Editora responsável: Profa. Dra. Fayga Bedê
https://orcid.org/0000-0001-6444-2631

doi:10.12662/2447-6641oj.v22i41.p34-62.2024

Submetido: 7 fev. 2024
Aprovado: 25 nov. 2024

El Derecho Fundamental de Protección de Datos de los Trabajadores y el Impacto de las Nuevas Tecnologías en el Ámbito Laboral en España

The Fundamental Right of Data Protection of Workers and the Impact of New Technologies in the Workplace in Spain

Daniel Martínez Cristóbal*

RESUMEN

Objetivos: El objetivo de este trabajo es analizar los requisitos que ha de cumplir la empresa y los límites que tiene a la hora de ejercer su facultad de control a través de medios tecnológicos de acuerdo con la legislación y los criterios que ha establecido la jurisprudencia para tal fin, de manera que se respeten los derechos y garantías de los trabajadores.

Metodología: Se estudiarán las garantías del trabajador en relación con la implantación de las nuevas tecnologías en el ámbito laboral, y se delimitará la facultad de control y poder de dirección del empresario reconocida en el artículo 20 del Texto Refundido del Estatuto de los Trabajadores en lo referente a la protección de datos personales en el uso de nuevas tecnologías y dispositivos electrónicos en relación con el derecho a la intimidad.

Resultados: En el escenario actual de innovación tecnológica se ha producido un aumento de la manipulación y distribución de datos personales que se recaban a través del uso de dispositivos electrónicos y de internet, dando lugar a fenómenos como el *Big*

* Profesor en la Universidad Rey Juan Carlos. Licenciado en Derecho por la Universidad Complutense de Madrid, y Doctor en Derecho por la Universidad de Alcalá de Henares con mención Cum Laude. Autor de diversos artículos publicados en revistas de impacto, libros y capítulos de libro y colaboraciones. España. E-mail: <danielmcristobal@gmail.com>. ORCID: https://orcid.org/0000-0001-9754-5688.

Data, lo cual puede llevar a importantes problemas de privacidad.

Conclusiones: La aprobación del Reglamento General de Protección de Datos se traslada al ordenamiento jurídico español con la Ley Orgánica 3/2018 de Protección de Datos personales y Garantías de los Derechos Digitales, que desarrolla el artículo 18 de la Constitución Española y cuya incorporación más relevante es la salvaguarda de los derechos fundamentales a la intimidad y la protección de datos de los trabajadores en la aplicación de técnicas de control y vigilancia empresarial mediante nuevas tecnologías, para que de esta forma sea lícito el tratamiento de datos de los trabajadores.

Palabras clave: datos personales; nuevas tecnologías; intimidad; ámbito laboral; derechos digitales.

ABSTRACT

Objectives: The objective of this work is to analyze the requirements that the company must meet and the limits it has when exercising its power of control through technological means in accordance with the legislation and the criteria established by jurisprudence to for this purpose, so that the rights and guarantees of workers are respected.

Methodology: The worker's guarantees will be studied in relation to the implementation of new technologies in the workplace, and the employer's power of control and management power recognized in article 20 of the Workers' Statute will be delimited in relation to the protection of personal data in the use of new technologies and electronic devices in relation to the right to privacy.

Results: In the current scenario of technological innovation, there has been an increase in the manipulation and distribution of personal data that is collected using electronic devices and the Internet, giving rise to phenomena such as Big Data, which can lead to important privacy issues.

Conclusions: The approval of the General Data Protection Regulation is transferred to the Spanish legal system with Organic Law 3/2018 on the Protection of Personal Data and Guarantees of Digital Rights, which develops article 18 of the Spanish Constitution and whose most relevant incorporation It is the safeguarding of the fundamental rights to privacy and data protection of workers in the application of business control and surveillance techniques through new technologies, so that the processing of workers' data is legal.

Keywords: personal data; new technologies; privacy; workplace; digital rights.

1 INTRODUCCIÓN

En la actualidad, el uso de internet y dispositivos electrónicos se ha convertido en un medio imprescindible para realizar cualquier actividad, sea de índole social económica o concerniente a cualquier área de nuestras vidas, lo que genera una recogida constante y masiva de nuestros datos. A ello hay que añadir el riesgo que supone para la privacidad el uso de dispositivos inteligentes, ya que permiten a los proveedores de servicios de geolocalización recopilar información en base a nuestros movimientos, al igual que el

acceso a motores de búsqueda o sitios web se registran las direcciones IP o información a través de *cookies*, cuya función es almacenar información de la actividad de los usuarios (Goñi Sein, 2017, p. 23).

El Tribunal de Justicia de la Unión Europea (TJUE) se pronunció sobre la transmisión de datos personales a través de internet en un asunto donde una empresa alemana de comercio electrónico insertó en su página web el botón "me gusta" de Facebook Ireland, lo cual dio lugar a que se transmitieran datos de los visitantes de la web alemana a Facebook Ireland, independientemente de que aquellas personas que visitaban la web fueran miembros o no de esta red social, y sin que fueran conscientes de dicha transmisión de información. La STJUE Asunto C-40/17 FD 85 manifestó que el administrador de un sitio web, como responsable de las operaciones de tratamiento de quienes visitan su página de internet, tiene el deber de comunicar a los visitantes en el momento de la recogida de datos su identidad, fines de tratamiento y transmisión de información. Además, para que pueda justificarse la recogida y transmisión de datos personales, estas operaciones deben obedecer a una finalidad legítima (STJUE Asunto C-40/17 FD 95).

La implantación de las tecnologías de información y comunicación (TICS) ha dado lugar a profundos cambios en los modos de producción, encontrándonos un uso generalizado de aplicaciones y plataformas virtuales para el desempeño de cualquier acción. Esta es una realidad que también ha llegado al mundo laboral, dando lugar a nuevas formas de organización y producción del trabajo como el *crowdsourcing* (externalización masiva de tareas) o la economía de plataformas (Gómez Salado, 2019, p. 300).

Este impacto tecnológico se vio especialmente acentuado en 2020 con la pandemia por COVID-19, y obligó a muchas empresas y trabajadores a amoldarse a nuevas formas de desempeñar su actividad para seguir adelante como el teletrabajo, que hasta el momento era una modalidad poco regulada y conocida.

El escenario actual es la consecuencia de un gran crecimiento de la manipulación y distribución de datos personales que se recaban a través del uso de dispositivos electrónicos y de internet, dando lugar a fenómenos como el *Big Data*, lo cual puede llevar a importantes problemas de privacidad ya que funcionan a través de algoritmos, de tal forma que se produce un intercambio de datos a favor de terceros, creándose un rastro informático de las actividades que realizamos, y ello permite que se pueda elaborar un perfil detallado sobre cada persona conociendo sus hábitos o intereses (López Balaguer; Ramos Moragues, 2020, p. 508).

En este sentido, el control de una empresa o incluso de las Administraciones Públicas se puede establecer mediante sistemas de geolocalización, como ocurrió con la implantación de aplicaciones móviles para conocer la ubicación de los usuarios con motivo de la detección y prevención del COVID-19. De esta manera, las TICS se

convierten en un arma de doble filo, como herramientas útiles y eficaces en el desarrollo de la sociedad, pero que a su vez pueden generar un mayor control y vigilancia de cada persona gracias a la información y circulación de datos (Polo Roca, 2020, p. 52).

Por ello, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), en vigor desde el 25 de mayo de 2018, sustituyendo a la Directiva 95/46/CE, irrumpió con el objetivo de respaldar el derecho a la privacidad e intimidad sin perjuicio de la libre gestión de nuestros datos (González Biedma, 2017, p. 239). En el ámbito empresarial, el auge tecnológico ha causado un impacto importante en los modelos de negocio convirtiéndose en una herramienta básica e imprescindible para las empresas puesto que les ha permitido evolucionar en sus medios de organización y producción, incrementando así su eficiencia y competitividad en el mercado.

El uso de las TICS en las relaciones laborales aporta grandes beneficios y mejoras en cuanto al acceso a información y facilidades en la comunicación, favoreciendo la interconexión y la eficacia a la hora de desarrollar la prestación de servicios, permitiendo una gestión más eficiente a las empresas de los datos de sus clientes y trabajadores. Sin embargo, en contraposición, se produce una mayor cesión de datos personales de los trabajadores, los cuales a veces se aportan voluntariamente pero que en otras muchas ocasiones se hace de manera inconsciente. La recolección y gestión de datos de los trabajadores es inherente a toda organización empresarial y es lógico que se trate con información de carácter laboral como la supervisión en el desarrollo de la jornada, presencia en el centro de trabajo o, información relativa a los conocimientos y capacidades de cada trabajador, pero también con datos de índole más personal como el nombre, dirección o incluso datos sobre su salud.

Gracias a las nuevas tecnologías se pueden recopilar gran cantidad de datos de los trabajadores, de tal forma que las empresas pueden crear un perfil de sus empleados y determinar el rendimiento o el desarrollo de funciones. Pero esto puede injerir en la esfera privada del trabajador, e incluso puede llegar a vulnerar su dignidad y derechos fundamentales si la información obtenida por el empresario se usa de forma indebida. Además, otra desventaja para el trabajador es que las nuevas tecnologías le permiten estar en todo momento conectado, incluso más allá de su jornada de trabajo, por lo que es fácil que se difuminen los límites entre la actividad laboral y la vida personal (Goñi Sein, 2017, p. 27).

Es en este punto donde entra en juego la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales (LOPDP-GDD) que, por una parte, ha establecido los límites a la facultad de control empresarial de manera concreta en lo relativo al uso de medios tecnológicos en los artículos 87 a 91 y, por otra parte, ha introducido el artículo 20 *bis* del Texto Refundido del Estatuto de los Trabajadores (TRET) que reconoce el derecho a la intimidad de los trabajadores en el uso de los dispositivos digitales que les otorgue el empresario y en la utilización de sistemas

de videovigilancia y geolocalización así como el derecho a la desconexión digital. Además, este derecho también se reconoce en el artículo 14 j) bis del Estatuto Básico del Empleado Público, ley que también ha sido modificada por la actual.

