



**Universitat de les
Illes Balears**

Facultad de Derecho

Memoria del Trabajo Fin de Grado

Control de la actividad del trabajador por medios tecnológicos

Anaís Batle Pons

Grado en Relaciones Laborales

Año académico 2019-2020

DNI del alumno: 43179266-D

Trabajo tutelado por: Luis Enrique Dot Hualde
Departamento de Derecho Público, Área de Derecho del Trabajo y de la Seguridad Social

Se autoriza a la Universidad a incluir este trabajo en el Repositorio Institucional para su consulta en acceso abierto y su difusión en línea, con finalidades exclusivamente académicas y de investigación.	Autor		Tutor	
	Sí	No	Sí	No
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Resumen

Este estudio trata de poner de manifiesto el conflicto existente entre la facultad de la que dispone el empresario para controlar la actividad laboral por medio de la tecnología y los derechos fundamentales del trabajador con los que colisiona; el derecho a la intimidad y al secreto en sus comunicaciones. Este choque limitará el mencionado poder de dirección y a su vez modulará los derechos fundamentales, que deben ceder para permitir el control.

Palabras clave

Control, actividad, tecnológico, derecho constitucional, derecho fundamental, intimidad, poder, vigilancia, videovigilancia, grabación, principio de proporcionalidad, comunicación, límite, GPS, ordenador, fichaje, registro.

Índice

Resumen	2
Palabras clave	2
I. Introducción	4
II. Marco jurídico.....	7
III. Conflicto de intereses	9
3.1. Evolución doctrina Constitucional	9
3.2. Principio proporcionalidad	10
3.3. Expectativa razonable de intimidad.....	11
IV. Sistemas de control tecnológico	15
4.1. Uso y control del teléfono empresarial.....	15
4.2. Uso y control del PC, portátil y correo empresarial	16
4.3. Videovigilancia y grabación de sonidos	18
4.4. Aparatos de geolocalización.....	20
4.5. Control de fichaje	22
V. Conclusión	24
VI. Bibliografía.....	25
6.1. Libros y revistas	25
6.2. Blogs, webs y coloquios	26

I. Introducción

Actualmente nuestro día a día está rodeado de tecnología, así como también el mundo laboral, donde cada vez existen menos actividades en las que no se utilicen instrumentos tecnológicos. De esta evolución del trabajo nace la necesidad de un nuevo planteamiento para llevar a cabo el control de la actividad laboral, ya que “el control presencial, caracterizado por la coincidencia espacio temporal de empresario y trabajador, ya forma parte del pasado artesanal... que cede el paso con rapidez al control tecnológico”¹ además, muchas actividades realizadas con las TIC no se pueden controlar mediante un *simple vistazo*², lo cual acrecentará la preocupación por parte del empresario del uso real que le dan sus empleados.

La tecnología en las relaciones laborales va a posibilitar al empresario, por una parte “al desarrollo de su actividad laboral, con la aportación de nuevas herramientas de trabajo [...] y, por otra parte, estas nuevas herramientas actúan como novedosos e intensos instrumentos de control de la prestación laboral. De esta forma, el empresario encontrará en las nuevas tecnologías un aliado muy importante que le facilitara el ejercicio de las facultades de organización, dirección y control de trabajo que le confiere el ordenamiento laboral”³.

Centrándonos en la segunda premisa, esta vigilancia más exhaustiva, la cual le dotará de un poder de control mucho mayor y a un menor coste, a su vez también hará que aparezcan controversias en cuanto a la intimidación de los trabajadores ya que estos, según avala consolidada jurisprudencia constitucional, “aunque se integran dentro de una organización y bajo las órdenes de un empresario, no se despojan de sus derechos inherentes como persona con la celebración de un contrato de trabajo, ni tampoco al iniciar su jornada laboral. Sí es cierto pero, que estos derechos van a verse limitados en la medida estrictamente necesaria para mantener un adecuado funcionamiento de la actividad productiva de la empresa”⁴. Al respecto de esta doctrina mencionaré la STC

¹ TASCÓN LOPEZ, Rodrigo. “El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica”. *Revista Doctrinal Aranzadi Social*, 2007 (núm.17) p.2.

² Al haber cambiado los sistemas de producción, la vigilancia debe situarse en el mismo plano que los instrumentos de uso en la prestación laboral, es decir, ese control y vigilancia se deberá desarrollar sobre la tecnología que se use, un control informático y tecnológico. Pensemos en el trabajador que, a simple vista, su jefe *ve* que está trabajando seriamente frente a su ordenador, pero pudiera ser que realmente de comprobar su historial web, estuviera navegando por internet, leyendo su correo particular o, en definitiva, dedicando su tiempo de trabajo en actividades privadas.

³ SELMA PENALVA, Alejandra, “Las peculiaridades prácticas del control en la empresa”, *Anales de Derecho*, 2009 (núm.27), p.106.

⁴ LLAMOSAS TRAPAGA, Aida, *Relaciones laborales y nuevas tecnologías de la información y de la comunicación*, Madrid, Editorial Dykinson, 2015, p.93.

88/1985 de 19 de julio⁵ en la que se expresa que “la celebración de un contrato de trabajo no implica de modo alguno la privación para una de las partes de los derechos que la Constitución le reconoce como ciudadano” y la STC 99/1994, de 11 de abril, que también se pronuncia al respecto, mencionando que “la inclusión de la persona como trabajadora en una organización conseguirá modular sus derechos fundamentales, produciendo una limitación en los mismos, en la medida estrictamente necesaria para el correcto funcionamiento de la actividad productiva, al verse sometido al control y dirección del empresario”⁶.

Menciona TASCÓN⁷, que el control que se podrá llevar a cabo mediante estas nuevas tecnologías será muy variado, prácticamente ilimitado; desde mecanismos de control de acceso y localización dentro de la empresa o la geolocalización del vehículo de empresa o dispositivos electrónicos cuando se está fuera del centro de trabajo, la videovigilancia, hasta registros del ordenador utilizado por el trabajador, su historial, el correo electrónico corporativo, el rastro que deja la navegación por internet, y un amplio etcétera ya que, como afirma, la lista “ha de ser *numerus apertus*”.

En ese control de la actividad laboral de los trabajadores se pretenderá básicamente, conocer si incurren en incumplimientos contractuales y, de ser así, conseguir prueba fehaciente para poder demostrarlo y hacer un correcto uso del poder sancionador. La gravedad del acto constituido por el trabajador definirá si es merecedor de castigo en cada caso, pudiendo traducirse incluso en la sanción más elevada; el despido disciplinario, que en estos casos generalmente se lleva a cabo según la causa tasada en el artículo 54.2 del ET, por la vía de transgresión de la buena fe contractual. El incumplimiento dependerá de las directrices y tolerancia de cada empresa, lo que puede considerarse incumplimiento en una, puede ser actitud tolerada en otra, a modo de ejemplo, el uso puntual del internet para acceder al correo personal o cuentas bancarias, o llamadas personales con el móvil de empresa.

