Las facultades empresariales de control de la actividad laboral*, Aranzadi, Cizur Menor (Navarra), 2003.

FOSSAS ESPALADER, E.: «Cosa interpretada en derechos fundamentales: jurisprudencia del TEDH y jurisprudencia constitucional», *Revista Vasca de Administración Pública*, n.º 82, 2, 2008, pp. 165-180.

GARCÍA RUBIO, M. A. y PÉREZ DE LOS COBOS ORIHUEL, F.: «El control empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal

Europeo de Derechos Humanos», *Nueva Revista Española de Derecho del Trabajo*, n.º 196, 2017, pp. 41-54.

GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales», *Comunicación presentada al XIX Congreso de ASNALA,* Málaga, 2018, pp. 1-49.

GONZÁLEZ GONZÁLEZ, C.: «Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016», *Revista Aranzadi Doctrinal,* n.º 5, 2016. Versión electrónica: www.westlaw.es (BIB 2016\21165).

GOÑI SEIN, J. L.: *El respeto a la esfera privada del trabajador*, Civitas, Madrid, 1988.

GOÑI SEIN, J. L.: «Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?», *Comunicación presentada al XXIX Congreso Nacional de Derecho del Trabajo y de la Seguridad Social*, Pamplona, 2014, pp. 1-98.

MARÍN ALONSO, I.: *El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones*, Tirant Lo Blanch, Valencia, 2005.

MARTÍNEZ FONS, D.: «El uso y control del correo electrónico e internet en la empresa: aspectos laborales», ROIG BATALLA, E. (Coord.), *El uso laboral y sindical del correo electrónico e internet en la empresa*, Tirant Lo Blanch, Valencia, 2007, pp. 175-227.

MARTÍNEZ LÓPEZ-SAEZ, M.: «Nuevos perfiles del derecho al olvido en Europa y España», en AA. VV, *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, Dykinson, Madrid, 2017, pp. 231-266.

MONTOYA MELGAR, A.: «Dirección y control de la actividad laboral», BORRAJO DACRUZ, E. (Dir.), *Comentarios a las leyes laborales. El Estatuto de los Trabajadores*, tomo V, Edersa, Madrid, 1985.

POQUET CATALÁ, R.: *La actual configuración del poder disciplinario empresarial*, Tirant Lo Blanch, Valencia, 2011.

PRECIADO DOMÈNECH, C. H.: «Comentario de urgencia a la STEDH de 5 de septiembre 2017. Caso Barbulescu contra Rumanía (Gran Sala). Recuperando la dignidad en el trabajo», *Revista de Información Laboral*, n.º 10, 2017. Versión electrónica: www.westlaw.es (BIB 2017\13278).

PRECIADO DOMÈNECH, C. H.: «Comentario de urgencia a la STEDH de 9 de enero. Caso López Ribalda y otras c. España», *Revista de Información Laboral*, n.º 1, 2018. Versión electrónica: www.westlaw.es (BIB 2018\6060).

QUÍLEZ MORENO, J. M.: «La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores», *Revista Española de Derecho del Trabajo*, n.º 217, 2019. Versión electrónica: www.westlaw.es (BIB 2019\1558).

RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*, Tirant Lo Blanch, Valencia, 2015.

SAN MARTÍN MAZZUCCONI, C. y SEMPERE NAVARRO, A. V.: «Sobre Nuevas Tecnologías y Relaciones Laborales», *Revista Doctrinal Aranzadi Social*, n.º 15, 2002. Versión electrónica: www.westlaw.es (BIB 2002\2021).

https://www.telegraph.co.uk/technology/2018/11/10/major-uk-companies-preparing-microchip-employees/ (última consulta, 8 de enero de 2020).

REPERTORIO NORMATIVO

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (*BOE* n.º 243, de 10 de octubre de 1979).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección civil 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 (*DOUE* n.º 119, de 4 de mayo de 2016).

Constitución Española (*BOE* n.º 311, de 29 de diciembre de 1978).

Ley 36/2011, de 10 de octubre, Reguladora de la Jurisdicción Social (*BOE* n.º 245, de 11 de octubre de 2011).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (*BOE* n.º 294, de 6 de diciembre de 2018).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (*BOE* n.º 298, de 14 de diciembre de 1999).