En los últimos años se ha dado una importante confrontación en el ámbito laboral con la injerencia de las nuevas tecnologías entre el poder de dirección del empresario frente a los derechos de los trabajadores en cuanto a la intimidad y al secreto de las comunicaciones. La irrupción de las TICS en el entorno empresarial ha supuesto trasladar los medios de control a un nuevo plano virtual o digital con el tratamiento de datos personales de los trabajadores que inciden sobre su propia imagen, como los sistemas de videovigilancia con la instalación de cámaras en el centro de trabajo o la grabación de imágenes a través de webcam o circuitos cerrados de televisión.

Pero esta facultad de control digitalizada también se materializa a través de otros medios como la verificación de datos a través de controles biométricos como el uso de huella dactilar o el reconocimiento facial a raíz de la pandemia, controles sobre la ubicación geográfica del trabajador mediante la implantación de sistemas de geolocalización, o el control sobre los medios de trabajo como la monitorización del equipo informático del teletrabajador, control de dispositivos móviles o injerencia en el correo electrónico, lo cual supone un conflicto con el secreto a las comunicaciones establecido en el artículo 18.3 CE.

El 26 de abril de 2023, el Comité Europeo de Protección de Datos actualizó las Directrices 05/2022 publicadas en mayo 2022 en las que unificó el criterio de Autenticación y e Identificación que la Agencia Española de Protección de Datos (AEPD) había mantenido separado, uniendo a ambos dentro de la "categoría especial" para el tratamiento de datos. A pesar de la diferencia, el artículo 12 de esta Directriz establece que ambas se relacionan con el procesamiento de datos biométricos relacionados con una persona física identificada o identificable y, por lo tanto, constituyen un tratamiento de datos personales, y más concretamente un tratamiento de categorías especiales de información personal.

A consecuencia de esto, en noviembre de 2023 la AEPD publicó la "Guía Tratamientos de control de presencia mediante sistemas biométricos" y cambió su criterio respecto al uso de los sistemas de biometría para el control de acceso como método de entrada o control horario por parte de las empresas, ya que se considerarán sistemas prohibidos salvo que exista una circunstancia excepcional que justifique su uso antes que otros métodos que no usen datos de alto riesgo de protección.

En esta guía ya se especifica el carácter de "categoría especial" para este tipo de uso de los datos biométricos, y en sus capítulos IV y V se desvincula a esa forma de control de acceso su carácter imprescindible que obliga el RGPD y deja patente que es imposible superar el requisito de necesidad establecido para realizar estos tratamientos, aun contando con el consentimiento de los trabajadores. Al no poder cumplir estos criterios,

el reconocimiento de huella dactilar o facial queda declarado prohibido con carácter general, salvo en los escasos supuestos de interés público, sanitario, o de seguridad pública recogidos en el artículo 9 del RGPD.

Este nuevo escenario implica la necesidad de adoptar en la empresa las medidas adecuadas respetando la dignidad del trabajador y su esfera privada, puesto que la verificación por parte del empresario de la realización de la prestación de servicios a través de las TICS intensifica el control empresarial y puede suponer la vulneración de derechos fundamentales en el tratamientode sus datos personales. Con la nueva interpretación de la AEPD, debe sustituirse un sistema de registro de huella dactilar o reconocimiento facial por una persona que controle y verifique el acceso o cualquier otro sistema de que no implique el uso de sus datos biométricos. Su aplicación es inmediata, por lo que cualquier empresa que utilice este sistema de reconocimiento biométrico puede ser sancionada.

Por tanto, surge la necesidad de establecer una nueva perspectiva sobre la protección de la dignidad de las personas de posibles afectaciones ajenas en su esfera personal en cuanto al su derecho de protección de datos y su derecho a la autodeterminación informativa (Álvarez Del Cuvillo, 2020, p. 288). La ingente circulación de datos puede llegar a producir un tratamiento indebido de la información personal ocasionando importantes problemas en cuanto a seguridad y privacidad.

Esta problemática, surge en muchas ocasiones por un uso inadecuado de las nuevas tecnologías, pero no necesariamente de manera intencionada, sino que, por su carácter novedosoy en constante evolución, se desconoce como emplearlas adecuadamente sin que ello suponga traspasar la barrera de la privacidad o la intimidad. Esta cuestión, aplicada al ámbito laboral exige que empresarios y trabajadores tengan una formación adecuada sobre las TICS que les permita tener un conocimiento claro de su funcionalidad, no solo por sus ventajas en cuanto al aumento de la competitividad empresarial sino también, desde el punto de vista de protección de datos, para un uso adecuado de los medios tecnológicos sin que se produzcan intromisiones indebidas en aspectos personales irrelevantes en la relación laboral.

2 DERECHOS Y GARANTÍAS DIGITALES DE LOS TRABAJADORES

El RGPD supuso un cambio cualitativo en materia de tratamiento de datos personales en el ámbito laboral (González Biedma, 2017, p. 224), tanto en el Considerando 155 como en el artículo 88 que especifica la necesidad de regular las condiciones en que puede realizarse el tratamiento de datos personales de los trabajadores en las distintas facetas de la relación laboral, desde la contratación, la ejecución del contrato de trabajo, hasta su rescisión, teniendo en cuenta su aplicación en materia de prevención de riesgos laborales y en el desarrollo de derechos individuales y colectivos de los trabajadores derivados de la relación contractual, teniendo presente que no es

necesario el consentimiento del trabajador cuando queda justificado el tratamiento de sus datos personales en el desempeño de la prestación de servicios (Blázquez Agudo, 2018, p. 140).

En España, la LOPDP-GDD reconoció un nuevo marco regulador sobre el ejercicio de derechos fundamentales en el contexto de las nuevas tecnologías. El Título X sobre Garantías de los Derechos Digitales, fijó el límite a la utilización de los medios informáticos para garantizar el honor y la intimidad personal y familiar de todos los individuos y el efectivo ejercicio de sus derechos estipulado en el artículo 18 de la Constitución Española (CE), centrándose en las situaciones que más discrepancias han generado, como el acceso al correo electrónico, el registro del ordenador o cualquier otro dispositivo propiedad de la empresa, pero en posesión del trabajador o los sistemas de control audiovisual.

Antes de la entrada en vigor de la LOPDP-GDD, el artículo 20.3 TRET dejaba la puerta abierta a posibles injerencias en la privacidad de los trabajadores ya que permitía al empresario adoptar las medidas de control y vigilancia que considerase oportunas sin que se estableciera ningún límite o concreción de forma clara salvo el respeto a la dignidad personal y la consideración de la capacidad de los trabajadores discapacitados. Con la promulgación de la LOPDP-GDD se subsanó la falta de limitación al poder de control empresarial, aunque la continua evolución de las nuevas tecnologías evidencia que la ley no abarca todos los posibles escenarios en los que puede verse afectado el derecho de protección de datos de los trabajadores en el ámbito de la empresa y es aquí donde debe entrar en juego la negociación colectiva estipulada en el artículo 91 LOPDP-GDD. Se encomienda así a las necesidades de las empresas para delimitar y racionalizar los poderes empresariales, así como el establecimiento de pautas a seguir en otras posibles situaciones distintas a las establecidas en los artículos 87 y ss. (Baz Rodríguez, 2019, p. 135).

2.1 DERECHO A LA INTIMIDAD Y AL USO DE DISPOSITIVOS ELECTRÓNICOS

El artículo 87.1 LOPDP-GDD establece que los trabajadores tendrán derecho a la intimidad en la utilización de los dispositivos digitales que el empresario ponga a su disposición. La STS 6128/2007 en el FD 2 manifiesta que el uso de medios electrónicos o informáticos que la empresa entrega a sus empleados para el desempeño de la actividad laboral puede dar lugar a conflictos que afecten a su intimidad en la navegación por internet, en el acceso a archivos personales en el ordenador y el uso del correo electrónico, en cuyo caso puede verse afectado también el derecho al secreto de las comunicaciones.

Dicho artículo supone una plasmación en el ámbito laboral del artículo 18.1 CE, que va a poder modularse o limitarse en virtud del interés legítimo del empresario, siempre que ello resulte imprescindible y estableciéndose las debidas garantías para los trabajadores. La STC 186/2000 en el FJ 5 manifestó que el derecho a la intimidad no es

absoluto y puede ceder ante intereses constitucionalmente relevantes, como la libertad de empresa (artículo 38 CE) o la propiedad privada (artículo 33 CE), siempre que su limitación sea necesaria y proporcionada para la consecución del fin legítimo que se pretende. Además, reconoce que el poder de dirección del empresario recogido en el artículo 20 TRET permite a éste adoptar las medidas que considere más oportunas para velar por el correcto desenvolvimiento de la actividad productiva y el cumplimiento de las obligaciones laborales de los trabajadores sin que ello pueda suponer en ningún caso una lesión de derechos fundamentales del trabajador.

No obstante, el uso de las TICS abre la puerta a que el empresario pueda establecer medidas de control y vigilancia de la actividad laboral cada vez más incisivas. La existencia de esta potestad empresarial no justifica por sí sola el hecho de injerir en la privacidad del trabajador, y resulta necesario que dichas medidas de control se sometan a un análisis de compatibilidad, previamente a su implantación, con los principios recogidos en el artículo 5 RGPD.

Es imprescindible delimitar que los datos de los trabajadores obtenidos mediante la supervisión de los dispositivos digitales se vayan a tratar de manera lícita, transparente y limitada a la finalidad de control laboral, y que para su tratamiento se apliquen los principios de minimización de datos, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva (Baz Rodríguez, 2019, p. 140).

