

**MONITORIZACIÓN DE LA ACTIVIDAD LABORAL
Y CUMPLIMIENTO NORMATIVO EN PROTECCIÓN
DE DATOS. ALGUNAS REFLEXIONES A PROPÓSITO
DE LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL
160/2021, DE 4 DE OCTUBRE DE 2021**

**Monitoring of work activity and personal data
protection compliance. Some reflections on the
judgment of the Constitutional Court 160/2021,
of October 4, 2021**

ROSA M^a GARCÍA PÉREZ
Universidad de Granada
rosagp@ugr.es

Cómo citar/Citation

García Pérez, R. M^a (2022).

Monitorización de la actividad laboral y cumplimiento
normativo en protección de datos. Algunas reflexiones a propósito
de la sentencia del Tribunal Constitucional 160/2021, de 4 de octubre de 2021.

Derecho Privado y Constitución, 41, 277-309.

doi:<https://doi.org/10.18042/cepc/dpc.41.02>

(Recepción: 31/08/2022; aceptación tras revisión: 18/10/2022; publicación: 21/12/2022)

Resumen

La sentencia del Tribunal Constitucional 160/2021, de 4 de octubre de 2021, es el último pronunciamiento del máximo intérprete de nuestra Carta Magna sobre la tensión existente entre el poder de control empresarial y los derechos fundamentales del trabajador desde la perspectiva de la protección de datos de carácter personal. Esta resolución judicial, aunque asentada en el sistema legal anterior a la nueva realidad normativa derivada de la aplicación del Reglamento General de Protección de Datos europeo y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, reviste interés por el enfoque ofrecido de dos

aspectos directamente ligados a elementos configuradores del derecho a la protección de datos, a saber, la imbricación de los principios aplicables a cualquier tratamiento de datos personales con el tradicional juicio de proporcionalidad exigido por la doctrina constitucional española y el papel de la negociación colectiva en la configuración del derecho a la protección de datos personales.

Palabras clave

Protección de datos personales; principios aplicables al tratamiento; control tecnológico empresarial; negociación colectiva.

Abstract

The judgment of the Constitutional Court 160/2021, of October 4, is the last pronouncement of the highest interpreter of our Magna Carta on the tension between the power of corporate control and the fundamental rights of the employee from the perspective of the personal data protection. This judicial resolution, although settled in the legal system of data protection prior to the new regulation derived from the application of the European General Data Protection Regulation and the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights, is of interest for the approach made to two aspects directly linked to configuring elements of the right to data protection: the principles applicable to any processing of personal data, and their interweaving with the traditional judgment of proportionality required by the Spanish constitutional doctrine, and the role of collective agreements in the configuration of the right to the protection of personal data.

Keywords

Personal data protection; principles relating to processing of personal data; business technology control; collective agreements in the employment context.

SUMARIO

I. INTRODUCCIÓN. II. MONITORIZACIÓN DE LA ACTIVIDAD LABORAL CON FUNCIONES DE CONTROL EMPRESARIAL Y PROTECCIÓN DE DATOS PERSONALES: LÍNEAS JURISPRUDENCIALES: 1. La jurisprudencia constitucional sobre la transparencia informativa del control empresarial. 2. La doctrina del Tribunal Europeo de Derechos Humanos. III. PODER DE DIRECCIÓN EMPRESARIAL Y TUTELA DE LOS DATOS PERSONALES DE LA PERSONA TRABAJADORA EN LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL 160/2021, DE 4 DE OCTUBRE DE 2021: 1. Antecedentes de hecho. 2. Doctrina: 2.1. *Inexistencia de afectación del derecho a la protección de datos por las grabaciones efectuadas a las personas trabajadoras*. 2.2. *No afectación del derecho fundamental a la protección de datos por el incumplimiento del compromiso pactado con la representación de los trabajadores de no utilizar las grabaciones con fines disciplinarios*. IV. NOTAS A PROPÓSITO DE LOS RAZONAMIENTOS JURÍDICOS DEL FALLO: 1. Control tecnológico laboral y cumplimiento normativo: no solo la transparencia, los principios de minimización y limitación de la finalidad como parte del núcleo esencial del derecho a la protección de datos personales. 2. La especial trascendencia constitucional: incidencia de la negociación colectiva en el derecho fundamental, ¿cuestión de legalidad ordinaria? BIBLIOGRAFÍA.

