Máster Universitario en Gestión de Personal y Práctica Laboral
Facultad de Ciencias del Trabajo
Universidad de León
Curso académico 2020/2021

DERECHOS DIGITALES DE LOS TRABAJADORES
(EMPLOYEES' DIGITAL RIGHTS)

Realizado por la alumna Dña. Inés García González

Tutorizado por la profesora Dña. Henar Álvarez Cuesta

ÍNDICE:

I. RESUMEN/ ABSTRACT

La promulgación de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales ha supuesto un antes y un después en la situación de los derechos digitales de los trabajadores, ya que con anterioridad a ésta no se encontraban regulados en el ordenamiento jurídico español, teniendo como único marco normativo los pronunciamientos de los tribunales españoles y europeos. Este Trabajo Fin de Máster se centra en analizar la interferencia que tiene el poder de control empresarial sobre los derechos fundamentales de los trabajadores, concretamente aquellas medidas de control tecnológico de la prestación laboral que afectan al derecho a la intimidad, al secreto de las comunicaciones y al derecho a la protección de datos personales. Se tratará el uso y control de los dispositivos digitales, la videovigilancia y grabación de sonidos, la geolocalización y el control biométrico. Además, se incluye un análisis de la situación jurídica actual del derecho a la desconexión digital, que debido al avance de las nuevas tecnologías ha cobrado especial importancia.

PALABRAS CLAVE: derechos digitales trabajadores, videovigilancia, control de dispositivos, geolocalización, control biométrico, desconexión digital, control tecnológico empresarial, derecho a la intimidad, derecho a la protección de datos personales.

The promulgation of the Organic Law 3/2018 on data protection and guarantee of digital rights has meant a before and after in the situation of employees' digital rights, since prior to this they were not regulated in the Spanish legal system, having the only regulatory framework is the pronouncements of the Spanish and European courts. This Master's Thesis focuses on analyzing the interference that the power of corporate control has on the fundamental rights of employees, specifically those measures of technological control of labor provision that affect the right to privacy, the secrecy of communications and to the right to the protection of personal data. The use and control of digital devices, video surveillance and sound recording, geolocation and biometric control will be discussed. In addition, an analysis of the current legal situation of the right to digital disconnection is included, which due to the advancement of new technologies has gained special importance.

KEY WORDS: employees' digital rights, video surveillance, device control, geolocation, biometric control, digital disconnection, business technology control, right to privacy, right to protection of personal data.

II. OBJETIVOS

El tema abordado es una materia de plena actualidad dada la evolución de las nuevas tecnologías y la necesidad de regular la interferencia de éstas en los derechos de los trabajadores. Con la realización de este Trabajo Final de Máster, se pretenden conseguir los siguientes objetivos:

- Obtener un conocimiento general de la situación jurídica en la actualidad en España respecto de los derechos digitales laborales; uso y control de los dispositivos, videovigilancia, geolocalización, control biométrico y desconexión digital.
- Analizar la situación jurídica anterior y posterior a la publicación de la LO 3/2018.
- Determinar el impacto práctico que ha supuesto esta ley con relación al reconocimiento de nuevos derechos digitales, los cuales no se encontraban regulados específicamente en nuestro ordenamiento.
- Delimitar los límites del control empresarial frente a los derechos fundamentales de los trabajadores.
- Observar la jurisprudencia existente sobre la materia.
- Determinar si la implantación de esta nueva ley ha tenido impacto en los convenios colectivos de diferentes sectores en España.
- Examinar cómo deben tratarse los datos personales de los trabajadores y cuáles son los principios que rigen para su tratamiento.

III. METODOLOGÍA

La realización de este trabajo de Fin de Máster se ha realizado gracias a la recopilación y revisión bibliográfica, de libros, artículos doctrinales, así como legislación y jurisprudencia relacionada con la materia. Se ha consultado desde bibliografía relacionada con derechos fundamentales clásicos, hasta material relativo a la evolución de los derechos digitales laborales.

En cuanto a la obtención de la información necesaria para realizar el mismo, se ha obtenido tanto en la Biblioteca de la Facultad de Derecho de la Universidad de León, como los recursos electrónicos facilitados por la misma, en especial la base de datos Aranzadi Digital.

Una vez realizada la recopilación, lectura y comprensión de las fuentes seleccionadas, se obtiene una visión general que ha permitido centrar el tema a tratar, diferenciando la materia en diferentes derechos digitales. Este trabajo se ha centrado en el estudio de una parte de la LO 3/2018, por lo que tras su lectura, se ha procedido a su interpretación y reflexión sobre la problemática que esta puede presentar. Se ha tenido en cuenta la fecha de publicación de la bibliografía utilizada para obtener un resultado de los objetivos del trabajo lo más actualizado posible.

En último lugar se procede a la elaboración de las conclusiones, que han sido fruto de la síntesis de cada apartado estudiado en el trabajo y la aplicación práctica de las novedades legislativas en los derechos digitales laborales.

IV. INTRODUCCIÓN: REGULACIÓN DE LOS DERECHOS DIGITALES EN EL TRABAJO

La digitalización de los procesos productivos ha conllevado la utilización por parte de los trabajadores de diferentes dispositivos digitales, equipos informáticos, canales de intercomunicación telemática, correos electrónicos, smartphones, etcétera. Estos dispositivos son susceptibles de ser empleados para uso personal o profesional.

El uso de las nuevas tecnologías en la empresa ha tenido grandes ventajas, pero también puede llegar a ser un inconveniente cuando los trabajadores hacen un uso indebido o excesivo de las mismas, provocando conflictos, y en ocasiones graves perjuicios para las empresas. Para evitarlo, las empresas quieren controlar el uso de los dispositivos facilitados a los trabajadores principalmente por las siguientes razones:

- Interfieren en la actividad del trabajador. Esto puede suponer una pérdida de tiempo de trabajo, que se puede traducir en una posible pérdida económica para la empresa.
- Problemas de seguridad por navegar en páginas webs poco seguras. Esto puede conllevar la intrusión de virus en los sistemas informáticos de la empresa y la consiguiente pérdida de datos.
- Transmisión de información confidencial. A través de correos electrónicos, o llamadas telefónicas, puede transmitirse información sensible que puede ocasionar daños a la reputación e imagen de la empresa.

Por estas razones, el art. 20.3 Real Decreto legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (en adelante, ET), reconoce al empresario la facultad de dirección y control de la actividad laboral, estableciendo que podrá adoptar las medidas que estime oportunas para vigilar y controlar el cumplimiento de las obligaciones laborales del trabajador.

Por otro lado, este control empresarial puede entrar en colisión con los derechos fundamentales de los trabajadores, como son el derecho a la intimidad y el secreto de las comunicaciones, reconocidos en el art. 18 de la Constitución Española, de 29 de diciembre de 1978 (en adelante, CE). También puede afectar al derecho a la protección de datos personales.

Según consolidada doctrina constitucional, la celebración de un contrato de trabajo no implica la privación de los derechos que la CE les reconoce a los trabajadores como ciudadanos, ni la empresa está legitimada para limitar de manera injustificada sus derechos fundamentales y libertades públicas[1]. Por lo tanto, el derecho del empresario de control de la actividad laboral de sus trabajadores no es ilimitado, si no que deberá llevarse a cabo siempre respetando los derechos fundamentales de los trabajadores.

Hasta hace relativamente poco tiempo, no existía una normativa legal específica que regulase los derechos digitales de los trabajadores, lo cual unido a que en la práctica no resultaba claro hasta dónde debía limitarse el derecho de control de actividad laboral del empresario en favor de los derechos fundamentales de los trabajadores, ha motivado numerosos conflictos laborales que han sido resueltos por los tribunales, dando lugar a la división de la doctrina durante muchos años[2].
Con el objeto de adaptar el ordenamiento jurídico español al Reglamento 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016 (en adelante RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de esos datos, y de garantizar los derechos digitales de

[1] RODRÍGUEZ ESCANCIANO, S.: *Derechos Laborales Digitales: Garantías e interrogantes*, Cizur Menor (Aranzadi), 2019, págs. 163 y 164.
[2] CAMAS RODA, F.: "La influencia del correo electrónico y de internet en el ámbito de las relaciones laborales", *Revista de Trabajo y Seguridad Social*, núm. 50, 2001, págs. 139 y ss.

los ciudadanos españoles con respeto al artículo 18.4 de la CE, se crea La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDyGDD), la cual introduce a los largo de sus arts. 87 a 90, contenidos en su título X, una regulación expresa de los derechos digitales de los trabajadores diferenciándolos por la modalidad de inspección digital que lleve a cabo el empleador. De tal forma que la norma diferencia el uso y control de dispositivos, la videovigilancia, la geolocalización y la desconexión digital.

En definitiva, esta nueva ley viene a tratar cuestiones hasta el momento no reguladas por el legislador, pero que sí han sido tratadas por los tribunales laborales, creando amplia jurisprudencia sobre el tema. Además, esta nueva norma deroga expresamente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y el Real Decreto-ley 5/2018, de 27 de julio, de medidas Urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

La regulación de estos derechos digitales por la LOPDyGDD, motivó la inclusión de un nuevo artículo en el ET, añadido por la disposición final 13 de la citada ley. Este nuevo artículo, 20 bis, situado en la sección 2ª de los Derechos y deberes derivados del contrato, titulado "los derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión", reconoce el derecho de los trabajadores a la intimidad en relación con el entorno digital, citando expresamente "el derecho a la intimidad en el uso de dispositivos digitales puestos a disposición del trabajador por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

Cabe destacar que toda esta regulación de derechos digitales es determinante y de vital importancia para las empresas, puesto que, si éstas obtienen pruebas de incumplimientos contractuales laborales de sus trabajadores, es esta ley la que aplicarán e interpretarán los tribunales para determinar si la prueba obtenida por estos medios es lícita o no, afectando de manera decisiva a los procesos que se sigan sobre estas materias en los tribunales sociales.

El preámbulo de la LOPDyGDD defiende la conveniencia de una futura reforma de la CE que incluya la actualización de la misma a la era digital, elevando a rango constitucional la nueva generación de derechos digitales, entendiendo que en este caso se han querido referir al derecho a la desconexión digital, puesto que como se indicará en su apartado correspondiente, no tiene rango de ley orgánica.