2.1.1 La licitud del acceso del empresario a los medios digitales a disposición de los trabajadores

Las bases jurídicas de la licitud tratamiento de datos derivados del uso de medios tecnológicos vienen delimitadas en el artículo 87.2 LOPDP-GDD, que establece controlar el cumplimiento de obligaciones laborales y garantizar la integridad de los dispositivos digitales puestos a disposición de los trabajadores como las únicas posibilidades para el empleador de acceder a estos dispositivos.

La supervisión del debido cumplimiento de las obligaciones laborales constituye una medida necesaria para la ejecución de un contrato de trabajo, por lo que se estaría dando cumplimiento al artículo 6.1 b) RGPD para el tratamiento lícito de datos, mientras que la protección de las herramientas electrónicas o digitales de la empresa y la seguridad de red informática empresarial suponen un interés legítimo de acuerdo con el artículo 6.1 f) RGPD.

Esta delimitación contenida en el artículo 87.2 LOPDP-GDD obstaculiza el tratamiento posterior de los datos extraídos a través de los dispositivos digitales para finalidades distintas de las que el precepto establece en virtud del artículo 6.4 RGPD, ya que no es admisible reutilizar los datos obtenidos más allá del objetivo de control empresarial que justificaba el acceso a estas herramientas de trabajo, por lo que la licitud

del tratamiento queda condicionada exclusivamente a los fines determinados en dicho artículo.

Ambas bases de licitud constituyen dos presupuestos de actuación autónomos, independientes el uno del otro, por lo que las medidas destinadas a la protección de los equipos informáticos de la empresa no pueden exceder de esta finalidad y de ningún modo sepueden emplear para vigilar a los trabajadores o comprobar su rendimiento. De esta forma, en el caso de implantarse medidas de monitorización para garantizar la seguridad de los equipos informáticos y de los datos manejados a través de estos, estas medidas no pueden tener como consecuencia un estado de vigilancia permanente y absoluto de la actividad en línea de los trabajadores salvo que no exista posibilidad alguna que sea menos invasiva para tal objetivo, cumpliendo así el principio de limitación de la finalidad establecido en el artículo 5.1 b) RGPD.

En ningún caso el consentimiento del interesado puede ser una vía de licitud para el tratamiento de sus datos obtenidos de medios tecnológicos de la empresa, como la autorización del trabajador para la instalación de un programa espía en su ordenador de trabajo. Antes de proceder al acceso a los dispositivos digitales con fines de control laboral, es necesario realizar una evaluación previa a la implantación de esta medida para comprobar que realmente es imprescindible para la verificación del cumplimientode la actividad productiva, y es preciso también que se haya descartado la posibilidad de una acción supervisora menos intrusiva en la privacidad del trabajador que permita alcanzar el mismo objetivo.

La obligación de transparencia para el empresario implica el deber de informar a los trabajadores con carácter previo y de manera completa sobre la categoría de datos que pueden ser tratados, formas de control sobre los datos registrados, finalidad de la medida de vigilancia, destinatarios o categorías de destinatarios de la información que se recoja, utilización de estos datos, existencia de posibles copias de seguridad o archivos de datos y vías de ejercicio de sus derechos.

Esta medida de control empresarial debe de tener carácter excepcional y su licitud debe de estar unida a una necesidad fundada, como la obtención de pruebas o confirmación de conductas irregulares o delictivas del trabajador, o bien de actuaciones de éstos que puedan implicar la responsabilidad del empleador. En estos casos no basta con quehaya meras sospechas de la comisión de un hecho ilícito, sino que debe haber indicios fundamentados que constituyan un motivo legítimo para que el empresario pueda llevar a cabo el acceso a los dispositivos digitales (Baz Rodríguez, 2019, p. 145).

2.1.2 Criterios de utilización de los medios digitales en la empresa

Para que el tratamiento de datos extraídos de los dispositivos digitales sea lícito, además de la existencia de los presupuestos de legitimación del artículo 87.2 LOPDP-

GDD, la empresa deberá establecer reglas sobre el uso de estos medios para el desarrollo de la prestación de serviciosde los trabajadores con el fin de supervisar el cumplimiento de sus obligaciones y deberes dimanantes del del contrato de trabajo.

Cuando se haya admitido el uso de estos medios para fines privados, el empleador tendrá que especificar de manera precisa cuáles serán los usos autorizados y las garantías para preservar la intimidad, como los periodos temporales enlos que se podrán utilizar los dispositivos para fines extralaborales. Junto a esta obligación para el empresario, el artículo 87.3 LOPDP-GDD añade la exigencia de participación de los representantes legales de los trabajadores en el establecimiento y negociación de estos criterios sin hacer ninguna otra especificación al respecto (Pérez de los Cobos Orihuel, 2019, p. 22). Por tanto, ya no basta con la mera advertencia sobre la prohibición del uso privado de los dispositivos para que sea lícito el tratamiento de datos de los trabajadores obtenidos por medio de las TICS, se refuerza la obligación de transparencia empresarial y se elevan a deber legal los criterios manifestados por la jurisprudencia anteriores a la llegada de la LOPDP-GDD.

Las STS 1323/2011 FD 3 y STS 119/2018 FD 6 señalan que los equipos informáticos puestos a disposición de los trabajadores son instrumentos de producción que pertenecen al empresario y, por tanto, puede examinar su uso de acuerdo con el artículo 20.3 TRET. Es por ello por lo que la empresa debeestablecer, en primer lugar, pautas de utilización de las herramientas empresariales puestas a disposición de los trabajad ores de forma previa a su utilización y conforme al principio de buna fe, como las prohibiciones parciales o totales de su uso extralaboral.

Por otra parte, la empresa tendrá que advertir con anterioridad a los trabajadores de que se van a llevar a cabo controles de sus deberes laborales con la obligación de informar detalladamente cómo se van a efectuar y su alcance, que ha de ser siempre de la forma menos invasiva posible en el marco del derecho a la intimidad. De esta forma, si se emplean los medios digitales para fines personales cuando se ha prohibido expresamente su uso para tales razonesy el trabajador tuviera conocimiento tanto de esa prohibición como del hecho de que se van a realizar acciones de supervisión empresariales de los dispositivos, no podrá aceptarse que el ejercicio de dichas acciones o controles ha vulnerado una expectativa razonable de intimidad

Siguiendo estas pautas, la STS 489/2018 FD 10 ha considerado nula la prueba obtenida para el despido cuando no se ha dado advertencia previa del registro del ordenador corporativo, aun existiendo motivos fundados de que el trabajador estaba utilizando esta herramienta de manera ilícita y realizándose el registro de forma proporcionada y de la manera menos invasiva posible para el trabajador. Esta doctrina del Tribunal Supremo ha sido avalada por el Tribunal Constitucional en la STC 241/2012 FJ 5 manifestando que corresponde a cada empresario, en el ejercicio de sus facultades organizativas, establecerla regulación de las condiciones en el uso de ordenadores u otros medios digitales por medio de diferentes instrumentos como pueden ser órdenes,

instrucciones, códigos de conducta o protocolos, de forma que la empresa no quede privada de su poder de control y dirección. No obstante, estos sistemas siempre deben de formularse acorde a los derechos fundamentales de los trabajadores y deben estar dirigidos a poner en conocimientodel empresario datos o comunicaciones profesionales necesarios para el desarrollo de la actividad productiva, sin que se produzca ninguna intromisión en la mensajería o datos personales de los trabajadores.

Para que una medida empresarial restrictiva del derecho a la intimidad supere el juicio de proporcionalidad, la STC 170/2013 FJ 5 establece que los criterios necesarios en relación con la colisión entre el derecho a la intimidad y la libertad de empresa deben cumplir que la medida sea necesaria y no exista otra acción más moderada para lograr el mismo propósito, la medida sea idónea y sea susceptible de conseguir el objetivo del buen funcionamiento de la actividad empresarial, y que la medida sea equilibrada con pleno respeto a los derechos fundamentales sin exceder la finalidad de su utilización (Sáez Lara, 2017, p. 189).

La doctrina elaborada por el Tribunal Supremo y el Tribunal Constitucional se muestra acorde con los criterios establecidos por el Tribunal Europeo de Derechos Humanos (TEDH) en la Sentencia 61/2017 (Barbulescu II) respecto al control empresarial de las comunicaciones de sus empleados, en la que es necesaria una información de las modalidades de control previa, clara y concisa a los trabajadores, el alcance temporal y material del control, la justificación legítima del acceso empresarial, la valoración sobre otras medidas más respetuosas con la privacidad del trabajador, el tratamiento y finalidad de lo información recabada y transparencia en el acceso al dispositivo (apartado 121 STEDH 61/2017).

En este sentido, la STEDH 35/2018 apartados 51, 52 y 55 (caso Libert contra Francia), tuvo su origen en el despido de un trabajador por incumplir gravemente el código deontológico de la empresa al contener en su ordenador documentos falsificados que habían sido descubiertos por otro trabajador que le sustituía. En los protocolos de la empresa se había previsto la autorización para uso privado del ordenador a los trabajadores, estableciéndose unas normas como el acceso del empresario a ficheros calificados como privados en el ordenador, únicamente en caso de riesgo o acontecimiento especial. En este caso, los archivos controvertidos no estaban calificados literalmente como privados o personales, y la empresa accedió a ellos para comprobar que efectivamente se había producido un comportamiento ilícito y se había transgredido la buena fe contractual, por lo que el TEDH consideró que la empresa tenía una razón legítima para abrir esos documentos, que era asegurar el correcto uso del ordenador por parte del trabajador en ejercicio de sus funciones como vigilante de seguridad.

2.2 SISTEMAS DE VIDEOVIGILANCIA Y GRABACIÓN DE SONIDOS

El artículo 89 LOPDP-GDD regula la videovigilancia en el lugar de trabajo como medio de control empresarial y reconoce el derecho del empleadora tratar las imágenes obtenidas mediante dispositivos de grabación, como sistemas de cámaras y videocámaras, en virtud de su potestad de control y dirección de la actividad laboral, en relación con el artículo 20.3 TRET siempre que estas funciones se ejerzan dentro de su marco legal y con la debida consideración a la dignidad de los trabajadores o empleados públicos y, en su caso, a su capacidad real si se trata de trabajadores con discapacidad.