Siendo legítimo, por tanto, el interés y necesidad del empresario en controlar la ejecución de la prestación laboral por parte de sus empleados y el uso que realizan de los instrumentos facilitados para tal será necesario que este, en su poder de control, se acoja a unas garantías suficientes para con sus trabajadores. Será necesario que alcance el mayor equilibrio posible entre los intereses empresariales y los derechos de los trabajadores, escogiendo medidas que resulten proporcionales al fin pretendido. Y

⁵ STC 88/1985, de 19 de julio, FJ.2.

⁶ STC 99/1994, de 11 de abril, FJ.4.

⁷ TASCÓN LOPEZ, Rodrigo, Op. Cit., p.4.

respecto de ello, expresa PURCALLA⁸, que la doctrina constitucional consagra el principio de proporcionalidad⁹ como criterio para valorar la necesidad imprescindible de las medidas empresariales que implican el menoscabo en los derechos fundamentales, señalando que;

“a) por una parte, que los derechos fundamentales del trabajador deben adaptarse a los requerimientos de la organización productiva en que se integra¹⁰;

b) por otra parte, que también las facultades empresariales se encuentran limitadas por los derechos fundamentales del trabajador, que son prevalentes y constituyen un límite infranqueable no solo a sus facultades sancionadoras, sino también a las facultades de organización y de gestión...¹¹; y

c) que cuando se prueba indiciariamente que una decisión empresarial puede enmascarar una lesión de derechos fundamentales, incumbe al empresario acreditar que su decisión obedece a motivos razonables y ajenos a todo propósito atentatorio del derecho [...]”¹².

⁸ PURCALLA BONILLA, Miguel A. “Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre”. *Revista española de Derecho del Trabajo*, 2019, (núm. 218/2019). Editorial Aranzadi, p.2.

⁹ STC 98/2000, de 10 de abril; STC 186/2000, de 10 de julio.

¹⁰ SSTC 5/1981; 47/1985; 77/1985; 106/1996 y 199/1999.

¹¹ SSTC 292/1993; 136/1996; 90/1997; 1/1998; 90/1999; 98/2000; 190/2001; 213/2002; 17/2003 y 49/2003.

¹² SSTC 38/1981, 41/2006, 342/2006 y 125/2007.

II. Marco jurídico

La Constitución Española le reconoce al empresario la libertad de empresa en su art. 38, y el poder de vigilancia y control que ostenta se encuentra recogido en el art. 20.3 del ET. En él se establece que podrá adoptar las medidas que estime necesarias para fiscalizar la prestación laboral y comprobar que el trabajador efectivamente cumple con las obligaciones que se le han encomendado. Este poder no será ilimitado, ya que también se estipula en el mismo artículo que las medidas adoptadas deberán ser necesariamente respetuosas con la dignidad del trabajador.

Estas medidas de control tendrán la finalidad de salvaguardar los intereses mercantiles del empresario y su derecho de propiedad privada existente en el art. 33 de la CE.

Como he mencionado, el poder del que dispone el empresario tendrá una limitación clara; no atentar contra los derechos fundamentales reconocidos constitucionalmente a los trabajadores como son el derecho a la intimidad recogido en el art. 18.1, el secreto de las comunicaciones del art. 18.3 y el derecho a la protección de datos de carácter personal en el art. 18.4. Además de los derechos constitucionales, también deberá respetar lo estipulado en el art. 4.2 del ET el cual reconoce al trabajador el derecho al respeto de su intimidad y dignidad en la relación laboral. A nivel internacional, referente a los derechos que pueden ser vulnerados con el control empresarial, encontramos el art. 8.1 del CEDH¹³ que establece que cualquier persona tiene derecho a que se respete el secreto de sus comunicaciones.

A su vez, el ET en su art. 20.2 establece la obligatoriedad que tiene el trabajador de cumplir con sus obligaciones laborales de conformidad con la buena fe.

Por otra parte, el art. 18 del ET posibilita al empresario, de ser necesario o de tener sospecha o indicios, a llevar a cabo registros en taquillas y “efectos personales” de los trabajadores en el centro y horas de trabajo para proteger el patrimonio empresarial y el de los demás trabajadores¹⁴. Aunque al respecto, el posicionamiento mayoritario de la doctrina judicial lo deja fuera de aplicación en cuanto al control de las tecnologías, aclarando que si bien hay también una cesión de uso en los pc, teléfonos y demás herramientas tecnológicas, no tienen consideración de “efectos personales”¹⁵. Los dispositivos informáticos que el trabajador utiliza para la prestación laboral son

¹³ Artículo 8 sobre el Derecho al respeto a la vida privada y familiar.

¹⁴ Si bien es cierto que el trabajador se puede negar a dichos registros, ello podría derivar en desobediencia y traer consigo consecuencias negativas, e incluso al despido.

¹⁵ SAN MARTÍN MAZZUCCONI, Carolina, SEMPERE NAVARRO, Antonio V. “Sobre el control empresarial de los ordenadores” *Revista Doctrinal Aranzadi Social*, 2012, (núm.3/2012), p.12.

instrumentos de producción de los que el titular es el empresario, en cambio una taquilla, aun siendo un bien mueble del empresario, existe una cesión de uso a favor del trabajador limitando su uso a éste¹⁶.

Esta poca concreción en la normativa laboral, e incluso ambigüedad, hace que resulte fundamental la jurisprudencia para su interpretación. La legislación no concreta límites para que la adopción de la vigilancia del empresario guarde la debida consideración con la dignidad del trabajador, ni cuándo dicha intromisión se justifica con la necesidad de salvaguardar el patrimonio de su empresa. Son los Tribunales quienes interpretarán en cada caso concreto si se está produciendo vulneración de los derechos fundamentales o se está actuando acorde a la legalidad, en ocasiones generando considerables contradicciones que provocan, evidentemente, un alto grado de inseguridad jurídica¹⁷.

Recientemente, la entrada en escena de la LO 3/2018 del 3 de diciembre de Protección de datos y garantía de los derechos digitales, tras la normativa comunitaria existente dentro de la UE (Reglamento UE 2016/679), viene a trasponer la jurisprudencia existente hasta el momento en una norma nacional¹⁸. Esta ley trae consigo la adición del apartado bis al art. 20 del ET, que expresa literalmente: "Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a disposición por el empleador, [...] y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección. Aún con la LO 3/2018 quedan muchos asuntos pendientes, que seguirá colmando la jurisprudencia, de datos personales y garantía de los derechos digitales". Esta norma se encargará de regular el derecho a la intimidad de los trabajadores con la libertad de empresa para controlar la actividad laboral por medios tecnológicos en sus artículos 87 (que viene a calibrar el derecho del trabajador a que se preserve su intimidad en el uso de los dispositivos electrónicos), 89 (referente al derecho a la intimidad en el uso de medios de control de grabación de video y sonido en el trabajo) y 90 (regula el mismo derecho de intimidad, pero referente a la geolocalización).

¹⁶ PURCALLA BONILLA, Miguel Á., Op. Cit., p.4.

¹⁷ TASCÓN LOPEZ, Rodrigo, Op. Cit., p.6.

¹⁸ SERRANO GARCÍA, Juana M^a "La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia" ED. Bomarzo 2019, Albacete. España p.13.