La importancia de la regulación de los derechos digitales ha aumentado con la llegada del Real Decreto-ley 28/2020, de 22 de septiembre de trabajo a distancia, debido a las características que definen este modo de trabajo, el cual se desarrolla principalmente mediante medios informáticos. Y en vista de la importancia de esta materia, la Agencia Española de protección de Datos, en adelante AEPD, publicó el 18 de mayo de 2021 una guía denominada "Protección de datos y relaciones laborales", con la finalidad de aportar una herramienta práctica a las empresas para cumplir de forma adecuada con la legislación en materia de protección de datos y derechos digitales laborales.

En este trabajo se analiza la situación previa y posterior a la LOPDyGDD en cada uno de los derechos digitales reconocidos por esta ley; uso y control de dispositivos, videovigilancia, geolocalización y desconexión digital, así como un apartado destinado al control biométrico y una breve introducción sobre cómo deben tratarse en el ámbito laboral los datos personales obtenidos por estos medios.

I. TRATAMIENTO DE DATOS PERSONALES EN EL ÁMBITO LABORAL

Todos los datos personales de los trabajadores, también los obtenidos por tecnologías digitales; imágenes, sonidos o datos biométricos, deben tratarse conforme a las exigencias legales. El RGPD incluye un reconocimiento de derecho de protección de datos personales a los trabajadores que incluye el derecho de acceso, de rectificación y de supresión de este tipo de datos. Estos derechos pueden ejercitarse frente al responsable del tratamiento de datos.

En primer lugar, el derecho de acceso, reconocido por el art. 15 RGPD, implica que los trabajadores tienen derecho a la confirmación de que se está realizando un tratamiento de

sus datos personales y que éstos tienen derecho a saber de que manera se esta produciendo este tratamiento. Los trabajadores podrán solicitar una copia de los datos personales que se están tratando.

En cuanto al derecho de rectificación, recogido por el art. 16 RGPD, significa que los trabajadores pueden exigir la rectificación de los datos erróneos que están siendo objeto de tratamiento, así como que se completen aquellos que sean incompletos.

Y finalmente el derecho de supresión, art. 17 RGPD, relativo a que los trabajadores podrán solicitar la eliminación de esos datos cuando ya no sean necesarios para los fines para los que fueron recogidos; cuando el trabajador retire su consentimiento al tratamiento de los datos, cuando este tratamiento sea ilícito o cuando éstos deban suprimirse por obligación legal. De tal forma que, por ejemplo, si finaliza la relación laboral, ya no existe base jurídica que justifique el mantenimiento del tratamiento de los datos personales de ese trabajador.

Una vez que se rectifique o se proceda a suprimir los datos personales, estos deben bloquearse, es decir deben reservarse para estar disponibles para jueces, tribunales, el Ministerio fiscal o las Administraciones Públicas, en caso de que surja algún proceso del que se puedan derivar responsabilidades por el tratamiento de esos datos. Los datos personales deberán bloquearse durante el periodo de duración del plazo de prescripción de las acciones que puedan derivarse de la responsabilidad indicada. Durante este periodo de bloqueo los datos no pueden modificarse, únicamente se permite la puesta a disposición de los datos a las autoridades competentes. Una vez que transcurra el plazo de prescripción, se debe proceder a la destrucción de los datos.

Para el tratamiento de datos personales de los trabajadores, exige el art. 5 del RGPD que se realice respetando el principio de minimización de datos, es decir, que por el hecho de que exista una relación laboral, no se admite que las empresas puedan conocer cualquier tipo de dato de los trabajadores, si no que los datos personales que se traten deben ser pertinentes y guardar relación con los fines para los que son obtenidos o tratados. Por ejemplo, las empresas tienen base jurídica para tratar los datos de afiliación a la Seguridad Social del trabajador, ya que son necesarios para elaborar el contrato de trabajo, pero no tienen base jurídica para tratar, por ejemplo, el nombre de usuario del trabajador en redes sociales, o datos relativos a su religión.

Además del principio de minimización de datos, rigen los principios de seguridad y secreto para el tratamiento de los datos. El art. 5 de la LOPDyGDD indica que los encargados del tratamiento de los datos deben estar sujetos al deber de confidencialidad y secreto profesional. Según la guía de la AEPD, para el adecuado cumplimiento de estos deberes es imprescindible contar con políticas de gestión de personal para distribuir las responsabilidades de la plantilla en función de su relación con el tratamiento de datos personales, así como formar a los profesionales que estarán en contacto con este tipo de datos sensibles, incluso advertir a los trabajadores que no tengan relación directa con los datos, pero que puedan poner en peligro el secreto o seguridad de los datos, como por ejemplo el personal de limpieza[3].

II. USO Y CONTROL DE DISPOSITIVOS:

Con el uso de las nuevas tecnologías en el ámbito laboral, los empleadores han puesto a disposición de los trabajadores diversos dispositivos digitales para que realicen el trabajo asignado, como ordenadores, smartphones y tablets. El uso de éstos ha ocasionado numerosos conflictos, y los empleadores han incluido nuevas formas de control de la actividad laboral adaptados a los dispositivos empleados por los trabajadores, como son la inspección de archivos, la intercepción de comunicaciones de mensajería instantánea o correos electrónicos, o el control de navegación por páginas web.

Toda esta actividad controladora por parte de la empresa puede llegar a lesionar los derechos fundamentales de los trabajadores tal y como se ha anticipado en el apartado anterior, el derecho a la intimidad, art. 18 CE, el derecho a la protección de datos o el secreto de las comunicaciones, art. 18.3 CE.

a) Situación previa a la LO 3/2018. Evolución de la doctrina

Con anterioridad a la publicación de la LOPDyGDD, debido a la inexistencia de regulación jurídica específica de la materia, las resoluciones de estos conflictos laborales se dejaban a la interpretación de los tribunales, que en ocasiones no seguían criterios uniformes, realizando incluso resoluciones contradictorias, e incrementando la

[3] AEPD: Guía "Protección de datos y relaciones laborales", 18 mayo, 2021, pág. 18.

inseguridad jurídica. Hasta la aparición de la LOPDyGDD se seguían los criterios de las resoluciones dictadas por la doctrina jurisprudencial, del Tribunal Constitucional (en adelante TC), el Tribunal Supremo (en adelante TS), el Tribunal de justicia de la Unión Europea (en adelante TJUE), e incluso las del Tribunal Europeo de Derechos Humanos (en adelante TEDH). Estos tribunales han asumido en cierto sentido una función legisladora al no existir una regulación específica en la materia[4].

Esta doctrina ha ido evolucionando, manifestando distintas posturas e intentando equilibrar los derechos fundamentales de los trabajadores con el derecho del art. 20.3 ET de control empresarial de la actividad laboral.

En primer lugar, mencionamos la teoría de la expectativa razonable de intimidad o confidencialidad, la cual a raíz de la STS de 26 de septiembre de 2007[5], sienta la base de que existe un hábito generalizado de los trabajadores de tolerancia al uso personal moderado de los medios informáticos facilitados por la empresa, y que esta situación genera por lo tanto una expectativa razonable de confidencialidad o intimidad para el trabajador. Por ello, si el empleador desea controlar el uso de los dispositivos, deberá crear protocolos, prohibiendo específicamente el uso de éstos para fines privados o personales, e informar a los trabajadores de que va a existir un control sobre los mismos. Si la empresa no informa debidamente al trabajador, puede llegar a considerarse como intromisión en la intimidad de éste.

Posteriormente el TC da un nuevo paso, estableciendo que se entenderá que no se vulnera el derecho a la intimidad de los trabajadores si se cumplen unos criterios de proporcionalidad, es decir que como requisito la medida de control que ejerza el empleador deberá ser proporcionada, idónea y necesaria sin que pueda existir otra menos agresiva contra los derechos fundamentales del trabajador. Se tiene que cumplir este triple juicio para que no se tenga en cuenta la expectativa razonable de intimidad.
Se consolida la doctrina con la STS de 6 de octubre de 2011[6], la cual expresa que no hay lesión del derecho a la intimidad por el control empresarial por existir una prohibición

[4] 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,* núm. 222, 2019, pág. 1.
[5] STS 26 septiembre 2007 (RJ 7514).
[6] STS 6 octubre 2011 (RJ 7699).

absoluta sobre el uso de medios de la empresa para fines personales, con independencia de la información que la empresa haya proporcionado a los trabajadores. De este modo, se favorece la posición empresarial y se devalúa la tesis del juicio de proporcionalidad, argumentando que si existe una prohibición expresa del uso de los dispositivos para uso personal o privado, se entenderá que decae la expectativa razonable de intimidad y el trabajador debe entender esto como una advertencia implícita del control del empleador sobre los dispositivos. Es decir, basta con que haya una prohibición absoluta del uso de los dispositivos para fines personales, para que se entienda que no se vulnera el derecho a la intimidad del trabajador. Esta posición casa mal con el art. 8.1 de la Carta Europea de Derechos Humanos, que reconoce el derecho de toda persona a la protección de datos de carácter personal[7]. La mera existencia de la prohibición del uso para fines personales, aunque no se haya informado debidamente a los trabajadores, legitima la vigilancia empresarial y no da garantías de confidencialidad a los trabajadores[8]. Esta tesis refuerza la posición de control del empresario en detrimento de los derechos de los trabajadores.
En relación a esto, es de ineludible mención en este apartado el famoso caso Barbulescu, en el cual un trabajador fue despedido por utilizar con fines personales un sistema de mensajería instantánea instalado en el ordenador de la empresa, controlando ésta el dispositivo sin previo aviso al trabajador, llegando además a difundir mensajes privados a terceras personas. El trabajador demandó a la empresa ante los Tribunales de su país (Rumania) por vulnerar sus derechos a la intimidad y al secreto de las comunicaciones, y éstos le negaron el amparo de estos derechos por considerar que la prohibición de uso de los dispositivos de la empresa para usos personales, legitima a la empresa para controlar la actividad laboral.

El trabajador planteó la demanda ante el TEDH, lo cual dio lugar a que se dictasen dos sentencias con pronunciamientos contradictorios. En la primera de ellas, de 12 de enero de 2016 conocida como Barbulescu I[9], se determinó que el trabajador no podía tener una expectativa razonable de intimidad puesto que existía en la empresa una normativa de prohibición del uso de los dispositivos para fines personales.