A su vez, el artículo 89.1 LOPDP-GDD atenúa el derecho de información a los trabajadores en el casode que se descubra la comisión de un hecho ilícito mediante los sistemas de videovigilancia, estableciendo que, en esta situación, este deber se considerará cumplido cuando se haya advertido mediante la colocación de un dispositivo visible el tratamiento de imágenes, la identidad del responsable y la posibilidad para los trabajadores de ejercer sus derechos reconocidos en los artículo 15 a 22 RGPD.

Por último, el artículo 89.3 LOPDP-GDD permite excepcionalmente la grabación de sonidos solo en aquellos casos que exista riesgo para la seguridad de las personas y del patrimonio empresarial siempre que se sigan los principios de proporcionalidad e intervención mínima.

2.2.1 Control de la actividad laboral mediante videovigilancia

El uso de sistemas de grabación en el centro de trabajo encuentra su base de legitimación en el artículo 6.1 f) RGPD con la finalidad exclusiva de salvaguarda de los sistemas de producción, la protección del patrimonio empresarial y la seguridad de las personas, y a través del artículo 6.1 b) RGPD la necesidad de tratamiento de la imagen de los trabajadores para la ejecución del contrato de trabajo queda subordinada a este interés legítimo (Baz Rodríguez, 2019, p. 154).

Según el artículo 4.1 RGPD la imagen es un dato de carácter personal, por lo que el artículo 89.1 LOPDP-GDD establece que es necesario que el empresario haya informado de forma clara, precisa e inequívoca a los trabajadores y, en su caso, a sus representantes legales, de que van a ser sometidos a mecanismos de grabación y siempre con carácter previo a la instalación o puesta en funcionamiento del sistema de videovigilancia (Guindo Morales; Ortega Lozano, 2020, p. 11).

El alcance de este deber de información acompaña a los principios de transparencia y lealtad en el tratamiento de datos personales, por lo que no es suficiente con establecer un aviso genérico de que se va a vigilar a los trabajadores, sino que se deben de concretar los aspectos que establece el artículo 13 RGPD de identidad y datos del responsable del tratamiento y, en su caso, del Delegado de Protección de Datos (DPD) de la empresa, fines del tratamiento de la imagen, interés legítimo que constituye la base jurídica del

tratamiento, destinatarios de los datos, plazo de conservación de éstos y derechos de los interesados conforme a los artículos 15 a 22 RGPD.

En el caso de que la seguridad sea encargada a una empresa externa dedicada al tratamiento de las imágenes de los trabajadores, el acceso a estos datos ha de estar regulado en virtud de un contrato y atendiendo a las reglas del artículo 28 RGPD. Por tanto, resultará lícito el control de la actividad productiva mediante videovigilancia siempre que se cumplan los parámetros y se produzca la debida observancia de los principios establecidos en el artículo 5 RGPD, especialmente el principio de limitación de los datos, por el cual las imágenes obtenidas a través de esta medida de control no pueden ser tratadas ulteriormente para otras finalidades distintas de aquellas que legitiman su recogida. Y también el principio de minimización de imágenes captadas por los sistemas de grabación, que deberán de ser adecuadas, pertinentes y acordes con los objetivos establecidos en base al interés legítimo empresarial. En base a esto, no resultará lícito el tratamiento de la imagen de los trabajadores con fines de gestión del empleo o para analizar su comportamiento, ni resultaría admisible el tratamiento automatizado o la elaboración de perfiles a partir de imágenes captadas por sistemas de grabación (Baz Rodríguez, 2019, p. 163).

De acuerdo con el principio de responsabilidad proactiva, el empresario tiene que aplicar medidas que hagan compatible su interés legítimo con los derechos fundamentales de los trabadores en el empleo de técnicas de videovigilancia, puesto que este mecanismo resulta intrusivo en la intimidad de los trabajadores y por ello debe mantener su carácter excepcional. Para ello deberá determinar el espacio físico en el que se va a grabar, durante cuánto tiempo y que sea el necesario para tutelar el interés legítimo del empresario. Lógicamente, no será admisible en ningún caso la instalación de dispositivos de grabación en lugares destinados al descanso o esparcimiento de trabajador como vestuarios, aseos y demás espacios de la misma naturaleza de acuerdo con el artículo 89.2 LOPDP-GDD (Pérez de los Cobos Orihuel, 2019, p. 25).

2.2.2 Videovigilancia y comisión de actos ilícitos por los trabajadores

Si se descubre a través de los sistemas de grabación que un trabajador ha llevado a cabo una conducta ilícita, el artículo 89.1 LOPDP-GDD establece que se trata de un control con posterioridad a los hechos, en el cual no se omite el deber de información previa sino que se flexibiliza, y el artículo 22.4 LOPDP-GDD establece como único requisito la colocación del dispositivo en un lugar visible para los trabajadores a través de cual se informe de que su imagen va a ser tratada, quien es el responsable del tratamiento y sus derechos conforme a los artículos 15 a 22 RGPD.

Desde el punto de vista procesal, para considerar válida la prueba obtenida mediante sistemas de videovigilancia conforme al artículo 90.4 LRJS, es necesario que, además de la

existencia de un objetivo fundamentado que legitime este mecanismo de control, así como el cumplimiento del deber de información a los afectados por el principio de transparencia, es preciso dicho control se realice de acuerdo con los criterios establecidos por el Tribunal Constitucional para continuar el juicio de proporcionalidad.

Así, los mecanismos de control visual deben de obedecer a una necesidad real que justifique su implantación, no bastando para ello la mera conveniencia o comodidad empresarial y siempre que no haya sido posible adoptar otra medida menos invasiva para la intimidad de los afectados. A su vez, debe ser una medida idónea para lograr el objetivo de detectar irregularidades de las cuales se tienen sospechas fundamentadas y no meras hipótesis, como la acreditación mediante auditoría de una desproporción entre lo facturado en la caja con el inventario y, por tanto, que existan motivos para suponer que se ha producido un hurto y adoptar medidas disciplinarias en ese sentido.

El principio de minimización de datos jugará un papel relevante y, además, debe ser una medida equilibrada, como que las cámaras hayan permanecido instaladas solamente unos días hasta detectar la irregularidad sospechada o que se haya grabado solo a los trabajadores que sean sospechosos de la conducta ilícita (Guindo Morales; Ortega Lozano, 2020, p. 14).

Sin embargo, el artículo 89.1 LOPDP-GDD no precisa cuál es el alcance de esos actos ilícitos para considerar válida la prueba videográfica por lo que ello debe interpretarse de acuerdo con la jurisprudencia. Así, la STS 630/2016 FD 2 ha considerado que es procedente el despido de un trabajador de una tienda de alimentación por consumir productos in situ sin abonar su importe, tras descubrirse esta conducta mediante las imágenes captadas por las cámaras de seguridad del almacén de la tienda, que era una zona restringida al público y accesible solo a los trabajadores. El Tribunal Supremo consideró que la prueba es lícita porque el almacén no es una zona en la que tengan lugar actividades referentes a la vida privada de los trabajadores, sino que es una zona de desenvolvimiento normal de la actividad de la empresa. Y, además, todos los trabajadores tenían constancia de la existencia de cámaras en el almacén mediante carteles informativos, por lo que se había cumplido el deber de información a los empleados, y la implantación de esta medida obedecía a la finalidad de combatir actividades generadoras de pérdidas económicas y para su consecución se había ajustado a las exigencias razonables del respeto a la intimidad.

Siguiendo esta línea, con la STS 77/2017 FD 2 se volvió a manifestar favorable acerca del despido de un trabajador por transgresión de la buena fe contractual, deslealtad y abuso de confianza que fue grabado mientras se apropiaba de importantes cantidades de dinero de la caja registradora que manejaba y manipulaba tickets de venta. El trabajador involucrado tenía conocimiento de la existencia de cámaras de seguridad y de su ubicación, pero la empresa no informó de la finalidad que tendría el tratamiento de las imágenes captadas. El Tribunal Supremo consideró que la instalación del sistema de

videovigilancia se justificaba en el control de la seguridad de la empresa y la rápida detección de siniestros, que era una medida idónea y necesaria para control de cobros en la caja en este caso en particular, y proporcionada de acuerdo con estos fines ya que se había informado a los trabajadores de que se iba a implantar esta medida de vigilancia por razones de seguridad, expresión que incluye la detección de actos ilícitos de trabajadores y terceros pero excluye otro tipo de control ajeno a la seguridad como el rendimiento en el trabajo, cumplimiento de la jornada laboral o conversaciones con compañeros.

En el mismo sentido, la STS 96/2017 FD 2 volvió a considerar lícita la prueba videográfica cuando ésta ha sido obtenida a través de cámaras visibles para los trabajadores aun cuando no se había informado a éstos expresamente sobre la finalidad que podría tener el tratamiento de imágenes a efectos disciplinarios, como esta situación en la que se despidió al trabajador de un club deportivo por abrir el torniquete de acceso a las instalaciones para dejar paso a una persona que no era cliente ni empleada del centro y sin realizar el registro previo que tenían que hacer todos los socios del centro. En este caso, el trabajador conocía la existencia de la videocámara de seguridad situada en un lugar visible en el acceso a las instalaciones y, aunque el empresario no lo había comunicado de forma expresa, era evidente que la finalidad de las mismas residía en la protección del patrimonio empresarial y la grabación de conductas que atentasen contra la seguridad de los bienes y las personas, por lo que el Tribunal Supremo consideró que la medida fue proporcionada y no vulneraba el derecho a la intimidad (Mercader Uguina, 2018, p. 121).