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (*BOE* n.º 157, de 2 de julio de 1985).

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 (*BOE* n.º 115, de 14 de mayo de 1982).

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 (B*OE* n.º 255, de 24 de octubre de 2015).

Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social (*BOE* n.º 189, de 8 de agosto de 2008).

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 cámaras o videocámaras (*BOE* n.º 296, de 12 de diciembre de 2006).

REPERTORIO JURISPRUDENCIAL

STEDH caso López Ribalda y otros contra España, de 17 de octubre de 2019 (*Aranzadi Westlaw*, referencia TEDH 2019\144).

STEDH caso López Ribalda y otros contra España, de 9 de enero de 2018 (*Aranzadi Westlaw*, referencia TEDH 2018\1).

STEDH caso Barbulescu contra Rumanía, de 5 de septiembre de 2017 (*Aranzadi Westlaw*, referencia TEDH 2017\61).

STEDH caso Barbulescu contra Rumanía, de 12 de enero de 2016 (*Aranzadi Westlaw*, referencia TEDH 2016\1).

STEDH caso Copland contra Reino Unido, de 3 de abril de 2007 (*Aranzadi Westlaw*, referencia TEDH 2007\23).

STEDH caso Niemietz contra Alemania, de 16 de diciembre de 1992 (*Aranzadi Westlaw*, referencia TEDH 1992\77).

STC 13/2017, de 30 de enero (*Aranzadi Westlaw*, referencia RTC 2017\13).

STC 39/2016, de 3 de marzo (*Aranzadi Westlaw*, referencia RTC 2016\39).

STC 170/2013, de 7 de octubre (*Aranzadi Westlaw*, referencia RTC 2013\170).

STC 61/2013, de 14 de marzo (*Aranzadi Westlaw*, referencia RTC 2013\61).

STC 29/2013, de 11 de febrero (*Aranzadi Westlaw*, referencia RTC 2013\29).

STC 241/2012, de 17 de diciembre (*Westlaw Aranzadi*, referencia RTC 2012\241).

STC 23/2010, de 27 de abril (*Aranzadi Westlaw*, referencia RTC 2010\23).

STC 230/2007, de 5 de noviembre (*Aranzadi Westlaw*, referencia RTC 2007\230).

STC 70/2002, de 3 de abril *(Aranzadi Westlaw*, referencia RTC 2002\70).

STC 292/2000, de 30 de noviembre (*Aranzadi Westlaw*, referencia RTC 2000\292).

STC 186/2000, de 10 de julio (*Aranzadi Westlaw*, referencia RTC 2000\186).

STC 98/2000, de 10 de abril (*Aranzadi Westlaw*, referencia RTC 2000\98).

STC 94/1998, de 4 de mayo (*Aranzadi Westlaw*, referencia RTC 1998\94).

STC 245/1993, de 20 de julio (*Aranzadi Westlaw*, referencia RTC 1993\254).

STC 129/1989, de 17 de julio (*Aranzadi Westlaw*, referencia RTC 1989\129).

STS 119/2018, de 8 de febrero (*Aranzadi Westlaw*, referencia RJ 2018\666).

STS 96/2017, de 2 de febrero (*Aranzadi Westlaw*, referencia RJ 2017\1628).

STS 723/2016, de 13 de septiembre (*Aranzadi Westlaw*, referencia RJ 2016\4843).

STS 630/2016, de 7 de julio (*Aranzadi Westlaw*, referencia RJ 2016\4434).

STS de 6 de octubre de 2011 (*Aranzadi Westlaw*, referencia RJ 2011\7699).

STS de 8 de marzo de 2011 (*Aranzadi Westlaw*, referencia RJ 2011\932).

STS de 26 de septiembre de 2007 (*Aranzadi Westlaw*, referencia RJ 2007\7514).

STSJ de Madrid 783/2019, de 12 julio (*Aranzadi Westlaw*, referencia JUR 2019\252146).

STSJ de la Comunidad Valenciana 1483/2019, de 16 de mayo (*Aranzadi Westlaw*, referencia JUR 2019\271326).