[7] RODRÍGUEZ ESCANCIANO, S.: *Derechos Laborales Digitales: Garantías e interrogantes*, Cizur Menor (Aranzadi), 2019, pág. 179.
[8] BLASCO JOVER, C.: "Trabajadores transparentes: la facultad fiscalizadora del empresario vs derechos fundamentales de los empleados", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Vol. 6, núm. 3, 2018, págs. 34 y 35.
[9] STEDH 12 enero 2016 (TEDH 1).

La segunda sentencia del TEDH sobre este caso, de fecha 5 de septiembre de 2017, conocida como Barbulescu II[10], se centra en argumentar que el trabajador no fue informado debidamente sobre la política de uso de los dispositivos de la empresa, ni del posible control sobre los mismos, y que por lo tanto para poder controlar el uso de los dispositivos es necesario que se atienda a los extremos contenidos en el siguiente test:

a) Debe valorarse si existió información previa y clara de las medidas de control, de su alcance y su puesta en práctica.

b) El grado de fiscalización empresarial y su extensión, tanto temporal como material.

c) Si existe un motivo legítimo que justifique la monitorización, al ser una medida invasiva.

d) Si concurren otras medidas menos intrusivas y más respetuosas con los derechos fundamentales del trabajador.

e) Qué uso les da el empresario a los datos obtenidos y si es legítimo para conseguir el objetivo que se pretenda.

f) Debe existir garantía para el trabajador, de tal modo que si se accede al contenido de sus comunicaciones debe haber sido previamente notificado. En virtud del principio de transparencia debe valorarse si la medida se ha realizado al inicio del procedimiento sancionador y no después[11].

La creación de este test de la sentencia Barbulescu II, constituye un importante avance en la materia, introduciendo unos cánones más estrictos a las empresas para controlar la actividad laboral por medio del control de los dispositivos electrónicos, y equilibrando los derechos entre trabajador y empresario. Se pasa de la teoría de expectativa de razonable confidencialidad, a otra en la que prima la transparencia, es decir, que la empresa comunique a los trabajadores porqué, cómo, cuándo y cuánto va a ejercer su derecho de control de la actividad laboral.

En este sentido, la doctrina del TEDH vuelve a recuperar el principio de proporcionalidad, aplicando controles más rigurosos de los que venían aplicando los tribunales españoles,

[10] STEDH 5 septiembre 2017 (TEDH 61).

[11] BLASCO JOVER, C.: "Trabajadores transparentes: la facultad fiscalizadora del empresario vs derechos fundamentales de los empleados", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Vol. 6, núm. 3, 2018, pág. 40.

y apostando por dar mayores garantías contra los abusos de los derechos fundamentales de los trabajadores.

b) Regulación jurídica actual

El derecho digital de uso y control de dispositivos está reconocido expresamente en el art. 87 de la LOPDyGDD, y lo regula con carácter de ley orgánica por ser una materia relativa al desarrollo de los derechos fundamentales. La finalidad de este artículo es la de establecer unas pautas para garantizar que la actuación de control empresarial del art. 20.3 ET sobre los dispositivos digitales que utilizan los trabajadores, no vulnera ni lesiona los derechos fundamentales de éstos.

El primer párrafo del artículo reconoce expresamente el derecho de los trabajadores y los empleados públicos a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador. Si los dispositivos son propiedad de los trabajadores, el empleador no puede tener ningún tipo de control sobre ellos.

En el segundo párrafo, se establecen cuáles son las únicas finalidades por las que el empleador podrá realizar el control de los dispositivos de los trabajadores, las cuales se limitarán a la vigilancia del cumplimiento de las obligaciones laborales o estatutarias y a garantizar la integridad de los dispositivos que se estén utilizando por el trabajador, es decir, para cuidar que los dispositivos propiedad de la empresa, no sufran desperfectos o daños por el uso inadecuado del trabajador. Por lo tanto, de este párrafo se deduce que, si el empleador accede a los dispositivos con otras finalidades o intenciones diferentes a éstas, se podría considerar vulneración del derecho de la intimidad del trabajador.

En el apartado número tres, se establece que los empleadores tienen que delimitar unos criterios de utilización de los dispositivos digitales e informar a los trabajadores sobre los mismos, para que éstos sean conscientes de los usos que están autorizados sobre esos dispositivos y cuándo podrán utilizarlos para fines privados o laborales. Además, indica que en la elaboración de los criterios de utilización deberán participar los representantes de los trabajadores.

Es importante destacar que el artículo cita que en aquellos casos en los que el empresario haya admitido el uso de los dispositivos con fines privados, se requerirá que se especifiquen cuáles son los usos permitidos y los periodos en los que podrán utilizarse, debiendo ser los trabajadores debidamente informados sobre estos criterios.

c) Criterios de uso de los dispositivos digitales

Para velar por el buen desarrollo de las relaciones laborales en las empresas, y tal y como establece el citado art. 87 de la LOPDyGDD, deviene necesario el establecimiento de unos criterios o normas de utilización de los dispositivos digitales facilitados a los trabajadores por parte de la empresa. Mediante estos criterios se establecerá qué actuaciones están permitidas, la finalidad de estas, la periodicidad, la regulación de acceso a servidores, el tratamiento de protección de datos, el régimen disciplinario derivado del incumplimiento del propio protocolo, etcétera.

La redacción del art. 87 LOPDyGDD es bastante general, no determina cómo deben establecerse esos criterios, y tal y como reza el art. 91 de la LOPDyGDD, se permite que los convenios colectivos podrán establecer garantías adicionales para salvaguardar los derechos digitales en el ámbito laboral. Por lo tanto, lo establecido en los convenios colectivos servirá para complementar lo indicado en la LOPDyGDD. Dependiendo del sector laboral de que se trate, se elaborarán los criterios de uso de los dispositivos más adecuados para cada sector concreto.

Por ejemplo, el XXIV Convenio colectivo del sector de la banca[12], incorpora un capítulo dedicado a la transformación digital y los derechos digitales, estableciendo en su art. 80.2 "Derecho a la intimidad y al uso de dispositivos digitales en el ámbito laboral", que las empresas en el supuesto de que permitan el uso privado de los dispositivos puestos a disposición de los trabajadores, deberán especificar mediante protocolos cuáles son los usos autorizados.

Otro ejemplo de ello es el Convenio colectivo de la industria del calzado[13], que además de lo indicado por la LOPDPyDD establece en su art. 72 "Nuevas tecnologías", que las

[12] XXIV Convenio colectivo del sector de la banca, 17 marzo 2021 (RCL 578).
[13] Convenio colectivo de la industria del calzado, 9 julio 2019 (RCL 1150).

empresas deben indicar de modo preciso los usos autorizados y que la información a los trabajadores deberá transmitirse de forma clara e inequívoca.

En el Convenio colectivo de la Industria de la alimentación de Granada[14], se incluye en el anexo X "Derechos derivados de la LO 3/2018. Desconexión digital y otros derechos", en su punto número 1 se cita expresamente que "las empresas deberán fijar los criterios de utilización de los dispositivos digitales a través de protocolos internos con la colaboración de los representantes de los trabajadores".

En resumen, se deduce que:
- Las empresas deberán crear políticas internas con protocolos de uso de los dispositivos digitales, conforme a lo establecido en la LOPDyGDD y a los convenios colectivos.
- En la elaboración de estos protocolos o políticas de uso de dispositivos digitales, deberán participar los representantes de los trabajadores.
- Los trabajadores deberán ser debidamente informados sobre estos criterios para que sea lícito efectuar medidas de control del uso de los dispositivos por parte del empleador.

Cualquiera que sea el medio que se utilice para la comunicación al trabajador de los criterios de utilización de los dispositivos, sería conveniente para la empresa obtener un justificante que acredite que esa información ha sido facilitada al trabajador para evitar que el empleado posteriormente pueda alegar su desconocimiento.

El incumplimiento por parte de las empresas de estas premisas, puede dar lugar a que se declare la vulneración de los derechos fundamentales de los trabajadores y que las pruebas obtenidas por medio del control de los dispositivos sean declaradas nulas en un futuro juicio.

Por último, indicar que será recomendable que estos protocolos de uso de dispositivos se actualicen de forma periódica, ya que debido al veloz avance de las nuevas tecnologías, pueden quedarse obsoletos con relativa facilidad.

[14] Convenio colectivo de la industria de la alimentación de Granada, 5 octubre 2020 (LEG 4176).

d) Control de dispositivos ante sospecha de conductas ilícitas.

Lo anteriormente expuesto y regulado por el art. 87 LOPDyGDD es aplicable a los controles ordinarios realizados por la empresa, sin embargo, en el citado artículo no se incluye nada sobre los controles extraordinarios "ad hoc", es decir, aquellos que se realizan en determinadas ocasiones, debido a la sospecha fundada de una conducta ilícita de un trabajador, como por ejemplo hurtos o acoso. Ante este tipo de situaciones se debe actuar con urgencia, y lógicamente este control "ad hoc" será más eficaz si es oculto, es decir, si el trabajador desconoce que se está realizando.

A diferencia del ámbito penal, en el que este tipo de controles requieren autorización judicial, en el ámbito social no está contemplado, por lo que los controles que se realicen "ad hoc" por existir sospechas fundadas de un incumplimiento laboral grave, tendrán que ajustarse a los criterios de ponderación; proporcionalidad, idoneidad, necesidad y justificación[15].

Esto no exime de tener que informar al trabajador sobre la existencia de ese control. Un ejemplo de ello es el caso de la STS de 23 de octubre de 2018[16], en la que se declara la nulidad de la prueba obtenida a través del examen del ordenador de un directivo ante sospechas de deslealtad, por no haber sido éste debidamente informado del control, a pesar de existir sospechas fundadas y que el examen del ordenador fuera una medida proporcionada y lo menos invasiva posible.

e) El uso de los dispositivos y el despido disciplinario.

En ocasiones el uso de los dispositivos digitales puestos a disposición del empleado, dan lugar a determinadas conductas de los trabajadores constitutivas de infracción grave del contrato laboral, dando lugar al despido disciplinario de éstos. Algunas de las conductas más repetidas por los trabajadores son la navegación por páginas web para fines personales o la interacción en redes sociales.