Es importante señalar que la información otorgada únicamente en los términos del artículo 22.4 LOPDP-GDD solo daría lugar a que la prueba fuese lícita cuando la comisión de un acto irregular por parte de los trabajadores estuviera vinculada con la seguridad de los bienes o las personas y excediera del mero incumplimiento de sus obligaciones laborales. En cambio, si la prueba obtenida mediante videovigilancia se refiere únicamente al incumplimiento de las obligaciones propias de la relación contractual, como las ausencias en el puesto de trabajo, no bastaría como único elemento de información el dispositivo al que se refiere el artículo y se habría vulnerado el derecho a la intimidad del trabajador (López Balaguer; Ramos Moragues, 2020, p. 513).

En sintonía con la doctrina del Tribunal Supremo, la STC 29/2013 FJ 7 y 8 determinó que la instalación de un sistema de videovigilancia para comprobar el correcto desarrollo de las obligaciones propias del contrato de trabajo, requiere que previamente se hayan concretado los casos que podrían examinarse en las grabaciones, durante cuánto tiempo y la posibilidad de utilizarlas para tomar medidas disciplinarias, siendo insuficiente un mero aviso a través de carteles informativos sobre el hecho de que los trabajadores van a ser grabados, por lo que se estaría vulnerando el derecho a la protección de datos.

Esta vulneración del artículo 18.4 CE no puede entenderse cometida en el caso de la existencia de una conducta ilícita por parte de un trabajador cuando previamente a que ésta fuese captada, la empresa haya avisado mediante distintivos informativos visibles de la

existencia de cámaras y su finalidad. Así ocurrió en la STC 39/2016 FJ 4 y 5, y conocido como caso Bershka, en el que la empresa tras observar que se estaban produciendo apropiaciones indebidas de dinero decidió instalar cámaras de video que enfocaban al escaparate de la tienda y a la caja registradora, con las cuales se identificó a la persona que estaba cometiendo las sustracciones, motivo por el que fue despedida. El Tribunal Constitucional consideró que la empresa cumplió el deber de información y la medida superaba el triple juicio de proporcionalidad.

Es necesario precisar que conforme a la literalidad de la ley no resultaría admisible la videovigilancia mediante cámaras ocultas, puesto que no se estaría produciendo el requisito mínimo de información que establece el artículo 89.1 LOPDP-GDD en relación con el artículo 22.4 LOPDP-GDD. En este sentido, la STEDH de 9 de enero de 2018 (caso López Ribalda y otros contra España), que se originó en una cadena de supermercados cuando la empresa descubrió a raíz de la disparidad entre los productos disponibles y la recaudación en las cajas registradoras que se habían estado produciendo sustracciones económicas. Con el fin de investigar estos hechos y permitir a la empresa tomar acciones disciplinarias, se instalaron unas cámaras visibles para empleados y clientes, así como otras cámaras que estaban ocultas y enfocaban directamente a las cajas sin que los empleados conocieran la existencia de estas últimas. A pesar de que los trabajadores involucrados admitieron los hechos, éstos impugnaron el despido por considerar que se habíavulnerado su derecho a la intimidad, y el TEDH en su resolución dio la razón a los trabajadores corrigiendo a los tribunales españoles que consideraron que el despido había sido procedente, porque la imagen de los empleados obtenida a través de mecanismos de grabación implicó eltratamiento de un dato de carácter personal. Por ello, y de acuerdo con el artículo 5 de la Ley 15/1999 de Protección de Datos de Carácter Personal, vigente en el momento que tuvieron lugar los hechos, los trabajadores debían ser informados de manera clara, precisa e inequívoca de la existencia de un fichero de almacenamiento de esta información, de la finalidad de su recogida, los destinatarios de los datos, así como de sus derechos de acceso, rectificación, cancelación y oposición. Este deber de información fue incumplido por el empresario, por lo que la STEDH de 9 de enero de 2018 apartados 64, 65 y 69 afirmó que la videovigilancia no había sido proporcionaday que la empresa podría haber cubierto su interés legítimo en la protección de su propiedad informando a los trabajadores, al menos de forma general, sobre la puesta en funcionamientode esta medida por lo que se habría dado de este modo un mecanismo de control menos intrusivo.

Sin embargo, la resolución se recurrió ante la Gran Sala del TEDH y, la STEDH de 17 de octubre de 2019 consideró que, a pesar de que solamente se había avisado a los trabajadores sobrela existencia de cámaras de seguridad que estaban a la vista, las cámaras que no se encontraban visibles estaban situadas en una zona específica del centro de trabajo que estabaabierta al público y donde tenían lugar actividades propias de las prestación de

servicios, como el cobro a los clientes, respetando dependencias privadas como aseos o vestuarios donde existe una expectativa razonable de intimidad para los trabajadores. Por otra parte, la empresa tenía indicios constatados de que se habían producido robos en el supermercado que se fundamentaban en las pérdidas económicas que estaba sufriendo la empresa y que justificaban la videovigilancia encubierta. Por ello, el hecho de haber informado a la plantilla sobre la existencia de cámaras ocultas hubiera puesto en riesgo la finalidad de la medida, que era identificar a los responsables de los robos y obtener pruebas de estos actos ilícitos a efectos disciplinarios. Además, la grabación a través de este sistema duró 10 días, que fue el tiempo necesario cumplir con este propósito. Por estos motivos, la STEDH 19 de octubre 2019 apartados 123, 124, 125, 126, 127 y 128 entendió que la grabación a través de cámaras ocultas fue una medida necesaria y que no hubiera sido posible esclarecer los hechos de forma menos incisiva en para la privacidad de los empleados, entendiendo que la grabación a través de cámaras ocultas fue una medida proporcionada basada en el interés legítimo del buen funcionamiento de la empresa y que no vulneró el derecho a la intimidad de los trabajadores.

Siguiendo la doctrina más reciente del TEDH y el artículo 89.1 LOPDP-GDD, cabe entender que la videovigilancia encubierta solo resultaría admisible en determinados supuestos muy puntuales en los que existiera una ruptura previa de la seguridad en la empresa respecto a bienes materiales o sobre las personas, que la conducta ilícita detectada revistiera especial gravedad y, siempre que el hecho de aportar información a los empleados suponga un riesgo para el buen fin del objetivo que se pretende, que deber ser la seguridad de los bienes y las personas.

2.2.3 Grabación de sonidos en el lugar de trabajo

El artículo 89.3 LOPDP-GDD regula de manera restrictiva la utilización de sistemas de audición o grabación de sonidos en la empresa. La base de legitimación del tratamiento de datos en los que puede entra en juego la voz de los trabajadores se encuentra fundamentada, aunque de manera muy restringida, en el interés legítimo empresarial en virtud del artículo 6.1 f) RGPD.

Para que esta medida resulte admisible se han de aplicar las garantías que establece el artículo 89.1 LOPDP-GDD para la videovigilancia, por el que el control a través de mecanismos de audición sólo será factible en el caso de que existan graves riesgos para los bienes patrimoniales de la empresa o para las personas derivados de la actividad concreta que se desarrolle en el centro de trabajo, y la exigibilidad de la estricta observancia de los principios de proporcionalidad, intervención mínima, así como de limitación y minimización de los datos.

Junto a estos criterios, no es posible flexibilizar el deber de información a los trabajadores informando únicamente a través del dispositivo al que se refiere el artículo

22.4 LOPDP-GDD, sino en este caso se refuerza el principio de transparencia en el deber de información específica en los términos del artículo 13 RGPD y 11 LOPDP-GDD. Además, el artículo 89.3 LOPDP-GDD establece que los sonidos que se recojan mediante estetipo de sistemas podrán ser conservados por el periodo máximo de un mes desde su captación, salvo que estos datos fueran necesarios para demostrar que se ha producido menoscabo en la seguridad de las instalaciones o bienes de la empresa o sobre las personas (Baz Rodríguez, 2019, p. 163).

Por lo tanto, a través del artículo 89.3 LOPDP-GDD y el carácter restringido con el que regula esta medida, se puede determinar que la grabación de sonidos no resultaría admisible en ningún caso para el control ordinario de correcto mantenimiento y desarrollo de las obligaciones propias de los trabajadores derivadas del contrato de trabajo. Sin embargo, el precepto no hace alusión a la posibilidad de controlar mediante grabación de sonidos aquellas prestaciones que por su naturaleza puedan requerir este tipo de control, como empresas de venta telemática que prestan sus servicios por teléfono. Para estos supuestos, hubiera sido deseable que el precepto especificara la posible validez del control mediante grabación de sonidos de no ser posible establecer una medida menos invasiva para la privacidad de los trabajadores, siempre de acuerdo con el principio de transparencia y minimización de los datos.

Conforme a este artículo, la STC 98/2000 señaló que no puede descartarse que en los lugares del centro de trabajo donde se desarrolla la prestación de servicios pueden producirse intromisiones ilegítimas del empresario en la intimidad de los trabajadores como podría ser a través de conversaciones entre empleados y clientes, o bien entre los propios trabajadores sobre cuestiones ajenas a la actividad laboral y que se integranen la esfera de desenvolvimiento del individuo. En este caso en particular los hechos tuvieron lugar en un casino en el que se colocaron unos mecanismos de grabación de sonidos en dos zonas específicas de las instalaciones, la caja y la ruleta francesa. El Tribunal Constitucional resaltó la utilidad y conveniencia que tuvo para la empresa esta medida de control, pero ello no es motivo suficiente para que el empresario estuviese legitimado a emplear estos sistemas ya que el casino disponía de personal encargado de la seguridad en las instalaciones, así como de un circuito cerrado de televisión por lo que no ha quedado acreditado que fuera indispensable instalar este sistema de audición para mantener la seguridad del lugar. Por otra parte, este sistema permitía escuchar conversaciones privadas de forma indiscriminada de trabajadores y de clientes que eran irrelevantes para el control delas obligaciones laborales y para la seguridad de los bienes y las personas por lo que esta medida de control no superaba el triple juicio de proporcionalidad ni el principio de intervención mínima (STC 98/2000 FJ 6 y 9). Por lo tanto, la captación y grabación de sonidos no puede tener amparo en las facultades de vigilancia y control reconocidas en el artículo 20.3 TRET y supone la vulneración del derecho a la intimidad de los trabajadores regulado en el artículo 18.1 CE.