I. INTRODUCCIÓN

La interacción entre el derecho fundamental a la protección de datos personales y el ámbito de las relaciones laborales ha experimentado un notable incremento en los últimos años. Así lo reflejan tanto los numerosos conflictos solventados por las diferentes instancias judiciales que conforman el sistema de protección multinivel de los derechos fundamentales (Tribunal Europeo de Derechos Humanos, Tribunal de Justicia de la Unión Europea, Tribunal Constitucional, Tribunal Supremo y el resto de jueces y Tribunales), como el aumento de procedimientos que, referidos al ámbito de las relaciones entre

empleador y empleado, acaban sometidos al control de la Agencia Española de Protección de Datos¹.

Uno de los terrenos más abonados como fuente de conflicto es la utilización de sistemas tecnológicos y digitales que comportan el tratamiento de datos personales del trabajador como instrumentos empresariales de control y vigilancia de sus obligaciones laborales, tales como la implementación de herramientas biométricas (reconocimiento facial, de voz, del iris de los ojos, de la huella dactilar...), de vídeo o audiovigilancia, de geolocalización, de monitorización de los dispositivos digitales facilitados por la empresa, de rastreo de correos electrónicos y de navegaciones por internet, entre otros.

En este sentido, conviene partir del dato normativo que proporciona el art. 20.3 del Texto Refundido del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre (en adelante, ET), el cual faculta al empresario para «adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad...».

No obstante esta habilitación legal, que exige el respeto a la dignidad de la persona, no cabe desconocer que el uso de estos sistemas tecnológicos con funciones de control laboral impacta de lleno en la privacidad de la persona trabajadora, destacadamente desde la perspectiva de varios de sus derechos fundamentales reconocidos en la Constitución Española (en adelante, CE), como son el derecho a la intimidad (art. 18.1 CE), el derecho al secreto de sus comunicaciones (art. 18.3 CE) y el derecho a la protección de sus datos personales (art. 18.4 CE)². Aunque cada uno de estos derechos tiene

¹ Para una visión de conjunto de diferentes aspectos de las relaciones laborales a los que alcanza la observancia del cumplimiento normativo sobre protección de datos, puede consultarse la Guía sobre «La protección de datos en las relaciones laborales» (disponible en: <https://bit.ly/3gTWMiw>), publicada en mayo de 2021 por la AEPD con la finalidad de «proporcionar una orientación de carácter práctico, no vinculante, que facilite a los responsables del tratamiento de datos personales y a las personas o entidades encargadas del tratamiento» el cumplimiento normativo.

² Es doctrina constitucional reiterada que «la celebración de un contrato de trabajo no implica, en modo alguno, la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano, ni la libertad de empresa (art. 38 CE) legitima que los trabajadores hayan de soportar limitaciones injustificadas de sus derechos fundamentales y libertades públicas (por todas, STC 80/2001, de 26 de marzo, FJ 3, con cita de la STC 88/1985, de 19 de julio, FJ 2)», así como que «tampoco el ejercicio de las facultades organizativas y disciplinarias del empleador pueden servir en ningún caso para limitar indebidamente derechos fundamentales

sus propios contornos y configuración jurídica, la determinación de cuándo esa injerencia en los derechos fundamentales de la persona trabajadora sigue los parámetros de necesidad, idoneidad y proporcionalidad que justifican su licitud y legitimidad, y cuándo resulta excesiva, desproporcionada o arbitraria ha sido una cuestión con límites difusos sobre la que no ha existido consenso, pero cuya resolución resulta decisiva, como ha resaltado la doctrina social, especialmente a efectos de determinar la validez o invalidez tanto de la prueba que derive de la utilización de estos sistemas de control tecnológico para acreditar judicialmente el incumplimiento de sus obligaciones por parte de la persona trabajadora (arts. 11.1 Ley Orgánica del Poder Judicial y 90.2 Ley Reguladora de la Jurisdicción Social), como de la sanción disciplinaria que pudiera adoptarse (art. 55.5 ET)³.