[15] RODRÍGUEZ ESCANCIANO, S.: *Derechos Laborales Digitales: Garantías e interrogantes*, Cizur Menor (Aranzadi), 2019, págs. 192 y 193.
[16] STS, Penal, 23 octubre 2018 (RJ 4937).

1) Navegación por páginas web.

Para determinar la gravedad de la conducta del trabajador, se deben analizar elementos relevantes circunstanciales, como, por ejemplo, el hecho de que la navegación por la web para fines personales sea una práctica habitual del trabajador, o, por el contrario se realice en una ocasión puntual. No revestirá la misma gravedad que el trabajador lo haga durante tres minutos o durante dos horas, que lo haga durante el tiempo de descanso o durante el tiempo efectivo de trabajo. Por lo tanto, si se despide al trabajador por navegar en un momento puntual, esto se consideraría como una falta leve y el eventual despido sería considerado como improcedente.

Además de atender a la proporcionalidad de la medida disciplinaria impuesta por el empresario al trabajador, es importante que la empresa haya establecido unas pautas previas sobre el uso de los dispositivos, de lo contrario el despido podría ser declarado improcedente como ha sucedido en numerosos casos[17].

2) Interacción en redes sociales.

De la misma forma que en el apartado anterior, será necesario atender a las circunstancias en las que se ha producido el hecho que ha motivado el despido del trabajador por la interacción en redes sociales. Hay que probar el tiempo de conexión efectivo del trabajador a la red social, ya que se han dado casos como el de la STSJ de Cataluña de 15 de diciembre, en el que se declaró la improcedencia de un despido por no acreditarse el tiempo de conexión del trabajador a una red social, ya que el tribunal consideró que tener abierto un chat durante cinco horas, no implica que se esté chateando de una manera continuada[18].

En cuanto a las manifestaciones vertidas por los trabajadores en las redes sociales, es importante señalar hasta dónde puede llegar la limitación de los derechos constitucionalmente reconocidos, como el derecho de libertad de expresión del trabajador, ya que el hecho de firmar un contrato de trabajo no implica renunciar a estos derechos[19]. El trabajador podrá hacer uso de dicho derecho siempre y cuando lo desarrolle

[17] STSJ Cataluña 6 abril 2018 (AS 1370). Se declara el despido improcedente de un trabajador, por la inexistencia de advertencia empresarial sobre los límites de utilización de los dispositivos digitales.
[18] STSJ Cataluña 15 diciembre 2014 (JUR 2015/38970).
[19] TALENS VISCONTI, E.E.: "La libertad de expresión de los sindicatos en las redes sociales", *Revista*

conforme a las exigencias de la buena fe, y no menoscabe los derechos de otras personas, ya sean físicas o jurídicas. Habrá que atender al contexto en el que se ha manifestado la expresión del trabajador, para determinar si puede catalogarse de leve o grave, ya que no es lo mismo infundir una simple crítica que proferir injurias sobre la empresa. También dependerá del número de seguidores de la red social del trabajador, ya que será más o menos perjudicial para la imagen de la empresa según la repercusión que tenga el comentario o publicación del trabajador en la red social[20].

La jurisprudencia suele considerar que las ofensas son menos graves si se transmiten de forma oral, ya que de forma escrita se presupone que el sujeto tiene más tiempo para pensar lo que escribe y, por tanto, se hace de forma premeditada. Pero en el caso de las ofensas vertidas en las redes sociales, éstas son en su mayoría escritas, y por lo tanto deberían ser consideradas más graves. Sin embargo, es importante destacar la inmediatez de las redes sociales y aplicaciones de mensajería instantánea, donde muchas veces se escribe sin pensar lo que se quiere decir realmente, y esto también puede llegar a que se interprete como falta leve. Además, este tipo de aplicaciones de mensajería instantánea reflejan el momento exacto en el que se han realizado, por lo que se podría interpretar por el tiempo en el que se ha hecho el comentario, si ha podido ir precedido de reflexión[21].

3) Pruebas tecnológicas de la transgresión de la buena fe.

En situaciones de incapacidad temporal, el contrato de trabajo se encuentra suspendido, pero no todas las obligaciones del trabajador se suspenden, ya que éste debe actuar conforme a la buena fe contractual.

En numerosas ocasiones, los trabajadores que se encuentran en situación de incapacidad temporal realizan tareas incompatibles con su recuperación o simulan esta incapacidad, a pesar de encontrarse en condiciones de desarrollar su actividad laboral, y torpemente dejan constancia de ello en sus redes sociales.

Aranzadi de Derecho y Nuevas Tecnologías, núm. 38, 2015, pág. 3.

[20] ANGULO GARZARO, A. y ANGULO GARZARO, N.: "Límites a las redes sociales como medio de expresión: la lesión al honor o a la imagen y el despido como consecuencias indeseables", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 43, 2017.

[21] NORES TORRES, L.E.: "Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales", *Revista de Información Laboral*, núm. 7, 2016, pág. 19.

Los empresarios han conseguido probar en muchos casos esta transgresión de la buena fe contractual a través de pruebas obtenidas en las redes sociales, como por ejemplo, el caso de una sentencia en la que los tribunales declararon procedente un despido disciplinario de una trabajadora que, durante su situación de incapacidad temporal, se fue de viaje con su familia, realizó fotografías durante el mismo, y las subió a las redes sociales[22]. En este caso se consideró que no se vulneraba el derecho a la intimidad de la trabajadora, ya que ésta tenía configurada su red social con carácter abierto, lo cual resulta determinante para valorar la legitimidad para obtener la prueba por parte de la empresa, puesto que de esta manera no se ve afectado el derecho a la intimidad, al dejar la propia trabajadora la red abierta al público y exponer ahí sus fotografías personales.

III. VIDEOVIGILANCIA Y GRABACIÓN DE SONIDOS

a) Situación previa a la LO 3/2018.

La instalación de cámaras de grabación de imágenes en los centros de trabajo está motivada fundamentalmente por razones de seguridad de los trabajadores, del centro de trabajo y/o de terceros. Sin embargo, también se utilizan para controlar el cumplimiento de las obligaciones de los trabajadores, siendo una medida del control empresarial legitimada por el artículo 20.3 del ET.

Estos controles, pueden afectar tanto al derecho a la intimidad de los trabajadores, como al derecho a la protección de datos personales, ya que, tanto las imágenes de los trabajadores como los sonidos, son considerados datos personales, y como tales, deben ser obtenidos, almacenados, registrados y suprimidos conforme a las exigencias legales.

Con anterioridad a la publicación de la LOPDyGDD, no existía una norma específica que regulara la forma de ejercer la vigilancia y control de las cámaras de videovigilancia. Ni si quiera la negociación colectiva llegó a alcanzar acuerdos que reemplazaran la falta de regulación de la materia[23]. Por lo tanto, la doctrina judicial acogió como guía para

[22] STSJ Andalucía/Sevilla 29 octubre 2015 (AS 2016/655).
[23] MOLINA NAVARRETE, C.: "El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente?", *Iuslabor*, núm. 3, 2017, pág. 290.

determinar la licitud de la medida de control por videovigilancia, el conocido y ya mencionado, principio de proporcionalidad elaborado por el TC, y la exigencia de información a los trabajadores sobre la existencia de la grabación de imágenes.

El principio de proporcionalidad exige que se debe atender a la idoneidad, necesidad y proporcionalidad de la medida empleada. Es decir, que el uso de las cámaras de grabación sea idóneo para conseguir el fin que se proponga la empresa, que no exista otra medida menos lesiva y eficaz, y que se deriven más beneficios que perjuicios con su aplicación[24]. Como ejemplo de ello, la STS de 7 de julio de 2016[25], la cual siguiendo el principio de proporcionalidad del TC, acepta como válida la prueba de videovigilancia obtenida en un establecimiento comercial que llevaba tiempo registrando falta de material, e instala cámaras de videovigilancia con carteles alertando de su existencia, para determinar si existían hurtos en el establecimiento por parte de los trabajadores. El TS en este caso, falla que se cumple el principio de proporcionalidad por considerar que la instalación de cámaras de videovigilancia son un medio idóneo, no existiendo otro más moderado e igual de eficaz, y del que se derivan más beneficios que perjuicios para el interés general. Además, se indica que los trabajadores habían sido informados de la existencia de cámaras de videovigilancia en el centro de trabajo, aunque no se especificara expresamente para qué fines se iban a utilizar esas imágenes.

Por lo tanto, podemos determinar que la tendencia de la doctrina era validar el uso de cámaras de grabación de imágenes, siempre que superase el principio de proporcionalidad y que se comunicase la existencia del circuito cerrado de televisión a los trabajadores, aunque no se indicase el fin que se le iba a dar a esas imágenes.

A raíz de la famosa sentencia del caso López Ribalda[26], se produce un cambio de tendencia en la doctrina. En este conocido caso, un supermercado estaba registrando descuadres de stock en su almacén, por lo que decidieron instalar cámaras de videovigilancia, algunas visibles, y otras ocultas en la zona de cajas del supermercado, informando a los trabajadores únicamente de la posición de las cámaras visibles. Las

[24] RODRÍGUEZ ESCANCIANO, S.: *Derechos Laborales Digitales: Garantías e interrogantes*, Cizur Menor (Aranzadi), 2019, pág. 210.
[25] STS 7 julio 2016 (RJ 4434).
[26] STEDH 9 enero 2018 (TEDH 1).

cámaras ocultas detectaron robos de varias trabajadoras, y la empresa despidió disciplinariamente a esas trabajadoras. Los tribunales españoles declararon estos despidos procedentes. Posteriormente fue recurrido ante el TEDH, quien en primera instancia determinó que se había producido vulneración al derecho de la intimidad de esas trabajadoras por no comunicar la existencia y el propósito para el que se habían instalado las videocámaras. Alega que las trabajadoras podían tener una expectativa razonable del respeto a la privacidad y considera que se vulneró el derecho a la intimidad de las mismas.