2.3 SISTEMAS DE GEOLOCALIZACIÓN

Actualmente están proliferando nuevos métodos de control empresarial de forma paralela a otros más clásicos como la videovigilancia. Este es el caso del control de la ubicación geográfica de los empleados mediante sistemas de geolocalización instalados, por ejemplo, en vehículos, tabletas electrónicas o dispositivos móviles, regulados en el artículo 90 LOPDP-GDD. A través de estos mecanismos se recogen datos de localización de los trabajadores, procedentes de nuevas tecnologías como redes de comunicaciones electrónicas o bien procedentes de satélites GPS, y que permiten a la empresa saber de manera concreta los movimientos y el paradero de los equipos electrónicos y de los trabajadores (Blázquez Agudo, 2019, p. 93).

La utilización de sistemas de geolocalización es una técnica muy habitual en empresas de transporte, reparto de mercancías o en el caso del trabajo a distancia en el que el empleado desarrolla su actividad en un lugar diferente al del centro de trabajo, lo cual en muchas ocasiones da lugar a que el trabajador tenga que desplazarse de un lugar a otro, como en el caso de los comerciales. No obstante, este escenario suscita como cuestión la posible afectación que puede tener el derecho a la intimidad de los trabajadores respecto a la posibilidad de geolocalización que tiene el empresario en virtud de sus potestades reconocidas en el artículo 20.3 TRET (Marín Malo, 2020, p. 111).

2.3.1 El control indirecto del trabajador

El artículo 90 LOPDP-GDD establece el derecho a la intimidad de los trabajadores en el uso de dispositivos de geolocalización y determina que el empresario podrá tratar los datos de los empleados obtenidos en la utilización de los mecanismos de geolocalización dentro del marco legal del artículo 20.3 TRET y con los límites inherentes al mismo.

La privacidad de los trabajadores es la referencia a la que ha de ceñirse la empresa para el tratamiento de datos personales sobre la localización de los trabajadores. Sin embargo, dada la gran imprecisión del precepto, resulta necesario que se complete con la remisión en bloque a la normativa sobre protección de datos, tanto RGPD como LOPDP-GDD, a la que hace referencia el artículo 20 *bis* TRET. Así, el empleador, como responsable del tratamiento de datos en el contexto de geolocalización, debe de obedecer los principios esenciales en esta materia regulados en el artículo 5 RGPD y que son la licitud, lealtad, transparencia, limitación de la finalidad, minimización de los datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva.

Por otra parte, el artículo 90 LOPDP-GDD no se ha especificado las diversas finalidades empresariales a las que puede obedecer la implantación de tecnologías de geolocalización. Por lo que hay que acudir al Comité Europeo de Protección de Datos (CEPD) para analizar la exigencia de una causa específica relacionada con la prestación

laboral para que sea legítimo el empleo de sistemas de geolocalización y, que de esta manera el tratamiento de datos personales de los trabajadores relativos a su ubicación geográfica pueda justificarse cuando el control de la posición del trabajador sea parte control del transporte de personas o bienes y no se pueda desligar de esta última finalidad, cuando sea preciso para la mejora de la distribución de recursos para servicios en puntos remotos, y cuando sea necesario para la seguridad del trabajador o los bienes a su cargocomo el vehículo empleado para desarrollar la prestación de servicios.

Como consecuencia de las directrices establecidas por el CEPD, el control directo hacia el trabajador mediante geolocalización tiene carácter subsidiario, pero éste no es el objetivo en sí mismo que se pretende con el empleo de estos mecanismos sino que es una consecuencia que se deriva del conjunto de actuaciones que el empresario puede llevar a cabo para el correcto desenvolvimiento de la producción. De acuerdo con este planteamiento, resultará ilícito el tratamiento de datos sobre el paradero del trabajador con el único fin de vigilar o supervisar la actividad laboral, siempre que ello pueda realizarse por otros medios.

Por lo tanto, según el artículo 6.1 b) RGPD la base de legitimación del tratamiento de estos datos en este caso se encontraría en el hecho de que éste fuese necesario para la ejecución de un contrato en el que el interesado es parte. En relación con esta finalidad, la AEPD estableció los datos que se pueden recoger mediante sistemas de GPS, como la hora de arranque, la hora de estacionamiento, los lugares de paso y paradas, la velocidad máxima y media de los vehículos, el consumo del vehículo en función de la distancia recorrida, las horas de funcionamiento, los kilómetros recorridos durante el tiempo de trabajo y la desviación de horas del vehículo en función de la configuración del horario de trabajo (Baz Rodríguez, 2020, p. 5).

La STSJ M 260/2014 FD 20 y 23 manifestó que la posibilidad de hacer un seguimiento permanente del vehículo de trabajo, más allá de su ubicación por motivos de seguridad, y que conlleve saber en todo momento dónde se encuentra exactamente el trabajador, así como el ulterior tratamiento de estos datos para una finalidad distinta de la anunciada sin que ello se haya puesto en conocimiento del interesado, tiene como consecuencia que las pruebas obtenidas mediante sistemas de geolocalización para demostrar presuntos incumplimientos contractuales del trabajador vulneran los derechos fundamentales a la intimidad y la protección de datos, por lo que deben de considerarse ilícitas y carentes de eficacia.

De acuerdo con los principios de limitación de la finalidad y minimización de datos, en ningún caso será viable el control por geolocalización de los trabajadores fuera de la jornada de trabajo en virtud del art 6.1 b) RGPD, lo cual supondría un menoscabo del derecho a la intimidad de los trabajadores. Así lo destacó la STSJ PV 5122/2011 FD 5 señalando que la implantación de un sistema de monitorización en tiempo real del vehículo particular de un trabajador durante el periodo de tiempo en el que su contrato

estabasuspendido vulnera su derecho a no estar permanentemente localizado, lo cual es un elemento del derecho a la intimidad conforme el artículo 18.1 CE. Por lo que una vez finalizada la jornada laboral las facultades empresariales dimanantes del artículo 20 TRET desaparecen, y el contrato de trabajo deja de ser vinculante para las partes, añadiendo la STSJ AS 3058/2017 FD 5 que para mantener en funcionamiento un GPS fuera del tiempo de trabajo de un empleado será preciso que éste otorgue su consentimiento.

Con relación a la aportación de los trabajadores de dispositivos de su propiedad que sirvan de soporte para la puesta en marcha de sistemas de geolocalización, la empresa Telepizza decidió implantar un servicio denominado "Proyecto Tracker", que permitía la geolocalización de pedidos por parte de los clientes desdeque salía del restaurante hasta que llegaba a sus domicilios a través de una aplicación móvil que tenía acceso a la posición del trabajador. Para ello, la empresa requirió a los empleados que aportaran sus propios teléfonos móviles durante la jornada laboral con conexión de datos y en plenas condiciones de uso, lo que implicaba el tratamiento de datos personales. La SAN13/2019 FD 6 determinó que este modelo de negocio era abusivo y vulneraba la intimidad de los trabajadores por no superar el juicio de proporcionalidad, y que la finalidad del servicio podría haberse logrado de otras formas que dieran lugar a una menor injerencia en la esfera privada de los trabajadores, como la instalación de un GPSen los vehículos donde se trasladaban los pedidos, de tal manera que no sería necesario que los empleados aportaran medios propios ni datos personales como su número de teléfono particular o su dirección de correo electrónico personal. Por otra parte, en este caso, la empresa no había informado a los trabajadores en los términos de los artículos 12 y 13 RGPD, incumpliendo el principio de transparencia que debe regir en el tratamiento de datos personales.

2.3.2 El deber de información plena sin excepción

El artículo 90.2 LOPDP-GDD recoge también la necesaria aplicación del principio de transparencia en el uso de dispositivos de geolocalización estableciendo la obligación para el empleador de informar a los trabajadores y, en su caso, a sus representantes legales, sobre la utilización deeste tipo de sistemas previamente a su implantación y de forma completa, clara, detallada e inequívoca, así como de los derechos de los trabajadores recogidos en los artículos 15 a 22 RGPD. Con esta regulación, el artículo 90.2 LOPD asimila el contenido de los artículos 13 y 14 RGPD sinque exista habilitación legal expresa que permita atenuar el requisito de información completa, como ocurría en el caso de la videovigilancia cuando se producía una conducta ilícita por parte de los trabajadores, por lo que, en el caso del control por geolocalización no es viable reducir el alcance del deber de información empresarial hacia los trabajadores, independientemente de cuál sea la causa que justifique esta medida (Baz Rodríguez, 2020, p. 7).

Sin embargo, el artículo 90.2 LOPDP-GDD no hace mención alguna la finalidad de la medida ni al posible tratamiento de los datos de localización a efectos disciplinarios. A este respecto, la STSJ M 376/2017 FD 2 establece que el derecho de los interesados a recibir información previa sobre el tratamiento de sus datos personales es contenido esencial del artículo 18.4 CE y su omisión no puede basarse en una mayor eficiencia de la facultad vigilancia del empresario. Por ello, el empresario, como responsable de tratamiento, debe garantizar suficiente información a los trabajadores sobre la instalación de dispositivos GPS, así como de la finalidad que se pretende lograr.

Para que los datos relativos a desplazamientos hechos por los trabajadores revelen su paradero durante la jornada laboral y sean considerados como prueba válida a efectos disciplinarios, es indispensable que se haya cumplido el requisito de información previa al trabajador. Por tanto, la jurisprudencia considera que es válida la prueba para el despido basada en datos personales sobre la ubicación geográfica una vez que se ha puesto en conocimiento del trabajador la transmisión de sus datos de localización como la posición en las rutas realizadas durante el tiempo de trabajo o el registro de los momentos de arranque del vehículo y sus paradas, que constituyen datos que no afectan a la intimidad personal.