En este trabajo se abordará la tensión entre el poder de control empresarial y los derechos fundamentales del trabajador desde la perspectiva de la

(por todas, STC 181/2006, de 19 de junio, FJ 6), dada su posición preeminente en nuestro ordenamiento jurídico, que, en cuanto «proyecciones de los núcleos esenciales de la dignidad de la persona» (art. 10.1 CE) y fundamento del propio Estado democrático proclamado en el art. 1 CE (entre otras, STC 56/2008, de 14 de abril, FJ 4), operan como límites infranqueables que el empresario no puede rebasar en ejercicio de su poder de dirección. De modo que, frente al ejercicio de un derecho fundamental, solo otro derecho fundamental o interés constitucionalmente relevante puede ser opuesto como límite» (STC 89/2018, de 6 de septiembre).

³ En la doctrina jurisprudencial no existe una respuesta uniforme sobre la incidencia que la ilicitud de la prueba, por vulnerar los derechos fundamentales del trabajador, tenga en la sanción disciplinaria o el despido. Fundamentalmente son tres las posiciones mantenidas: a) La nulidad de la prueba irradia sus efectos al despido, debiendo considerarse este también nulo; b) No existe comunicación de la nulidad de la prueba al despido, pues el art. 55.5 ET solo impone la nulidad del despido cuando la decisión empresarial de despedir viene motivada o tiene por objetivo vulnerar un derecho fundamental del trabajador; y c) La ilicitud de la prueba solo conlleva la imposibilidad de utilizarla para acreditar el incumplimiento laboral del trabajador, pero no excluye la posibilidad de analizar la licitud del despido con el resto de medios de prueba. En relación con esta cuestión, la reciente STC 61/2021, de 15 de marzo, considera que los efectos de la nulidad de una prueba ilícita sobre la calificación del despido es una cuestión de legalidad ordinaria, que no entra dentro del contenido esencial del derecho fundamental vulnerado, correspondiendo a la jurisdicción ordinaria su determinación. La sentencia cuenta con un voto particular de la magistrada Balaguer Callejón en el que manifiesta su discrepancia con la mayoría, argumentando a favor de la trascendencia constitucional de la cuestión y de la irradiación de la nulidad de la prueba a la calificación del despido. Para un comentario sobre la misma, vid. Todolí Signes, A. (2021a: 237-244); Valle Muñoz, F.A. (2021: 42-46); (2022: 16-17).

protección de datos de carácter personal, al hilo del análisis y comentario de uno de los últimos pronunciamientos del Tribunal Constitucional (en adelante, TC). Se trata de la sentencia 160/2021, de 4 de octubre de 2021. Esta resolución judicial, aunque asentada en el sistema legal de protección de datos anterior a la nueva realidad normativa derivada de la aplicación del Reglamento General de Protección de Datos europeo (en adelante, RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), reviste interés por el enfoque realizado de dos aspectos directamente ligados a principios configuradores del derecho a la protección de datos, que han sido reforzados con perfiles innovadores en el nuevo régimen normativo.

El primero de los aspectos se refiere a la incidencia que, sobre la validez de los sistemas de control laboral, pueda tener un deficitario cumplimiento de los principios aplicables a cualquier tratamiento de datos personales (art. 5. RGPD) y la necesaria ponderación de los intereses en juego materializada en el tradicional juicio de proporcionalidad exigido por la doctrina constitucional, en el sentido de que cualquier medida limitativa de derechos fundamentales debe superar un triple enjuiciamiento: su idoneidad para conseguir el objetivo propuesto; su necesidad, de modo que no exista otra medida más moderada o menos gravosa para conseguir el propósito buscado; y, finalmente, su razonabilidad o equilibrio, en el sentido de que se deriven de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, no excediendo, objetiva y temporalmente, el grado de intrusión en el derecho fundamental más de lo estrictamente necesario⁴.

El segundo elemento de interés se refiere al papel que la negociación colectiva en el ámbito laboral pueda desempeñar en la propia configuración del derecho a la protección de datos personales, cabiendo plantear si la infracción de lo pactado constituye o no una vulneración constitucional del derecho fundamental a la protección de datos personales de las personas trabajadoras.

Conviene previamente repasar la doctrina recaída hasta la fecha sobre la colisión entre ejercicio de las potestades de control laboral por el empleador y el derecho a la protección de datos de la persona trabajadora, tanto en la jurisprudencia constitucional como, en razón de su valor interpretativo reconocido por el art. 10.2 CE, en el acervo doctrinal resultante de la interpretación efectuada por el Tribunal Europeo de Derechos Humanos del Convenio para la Protección de los Derechos Humanos y de las Libertades

⁴ Véase, por todas, STC, Sala Primera, 207/1996, de 16 de diciembre de 1996 (Fundamento jurídico 4.E).