III. Conflicto de intereses

Los criterios que han ido estableciendo los Tribunales para solventar el mencionado choque de intereses del control de la actividad laboral a través de medios tecnológicos en relación a la intimidad personal no han permanecido inmóviles a lo largo del tiempo, si no que siguen en constante evolución. A grandes rasgos, la doctrina Constitucional de los últimos años podría resumirse como sigue.

3.1. Evolución doctrina Constitucional

Los casos del Casino de La Toja¹⁹ (STC 98/2000) y Economato de Ensidesa²⁰ (STC 186/2000) marcan un cambio en la doctrina Constitucional con el anterior periodo, ya que hasta el momento, predominaba la permisividad del legislador al control ejercido sobre los trabajadores por parte del empresario y es que, en las mencionadas sentencias, se parte de la premisa de que la instalación de medidas de control va a comportar necesariamente una restricción de los derechos de los trabajadores y, como tal, se deberá acudir a su aplicación de manera “limitada”.

Aunque las resoluciones de las mencionadas sentencias son opuestas, los fundamentos son coincidentes en cuanto a que resuelven los conflictos entre la facultad de control de la empresa y el derecho del trabajador a su intimidad, aplicando el juicio de ponderación para valorar la licitud de la medida de vigilancia aplicada, resolviendo en el primer caso que los medios de control se exceden de la legitimidad, vulnerando excesivamente el derecho a la intimidad del trabajador (STC 98/2000) y en el segundo caso, contrariamente, pronunciándose en referencia a que el derecho a la intimidad debe ceder y modularse ante el necesario control de la empresa (STC 186/2000).

La resolución de los conflictos dependerá de la aplicación del juicio de ponderación que se haga en cada caso por el Tribunal.

Por otra parte, en el mismo período, en la fundamentación de la STC 29/2013 del 11 de febrero (Universidad de Sevilla), estipula la necesidad de una información previa al trabajador para que una grabación se considere lícita para su control, aviso que deberá darse de forma “expresa, precisa, clara e inequívoca de la finalidad de control de la actividad”²¹.

¹⁹ STC 98/2000, de 10 de abril.

²⁰ STC 186/2000 de 10 de julio.

²¹ STC 29/2013 de 11 de febrero.

En el siguiente periodo, la novedad que se crea con respecto de la anterior doctrina es que la prohibición mediante CC²² de usar la tecnología puesta a disposición del trabajador, para su uso particular, facultará al empresario²³ a controlar lo que contienen los e-mails enviados y recibidos por el trabajador sin necesidad de preaviso individual y a eliminar toda expectativa de confidencialidad, lo cual evitará la vulneración del derecho a la intimidad del trabajador.

Esta “prohibición” mediante CC podía consistir simplemente en tipificar como falta de mayor o menor nivel el uso de dispositivos electrónicos para su uso privado.

Por último, nos encontramos con la STC 39/2016 del 3 de marzo (caso Bershka)²⁴ por el que se establece que el consentimiento para el tratamiento de datos se da conjuntamente con el establecimiento de la relación laboral y que el deber de información por parte de la empresa de la aplicación de medidas de videovigilancia se considerará cumplido si se ha procedido a la colocación del distintivo legal en lugar visible.

3.2. Principio proporcionalidad

10

El principio de proporcionalidad es un criterio metodológico consistente en determinar si la incidencia sobre los derechos fundamentales es constitucional, que lo será siempre y cuando consiga superar un triple test²⁵. La STC 186/2000²⁶ se pronuncia al respecto del mencionado precepto:

“la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo, FJ 5; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes:

- Si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad);
- Si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad);

²² Como ejemplo de empresas que regulan en sus CC el uso de los medios tecnológicos nos encontramos con el CC del Grupo Axa Arts. 14 y 15 (BOE núm. 244 de 10/10/2017).

²³ STC 170/2013 de 7 de octubre.

²⁴ STC 39/2016 de 3 de marzo.

²⁵ SAN MARTÍN MAZZUCCONI, Carolina, SEMPERE NAVARRO, Antonio V. “Sobre Nuevas Tecnologías y Relaciones Laborales” *Revista Doctrinal Aranzadi Social*, 2002, (núm. 15/2002), pp.45-46.

²⁶ SSTC 186/2000 de 10 de julio.

- y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)."

Así pues, SEMPERE²⁷ remarca que la vigente doctrina exige a la medida adoptada por el empleador la superación de cada uno de los tres requisitos expuestos para que pueda adoptarla ante sus trabajadores: juicio de idoneidad, es decir, si con la medida es posible alcanzar la finalidad pretendida, sin obedecer a una medida caprichosa o irracional, juicio de necesidad, de no existir una medida menos invasiva para alcanzar el mismo propósito, ya que como dice la STC 98/2000²⁸ "si existen otras posibilidades de satisfacer el interés empresarial menos agresivas y afectantes al derecho en cuestión habrá que emplear estas últimas", por tanto, a demás de cumplir con el juicio de idoneidad, debe tratarse de la medida de igual eficacia pero menos dañina para el trabajador y, por último, el juicio de proporcionalidad en sentido estricto, también conocido como juicio de ponderación, exigiendo a la misma que ésta produzca más ventajas para el interés general que daños sobre otros bienes en conflicto y, además, con la necesidad de que se respete el contenido esencial del derecho fundamental mermado.

Adicionalmente al triple test, afirma MORALES VALLÉS²⁹, nos encontramos con el principio de intervención indiciaria por el cual se exige justificar las medidas adoptadas para fiscalizar al trabajador, acreditando que existían indicios que revelaban una actuación irregular por parte de este³⁰. Según el art. 181.2 LRJS, una vez justificada la concurrencia de indicios de que se ha producido violación del derecho fundamental o libertad pública, corresponderá al demandado la aportación de una justificación objetiva y razonable, suficientemente probada, de las medidas adoptadas y de su proporcionalidad.

3.3. Expectativa razonable de intimidad

Toda empresa está facultada para decidir el uso que puede permitir que se haga de los dispositivos electrónicos puestos a disposición de los trabajadores en su empresa, pero si pretende controlar la actividad de sus trabajadores para evitar su incumplimiento, debería establecer primeramente unas pautas de uso de los mismos (lo que está permitido, lo que está prohibido y la sanción que podría acarrear de hacer caso omiso de las normas) para evitar que el desconocimiento del trabajador derive en un uso de dichos aparatos para actividades extra laborales, por entender que se permite su uso o que existe una mínima tolerancia en el uso privado.

²⁷ SEMPERE NAVARRO, Antonio V. "Ponencia sobre la intimidad en el ámbito laboral a la luz de los últimos pronunciamientos judiciales nacionales e internacionales".

²⁸ STC 98/2000, de 10 de abril.

²⁹ MORALES VÁLLEZ, CONCEPCIÓN E., "El control de los medios tecnológicos por el empresario a la luz de la sentencia del TEDH de 12 de enero de 2016".

³⁰ STSJ 1543/2014, de 4 de septiembre.

Como venimos diciendo, la fiscalización de la actividad del trabajador mediante las nuevas tecnologías, o el uso de las mismas, tiene una clara incidencia sobre el derecho constitucionalmente reconocido a todas las personas, el derecho a la intimidad. Este derecho fundamental se define como la libertad que tiene toda persona para controlar y decidir toda información de carácter privado que otra persona pueda conocer³¹ y se regula principalmente en los siguientes artículos: art. 18 CE, art. 4.2 e) ET y art. 8.1 CEDH.