España recurre la sentencia del TEDH, y este falla en segunda instancia dando lugar a la sentencia denominada López Ribalda II[27], en la que finalmente se da un giro contrario a lo indicado en el pronunciamiento anterior y se considera que no se vulneró el derecho a la intimidad de las trabajadoras del supermercado, alegando en este caso que la zona donde se captaron las imágenes prueba de los robos, se realizaron en una zona abierta al público donde la expectativa de privacidad es menor, y que pocas personas tuvieron acceso a las imágenes, por lo que el impacto en la intimidad de las trabajadoras despedidas era muy limitado. Además, indica que si se hubiera notificado la existencia de las cámaras ocultas a las trabajadoras, no habría sido posible determinar quienes eran los responsables de los hurtos.

b) Regulación actual

1) Derecho a la intimidad frente al uso de dispositivos de videovigilancia

El derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, está regulado en el art. 89 de la LOPDyGDD. Su apartado número 1, expresa que "Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma

[27] STEDH 17 octubre 2019 (TEDH 144).

expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida".

Por lo tanto, de este primer apartado deducimos que es requisito indispensable la información previa, expresa, clara y concisa a los trabajadores o empleados públicos, de la utilización de este tipo de medida de control. De lo contrario, se considerará que la prueba obtenida por medio de videocámaras vulnera el derecho a la intimidad de los trabajadores y puede ser considerada ilícita, como sucedió por ejemplo en el caso de la STSJ de Madrid, de 23 de abril de 2018[28], en el cual la empresa no informó al trabajador de la existencia de cámaras de grabación.

A continuación, y dentro del punto número 1, se indica que en los supuestos en los que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o empleados públicos, se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de la LOPDyGDD, es decir, un dispositivo informativo colocado en lugar suficientemente visible identificando la existencia del tratamiento de datos. Esto se refiere a que en ocasiones la vigilancia a través de cámaras de seguridad se realiza con la finalidad de acreditar que ciertos trabajadores están incumpliendo sus obligaciones laborales cuando ya existen sospechas fundadas de que existe una conducta irregular del trabajador y que ésta puede ser constitutiva de falta grave de sus deberes contractuales laborales.

El segundo apartado del art. 89 LOPDyGDD, establece que no se admitirá en ningún caso la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, como son los vestuarios, aseos, comedores o zonas análogas. El motivo es obvio, ya que en estas zonas es donde más puede verse vulnerado el derecho a la intimidad de los trabajadores, ya que son zonas donde los trabajadores cambian su vestimenta para ponerse el uniforme, asearse, o relajarse, puesto que suelen ser lugares que los empleados utilizan en su tiempo de descanso, de inicio o final de su jornada laboral.

[28] STSJ Madrid 23 de abril de 2018 (AS 1299).

2) Derecho a la protección de datos de las imágenes

El art. 22.1 de la LOPDyGDD, permite que "las personas físicas o jurídicas, públicas o privadas, puedan llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones".

El segundo apartado del mismo artículo, indica que únicamente se podrán captar imágenes de la vía pública si es imprescindible para la seguridad de personas, bienes o instalaciones. Estableciendo como única excepción, la captación de la imagen de la vía pública en una extensión superior cuando sea necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte. Puntualiza también en este apartado, que no se podrá captar imágenes del interior de un domicilio privado en ningún caso.

En cuanto a la supresión de los datos registrados por las cámaras de videovigilancia, se indica en el tercer apartado del art. 22 LOPDyGDD, que deberán ser suprimidos en el plazo máximo de un mes desde su captación, "salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación".

En resumen, si una empresa quiere instalar cámaras de videovigilancia, debe informar debidamente a sus trabajadores de la existencia de instalación de las cámaras, así como de la existencia de un fichero con datos de carácter personal, ya que la imagen de una persona se considera dato personal. Asimismo, deben ser informados de la finalidad de las grabaciones, es decir, de que estas pueden ser utilizadas para justificar un incumplimiento por parte del trabajador de sus obligaciones laborales.

Si no existe información del tratamiento de los datos, la prueba obtenida de la grabación sería ilícita y el despido basado en la misma, sería nulo, tal y como sucedió por ejemplo

en el caso de la STSJ de Cataluña de 12 de julio de 2018[29], en el que no se informó a los trabajadores de la existencia de aparatos de grabación de imágenes.

c) Grabación de sonidos.

De la misma forma que la imagen se trata como dato personal, el sonido tiene la misma consideración, con la diferencia de que la grabación de una conversación puede ser incluso más sensible que la de la imagen, ya que las palabras revelan pensamientos y sentimientos que son más característicos de la esfera íntima y personal de una persona, en ocasiones más que la propia imagen.

El control por parte de la empresa de las conversaciones de los trabajadores afecta tanto al derecho a la intimidad, como al secreto de las comunicaciones reconocido por el art. 18.3 CE, y solo mediante autorización judicial se podrá interferir en estas comunicaciones. Según el TC[30], quien graba una conversación ajena, atenta al secreto de las comunicaciones, pero si se graba una conversación de la que se es parte, no afecta al secreto de las comunicaciones.

La LOPDyGDD en su art. 89.3, establece un marco jurídico para la utilización de grabación de sonidos por parte del empleador, estableciendo que la utilización de sistemas para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores.

Cabe mencionar en este apartado la famosa STC de 10 de abril de 2000[31], referida a la instalación de micrófonos por el Casino de La Toja. El TC declaró que se había producido la vulneración del derecho a la intimidad por instalar aparatos de grabación del sonido en el centro de trabajo, no siendo indispensable para la seguridad de la empresa. Destaca el TC en esa sentencia, que el uso de un sistema que permite la audición continuada e

[29] STSJ Cataluña 12 julio 2018 (JUR 281030).
[30] STCo, 175/2000, de 26 de junio.
[31] STC 10 de abril 2000 (RTC 98).

indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores, como de los clientes, constituye una actuación que excede de las facultades de control empresarial.

Como sucede con la grabación de las imágenes, los trabajadores deben ser informados de la existencia de la grabación de audio, de lo contrario, se entenderá vulnerado el derecho a la intimidad. Un ejemplo de ello es el caso de la STSJ de Castilla y León de 11 de abril de 2018[32], en el que la empresa instaló un sistema de grabación de imagen y sonido en el vehículo de la empresa que utilizaba el trabajador, sin previo aviso, ya que la empresa sospechaba que éste sustraía material propiedad de la entidad. Además, no de no haberse informado previamente al trabajador de la existencia de la existencia del sistema de grabación, se grabaron conversaciones privadas que éste mantuvo en el vehículo.

La última parte del art. 89.3 LOPDyGDD, alude a la supresión de los datos personales referidos a los sonidos grabados. Los empleadores tendrán un plazo máximo de un mes desde la captación de los sonidos, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En esos casos, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación. Estos plazos están recogidos en el art. 22.3 de la misma ley.

En resumen, serán aplicables los mismos criterios de proporcionalidad, idoneidad, necesidad y justificación, a la hora de realizar controles de sonidos en el puesto de trabajo de los empleados, y la exigencia de información previa a los trabajadores de la existencia de las grabaciones.

d) Aplicación en Convenios Colectivos

Siguiendo lo establecido por la LOPDyGDD, los nuevos convenios colectivos que se están suscribiendo a partir de la fecha de entrada en vigor de esta ley, ya reflejan lo recogido por la misma. Por ejemplo, en el caso de la videovigilancia, el XXIV Convenio

[32] STSJ Castilla y León/Valladolid 11 abril 2018 (AS 1211).

colectivo del sector de la banca[33]: en su artículo 80.3 establece expresamente que "para los casos de grabaciones de imágenes y sonidos, se procurarán establecer los medios necesarios para grabar aquellas imágenes y/o conversaciones consideradas como necesarias por la Empresa para garantizar la seguridad y/o la calidad de la actividad desarrollada en el centro de trabajo y/o la exigible cuando así sea requerido por la normativa legal en materia de protección de la clientela".

Otro ejemplo de ello es el III Convenio colectivo estatal de la industria, tecnología y los servicios del sector del metal[34], que en su artículo 117 relativo al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, establece que "el empresario deberá informar con carácter previo, y de forma expresa, clara y concisa, a las personas trabajadoras y, en su caso, a sus representantes, acerca de la instalación de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo". También recoge que en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores, se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo de información de videovigilancia. Incluye que en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso de los trabajadores, así como en vestuarios, aseos, comedores y análogos. Destaca que para la instalación de estos sistemas se respetará siempre el principio de proporcionalidad y de intervención mínima.

En definitiva, los nuevos convenios colectivos que recogen el reconocimiento de estos derechos digitales, vienen reproduciendo lo establecido en la LOPDyGDD.

IV. GEOLOCALIZACIÓN

a) Situación previa a la LO3/2018

En aquellos supuestos en los que la actividad laboral se desarrolla fuera de un centro de trabajo fijo, resulta más complicado ejercer el control empresarial sobre el desempeño de la actividad laboral. Esto puede favorecer que los trabajadores se relajen en el

[33] XXIV Convenio colectivo del sector de la banca, 17 marzo 2021 (RCL 578).
[34] III Convenio colectivo estatal de la industria, tecnología y los servicios del sector del metal, 11 diciembre 2019 (RCL 1835).

cumplimiento de sus obligaciones laborales al sentir que no están tan controlados durante su jornada laboral. Lo cual conlleva un aumento de infracciones contractuales laborales, como por ejemplo un incumplimiento del horario o la variación de itinerarios marcados. Por ello, para evitarlo, los empresarios han utilizado cada vez más, sistemas de geolocalización para ejercer el derecho de control empresarial del artículo 20.3 ET. El más habitual es el *Global Positioning System*, conocido como GPS, que permite localizar, en este caso a los trabajadores, en la ubicación concreta en la que se encuentren. Este sistema va acoplado a una red GSM[35]. Este sistema es especialmente útil si se trata de vehículos de empresa y en el caso de empresas del sector de transporte por carretera. Antes de la aparición de este famoso sistema de geolocalización, las empresas del sector de transportes sólo podían vigilar las circunstancias de los trayectos de sus vehículos mediante un tacógrafo, controlando las horas de circulación, parada, duración de los desplazamientos y velocidad, todo ello como consecuencia de una obligación legal impuesta por el Real Decreto 640/2007, de 18 de mayo[36]. La utilización del tacógrafo no muestra la posición del vehículo en el que se instala, por lo que el empleo de este sistema no ha implicado problemas de vulneración del derecho a la intimidad[37]. Sin embargo, la utilización del GPS si se considera que afecta al derecho a la intimidad, concretamente al derecho a que los demás no sepan dónde se está en cada momento, a no estar permanentemente localizado, ya sea por colocación de GPS en el vehículo, en el teléfono móvil, ordenador o tablet[38].