Fundamentales (en adelante, CEDH); revisión que permitirá, a buen seguro, una mejor comprensión y valoración de la sentencia objeto de análisis.

No obstante, en la actualidad, hay que destacar las novedades introducidas por la LOPDGDD, norma que por primera vez en el ordenamiento jurídico español presta atención al conflicto entre el control empresarial de la actividad laboral y los derechos fundamentales de las personas trabajadoras. En este sentido, y partiendo del art. 88 RGPD, que faculta a los Estados miembros para que, a través de disposiciones legislativas o de convenios colectivos, puedan establecer previsiones específicas para la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, haciendo una llamada de atención a la observancia del principio de transparencia del tratamiento, el legislador español ha insertado ciertas previsiones normativas en relación con el derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral —art. 87—, de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo —art. 89— y de sistemas de geolocalización en el ámbito laboral —art. 90—. Asimismo, el art. 91 de la norma nacional contempla expresamente la posibilidad de que el convenio colectivo sirva de cauce para incorporar garantías adicionales en materia de protección de datos de las personas trabajadoras.

II. MONITORIZACIÓN DE LA ACTIVIDAD LABORAL CON FUNCIONES DE CONTROL EMPRESARIAL Y PROTECCIÓN DE DATOS PERSONALES: LÍNEAS JURISPRUDENCIALES

1. LA JURISPRUDENCIA CONSTITUCIONAL SOBRE LA TRANSPARENCIA INFORMATIVA DEL CONTROL EMPRESARIAL

El derecho fundamental a la protección de datos de las personas trabajadoras, en actuaciones desarrolladas en el ejercicio de las potestades de control empresarial de la prestación laboral, es invocado por primera vez en la jurisprudencia constitucional en la STC 29/2013, de 11 de febrero.

Previamente, la conflictividad pivotaba principalmente sobre la eventual intromisión ilegítima en el derecho a la intimidad de la persona trabajadora provocada por los mecanismos o dispositivos de control utilizados por el empleador, señaladamente, a través de la vídeo o audio vigilancia empresarial. Así, en la STC 98/2000, de 10 de abril, a propósito de la instalación de micrófonos en las dependencias del Casino de La Toja con conocimiento de los trabajadores y del comité de empresa (vigilancia conocida e informada), el TC apreció la existencia de una vulneración del derecho a la intimidad al exceder

las medidas de audiovigilancia de lo estrictamente necesario para garantizar el interés empresarial, considerando la instalación microfónica una intromisión ilegítima en el derecho a la intimidad, al no quedar acreditado que su uso resultase indispensable para la seguridad y el buen funcionamiento del casino, que ya contaba con un sistema de cámaras de seguridad. En la STC 186/2000, de 10 de julio, relativa a un supuesto de grabación secreta de la actividad laboral mediante la instalación de un circuito cerrado de televisión, con la finalidad de controlar las cajas registradoras y mostradores de un economato ante las sospechas de hurto por parte de las trabajadoras, el TC afirma su legitimidad, y consiguiente validez probatoria de las grabaciones, al considerar la medida, adoptada con carácter temporal, ajustada al principio de proporcionalidad, aún no habiendo sido puesta en conocimiento del comité de empresa ni de los trabajadores afectados. No obstante, conviene indicar que los hechos que motivan esta resolución son anteriores a la entrada en vigor de la actualmente derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), cuyo art. 5 consagraba el derecho a recibir información por parte de los interesados, de «modo expreso, preciso e inequívoco» en el momento de la recogida de datos.

El primer pronunciamiento, como se ha indicado, que tiene como eje el derecho fundamental a la protección de datos es la STC 29/2013, de 11 de febrero, en un conflicto de incumplimiento laboral acreditado a través de las imágenes obtenidas por el sistema de videovigilancia implementado por la Universidad de Sevilla con la finalidad de garantizar la seguridad de sus instalaciones y controlar los accesos. Frente a la tesis del Fiscal, para quien, cumplidas las exigencias previstas en la Ley Orgánica 15/1999 relativas a la inscripción del fichero en la AEPD y a la existencia de carteles informativos, la utilización de las imágenes con finalidad de control laboral resultaba una medida idónea, necesaria y proporcionada (test de proporcionalidad), el TC pone en valor el derecho del afectado a ser informado sobre quién posee los datos personales y con qué fin como parte del núcleo esencial de la definición constitucional del art. 18.4 CE (en el mismo sentido que ya recogiera la STC 292/2000, de 30 de noviembre), aunque advierte que tal «exigencia informativa no puede tenerse por absoluta, dado que cabe concebir limitaciones por razones constitucionalmente admisibles y legalmente previstas, pero no debe olvidarse que la Constitución ha querido que la ley, y solo la ley, pueda fijar los límites a un derecho fundamental, exigiendo además que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido».