STSJ de Castilla y León (Burgos) 319/2019, de 15 de mayo (*Aranzadi Westlaw*, referencia 2019\1751).

STSJ de Madrid 388/2019, de 24 de abril (*Aranzadi Westlaw*, referencia 2019\2359).

STSJ de Madrid 75/2019, de 25 de enero (*Aranzadi Westlaw*, referencia AS 2019\1174).

STSJ de la Comunidad Valenciana 3390/2018, de 19 de noviembre (*Aranzadi Westlaw*, referencia AS 2019\1207).

STSJ de Andalucía (Granada) 2459/2018, de 25 de octubre (*Aranzadi Westlaw*, referencia JUR 2019\26436).

STSJ de Islas Canarias (Santa Cruz de Tenerife) 1002/2018, de 16 de octubre (*Aranzadi Westlaw*, referencia AS 2019\1522).

STSJ de Madrid 591/2018, de 13 de septiembre (*Aranzadi Westlaw*, referencia AS 2019\923).

STSJ de Castilla La Mancha 670/2018, de 11 de mayo (*Aranzadi Westlaw*, referencia JUR 2018\183155).

STSJ de Castilla y León (Valladolid), de 11 de abril de 2018 (*Aranzadi Westlaw*, referencia AS 2018\1211).

STSJ de Islas Canarias (Las Palmas) 53/2018, de 26 de enero (*Aranzadi Westlaw*, referencia AS 2019\822).

STSJ de Madrid 531/2017, de 19 de julio (*Aranzadi Westlaw*, referencia JUR 2017\249682).

STSJ de Andalucía (Granada) 1730/2017, de 12 de julio (*Aranzadi Westlaw*, referencia AS 2017\2114).

STSJ de Andalucía (Málaga) 670/2017, de 5 de abril de 2017 (*Aranzadi Westlaw*, referencia JUR 2017\163007).

STSJ de Andalucía (Sevilla) 899/2017, de 22 de marzo (*Aranzadi Westlaw*, referencia AS 2017\1052).

STSJ de País Vasco 1757/2015, de 29 de septiembre (*Aranzadi Westlaw*, referencia AS 2015\1922).

STSJ de Madrid 715/2012, de 29 de octubre (*Aranzadi Westlaw*, referencia AS 2012\380458).

STSJ de País Vasco 1072/2012, de 17 de abril (*Aranzadi Westlaw*, referencia AS 2012\1676).

STSJ de Murcia 47/2010, de 25 de enero (*Aranzadi Westlaw*, referencia AS 2010\165).

STSJ de Madrid 685/2009, de 5 de noviembre (*Aranzadi Westlaw*, referencia AS 2009\133).

STSJ de Madrid 775/2009, de 30 de octubre (*Aranzadi Westlaw*, referencia JUR 2010\27623).

STSJ de País Vasco, de 6 de noviembre de 2007 (*Aranzadi Westlaw*, referencia AS 2008\1556).

STSJ de País Vasco, de 12 de septiembre de 2006 (*Aranzadi Westlaw*, referencia AS 2006\2602).

STJS de Madrid 452/2004, de 11 de mayo (*Aranzadi Westlaw*, referencia JUR 2004\241595).

STSJ de Asturias 1482/2004, de 30 de abril (*Aranzadi Westlaw*, referencia AS 2004\2112).

STSJ de Madrid 432/2003, de 13 mayo (*Aranzadi Westlaw*, referencia AS 2003\3649).

STSJ de Andalucía (Sevilla) 1619/2003, de 9 de mayo (*Aranzadi Westlaw*, referencia AS 2003\2840).

STSJ de Cantabria 583/2002, de 29 de abril (*Aranzadi Westlaw*, referencia JUR 2002\157929).

STSJ de Galicia, de 4 de octubre de 2001 (*Aranzadi Westlaw*, referencia AS 2001\3366).

STSJ de Islas Canarias (Las Palmas) 628/2001, de 25 de julio (*Aranzadi Westlaw*, referencia AS 2001\4603).

SJS n.º 3 de Pamplona 52/2019, de 18 de febrero (*Aranzadi Westlaw*, referencia AS 2019\1014).