El avance de las nuevas tecnologías hace que cada vez existan más dispositivos relacionados con la geolocalización, como por ejemplo las pulseras rastreadoras creadas por la multinacional Amazon, quien registró la patente de un dispositivo colocado en la muñeca, capaz de rastrear en tiempo real a sus empleados en los almacenes de la empresa, que vibran cuando el empleado está cerca del artículo que busca dentro del almacén. A pesar de haber sido creadas presuntamente como una herramienta que potencie la eficiencia de las tareas del almacén, desde el punto de vista jurídico esto puede vulnerar

[35] *Global System for Mobile communications.* Servicio ofrecido por las empresas de telefonía móvil para determinar con cierta precisión la ubicación física de un terminal móvil.
[36] Real Decreto 640/2007, de 18 de mayo, por el que se establecen excepciones a la obligatoriedad de las normas sobre tiempos de conducción y descanso y el uso del tacógrafo en el transporte por carretera.
[37] RODRÍGUEZ ESCANCIANO, S.: *Derechos Laborales Digitales: Garantías e interrogantes*, Cizur Menor (Aranzadi), 2019, págs. 225 y 226.
[38] PURCALLA BONILLA, M.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*, núm. 218, 2019.

el derecho a la intimidad, y deberá ajustarse a la normativa sobre protección de datos, ya que según un informe de la Agencia Española de Protección de Datos[39], los datos de localización se consideran datos personales. Por el momento nuestros tribunales no han tenido ocasión de analizar medios de control similares a los que plantea la novedosa patente de las pulseras rastreadoras[40], pero sí que ha habido todo tipo de pronunciamientos.

Con anterioridad a la entrada en vigor de la LOPDyGDD, respecto al uso de los sistemas de geolocalización en el ámbito laboral, no se ha creado por el TS unificación de doctrina, sino que existen sentencias dictadas sobre todo por diferentes TSJ que defienden distintos argumentos. Unas abogan por requerir a las empresas que se informe al trabajador de la existencia de dispositivos de localización, y otras defienden que no es preciso ni el conocimiento, ni el consentimiento del trabajador de la existencia de colocación de dichos dispositivos.

En el primer caso, por ejemplo, la STSJ de la Comunidad Valenciana de 2 de mayo de 2017[41], en la cual el tribunal falla a favor del trabajador declarando como ilícita la prueba obtenida mediante sistema de geolocalización instalado en el vehículo comercial de la empresa sin previa información al trabajador de su existencia. Esta sentencia se apoya en el Dictamen 5/5005 de la UE, que establece el criterio de información al trabajador como una recomendación.

También ha habido sentencias con pronunciamiento opuesto al anterior, como es el caso de la STSJ de Galicia de 26 de abril de 2017[42], que igual que en el caso anterior se colocó un dispositivo de geolocalización en el vehículo de la empresa de un trabajador del sector comercial, sin informarle previamente de ello. En este caso el Tribunal considera que el uso de dispositivos GPS no se pueden considerar ilícitos, pues la empresa tiene un claro interés en tener localizados sus vehículos, lo que no incide en la violación de ningún derecho fundamental.

[39] Informe 0090/2009 AEPD.
[40] VIDAL LÓPEZ, P.: "`Black mirror´ya está aquí (o nuevas formas de control laboral), *Actualidad jurídica Aranzadi*, núm. 938, 2018.
[41] STSJ Comunidad Valenciana 2 mayo 2017 (JUR 221347).
[42] STSJ Galicia 26 abril 2017 (JUR 125997).

Además de la información al trabajador, otra circunstancia relevante es el límite temporal del control empresarial por medio de la geolocalización, es decir, durante cuanto tiempo se puede controlar la posición del trabajador. Lógicamente existen más pronunciamientos que defiendan la tesis de que cuando finaliza la jornada laboral, las facultades de control empresarial mediante GPS deben desaparecer, no pudiendo estar operativo este sistema durante vacaciones, días de descanso, o más allá del fin de la jornada laboral.

De la misma manera que ocurre con los otros derechos digitales tratados en los apartados anteriores, existe unanimidad en la premisa de que, para poder registrar este tipo de datos, también regirá el principio de proporcionalidad. Es decir, se exige que el registro de la localización física de los empleados sea proporcionado a la finalidad que lo motiva, es decir que esté relacionado con la actividad de la empresa y la prestación de servicios de la misma y que tenga una finalidad específica[43].

b) Regulación actual

Con la llegada de la LOPDyGDD, se establece un marco normativo para regular estas situaciones. El derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, está regulado en su art. 90, que en su primer apartado indica que "los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo".

En su segundo y último apartado, el art. 90 LOPDyGDD, establece 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."

Por lo tanto, se deduce que a partir de la entrada en vigor de esta ley es requisito indispensable informar de forma expresa y clara a los trabajadores de la existencia de

[43] VIDAL LÓPEZ, P.: "`Black mirror´ya está aquí (o nuevas formas de control laboral), *Actualidad jurídica Aranzadi*, núm. 938, 2018.

sistemas de geolocalización. De lo contrario, la prueba obtenida por medio de estos sistemas será declarada ilícita.

Finaliza el art. 90 aludiendo al derecho a la protección de datos obtenidos por sistemas de geolocalización. Expresamente se cita que "Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión."

c) Aplicación en Convenios Colectivos

Numerosos convenios colectivos de diferentes sectores vienen ya introduciendo en su articulado lo establecido por la LOPDyGDD con respecto a la geolocalización. Por ejemplo, el VIII Convenio Colectivo estatal del corcho[44], reconoce expresamente en su artículo 112 el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.

En el caso del Convenio colectivo del sector de la banca[45] se indica en su artículo 80.3, indica el control de la prestación laboral llevada a cabo por las nuevas tecnologías se realizará conforme a la legislación vigente, así como que estos controles deberán ser proporcionales a la finalidad de verificar el cumplimiento de las obligaciones laborales de los trabajadores.

En el sector de transportes, destaca en Convenio colectivo de la Agencia de Transportes Robles[46], que en su art. 48 dedicado a la geolocalización, videovigilancia y medios informáticos, indica que se realizarán controles sobre la ubicación física del trabajador mediante geolocalización pudiendo ser utilizados para fines disciplinarios. Indica también que estas medidas serán proporcionales y necesarias para la finalidad de verificar el cumplimiento por parte del trabajador de sus obligaciones laborales y que se debe respetar la dignidad y el derecho a la protección de datos de carácter personal, así como la vida privada de los trabajadores. Finaliza el art. Estableciendo que se debe cumplir el derecho de información al trabajador aun cuando no se requiere del consentimiento del trabajador.

[44] VIII Convenio colectivo estatal del corcho, 6 marzo 2020 (RCL 788).
[45] XXIV Convenio colectivo del sector de la banca, 17 marzo 2021 (RCL 578).
[46] Convenio colectivo de Agencia de Transportes Robles SA, 13 septiembre 2019 (LEG 9568).

El Convenio Colectivo del Sector de Comercio Vario, suscrito por la Confederación General de las Pequeñas y Medianas Empresas del Estado Español y por los sindicatos UGT y CCOO[47], en su art. 85 relativo al derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral, expresa que las empresas del sector únicamente podrán tratar los datos obtenidos por sistemas de geolocalización en ejercicio de función de control. Establece también la obligación de garantizar que los dispositivos de geolocalización implantados dejen de estar operativos a partir de la finalización de la jornada del trabajador, y que el trabajador debe conocer de forma clara e inequívoca la existencia y características de los dispositivos utilizados.

En definitiva, los acuerdos colectivos publicados hasta la fecha no completan la normativa introducida por la LOPDyGDD, si no que más bien se limitan a reproducir lo establecido por ésta.

V. REGISTRO HORARIO Y CONTROL BIOMÉTRICO

El control biométrico es una tecnología que permite identificar a los individuos mediante el reconocimiento de sus características únicas y singulares, como por ejemplo la huella dactilar, el rostro, la voz o la lectura de iris, entre otros. Este tipo de control es utilizado en las empresas para registrar las horas de entrada y salida de los trabajadores en el centro de trabajo, y por lo tanto, también pueden determinar su posición en tiempo y lugar determinados.

La implantación de este tipo de controles en las empresas ha aumentado debido a las exigencias legales introducidas por el Real Decreto Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, que en su artículo 10 sobre el registro de jornada incluye una modificación del artículo 34 del ET, añadiendo un nuevo apartado al mismo, con la siguiente redacción: "La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo." Esta

[47] Convenio Colectivo del Sector de Comercio Vario, 2 octubre 2019 (LCM 293).

exigencia legal se incluía desde 2013 para los trabajadores a tiempo parcial, y que con esta nueva ley se ha ampliado al resto de trabajadores.

El registro diario de la jornada de los trabajadores puede llevarse a cabo mediante tornos con sistema de control de presencia automático, firma manual de los trabajadores a la entrada y salida de su jornada indicando la fecha y hora en la que éstas se producen, etc. Sin embargo, la elevada fiabilidad de los controles biométricos hace que sean los más utilizados en las grandes empresas[48], ya que es más complicado que un empleado pueda suplantar la huella dactilar de otro, que la utilización de una simple firma manuscrita.

El dilema que plantea este tipo de controles es si puede llegar a afectar a los derechos fundamentales de los trabajadores, concretamente al derecho a la intimidad del art. 18 CE. Esto es debido a que en la fase de recopilación de la muestra biométrica es donde se muestran los datos que identifican al individuo concreto, por ejemplo, el iris de un trabajador, que puede por ejemplo revelar datos personales íntimos como el consumo de drogas, alcohol, o si la persona padece algún tipo de enfermedad como hipertensión o diabetes[49].

En general, los tribunales españoles coinciden en determinar que este tipo de controles no son invasivos para el derecho a la intimidad, ni para la esfera de la protección de datos, sirviendo de referencia la STS de 2 de julio de 2007[50], la cual establece además, que la finalidad del control del cumplimiento horario es legítima y que no es necesario obtener consentimiento previo de los trabajadores.