En caso examinado, el TC consideró no ser suficiente la mera existencia de distintivos informativos de la presencia de cámaras, afirmando ser

«necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo». A ello se le sumaba, según el TC, la falta de una habilitación legal expresa que tolerase la limitación del derecho de información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales y la insuficiente justificación que tal omisión encontraría en la protección del interés empresarial de controlar la actividad laboral. En relación con este último aspecto, se afirma que esa «lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial. En efecto, se confundiría la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art. 20.3 LET en relación con el art. 6.2 LOPD) con la constitucionalidad del acto (que exige ofrecer previamente la información necesaria, art. 5 LOPD)».

Por tanto, el TC dictamina no ser suficiente que «el tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa». Consecuentemente, declaró nulas las sanciones disciplinarias impuestas con base únicamente en la grabación de imágenes dirigidas a controlar los accesos pero utilizadas con fines de supervisión laboral sin haber advertido de ello a las personas trabajadoras, por ser una prueba lesiva del derecho fundamental a la protección de datos personales.

Tal interpretación del principio de transparencia, como contenido esencial del derecho a la protección de datos en el ámbito de las facultades de control empresarial, experimenta un notable giro en una sentencia posterior que, considerando cumplido el deber de información cuando la persona trabajadora conoce la existencia de cámaras de vigilancia a través de carteles informativos, admite la validez de las grabaciones de imágenes como prueba del incumplimiento laboral aunque fuesen realizadas con finalidades distintas a la de control laboral. Se trata de la STC 39/2016, de 3 de marzo de 2016 en la que se enjuicia la eventual nulidad de un despido acreditado por un sistema de videograbación, cuya doctrina viene siendo reiteradamente aplicada por

el Tribunal Supremo, especialmente desde la sentencia 654/2017, de 31 de enero de 2017 hasta la actualidad⁵.

En este caso, el TC otorga validez, como medio para acreditar la apropiación de dinero por parte de una empleada mediante falsas operaciones de devolución de prendas de vestir, a las imágenes obtenidas por las cámaras de seguridad instaladas en una tienda de la empresa Bershka BSK España S.A. (perteneciente al grupo Inditex), cuya existencia, no comunicada a los trabajadores, estaba advertida a través de un cartel en un lugar visible del escaparate. Entiende el máximo intérprete constitucional que, «teniendo la trabajadora información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo, y habiendo sido tratadas las imágenes captadas para el control de la relación laboral, no puede entenderse vulnerado el art. 18.4 CE», dado que lo «importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque solo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados».

De esta nueva doctrina constitucional, disienten los magistrados Valdés Dal-Ré, Asua Batarrita y Xiol Ríos en dos votos particulares, en los que, resumidamente: a) se critica el retroceso en la protección de los derechos de los trabajadores que representa el cambio jurisprudencial operado respecto de la STC 29/2013, sin que se haya ofrecido al mismo tiempo la necesaria justificación jurídico-constitucional de tal modificación; b) se entiende que los poderes empresariales de control no son expresiones directas de los derechos amparados por los arts. 33 y 38 CE que proceda confrontar, de manera mecánica y sin mayor argumentación, con los derechos fundamentales de los trabajadores, provocando un juicio de ponderación entre derechos constitucionales; c) se censura que pueda erigirse como elemento decisivo para el juicio de constitucionalidad el contenido de la Instrucción 1/2006 sobre videovigilancia de la AEPD; d) se considera inaceptable que la mera información dirigida al público sea suficiente para cumplir el deber de información a los trabajadores; y e) se sostiene que representa dinamitar el contenido esencial del derecho fundamental a la protección de datos el admitir que «el empresario, ante cualquier sospecha que pueda abrigar, está autorizado por la Constitución a instalar libremente (siempre que en el entorno haya un aviso al público sobre la existencia de cámaras de seguridad) cámaras para el control

⁵ Entre las sentencias de la Sala de los Social más recientes, por ejemplo, véanse SSTs 817/2021 de 21 de julio; 285/2022, de 30 de marzo; y 2252/2022, de 1 de junio.

del trabajo orientadas a seleccionar en primer plano determinadas posiciones ocupadas por los trabajadores», equiparando el supuesto de cámaras instaladas para una concreta vigilancia de determinado trabajador ante la sospecha de actos ilícitos, al del hallazgo casual por las cámaras de vigilancia al público.