Esta injerencia en los derechos de los trabajadores puede darse por el registro del ordenador del trabajador o su correo electrónico, el uso de los datos obtenidos por geolocalización del lugar en el que se encuentra él o su vehículo de empresa, la revisión, la videovigilancia y grabación de sonidos en su puesto de trabajo, el control de las llamadas de teléfono o su mensajería instantánea...³² y, de ocurrir esto, se debe conseguir alcanzar el equilibrio entre el derecho del trabajador a su intimidad y el interés del empleador en controlar y proteger la actividad productiva.

El criterio de la “expectativa razonable de intimidad” se incorporó por el Tribunal Europeo de Derechos Humanos, según lo establecido en las SSTEDH de 25 de junio de 1997 (caso Halford³³) y del 3 de abril de 2007 (caso Copland³⁴) al valorar la existencia de una vulneración del art. 8 del CEDH. Tras ellas pasó a formar parte de la jurisprudencia del Tribunal Supremo y más adelante del Tribunal Constitucional³⁵.

Con la STS 7699/2011³⁶ del 6 de octubre, se estableció que no podrá existir dicha “expectativa razonable de intimidad” si mediaba advertencia previa de prohibición absoluta de su uso extra laboral de los aparatos electrónicos y se considerará al empresario legitimado para comprobar o controlar la actividad realizada por los trabajadores sin previo aviso, ya que “no existe tolerancia empresarial en el uso de los medios tecnológicos para usos particulares y se ha establecido una regla general de prohibición absoluta”³⁷. Parece lógico pensar pues, que si no existe tolerancia alguna al uso personal de los dispositivos facilitados, tampoco existirá un derecho a hacerlo en

³¹ “Derecho a la intimidad de la persona trabajadora”, *Revista Iberley*, 03/02/2020, p.1.

<https://www.iberley.es/temas/derecho-intimidad-persona-trabajadora-64287>.

³² *Ibidem*, p.1.

³³ STDH de 25 de junio de 1997 (TEDH 1997/37).

³⁴ STDH de 3 de abril de 2007 (TEDH 2007/23), que establece que la expectativa de intimidad y confidencialidad solo desaparecerá si la empresa advierte de la fiscalización de la actividad.

³⁵ LLUCH CORELL, Francisco, “El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador”, *Revista de Jurisprudencia*, (número 15/12/2016) ap. V

³⁶ Sentencia del 6 de octubre de 2011 [RJ/2011/7699].

³⁷ GONZALEZ GONZALEZ, Carlos, “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”. *Revista Aranzadi Doctrinal*, 2019, (núm. 4), p.9.

condiciones de respeto a su intimidad, truncando toda expectativa de confidencialidad o secreto en sus comunicaciones³⁸. Así, en la STC 170/2013 del 7 de octubre, no se entiende vulnerado el derecho al secreto de las comunicaciones por controlar el correo electrónico privado del trabajador, al haber incumplido una prohibición expresa del uso no laboral, entendiendo que esa prohibición lleva implícita la facultad de controlar su uso.

Esta doctrina se aplicó en nuestra jurisprudencia y en la del TEDH³⁹ que indicaba que “una empresa puede controlar los mensajes de sus trabajadores en un servicio de mensajería instantánea profesional a través de internet, siempre que previamente hubiera prohibido de modo expreso el uso de los medios de comunicación de la empresa para fines personales, en sintonía con la potestad disciplinaria de las empresas cuando el trabajador incumple la prohibición de uso personal establecido”⁴⁰.

Sin embargo actualmente la doctrina constitucional se ha visto modificada consecuencia del asunto *Barbulescu-II* de 5 de septiembre de 2017, dictada por el TEDH, que revoca el criterio seguido en el caso *Barbulescu-I* y anula la sentencia dictada indicando que “Es una vulneración del derecho a la intimidad y al secreto de las comunicaciones vigilar los mensajes enviados por un trabajador mediante medios propios de la empresa y acceder al contenido de los mismos, si no ha sido previamente informado de esta posibilidad, incluso existiendo normas en la empresa que prohíban su utilización para fines personales”⁴¹.

Por tanto, conforme a lo expuesto por diversos autores⁴² “la expectativa razonable de privacidad de los trabajadores está directamente relacionada con el nivel de detalle de información que, en su caso, el empleador haya puesto a disposición de sus trabajadores. Sin embargo, dicha información tampoco será suficiente si el empresario es incapaz de probar el conocimiento real y la aceptación expresa de aquella por parte de los trabajadores”.

Con todo ello, la doctrina actual establece que el trabajador tiene una “expectativa razonable de confidencialidad” en el uso, moderado y no con abuso, de los dispositivos electrónicos en el ámbito laboral, aun cuando tiene prohibición expresa para el uso privado de los mismos. El control que puede ejercer el empresario queda limitado por el derecho a la intimidad del trabajador, donde QUÍLEZ MORENO afirma;

³⁸ STC 170/2013 de 7 de octubre.

³⁹ STEDH del 12 de enero de 2016 (asunto *Barbulescu-I*).

⁴⁰ PURCALLA BONILLA, Miguel Á., Op. Cit., p.7.

⁴¹ *Ibídem*, p.7.

⁴² GARCÍA, Jesús D., BERMEJO, Reyes y PÉREZ, Alba, “Tecnología y control laboral”, *Actualidad Jurídica Uría Menéndez*, 2018, (núm. 48), p.153.

“una orden empresarial o una cláusula de un CC no tienen la fuerza necesaria para desvirtuar o modular derechos fundamentales tan significativos como la intimidad de las personas y, además, que la legitimación de acceso empresarial a las comunicaciones electrónicas del trabajador no puede ser ofrecida por una norma, instrucción, código, protocolo o artículo del convenio que simplemente vede el uso personal de las herramientas informáticas puestas a disposición del trabajador sino que es necesario que previamente la empresa haya informado a sus trabajadores, de forma exhaustiva, sobre los controles o mecanismos de inspección que se desarrollarán para fiscalizar el uso correcto y estrictamente profesional de los medios informáticos puestos a su disposición”⁴³.

Por tanto, para que el empresario pueda eliminar la “expectativa de confidencialidad” y controlar plenamente la actividad del empleado requerirá de dos premisas:

1. Que establezca unas reglas de uso correcto de los equipos informáticos clarificando las prohibiciones absolutas o parciales.
2. Que informe expresamente a los trabajadores de que su actividad va a ser fiscalizada para la comprobación de que se cumplen dichas reglas de uso y de las medidas que podrán ser adoptadas en su caso por el empleador.

A su vez, también podrá ser de aplicación otras medidas preventivas como la privación de determinadas conexiones.

Si estas medidas se cumplen, previsiblemente el empresario quedará facultado para comprobar el uso de los dispositivos, sin poder entenderse vulnerado el derecho a la intimidad y secreto de las comunicaciones del trabajador, al eliminar toda posible “expectativa razonable de intimidad”.

⁴³ QUÍLEZ MORENO, José M^a: “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*, 2019, (núm. 217), p.6.