Por su parte, la STS 766/2020 FD 2 manifestó el rechazo a que se produzca vulneración del derecho a la intimidad de los trabajadores cuando éstos han tenido conocimiento previo sobre la limitación del uso del vehículo a la jornada laboral, con expresa asunción de responsabilidad de su estado y quedado totalmente prohibido su uso fuera del horario de trabajo o para fines privados.

La expectativa razonable de intimidad de los trabajadores respecto al uso de dispositivos digitales en el contexto del posible uso particular que un trabajador puede hacer del vehículo que la empresa le otorga para realizar sus labores, el Tribunal Supremo que los datos obtenidos mediante GPS se refieren a la posición y al movimiento del vehículo, sin captar circunstancia personal alguna de sus ocupantes y que la instalación de este sistema tenía como finalidad garantizar la seguridad y la coordinación en el trabajo por lo que, aun estando el vehículo geolocalizado permanentemente, no resulta viable considerar que se ha lesionado el derecho a la protección de datos. Por lo tanto, no se produce menoscabo de derechos fundamentales ya que la empresa ha cumplido con el deber de información aportando instrucciones claras sobre la utilización del vehículo durante la jornada laboral y determinando expresamente su uso en exclusiva durante el tiempo de trabajo, lo que da lugar a que los datos recogidos mediante sistemas de geolocalización sean lícitos y constituyan prueba válida para fundamentar el despido.

En este sentido, el elemento central para determinar la validez de la prueba basada en el tratamiento de datos personales de localización es el cumplimiento del deber de información de forma plena y sin que sea posible realizar modulación alguna. Además, a diferencia de la videovigilancia, en cuyo caso resultaba admisible la vigilancia encubierta,

aunque con muchas reservas, el control no informado a través de GPS o cualquier otro medio que permita conocer la ubicación del trabajador no es viable jurídicamente, ni siquiera de manera restringida.

Sin perjuicio del hecho de que la información a los trabajadores se tiene que aportar de manera previa a la implantación de las herramientas de geolocalización, este deber empresarial no se agota en este momento, sino que es necesario que se produzca un proceso de emisión continua de información actualizada sobre el funcionamiento de estos sistemas. Esta información tiene que hacer referencia no solo a las características o propiedades de los mecanismos de geolocalización, sino también a su finalidad, ejercicio de derechos de los trabajadores y periodo de conservación de los datos, que son aspectos que se omiten en el artículo 90 LOPDP-GDD.

El periodo de conservación de los datos ha de estar unido al principio de limitación de la finalidad, por lo que podrán conservarse como máximo el tiempo que sea necesario para lograr la finalidad por la cual se recogieron. No obstante, el CEPD ha recomendado que el plazo de conservación sea de dos meses, y si fuese necesario un periodo de tiempo superior a este, sería recomendable que los datos se convirtieran en anónimos.

En cuanto al principio de responsabilidad proactiva, por el que responsable del tratamiento de datos tiene que demostrar el cumplimiento de la normativa relativa a esta materia, tampoco se recoge en el artículo 90 LOPDP-GDD. El precepto también guarda silencio sobre la necesidad de adoptar garantías en el tratamiento de datos de localización y de consultar a las autoridades de protección de datos. En este aspecto, resultaría exigible realizar una evaluación de impacto de acuerdo con el artículo 35 RGPD en el momento en que la empresa decida poner en marcha sistemas de geolocalización prestando especial atención al artículo 35.9 RGPD, que requiere la opinión de los interesados o sus representantes acerca del tratamiento de sus datos, lo cual se traduce en el carácter preceptivo de la intervención de la negociación colectiva a través de la emisión de un informe previo de los representantes legales a la toma de decisiones empresariales respecto a los sistemas de geolocalización según el artículo 64.5 f (Baz Rodríguez, 2020, p. 8).

2.4 DERECHO A LA DESCONEXIÓN DIGITAL

El artículo 88 LOPDP-GDD recoge el derecho a la desconexión digital en el ámbito laboral, aunque el legislador no ha desarrollado un concepto sobre esta cuestión, por lo que al incluirse esta facultad en la lista de derechos digitales, debe interpretarse que está haciendo referencia a la protección de los empleados frente a posibles comunicaciones que el empresario pueda realizar fuera de la jornada laboral, por lo que no se estaría estableciendo un nuevo derecho sino que sería una precisión en la LOPDP-GDD de los derechos de descanso que ya se encuentran recogidos en el TRET. Así, el trabajador tendrá derecho a oponerse a que el empresario contacte con él fuera del tiempo de trabajo, puesto

que este espacio temporal es ajeno a la relación laboral o al vínculo contractual.

El artículo 88.2 LOPDP-GDD busca potenciar la conciliación de la vida laboral con la vida personal, pero no regula el ejercicio de estos derechos en relación con el entorno digital sino que remite a la negociación colectiva o, en su defecto, a lo pactado entre el empresario y los representantes legales de los trabajadores, adecuando estas medidas a cada sector o la naturaleza de la actividad laboral, lo cual tiene sentido si tenemos en cuenta las diferencias que pueden darse en empresas con un alto componente tecnológico o, en el caso del teletrabajo, frente a empresas más tradicionales donde el impacto de las TICS es menor (Taléns Visconti, 2019, p. 158).

La aportación del artículo 88.3 LOPDP-GDD establece la obligación para la empresa de elaborar políticas que regulen el derecho a la desconexión digital. Estas políticas definirán las modalidades de desconexión, acciones de formación y sensibilización del personal sobre el uso razonable de las nuevas tecnologías con la finalidad de evitar la fatiga informática. No se impone en el texto legal que estas políticas tengan que ser negociadas, pero resulta conveniente escuchar a los representantes de los trabajadores y no dejar esta cuestión al criterio unilateral de la empresa. La finalidad del precepto en este punto no es solo la concienciación para el empresario de la necesidad de desconexión de los empleados, sino también la de los trabajadores con el fin de evitar su sobreexposición a los medios tecnológicos. Sin perjuicio de ello, no se puede olvidar que el uso de la tecnología fuera del horario de trabajo en virtud de la prestación de servicios se convierte en ocasiones en un medio idóneo para flexibilizar la jornada laboral en beneficio de la conciliación familiar y la vida personal (Blázquez Agudo, 2019, p. 95).

2.5 DERECHOS DIGITALES Y NEGOCIACIÓN COLECTIVA

El artículo 91 LOPDP-GDD parte del desarrollo de los derechos digitales en el ámbito laboral a la negociación colectiva. De esta manera, la ley ha ampliado el papel de los representantes legales en materia de protección de datos y la garantía del ejercicio de los derechos establecidos en los artículos 88 a 90 LOPDP-GDD.

No obstante, hubiera sido adecuado que la ley especificara el espacio de actuación en el que la autonomía colectiva pueda intervenir (Blázquez Agudo, 2019, p. 98). Si bien es cierto que el precepto se refiere literalmente a garantías adicionales en el tratamiento de datos personales de los trabajadores y salvaguarda de los derechos digitales, ello no sería óbice para que la negociación colectiva extendiera su función a otros aspectos como la concreción del principio de transparencia, limitación del tratamiento de datos, aplicación del principio de responsabilidad proactiva, cesión de datos a terceros o entre empresas dentro de un mismo grupo empresarial, sistema de denuncias internas o solución de discrepancias internas, entre otros.

No obstante, con el término "adicional" la LOPDP-GDD ya está determinando que

la negociación colectiva debe tener, como punto de partida para su desarrollo, un contenido obligatorio al que ceñirse, sin que sea admisible una modificación de la normativa por vía convencional. Porlo tanto, la intervención del convenio colectivo debe dirigirse a acotar las facultades empresariales de control y dirección sobre el cumplimiento de las obligaciones laborales de los trabajadores para hacer efectivas las garantías adicionales de los trabajadores a las que hace referencia el artículo 91 LOPDP-GDD.

Respecto al derecho a la intimidad en el uso de dispositivos digitales, es preciso destacar que su papel para delimitar el uso privado de las herramientas tecnológicas empresariales puede ser de gran importancia, así como de soporte para proyectar a través del convenio colectivo los criterios de utilización de estos medios en cuya determinación deberánde participar necesariamente los representantes legales de acuerdo con el artículo 87.3 LOPDP-GDD. También es una vía adecuada para determinar si el derecho a la intimidad es extensivo a softwares o aplicaciones de titularidad empresarial cuando se instalan en dispositivos personales de los trabajadores, cuestión a la que el legislador no ha hecho referencia.

En relación con las medidas de videovigilancia y control de sonidos, el artículo 89.1 LOPDP-GDD establece con carácter obligatorio el deber de informar a los trabajadores y a sus representantes legales acerca de la implantación de estas medidas. Aunque el precepto no exige la negociación de las medidas de forma expresa, se refuerza el contenido del artículo 64.5 f) TRET, aunque este deber se puede modular de manera excepcional en caso de comisión de actos ilícitos por parte de los trabajadores. En este caso es vital la participación de la negociación colectiva para determinar cómo debe materializarse el principio de transparencia, cuándo es lícita la videovigilancia y en qué casos las medidas deben ser verificadas por los representantes legales de los trabajadores, como la videovigilancia encubierta y la grabación de sonidos.

El papel de la negociación colectiva sobre los sistemas de geolocalización se dirige al establecimiento de medidas que garanticen la intimidad de los trabajadores, como la determinación de las causas justificativas de su implantación,así como del desarrollo y concreción del derecho de información sobre estos dispositivos y, especialmente, cuando vaya a producirse el tratamiento automatizado de datos.