2. LA DOCTRINA DEL TRIBUNAL EUROPEO DE DERECHO HUMANOS

La Gran Sala del Tribunal Europeo de Derechos Humanos (TEDH) ha tenido oportunidad de pronunciarse sobre el derecho al respeto a la vida privada (art. 8 CEDH) en el ámbito laboral en lo que a la protección de datos personales se refiere, con motivo de revisiones extraordinarias de decisiones previamente adoptadas por diferentes secciones del propio Tribunal.

Destacamos en primer lugar la sentencia de 5 de septiembre de 2017, en el caso conocido como «Bărbulescu II». En esta resolución, el TEDH rectifica el criterio adoptado por la sección cuarta del mismo Tribunal en sentencia de 12 enero de 2016 («Bărbulescu I») y estima la demanda interpuesta por un ciudadano rumano contra la República de Rumanía por considerar que ha existido una intromisión indebida en su vida privada y una violación del derecho al secreto de las comunicaciones en el despido del demandante, decidido tras el control y revisión por la parte empresarial de los mensajes y comunicaciones personales verificadas a través de la utilización de un sistema de mensajería instantánea en el centro de trabajo. El TEDH entiende que la monitorización de los equipos de los empleados requiere que estos hubiesen sido debidamente informados mediante un aviso o comunicación previa del alcance y la naturaleza de la supervisión o de la posibilidad de acceder al contenido de sus comunicaciones, lo que no quedó acreditado en el caso enjuiciado.

Pero, además de esa necesaria información previa sobre la naturaleza de la vigilancia, el TEDH establece un elenco de requisitos o reglas adicionales, a tener en cuenta a efectos de garantizar el respeto a la vida privada y el secreto de la correspondencia en el ámbito de la vigilancia laboral, relativos a los siguientes aspectos: a) el alcance de la vigilancia por el empleador y el grado de intrusión en la vida privada del empleado (nivel de privacidad en la zona objeto de la vigilancia, limitaciones de tiempo y espacio, y número de personas que tienen acceso a los resultados); b) las razones legítimas del empleador que justifican la vigilancia y el alcance de la misma (a mayor intrusión, mayor justificación); c) la posible existencia de un sistema de vigilancia basado en métodos y medidas menos intrusivos; d) las consecuencias de la vigilancia para el empleado sometido a ella; e) la facilitación al trabajador de medidas apropiadas para impedir la injerencia en su vida privada (entre otras, el suministro de información a los interesados o a los representantes del personal en cuanto a la

instalación y el alcance de la vigilancia, la declaración de esa medida a un órgano independiente o la posibilidad de presentar una denuncia).

Relevante es también la sentencia de la Gran Sala de 17 de octubre de 2019, en el caso conocido como «López Ribalda II» contra España, en la que el TEDH revisa el pronunciamiento de su Sala tercera de 9 de enero de 2018 (conocido como «López Ribalda I»). El TEDH examina la eventual violación por la entidad Mercadona del derecho al respeto a la vida privada en el despido de varias trabajadoras producido a raíz de unas grabaciones de imágenes. La empresa, tras detectar en uno de sus establecimientos ciertos descuadres entre el inventario y el saldo de caja que provocaron pérdidas, instaló cámaras de vigilancia, algunas visibles y otras ocultas con el fin de confirmar sus sospechas sobre el origen de la situación. Las visibles enfocaban los accesos al establecimiento, mientras que las ocultas lo hacían a los mostradores y cajas registradoras. La empresa solo informó a sus trabajadores de la instalación de las cámaras visibles, pero no de las cámaras ocultas. Las grabaciones de las cámaras ocultas, realizadas durante dos semanas, revelaron que cinco trabajadoras eran las responsables de los robos y se procedió a su despido disciplinario. La impugnación por las trabajadoras de esa extinción contractual con base en una vulneración de su derecho a la intimidad, al no haber sido debidamente informadas sobre la instalación y el uso de las cámaras ocultas, es desestimada por las diferentes instancias judiciales nacionales, que consideran el uso de la videovigilancia encubierta en el lugar de trabajo, sin una comunicación previa, conforme a la potestad conferida al empresario de utilizar de medidas de control y vigilancia que considere adecuadas (art. 20 ET), siempre que resulten necesarias, idóneas y proporcionadas.