IV. Sistemas de control tecnológico

Los dispositivos digitales que el empresario puede poner a disposición de los trabajadores y por los cuales puede llevar a cabo su fiscalización son muy diversos. Analizaremos a continuación los más significativos dando las pautas establecidas para que dichos controles sean considerados lícitos. Tal y como menciona PURCALLA, “existe jurisprudencia y doctrina judicial que ha abordado dicha cuestión hace ya años”⁴⁴.

Nos encontramos ante dos límites contrapuestos entre sí: por una parte, el límite al uso que establezca el empresario al uso extra laboral, por parte de los trabajadores, de las herramientas tecnológicas proporcionadas y, por otra parte, el límite marcado por los derechos fundamentales de los trabajadores al ejercer ese control de la prestación laboral.

El art. 87 de la LO 3/2018⁴⁵ viene a aclarar, en referencia a los equipos tecnológicos entregados para la prestación laboral, que el empresario deberá transmitir previamente a los trabajadores la información necesaria para que sepan con claridad qué pueden y qué no pueden hacer con ellos (en referencia al tiempo y forma de utilizarlos) y, además, estará legitimado para el control del uso e integridad de los mismos, preservando el derecho de protección de la intimidad de sus trabajadores.

15

4.1. Uso y control del teléfono empresarial

Para evitar el uso no laboral del teléfono corporativo por parte del trabajador (ya sea fijo o móvil) debe establecerse prohibición expresa, de lo contrario, por norma general, se entenderá que existe una tolerancia a su uso y, consecuentemente, no se podrá sancionar⁴⁶. Esta tolerancia entrará en juego siempre y cuando su uso extra laboral entre dentro de una facturación con tarifa plana y no suponga un sobre coste a la empresa, si bien un uso abusivo de llamadas o datos de internet sin autorización, que acarree un sobre coste notable, podría traducirse en una sanción disciplinaria de mayor o menor grado (e incluso llegar al despido disciplinario y que éste sea calificado como procedente⁴⁷ STSJ de Castilla y León del 22 de diciembre de 2017).

⁴⁴ PURCALLA BONILLA, Miguel Á., Op. Cit., p.4.

⁴⁵ LO 3/2018, de 5 de diciembre, art. 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.

⁴⁶ Como se menciona en la STSJ de Cataluña, de 16 de diciembre de 2016, “Sin prohibición expresa se entenderá permitido, ya que nos encontramos en una sociedad con un marcado hábito social arraigado a las TICs”

⁴⁷ PURCALLA BONILLA, Miguel Á., Op. Cit., p.4..

Otro asunto que difiere del tratado es el uso del teléfono *propio* del trabajador en su jornada laboral, lo que puede acarrear pérdidas de tiempo, repercutiendo directamente en el rendimiento del trabajador. No existe regulación laboral que establezca la prohibición de usar el teléfono móvil en el puesto de trabajo y, por tanto, se deberá estar a lo establecido por cada empresa. De existir tal prohibición y se necesitase hacer uso del mismo por una urgencia, lo conveniente sería pedir permiso para evitar una posible sanción. De no existir regulación interna, se presupone que existe una tolerancia a su uso de tal manera en que no interfiera a nuestro desarrollo de la actividad laboral.

Por otra parte, esa prohibición o limitación en el uso de los teléfonos móviles privados no se referirá a los descansos legalmente estipulados, sino que únicamente podrá prohibirse su uso en el cómputo de la jornada de trabajo efectiva.

El control que puede ejercer el empresario sobre el dispositivo que le ha facilitado al trabajador (no sobre el personal), estará avalado por los mismos principios que venimos comentando, a modo resumen:

- El empresario deberá de haber informado previamente al trabajador de cuáles son las prohibiciones que existen en cuanto al uso del móvil.
- Deberá de haber informado también de cuáles van a ser los controles que va a desarrollar sobre el aparato electrónico y cuál va a ser su alcance.

El control deberá adecuarse al principio de proporcionalidad en todo caso.

4.2. Uso y control del PC, portátil y correo empresarial

Con la STS del 26 de septiembre de 2007⁴⁸ el TS sentó doctrina respecto de que los dispositivos electrónicos puestos a disposición de los trabajadores no son considerados efectos personales y, por lo tanto, no le son de aplicación los preceptos del art. 18 del ET⁴⁹, sino que su control se regía por el art. 20.3 ET.⁵⁰

Por otra parte, no se entenderá vulnerado el “secreto de las comunicaciones” ni la intimidad del trabajador si el empresario en su control utiliza mecanismos menos intrusivos, como por ejemplo practicando una prueba pericial informática para no

⁴⁸ STS de 26 de septiembre de 2007, U.D. 966/2006 FD.2

⁴⁹ STSJ de Madrid del 30 de octubre de 2009 la cual indica que “...únicamente podrán registrarse efectos personales en caso de que el patrimonio empresarial y el resto de trabajadores necesiten protección, respetando la intimidad y dignidad del trabajador, dentro de la jornada laboral y ante un representante de los trabajadores si lo hay, y si no, ante otro compañero. La empresa actúa de este modo como un policía privado en defensa de su patrimonio, o el de sus trabajadores, ajeno a los poderes que le concede el art. 20 ET ...”

⁵⁰ PURCALLA BONILLA, Miguel Á., Op. Cit., p.5.

acceder a toda la información privada no necesaria, sino a detectar aspectos relevantes para la empresa, y con una causa concreta como pueda ser la obtención de una prueba para demostrar un incumplimiento del trabajador. Según expone PURCALLA “la técnica de búsqueda ciega por palabras clave (programa Encase Forensic- a modo de ejemplo, STSJ Andalucía-Sevilla 17/12/2007, rec.1050/2007) en los datos que quedan en el disco duro de un ordenador, consecuencia de las comunicaciones realizadas entre un trabajador y terceros, a efectos de demostrar una competencia desleal, debe ir de la mano de una *impecable cadena de custodia*, ...sin que dicha prueba constituya vulneración del secreto de comunicaciones”⁵¹ al tratarse de un método poco invasivo.

La prueba obtenida por “*hallazgo casual*” a raíz de un examen informático buscando confirmar una sospecha relacionada con otros indicios de algún incumplimiento, serán considerados lícitos en el ámbito laboral, si se ha cumplido con el resto de requerimientos⁵².

En este sentido cabe mencionar la STS del 8 de febrero de 2018⁵³ donde la empresa Inditex, tras el hallazgo casual de unas fotocopias de transferencias de un proveedor a favor de un trabajador, indicio de conducta contraria a la normativa de la empresa, se procede a examinar el correo de éste mediante un programa de búsqueda de palabras clave relevantes para así esclarecer los hechos. En la empresa existían directrices que prohibían el uso personal de los medios electrónicos e información de la posible fiscalización de los mismos. Finalmente, tras el análisis de la jurisprudencia del TC y TS, se establece que se han cumplido los requisitos establecidos y, a su vez, se constata que la doctrina nacional es coincidente con la del Alto Tribunal europeo tras el caso *Barbulescu II*. La sala desestima el recurso del trabajador y da plena validez procesal a la prueba de correo obtenida inadmitida en los anteriores pronunciamientos, ya que cumple *holgadamente* con los requisitos exigidos jurisprudencialmente establecidos.