El control mediante geolocalización debe de ajustarse a los tiempos de trabajo en los que se desarrolla la prestación de servicios, excluyendo periodos temporales ajenos a la jornada laboral. Por ello, la negociación colectiva es el cauce adecuado para determinar cómo se va arealizar el tratamiento de datos de ubicación en virtud de la ejecución del contrato laboral y dentro del tiempo de duración del horario de trabajo, detallando los periodos en los que se pueden desactivar los GPS u otros dispositivos que permitan obtener la localización de los trabajadores.

También es necesario destacar que la negociación colectiva podrá inmiscuirse en otras cuestiones de relevancia como la adecuaciónde los medios de geolocalización a los

fines que se pretendan, los datos que se van a recabar como itinerarios o velocidad del vehículo, momento a partir del cual se empiezan a recoger los datos, plazo de conservación de estos datos siempre inferior a dos meses, uso que se les va a dar aestos datos o quién va a tener acceso a ellos.

En cuanto al derecho a la desconexión digital, la ley remite prácticamente en su totalidad a la negociación colectiva el establecimiento de pautas a seguir en la modulación deeste derecho. Por medio de esta vía se delimitará su alcance cuando el trabajador se considerará fuera de su horario de trabajo y comience a aplicarse el derecho a la desconexióndigital, así como las formas en que podrá llevarse a cabo su ejercicio (Llorens Espada, 2020, p. 15).

3 CONCLUSIONES

Las nuevas tecnologías han revolucionado los procesos organizativos y productivos en el mundo laboral, lo que supone un avance en cuanto a eficiencia en el trabajo, pero puede traer consecuencias negativas como el enorme tráfico de datos personales o la sobreexposición al uso de las TICS. Sería recomendable la implementación de planes de formación teórica ypráctica en las empresas sobre su uso, adaptándose progresivamente conforme al avance delas nuevas tecnologías, con una orientación al uso responsable de los medios tecnológicos y no solo a la consecución del mayor rendimiento de la producción en la empresa.

La aprobación de RGPD en 2016 fijó el principio de transparencia y el de responsabilidad proactiva como pilares básicos, además de la incorporación de los derechos de supresión y portabilidad, la creación de figura del Delegado de Protección de Datos en empresas y en las Administraciones Públicas. Su materialización en España fue la aprobación de la Ley Orgánica 3/2018 de Protección de Datos personales y Garantías de los Derechos Digitales que desarrolla el artículo 18 de la CE y cuyas incorporaciones más relevantes a efectos laborales son los artículos 87 a 91 LOPD, como salvaguarda de los derechos fundamentales a la intimidad y la protección de datos de los trabajadores en la aplicación de técnicas de control y vigilancia empresarial mediante nuevas tecnologías, para la licitud del tratamiento de atos de los trabajadores.

Por ello, es necesario la implantación de políticas de empresa que establezcan los derechos de los trabajadores conforme a los artículos 15 a 22 RGPD, sobre el posterior uso de sus datos personales, el personal responsable del tratamiento, la base de licitud que lo fundamenta, y la posible transmisión y receptores de los datos y responsabilidad proactiva delempresario.

Es indiscutible que el empresario pueda determinar el uso que estime conveniente sobre las herramientas que pone a disposición de los empleados para realizar la prestación de servicios y ejercer sobre éstos las facultades quele confiere el artículo 20.3 TRET, pero

esa potestad siempre ha de tener como límite el respeto a la dignidad de los trabajadores y sus derechos fundamentales.

Uno de los aspectos más criticables de la actual LOPDP-GDD es la falta de concreción acerca de justificación legítima que puede tener el empresario para graduar la intensidad de control, aspecto que hubiera sido deseable desarrollar directamente en la ley o bien por vía reglamentaria. Por lo tanto, a falta de mayor precisión legal, será la autonomía colectiva la encargada de configurar esta cuestión y, en última instancia, los tribunales serán quienes decidirán caso por caso si concurre o no esa finalidad legítima.

Por otra parte, la débil protección que establece el artículo 90 LOPDP-GDD en cuanto al derecho del empleador a ejercer sus funciones conforme al artículo 20.3 TRET en el marco de las técnicas de geolocalización y a reiterar el deber de información previa a los trabajadores acerca de esta medida, ha de ser completado necesariamente con los criterios establecidos por el CEPD, la jurisprudencia y por la negociación colectiva para determinar la licitud del tratamiento de datos relativos a la ubicación geográfica de los interesados.

En cuanto a los criterios que han seguido los tribunales para establecer límites a la potestad de control y dirección del empresario es preciso destacar la doctrina sobre la expectativa razonable de intimidad sobre en el uso de dispositivos digitales por parte de los trabajadores asentada por el Tribunal Supremo, y el triple juicio de proporcionalidad establecido por el Tribunal Constitucional basado en que una medida sea necesaria, idónea y equilibrada o proporcionada en sentido estricto. Estas pautas jurisprudenciales han constituido la base sobre la cual los tribunales han determinado la licitud del tratamiento de datos realizado mediante herramientas tecnológicas que puedan poner en riesgo derechos fundamentales, así como su validez a efectos disciplinarios.

Por último, cabe destacar el papel de la negociación colectiva como medio para suplir las lagunas de la LOPDP-GDD, especialmente en el ámbito de la desconexión digital, donde la ley parece haberle otorgado especial protagonismo. No obstante, en virtud del principio de transparencia, se configura con carácter preceptivo el deber de información a los trabajadores y a sus representantes legales en materia de derechos digitales.

REFERENCIAS

ÁLVAREZ DEL CUVILLO, Antonio. La delimitación del derecho a la intimidad de los trabajadores en los nuevos escenarios digitales. **Temas laborales: Revista Andaluza de trabajo y bienestar social**, n. 151, p. 275-292, 2020.

BAZ RODRÍGUEZ, Jesús. Protección de datos y garantía de los derechos digitales laborales en el nuevo marco normativo europeo e interno (RGPD 2016 y LOPDP-GDD 2018). **Ars Iuris Salmanticensis: Ais: revista europea e iberoamericana de pensamiento**

y análisis de derecho, ciencia política y criminología, v. 7, n. 1, p. 129-171, 2019.

BAZ RODRÍGUEZ, Jesús. Geolocalización, dispositivos móviles y trabajo ubicuo. **Trabajo yderecho: nueva revista de actualidad y relaciones laborales**, n. Extra 11, 2020.

BLÁZQUEZ AGUDO, Eva María. **Aplicación práctica de la protección de datos en las relaciones laborales**. Madrid: CISS, 2018.

BLÁZQUEZ AGUDO, Eva María. Novedades laborales en la Nueva Ley orgánica de protección de datos. **Trabajo y derecho: nueva revista de actualidad y relaciones laborales**, n. 50, p. 89-102, 2019.

GÓMEZ SALADO, Miguel Ángel. La cuarta revolución industrial, ¿una gran oportunidad o un verdadero desafío para el pleno empleo y el trabajo decente? **Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo**, v. 7, n. 4, p. 276-315, 2019.

GONZÁLEZ BIEDMA, Eduardo. Derecho a la información y consentimiento del trabajador en materia de protección de datos. **Temas laborales: Revista Andaluza de trabajo y bienestar social**, n. 138, p. 223-247, 2017.

GOÑI SEIN, José Luis. Nuevas tecnologías digitales, poderes empresariales y derechos de lostrabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016. **Revista de derecho social**, n. 78, p. 15-42, 2017.

GUINDO MORALES, Sara; ORTEGA LOZANO, Pompeyo Gabriel. La monitorización del correo electrónico corporativo y la grabación del centro de trabajo por cámaras (visibles y ocultas). **Trabajo y derecho: nueva revista de actualidad y relaciones laborales**, n. 71, 2020.

LLORENS ESPADA, Julen. Los derechos digitales en la negociación colectiva. **Trabajo y derecho: nueva revista de actualidad y relaciones laborales**, n. Extra 11, 2020.

LÓPEZ BALAGUER, Mercedes; RAMOS MORAGUES, Francisco. Control empresarial del uso de dispositivos digitales en el ámbito laboral desde la perspectiva del derecho a la protección de datos y a la intimidad. **Lex social: revista de los derechos sociales**, v. 10, n. 2, p. 506-540, 2020.

MARÍN MALO, Mirentxu. La geolocalización del trabajador. Reflexiones a la luz de la jurisprudencia reciente. **LABOS: Revista de Derecho del Trabajo y Protección Social**, v. 1, n. 1, p. 109-121, 2020.

MERCADER UGUINA, Jesús Rafael. Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento UE 2016/679. **Trabajo y derecho: nueva revista de actualidad y relaciones laborales**, n. 41, p. 113-126, 2018.

PÉREZ DE LOS COBOS ORIHUEL, Francisco. Poderes del empresario y derechos

digitales deltrabajador. **Trabajo y derecho: nueva revista de actualidad y relaciones laborales**, n. 59, p. 16-29, 2019.

POLO ROCA, Andoni. Sociedad de la Información, Sociedad Digital, Sociedad de Control. **Ingurauk: Soziologia eta zientzia politikoaren euskal aldizkaria=Revista vasca de sociología y ciencia política**, n. 68, p. 50-77, 2020.

SÁEZ LARA, Carmen. Derechos fundamentales de los trabajadores y poderes de control del empleador a través de las tecnologías de la información y las comunicaciones. **Temas laborales: Revista Andaluza de trabajo y bienestar social**, n. 138, p. 185-221, 2017.

TALÉNS VISCONTI, Eduardo Enrique. El derecho a la desconexión digital en el ámbito laboral.**Pertsonak eta Antolakunde Punlikoak Kudeatzekp Euskal Aldizkaria= Revista Vasca deGestión de Personas y Organizaciones Públicas**, n. 17, p. 150-161, 2019.

Como citar este documento:

MARTÍNEZ CRISTÓBAL, Daniel. El derecho fundamental de protección de datos de los trabajadores y el impacto de las nuevas tecnologías en el ámbito laboral en España. **Revista Opinião Jurídica**, Fortaleza, v. 22, n. 41, p. 34-62, set./dez. 2024. Disponível em: link do artigo. Acesso em: xxxx.