La AEPD en su guía publicada el 18 de mayo de 2021, recomienda que "los sistemas biométricos se basen en la lectura de este tipo de datos almacenados como plantillas cifradas en soportes que puedan ser conservados exclusivamente por las personas trabajadoras, por ejemplo, tarjetas inteligentes o dispositivos similares. Por ejemplo, en el caso del tratamiento de datos biométricos para el fichaje en el momento de acceso al edificio, se utilizarán por la persona trabajadora terminales en los que será necesario tanto

[48] GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J.R.: "El control biométrico de los trabajadores", *Revista de Información Laboral*, núm. 3, 2017.
[49] POQUET CATALÁ, R.: *El teletrabajo: análisis del nuevo marco jurídico*, Cizur Menor, (Aranzadi), 2020.
[50] STS, Cont.-Admtivo., 2 julio 2007 (RJ 6598).

la aproximación de la tarjeta como la lectura de la huella. Es decir, el lector generará el identificador numérico de la huella que habrá de corresponderse con el de la tarjeta, entendiéndose que se ha producido el acceso al puesto de trabajo como consecuencia de la coincidencia entre el identificador generado y el que consta en la huella[51]".

En esta misma guía introduce la AEPD, que los trabajadores itinerantes o trabajadores a distancia, realizarán su registro de jornada por geolocalización. En todo caso, la finalidad de este registro deberá ser el control de la jornada horaria, es decir, cuándo el trabajador inicia y finaliza su jornada y no determinar cuál es su posición. Debe ser un instrumento de comprobación del tiempo de trabajo y no del lugar en el que se desarrolle su actividad.

En cuanto a la licitud de la obtención de pruebas obtenidas mediante este tipo de controles la LOPDyGDD no incluye un apartado específico, sin embargo, hay pronunciamientos actuales de tribunales españoles que, siguiendo la línea de los anteriores derechos digitales tratados en este trabajo, aluden a la proporcionalidad y ponderación de la medida de control utilizada para determinar la licitud de la misma. Por ejemplo, la sentencia del Juzgado de lo Social de Barcelona de 1 de marzo de 2021[52], que determina que es válida la utilización del sistema de control de acceso de una empresa para acreditar una falta grave del trabajador, quien no fichaba correctamente su jornada laboral y descansos, llegando a superar 40 horas de tiempo no efectivo de trabajo durante la jornada durante tres meses consecutivos. La sentencia falla que no se produce vulneración de la intimidad personal ya que la incidencia en el derecho fundamental del trabajador es mínima, considera que se cumple el principio de proporcionalidad en el uso de datos personales, y en definitiva declara adecuada la suspensión de empleo y sueldo del empleado.

VI. DESCONEXIÓN DIGITAL

El avance de las nuevas tecnologías y la proliferación de dispositivos digitales, así como su integración en el día a día del trabajo de la mayoría de las empresas, ha provocado una "hiperconexión digital" que dificulta cada vez más la delimitación de lo que es tiempo de

[51] AEPD: Guía "Protección de datos y relaciones laborales", 18 mayo, 2021, pág. 31.
[52] SJS Barcelona, 1 marzo 2021 (núm. rec. 626/2019).

trabajo y tiempo de descanso[53]. Gracias a los nuevos sistemas de telecomunicaciones como las videoconferencias, las redes sociales, el correo electrónico, las aplicaciones de mensajería instantánea, las herramientas de negocio colaborativo online, etc., los trabajadores pueden recibir órdenes de los empresarios con mayor facilidad en cualquier momento de la semana o del día, incluso en algunos casos sin tener en cuenta el horario. Este tipo de herramientas, unidas al trabajo a distancia que permite que el trabajador realice sus tareas desde cualquier lugar y en ocasiones con jornadas horarias flexibles, pueden conllevar a una percepción errónea de disponibilidad horaria ilimitada del trabajador, y a que se cometan abusos por parte de los empresarios para que los trabajadores atiendan llamadas o mensajes en cualquier momento del día, dando lugar en ocasiones a ampliación del horario de trabajo, a una falta de conciliación laboral y familiar y en definitiva, a problemas de salud derivados de la falta de desconexión digital laboral, como por ejemplo tecnoestrés, degeneración visual o inflamaciones de articulaciones y tendones, entre otras[54].

a) Situación previa a la LO3/2018

Con anterioridad a la entrada en vigor de la LOPDyGDD, la desconexión laboral de los trabajadores estaba apoyada en el art. 40 CE, que establece que los poderes públicos promoverán fomentar políticas que garanticen el descanso necesario de la jornada laboral. También en el ET en su sección 5ª se regula el tiempo de trabajo, aludiendo en sus arts. 34 a 38 al régimen jurídico de la jornada laboral, incluyendo límites a los horarios con el reconocimiento de descansos diarios, semanales y anuales a los trabajadores.

Además, los tribunales españoles han dictado pronunciamientos judiciales que ya venían apoyando el derecho a la desconexión digital laboral colmando la laguna normativa existente en el ordenamiento jurídico español[55]. La primera sentencia sobre la desconexión digital se produjo por la Audiencia Nacional el 17 de julio de 1997[56], en la cual una empresa obligaba a sus trabajadores a mantener una conexión ininterrumpida de

[53] MARTÍN MUÑOZ, M.R.: "El derecho a la desconexión digital en España: un análisis de su regulación legal y convencional", *Revista Española de Derecho del Trabajo*, núm. 239, 2021.
[54] RODRÍGUEZ ESCANCIANO, S.: *Derechos Laborales Digitales: Garantías e interrogantes*, Cizur Menor (Aranzadi), 2019, pág. 242.
[55] TALENS VISCONTI, E.E.: "El derecho a la desconexión digital en el ámbito laboral", *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 17, 2019.
[56] SAN 17 julio 1997 (AS 3370).

sus teléfonos móviles con los de la empresa y sus clientes incluso cuando había finalizado la jornada laboral. El tribunal declaró que la empresa se había extralimitado en sus facultades organizativas y de dirección de la actividad laboral reconocidas por el art. 20 del ET.

Otro pronunciamiento destacable fue el de la STSJ Castilla y León de 3 de febrero de 2016, que expresa que "el respeto de los límites de jornada y descansos forma parte del derecho del trabajador a la protección de su seguridad y salud, que es responsabilidad del empresario, a partir de la obligada evaluación de riesgos y planificación de la actividad preventiva. Aunque el trabajador preste su trabajo en su domicilio corresponde a la empresa establecer las pautas necesarias sobre tiempo de trabajo para garantizar el cumplimiento de los límites de jornada y descansos"[57].

b) Regulación actual

La importancia de la regulación de este derecho ha aumentado con la implantación del teletrabajo como consecuencia de los confinamientos motivados por la pandemia del COVID-19. Tras esta situación de alerta sanitaria el legislativo español promulgó el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia, con el objetivo de regular esta modalidad de trabajo e incluyendo en su sección 5ª el art. 18, relativo al derecho a la desconexión digital. Sin embargo, esta nueva ley no ha aportado más que lo que ya se establecía en la LOPDyGDD.

El derecho a la desconexión digital en el ámbito laboral se encuentra reconocido por la LOPDyGDD en su art. 88, para cuya redacción el legislador español se inspiró en leyes europeas, una de la República francesa pionera en regular esta materia[58], y otra italiana[59], comienza expresando que "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". Los sujetos protegidos por este

[57] STSJ Castilla y León/Valladolid 3 febrero 2016 (AS 99).
[58] LOI nº 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels (JORF nº 0184 su 9 août 2016).
[59] Legge 22 maggio 2017, nº 81. Misure per la tutela del la- voro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato.

artículo serán todos los trabajadores incluidos los empleados públicos, y como se verá más adelante en su párrafo tercero, destaca a los directivos ya que suelen estar más expuestos a la conexión digital por las características de su puesto y la responsabilidad que éste conlleva.

En su segundo apartado, alude a que "las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores". Se refiere la primera parte de este párrafo a aquellas modalidades de trabajo en las que será aplicable este derecho a la desconexión, atendiendo por ejemplo a la flexibilidad horaria del puesto de trabajo o al sector productivo de que se trate, ya que por ejemplo una empresa tecnológica se verá más afectada por esta problemática que otra más tradicional. Sigue el párrafo indicando que se seguirá lo acordado entre la empresa y los representantes de los trabajadores, pero no especifica cómo se debe actuar en defecto de pacto colectivo o acuerdo entre empresa y representantes de los trabajadores.

En el tercer y último apartado del art. 88 se establece que "el empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas". La primera frase de este apartado indica que el empresario únicamente deberá informar a los representantes de los trabajadores, por lo que no establece que sea necesario un acuerdo entre empresa y representantes de los trabajadores, sobre la elaboración de políticas internas relativas a desconexión digital. De este apartado deducimos que las empresas deberán elaborar protocolos de actuación, igual que se ha visto con el derecho al uso y control de los dispositivos digitales facilitados por la empresa al trabajador, y este art. 88 deja en manos de la negociación colectiva y la política interna

de las empresas la introducción de normativa que regule este derecho de una manera más concreta.

Además, este art. 88 no incluye una definición legal de la desconexión digital y tampoco establece sanciones concretas para los empresarios en caso de vulneración de este derecho de los trabajadores, lo cual puede poner en duda la efectividad práctica de esta norma[60], y por lo tanto se entiende que se ha configurado esta materia como un derecho del trabajador, y no como un deber empresarial[61].

Finalmente concluimos que, a diferencia de los anteriores derechos digitales, la desconexión digital no tiene naturaleza de ley orgánica, puesto que no afecta a ningún derecho protegido constitucionalmente, como por ejemplo ocurre con el derecho a la intimidad en los anteriores derechos tratados en este trabajo. Esto se encuentra reconocido en la disposición final primera de la LOPDyGDD, relativa a la naturaleza de dicha ley, en la que se indica que el artículo 88 tiene carácter de ley ordinaria.

c) Aplicación en Convenios Colectivos

Antes de pasar a ejemplificar la aplicación de la LOPDyGDD en los convenios colectivos publicados a partir de su fecha de entrada en vigor, cabe destacar un precedente convencional y pionero en el reconocimiento de la desconexión digital en España, el Convenio colectivo del grupo AXA[62]. En este texto de la citada compañía de seguros se introduce un Capítulo III denominado organización del trabajo y nuevas tecnologías, donde se reconoce expresamente el derecho a la desconexión digital en su art. 14, incidiendo en la fina línea existente entre el tiempo de trabajo y descanso que ha sido acentuada por las nuevas tecnologías. En este art. 14 se indica expresamente "que las partes firmantes de este Convenio coinciden en la necesidad de impulsar el derecho a la desconexión digital una vez finalizada la jornada laboral. Consecuentemente, salvo causa de fuerza mayor o circunstancias excepcionales, AXA reconoce el derecho de los

[60] MARTÍN MUÑOZ, M.R.: "El derecho a la desconexión digital en España: un análisis de su regulación legal y convencional", *Revista Española de Derecho del Trabajo*, núm. 239, 2021.
[61] TALENS VISCONTI, E.E.: "El derecho a la desconexión digital en el ámbito laboral", *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 17, 2019.
[62] Convenio colectivo grupo AXA, 21 septiembre 2017 (LEG 10434).

trabajadores a no responder a los mails o mensajes profesionales fuera de su horario de trabajo".