El TEDH cambia la doctrina adoptada por el TC y el TS hasta el momento, marcando unas pautas a seguir a la hora de controlar el ordenador del trabajador y endureciendo los criterios y adoptando una postura más protectora con el trabajador y su derecho a la privacidad:

1. Será necesario “según el principio de transparencia” que el empresario haya informado con claridad y previamente de las medidas que van a usarse para su fiscalización y el alcance de las mismas (anteriormente bastaba con el previo aviso de que podía ser controlado).

⁵¹ *Ibidem*, p.6.

⁵² *Ibidem*.

⁵³ STS de 8 de febrero de 2018 (RJ 2018\666)

2. El empresario debe ponderar la proporcionalidad de las medidas adoptadas, con la intromisión que ha comportado su actuación y si existía otra medida menos intrusiva con la que alcanzar el mismo propósito, debiendo de haber optado por esta.
3. Debe acreditar un motivo por el cual se justifica su fiscalización.
4. El orden si altera el producto en este caso, puesto que requiere que la medida preceda al procedimiento sancionador y no a la inversa (lo que sería que tras la sanción se buscara el motivo para su justificación).

Previsiblemente, estas actuaciones impuestas por el TEDH referidas a la fiscalización y control de los ordenadores de los trabajadores serán extendidas al resto de controles que puede establecer el empresario con medios electrónicos.

Cabe destacar que la mencionada “expectativa razonable de confidencialidad” podría ser destruida por el mismo interlocutor a consecuencia de que permita conocer la “comunicación confidencial” a terceros ajenos a la misma como, por ejemplo, enviando mensajes privados desde un correo electrónico al que más compañeros tienen acceso o utilizar una aplicación de mensajería instalada en un ordenador de uso compartido, como pasa en la STC 241/2012 del 17 de diciembre, lo cual convertía la comunicación en abierta.

18

4.3. Videovigilancia y grabación de sonidos

La video vigilancia, consecuencia de tratar datos de carácter personal, deberá usarse restrictivamente y con adecuación a los mencionados principios de proporcionalidad. Se debe acudir primero a otros medios menos intrusivos a la intimidad para proteger, en la medida de lo posible, los derechos fundamentales de las personas. Para dar cumplimiento a la normativa dictada por la AEPD 1/2006⁵⁴, la instalación de cámaras de seguridad debe ser señalizada como “zona videovigilada” en lugar suficientemente visible e informar del tratamiento que se le van a dar a los datos obtenidos.

La aplicación de la videovigilancia en el ámbito laboral, usada por los empresarios para vigilar la seguridad del centro de trabajo respecto de terceros ajenos a él, también puede ser usada para controlar la actividad de los trabajadores, que se considerará lícito siempre y cuando sea una medida justificada e idónea para la consecución del fin buscado a demás de proporcionada. En ningún caso estará permitida la instalación de

⁵⁴ Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras art.3.a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados.

cámaras de vigilancia en zonas privadas tales como vestuarios o servicios, salvo su entrada y salida, que están consideradas como *zonas reservadas*⁵⁵.

El deber de información respecto de la instalación de las cámaras de videovigilancia genérica se establece en la pronunciación del TC en la STC 29/2013, de 11 de febrero, con el “deber de información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podría estar dirigida” y podrá instalarse por tiempo ilimitado. Adicionalmente deberá informar de la inclusión de los datos recabados en un fichero de datos de carácter personal y constatando de que dichas imágenes podrán usarse para constatar la comisión de un incumplimiento laboral. En cambio, la doctrina a aplicar en la videovigilancia por cámara oculta difiere de la genérica que, excepcionalmente, cuando existen sospechas fundadas de incumplimiento contractual por parte de algún trabajador, se permite su instalación por tiempo *limitado y localizado* (no a toda la plantilla ni ilimitadamente, sólo para la acreditación del incumplimiento⁵⁶) y, además, sin previa información al trabajador en tanto que no se lograría el fin buscado de existir la misma, según establece la STC 186/2000. Así mismo será necesario ponderar la medida con la aplicación del principio de proporcionalidad.

La prueba obtenida del uso de este medio sin existir ningún indicio de incumplimiento por parte de los trabajadores y empleado únicamente por decisión del empresario para controlar la actividad laboral, sin información previa a los trabajadores, se considerará ilícita, máxime si a demás la grabación también es sobre las conversaciones (STC 98/2000⁵⁷), ya que resulta más lesivo para el trabajador la grabación de sus “comentarios privados”, irrelevantes en la mayoría de los casos en la relación laboral, y consecuentemente no superaría el juicio de proporcionalidad. A estos efectos, la STSJ de Asturias del 22 de enero de 2019 indica que “la instalación de un sistema de grabación de esa naturaleza no queda a la conveniencia de la empresa ni puede justificarse sólo por la circunstancia de tener atribuida la facultad de dirección y control del cumplimiento del contrato de trabajo...”⁵⁸.

En referencia al “derecho a la intimidad y uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo”, regulado en el art. 89 de la LO 3/2018, se establece la exigencia de información previa, aunque en caso de grabar la “comisión

⁵⁵ PURCALLA BONILLA, Miguel Á., Op. Cit., p.9.

⁵⁶ Sentencia STEDH del 9 de enero de 2018, caso López Ribalda, donde se tenían sospechas razonables de infracción laboral, desconociendo qué trabajador era el responsable, actuación que estaba afectando gravemente a los intereses de la empresa, y no existiendo otros medios menos invasivos para conseguir probar los indicios, se grabó el puesto de caja con cámaras ocultas y en otros lugares por cámaras visibles, informando únicamente a los trabajadores de estas últimas.

⁵⁷ STC 98/2000 de 10 de abril – asunto Casino La Toja.

⁵⁸ PURCALLA BONILLA, Miguel Á., Op. Cit., p.10.

flagrante de un acto ilícito por los trabajadores [...] se entenderá cumplido el deber de informar cuando exista, al menos, el dispositivo informativo visible”⁵⁹. En cuanto a la grabación del sonido sólo podrán realizarse si se consideran suficientemente relevantes para salvaguardar las instalaciones, bienes y/o personas y siendo ponderada dicha medida con el principio de proporcionalidad e intervención mínima⁶⁰.

Para la conservación de los datos de sonido obtenidos se estará a lo dispuesto en el art. 22.3 de la mencionada ley; “Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación”⁶¹.

4.4. Aparatos de geolocalización

El sistema de posicionamiento global, o más conocido como GPS, que permite determinar la localización de cualquier objeto en cualquier lugar del mundo, es utilizado muchas veces por empresarios para controlar la prestación laboral de trabajadores en “movimiento” ya sea porque son transportistas, comerciales, u otros. Este sistema puede instalarse en el medio de transporte del trabajador (cualquier tipo de vehículo, por ejemplo en un tractor, STSJ de Galicia del 9 de septiembre de 2019, rec. 264/2019; en una aeronave de extinción de incendios, TSJ del País Vasco, del 21 de junio de 2019, rec. 959/2019⁶²), o incluso sobre el portátil, teléfono móvil o tablet facilitado por la empresa.

Esta constante localización del trabajador puede afectar a su derecho fundamental a la intimidad. El TEDH estableció, en la STEDH del 2 de septiembre de 2010, que el control vía GPS y la utilización de los datos obtenidos “supone una injerencia en el derecho a la vida privada de las personas”⁶³. A demás, los datos de localización del trabajador suponen datos de carácter personal, tal y como se especifica en el art. 4.1 del Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27/04/2016. En todo caso, someter al control laboral por este medio conllevará a aplicar el juicio de

⁵⁹ LO 3/2018, de 5 de diciembre, art. 89 Derecho a la intimidad frente al uso de dispositivos de videovigilancia de grabación de sonidos en el lugar de trabajo.

⁶⁰ PURCALLA BONILLA, Miguel Á., Op. Cit., p.11.

⁶¹ *Ibíd*em, P.11.

⁶² PURCALLA BONILLA, Miguel Á., en seminario sobre el despido laboral impartido en el Ilustre Colegio de Abogados de les Illes Balears, el 20 de noviembre de 2019.

⁶³ de los COBOS ORIHUEL, Francisco Pérez, “El derecho al respeto de la vida privada: Los retos digitales, una perspectiva de derecho comparado”, 2018, p.25.

proporcionalidad, ya que como hemos mencionado, supone una injerencia en los derechos fundamentales de los trabajadores⁶⁴.

En referencia a la utilización del sistema de geolocalización, la LO 3/2018 se pronuncia al respecto en su art. 90 diciendo que “con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión”⁶⁵, estipulando así la obligatoriedad de información previa a su instalación y al alcance de dicha medida de control.

No será necesario consentimiento previo del trabajador, al igual que en la videograbación, del tratamiento de sus datos personales, puesto que tal y como explica QUILEZ “dicho consentimiento se considerará otorgado con la relación laboral preexistente, siempre que el tratamiento de datos personales sea necesario para mantener el contrato laboral”⁶⁶. Dicho esto, si media previo aviso, se habrá cubierto el mandato legal, y si el trabajador incurre en un incumplimiento laboral podrá ser sancionado (STSJ de Asturias 3 del octubre de 2017, rec. 1908/2017⁶⁷; STSJ Comunidad Valenciana del 2 de mayo de 2017, rec. 3689/2016⁶⁸).

A demás, el art. 20. Bis del ET establece que “los trabajadores tienen derecho [...] a la desconexión digital⁶⁹ y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización...”⁷⁰. Este precepto actúa de límite infranqueable en cuanto al funcionamiento de los GPS, que obliga al empresario a que se asegure de que el dispositivo que instale para controlar al trabajador no deberá recopilar datos, ni estar en funcionamiento fuera de la jornada de trabajo. La facultad de control que le confiere el mencionado artículo acaba tras el cumplimiento del horario laboral, pues

⁶⁴ PURCALLA BONILLA, Miguel Á., en seminario...

⁶⁵ LO 3/2018, de 5 de diciembre, art. 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

⁶⁶ QUILEZ MORENO, José M^a, “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*, 2019, (núm.217), p. 8.

⁶⁷ Informado el trabajador, se declara procedente el despido de un comercial que incumplía con su jornada laboral, añadiendo visitas inexistentes al día de trabajo.

⁶⁸ No se considera que exista vulneración de derechos fundamentales si el trabajador es conocedor del mecanismo de control GPS utilizado.

⁶⁹ Configurado en el art. 88.1 de la LO 3/2018 “Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar”.

⁷⁰ Art. añadido al ET por la disposición final 13 de la LO 3/2018, de 5 de diciembre.

de constatarse lo contrario, la prueba obtenida por tales medios se tornará ilícita (salvo mediar consentimiento del trabajador para permitir su funcionamiento fuera de su jornada laboral⁷¹). Esto mismo ocurre en la STSJ de Madrid del 12 de julio de 2019 763/2019⁷², donde no se procedió a informar previamente de la instalación del GPS que, a su vez, reportaba datos de forma permanente las 24h del día. Esta invasión del empresario en cuanto a la intimidad del trabajador se dará, aunque dichos datos no hayan sido consultados.

4.5. Control de fichaje

Debido al incremento de la flexibilidad laboral en estos últimos años, es creciente el interés que le suscita al empresario controlar el cumplimiento de la jornada de trabajo por parte de los trabajadores, el cual tiene libertad de aplicar la medida que estime oportuna para hacerlo siempre y cuando dicho control y el tratamiento de los datos obtenidos cumpla con el deber de respeto y dignidad de los trabajadores⁷³. En este sentido sería excesivo, por ejemplo, el control del movimiento del trabajador en el centro de trabajo durante su jornada, ya que se consideraría desproporcionado para la finalidad buscada, que debiera ser controlar la puntualidad o ausencias laborales⁷⁴.

Si bien es cierto, este control horario también puede ser beneficioso para el trabajador, en cuanto a poder tener conocimiento certero de las horas que ha realizado y poder demostrar excesos de jornada en caso de desavenencia, ya que “la falta de registro hacía prácticamente imposible para el trabajador cumplir en juicio con la carga de probar las horas extraordinarias realizadas”⁷⁵.

Son muchos los empresarios que, con la entrada en vigor del art. 34.9 del ET en cuanto a la obligación de “Registro de jornada”⁷⁶ a toda empresa, han optado por establecer un mecanismo tecnológico de fichaje para sus trabajadores de control biométrico, mediante huella dactilar, reconocimiento facial, tarjeta de acceso, código personalizado u otros. La implantación de este mecanismo, que va a recoger unos datos personales los cuales “no expresan ningún aspecto concreto de la

⁷¹ PURCALLA BONILLA, Miguel Á., en seminario...

⁷² ARETA MARTINEZ, María, “Geolocalización de trabajadores asalariados y tutela de sus derechos fundamentales”, *Revista de Jurisprudencia Laboral*, 2020, (núm. 1), p.8.

⁷³ FERRER SERRANO, Roberto L., “El control horario del personal mediante utilización de sistemas de fichaje por huella dactilar”. 2019, p.2.

⁷⁴ *Ibidem*, p.3.

⁷⁵ LOUSADA AROCHENA, José F., “Registro y control de la jornada de trabajo”, *Revista Española de Derecho del Trabajo*, 2016, (núm.192), p.5.

⁷⁶ Consecuencia de la entrada en vigor del Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo. art. 10. Registro de jornada.

personalidad”⁷⁷, no es considerado como una intromisión a la privacidad del trabajador, tal y como afirma la STSJ de Canarias del 29 de mayo de 2012⁷⁸ “...La captación de imágenes o registros de distintas partes del cuerpo humano a efectos de identificación no es desconocida. Así, no se considera lesiva la fotografía del rostro o del cuerpo entero, se admite la toma de huellas digitales o del pie, el registro del iris o de la voz y hasta del mismo ADN en determinados supuestos”.

Esto no significa que no siga existiendo la obligatoriedad por parte de la empresa de informar a los trabajadores de que existe un registro de datos de carácter personal al que podrá tener acceso, así como su derecho a rectificación y cancelación⁷⁹.