Tras la fecha de publicación de la LOPDyGDD observamos algunos convenios colectivos que ya han introducido algunas medidas relativas a la desconexión digital, por ejemplo, el VIII Convenio colectivo de Iberdrola Grupo[63], que en su disposición final octava se compromete la empresa al cumplimiento de medidas de desconexión digital, destacando entre ellas; impulsar una cultura enfocada a resultados eliminando la cultura del presentismo, fomentar la racionalización del tiempo invertido en reuniones evitando convocarlas a partir de las 6 de la tarde, promover un uso eficiente y racional del e-mail y el teléfono corporativo no solicitando respuesta fuere de los horarios de trabajo, ni en tiempos de descanso, así como realización de campañas informativas para concienciar a los trabajadores sobre la necesidad de cumplir con el derecho a la desconexión digital fuera de las horas de trabajo.

Otro convenio que ha incluido en su art. 80.1 el derecho a la desconexión digital es el Convenio colectivo del sector de la banca[64], que acuerda algunas medidas como que las comunicaciones sobre asuntos profesionales se realizarán dentro de la jornada de trabajo y que los trabajadores tienen derecho a no responder a ninguna comunicación una vez finalizada su jornada laboral. Indica también que se procurará la adopción de medidas como la de programar respuestas automáticas durante los periodos de ausencia del trabajador indicando las fechas en las que no se estará disponible y designando el correo o datos de otra persona que le esté sustituyendo. Finalmente concluye el art. 80.1 de este convenio expresando que las empresas de este sector garantizarán que las personas que ejerzan el derecho a la desconexión digital no se verán afectadas por ningún tipo de sanción, ni se verán perjudicadas en las evaluaciones de desempeño o en sus posibilidades de promoción.

Por otro lado, hay empresas que han creado políticas internas estableciendo medidas a favor de la desconexión digital, por ejemplo, la empresa Telefónica[65], de la cual

[63] VIII Convenio colectivo Iberdrola Grupo, 18 febrero 2021 (LEG 982).
[64] XXIV Convenio colectivo del sector de la banca, 17 marzo 2021 (RCL 578).
[65] Anexo al Acuerdo Marco Internacional que tienen suscrito Telefónica, el sindicato Internacional UNI Global Union, así como las organizaciones sindicales españolas UGT y CCOO, con fecha 28 de enero de 2019, en el que se recogen los principios sobre el derecho a la desconexión aplicable a las operaciones globales de Telefónica.

destacamos que resalta que quienes tengan la responsabilidad sobre un equipo de personas deben cumplir especialmente las políticas de desconexión digital, debido a las características del puesto. También indica que los superiores jerárquicos se abstendrán de requerir respuesta en las comunicaciones enviadas fuera del horario laboral.

Tanto en esta política como en la de otras empresas y en varios convenios, también se establece que se excluirá la aplicación del derecho a la desconexión digital para aquellos trabajadores que deban permanecer a disposición de la empresa y que perciban por ello un complemento de disponibilidad, por ejemplo, las guardias. También se excluirá en aquellos casos de fuerza mayor que supongan un grave perjuicio para la empresa y que requieran respuesta inmediata.

En general la mayoría de los convenios colectivos publicados a partir de la LOPDyGDD reproducen lo indicado por su art. 88, sin aportar grandes novedades ni mecanismos concretos para garantizar efectivamente el ejercicio de este derecho.

VII. CONCLUSIONES

Del estudio de la materia tratada se sacan las siguientes conclusiones respecto a los derechos digitales de los trabajadores:

I- Los empleadores para poder adoptar una medida de control sobre la correcta prestación laboral de los trabajadores, deben someterla a un test de proporcionalidad, a través del cual se valorará si la medida de control aplicada por la empresa es idónea para conseguir el objetivo de control, si la medida es necesaria, sin que exista otra menos lesiva para los derechos de los trabajadores, y que ésta sea proporcionada, es decir que se deriven de ella más beneficios o ventajas para el interés general que perjuicios.

II- Además de respetar estos principios de actuación, los empleadores deben tener en cuenta el derecho a la protección de datos personales, siguiendo los principios básicos de información a los trabajadores sobre la existencia del tratamiento de los datos y el propósito del mismo, el principio de minimización, que implica recoger los datos estrictamente necesarios, y

siempre respetando los principios de seguridad y secreto.

III- En relación con el uso y control de los dispositivos digitales propiedad del empleador, para que no afecte al derecho a la intimidad de los trabajadores, se deben seguir las siguientes pautas:

- Deviene necesaria la elaboración por parte de la empresa de unos protocolos de uso, políticas internas o normas de utilización de los dispositivos
- Los trabajadores tienen que ser debidamente informados sobre los mismos.
- La finalidad para el control debe ser únicamente la del control del cumplimiento de las obligaciones laborales o de vigilar que los dispositivos no sufran desperfectos.

IV- En cuanto a la videovigilancia extraemos las siguientes conclusiones:

- Este tipo de medida de control sólo debe utilizarse cuando no exista otro medio igual de eficaz y menos lesivo para el derecho a la intimidad de los trabajadores.
- Se debe informar expresamente y con carácter previo sobre la implantación de esta medida de control.
- Cuando se realice un control extraordinario "ad hoc" captando la comisión flagrante de un acto ilítico, se entenderá cumplido el deber de informar cuando se haya colocado un dispositivo informativo perfectamente visible que indique la existencia del circuito de cámaras de videovigilancia.
- No se admite la instalación de cámaras de videovigilancia en lugares del centro de trabajo destinados al esparcimiento o descanso de los trabajadores, como vestuarios, aseos o comedores.
- En relación con la grabación de sonidos, únicamente se admite cuando se acredite que existe riesgo para la seguridad de las instalaciones, bienes y personas, y siempre respetando los principios ya indicados.

V- Si se emplea el control por geolocalización también se debe informar debidamente a los trabajadores de forma expresa y clara, y respetando los mismos principios de minimización y proporcionalidad de la medida y

tratamiento de los datos personales.

VI- Para los datos obtenidos por controles biométricos, regirán los mismos principios que para el resto, ponderación, proporcionalidad e información.

VII- Finalmente, del estudio del derecho a la desconexión digital deducimos que la nueva regulación legal del mismo no incluye sanciones, ni normas mínimas de aplicación en defecto de pacto, por lo que no aporta grandes novedades ya que los trabajadores ya tenían reconocido el derecho a no trabajar fuera de su jornada laboral según lo establecido en los arts. 34 y siguientes del ET. Es por ello por lo que el reconocimiento de este derecho por la LOPDyGDD parece tener más una finalidad preventiva de riesgos laborales que sancionadora o reguladora.

VIII- En cuanto a los Convenios colectivos, se ha observado que no han completado la regulación de la LOPDyGDD, si no que más bien se han inclinado por reproducir lo indicado por ésta, sin aportar novedades o soluciones prácticas.

IX- En conclusión, es posible que con la LOPDyGDD no baste para zanjar todos los posibles conflictos que puedan surgir por la interferencia de estas medidas de control sobre los derechos fundamentales de los trabajadores, pero sí que proporciona mayor seguridad jurídica a estos derechos que la situación anterior a esta regulación.

VIII. BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: "Protección de datos y relaciones laborales", 18 de mayo, 2021.

ANGULO GARZARO, A. y ANGULO GARZARO, N.: "Límites a las redes sociales como medio de expresión: la lesión al honor o a la imagen y el despido como consecuencias indeseables", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 43, 2017.

BLASCO JOVER, C.: "Trabajadores transparentes: la facultad fiscalizadora del empresario vs derechos fundamentales de los empleados", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Vol. 6, núm. 3, 2018.

CALVO MORALES, D. y TOSCANI GIMÉNEZ, D.: "El uso de internet y el correo electrónico en la empresa: límites y garantías", *REDT*, núm. 165, 2014.

CAMAS RODA, F.: "La influencia del correo electrónico y de internet en el ámbito de las relaciones laborales", *Revista de Trabajo y Seguridad Social*, núm. 50, 2001.

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,* núm. 222, 2019.

GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J.R.: "El control biométrico de los trabajadores", *Revista de Información Laboral*, núm. 3, 2017.

MARTÍN MUÑOZ, M.R.: "El derecho a la desconexión digital en España: un análisis de su regulación legal y convencional", *Revista Española de Derecho del Trabajo*, núm. 239, 2021.

MOLINA NAVARRETE, C.: "El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente?", *Iuslabor*, núm. 3, 2017.

NORES TORRES, L.E.: “Algunos puntos críticos sobre la repercusión de las redes sociales en el ámbito de las relaciones laborales”, *Revista de Información Laboral*, núm. 7, 2016.

POQUET CATALÁ, R.: El teletrabajo: análisis del nuevo marco jurídico, Cizur Menor, (Aranzadi), 2020.

PURCALLA BONILLA, M.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*, núm. 218, 2019.

QUÍLEZ MORENO, J.M.: “La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores”, *REDT*, núm. 217, 2019.

RODRÍGUEZ ESCANCIANO, S.: *Derechos Laborales Digitales: Garantías e interrogantes*, Cizur Menor (Aranzadi), 2019.

TALENS VISCONTI, E.E.: “El derecho a la desconexión digital en el ámbito laboral”, *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, núm. 17, 2019.

TALENS VISCONTI, E.E.: “La libertad de expresión de los sindicatos en las redes sociales”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 38, 2015.

VIDAL LÓPEZ, P.: “`Black mirror´ya está aquí (o nuevas formas de control laboral), *Actualidad jurídica Aranzadi*, núm. 938, 2018.