Cabe señalar que en cualquier supuesto de control de los que hemos hablado durante estas páginas, en el que se acredite daño moral (cosa que irá de la mano con la acreditación de la vulneración del derecho fundamental), “irá aparejada de una indemnización por daños morales” y que, para fijar la cuantía, el art. 183.2 de la LRJS establece que “el tribunal se pronunciará sobre la cuantía del daño, determinándolo prudencialmente cuando la prueba de su importe exacto resulte demasiado difícil o costosa, para resarcir suficientemente a la víctima y restablecer a ésta, en la medida de lo posible...”⁸⁰.

⁷⁷ PURCALLA BONILLA, Miguel Á., Op. Cit., p.14.

⁷⁸ STSJ de Canarias del 29 de mayo de 2012.

⁷⁹ CCOO industria, “Límites al control empresarial y capacidad de intervención de la RLT ante el tratamiento de datos personales de los trabajadores y trabajadoras”.

⁸⁰ *Ibíd*em, p.10.

V. Conclusión

Como consecuencia de lo expuesto en estas páginas, las ideas principales son las siguientes.

La tecnología y su uso en el ámbito laboral ha traído consigo beneficios e inconvenientes; ha permitido aumentar la productividad y sumar eficiencia en los trabajadores pero, por el contrario, les ha capacitado para incurrir en incumplimiento de sus obligaciones laborales con su uso para fines privados, y a su vez ha facilitado al empresario nuevas formas de control.

Este control laboral por medio de las tecnologías va a resultar mucho más intrusivo, chocando, a veces, con los derechos a la privacidad de los trabajadores. Una de las partes deberá ceder: el derecho a controlar del empresario o el derecho a la privacidad del trabajador.

La escasa normativa existente ha desembocado en la creación de jurisprudencia para abordar la problemática, generando inseguridad jurídica, al ser poco uniforme en algunos de sus pronunciamientos.

Para ponderar si la situación de control llevada a cabo es legítima, los tribunales establecieron el principio de proporcionalidad, consistente en la superación de; el juicio de idoneidad, el juicio de necesidad y juicio de proporcionalidad en sentido estricto (triple test).

Se estableció también que, junto al triple test, también existe deber de información de uso permitido de los dispositivos facilitados, y además mediar preaviso de la fiscalización que se va a llevar a cabo, junto con la información clara de qué uso se le va a dar a los datos obtenidos.

La vigilancia masiva e indiscriminada será considerada desproporcional.

No será necesario el consentimiento del trabajador para la utilización de datos de carácter personal, que ya se considera otorgado en la relación contractual que les une.

Con la LO 3/2018 se unifica normativa existente, jurisprudencia consolidada y también el Reglamento UE 2016/679.

VI. Bibliografía

6.1. Libros y revistas

ARETA MARTINEZ, María, “Geolocalización de trabajadores asalariados y tutela de sus derechos fundamentales”, *Revista de Jurisprudencia Laboral*, 2020, (núm.1)

FERRER SERRANO, Roberto L., “El control horario del personal mediante utilización de sistemas de fichaje por huella dactilar”. *www.tirantonline.com*, 2019, (DocumentoTOL7.687.923)

GARCÍA SANCHEZ, Jesús D., BERMEJO BOSCH, Reyes y PÉREZ CANET, Alba, “Tecnología y control laboral”, *Actualidad Jurídica Uría Menéndez*, 2018, (núm.48), pp.150-153, ISSN1578-956X

GONZALEZ GONZALEZ, Carlos, “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”. *Revista Aranzadi Doctrinal*, 2019, (núm.4), ISSN1889-4380

LLAMOSAS TRAPAGA, Aida, *Relaciones laborales y nuevas tecnologías de la información y de la comunicación*, Madrid, Editorial Dykinson, 2015, ISBN: 978-84-9085-533-1

LLUCH CORELL, Francisco, “El secreto de las comunicaciones en la empresa: el control empresarial del correo electrónico que utiliza el trabajador”, *Revista de Jurisprudencia*, 2016 (núm.1512)

LOUSADA AROCHENA, José F., “Registro y control de la jornada de trabajo”, *Revista Española de Derecho del Trabajo*, 2016, (núm.192), BIB2016\85595

MORALES VÁLLEZ, CONCEPCIÓN E., “El control de los medios tecnológicos por el empresario a la luz de la sentencia del TEDH de 12 de enero de 2016”, *CEFGestión; Revista de actualización empresarial*, 2016 (núm.211), pp. 111-120. ISSN1139-4986

PURCALLA BONILLA, Miguel Á. “Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre”. *Revista española de Derecho del Trabajo*, 2019, (núm.218), BIB2019\2891

QUÍLEZ MORENO, José M^a, “La garantía de Derechos Digitales en el ámbito laboral: el nuevo art. 20 bis del Estatuto de los Trabajadores”, *Revista Española de Derecho del Trabajo*, 2019, (núm.217), BIB2019\1558

SAN MARTÍN MAZZUCCONI, Carolina, SEMPERE NAVARRO, Antonio V. “Sobre <Nuevas Tecnologías> y Relaciones Laborales” *Revista Doctrinal Aranzadi Social*, 2002, (núm. 15/2002) BIB2002\2021

SAN MARTÍN MAZZUCCONI, Carolina, SEMPERE NAVARRO, Antonio V. “Sobre el control empresarial de los ordenadores” *Revista Doctrinal Aranzadi Social*, 2012, (núm.3/2012), BIB2012\984

SELMA PENALVA, Alejandra, “Las peculiaridades prácticas del control en la empresa”, *Anales de Derecho*, 2009 (núm.27), pp. 92-130. ISSN1989-599

SERRANO GARCÍA, Juana M^a *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia*, ED. Bomarzo, 2019, Albacete. ISBN: 9788417310813

TASCÓN LOPEZ, Rodrigo. “El lento (pero firme) proceso de decantación de los límites del poder de control empresarial en la era tecnológica”. *Revista Doctrinal Aranzadi Social*, 2007 (num.17), BIB2007\3032

26

6.2. Blogs, webs y coloquios

CCOO industria, “Límites al control empresarial y capacidad de intervención de la RLT ante el tratamiento de datos personales de los trabajadores y trabajadoras”. <https://industria.ccoo.es/>, 2019 (última consulta 07/04/2020)

“Derecho a la intimidad de la persona trabajadora”, (<https://iberley.es>) <https://www.iberley.es/temas/derecho-intimidad-persona-trabajadora-64287>, 2020 (última consulta 12/03/2020)

De los COBOS ORIHUEL, Francisco Pérez, “El derecho al respeto de la vida privada: Los retos digitales, una perspectiva de derecho comparado”, <http://www.europarl.europa.eu/thinktank>, 2018, (Última consulta 27/03/2020)

PURCALLA BONILLA, Miguel Á., en seminario sobre el despido laboral impartido en el Ilustre Colegio de Abogados de les Illes Balears, el 20 de noviembre de 2019

SEMPERE NAVARRO, Antonio V. “Ponencia sobre la intimidad en el ámbito laboral a la luz de los últimos pronunciamientos judiciales nacionales e internacionales”, (<https://confilegal.com>) <https://confilegal.com/20180427-sempere-advierte-que-el-control-de-la-actividad-laboral-esta-sujeto-a-criterios-de-proporcionalidad-y-necesidad/>. 2018, (última consulta 05/04/2020)