La Sala tercera del TEDH en el primer pronunciamiento de 2018 («López Ribalda I») entendió que la empresa, con la medida adoptada, había vulnerado derecho al respeto de la vida privada y a la protección de datos personales, por una parte, por no haber cumplido con la obligación de informar previamente, de manera precisa e inequívoca a los interesados sobre la existencia y las características particulares de un sistema que recopila datos personales (art. 5 LOPD) y, por otra parte, por no superar el test de proporcionalidad al someter a videovigilancia a todos los trabajadores, no solo a los sospechosos, durante toda la jornada laboral y sin límite temporal.

La Gran Sala del TEDH, al conocer del recurso contra este pronunciamiento, lo rectifica considerando que, a fin de garantizar la proporcionalidad de las medidas de videovigilancia en el lugar de trabajo, deben tenerse en cuenta los requisitos o criterios fijados en la sentencia *Bărbulescu II* y, aplicándolos al caso enjuiciado, dictamina que no se ha vulnerado el derecho al respeto de la vida privada de los demandantes en atención a que:

- a) La instalación de la videovigilancia estaba justificada por razones legítimas (la sospecha de robos ante las pérdidas significativas registradas durante varios meses y el fin de garantizar la protección de su propiedad y el buen funcionamiento de la empresa);
- b) La medida fue limitada en cuanto a las áreas y al personal que se vigilaba (puesto que solo cubrían el área de pago, centrándose en las zonas de cajas donde probablemente se cometían los robos); el lugar (abierto al público en contacto permanente con los clientes); la duración (que no excedió de lo necesario para identificar a los responsables); y en razón a que las grabaciones no fueron utilizadas por el empleador para ningún propósito diferente al de descubrir a los responsables de las pérdidas y adoptar medidas disciplinarias contra ellos.
- c) La existencia en la legislación interna de instrumentos y recursos para evitar la indebida injerencia en el derecho a la protección de datos de los interesados (derecho de información, derechos de acceso, rectificación y supresión respecto de los datos recogidos, test de proporcionalidad implementado por la jurisprudencia constitucional).
- d) A propósito de la falta de información a los trabajadores sobre las cámaras ocultas, el Tribunal considera que el principio de transparencia, y consiguiente derecho de información de las personas interesadas, es fundamental en el marco de las relaciones laborales, de modo que «solo un requisito primordial relacionado con la protección de intereses públicos o privados importantes podría justificar la falta de información previa». Sentado lo anterior, no obstante y a la vista de las circunstancias del caso concreto, la falta de información previa por la empresa se entiende justificada por la concurrencia de tales importantes intereses. Advierte el TEDH que, si bien no es aceptable la instalación de una videovigilancia encubierta ante la más mínima sospecha de apropiación indebida o de cualquier otro acto ilícito por parte de los empleados, «la existencia de una sospecha razonable de que se ha cometido una falta grave y la magnitud de las pérdidas identificadas en el presente caso pueden parecer una justificación de peso», más aún cuando «el buen funcionamiento de una empresa se ve amenazado no solo por la sospecha de mala conducta de un solo empleado, sino más bien por la sospecha de una acción concertada de varios empleados».

De estos pronunciamientos, puede concluirse que la doctrina del TEDH resulta ser más respetuosa con la configuración del derecho fundamental a la protección de datos personal que la derivada de la STC 39/2016, de 3 de

marzo de 2016, reiteradamente acogida por nuestro Tribunal Supremo⁶. Para el Tribunal de Estrasburgo el principio de transparencia, y consiguiente deber de información en el ámbito del control laboral, exige aplicar el principio de limitación de la finalidad del tratamiento de manera más rigurosa, siendo necesario como regla de principio la notificación o comunicación previa, clara y precisa de la existencia y alcance del sistema de supervisión implementado que recopila datos de carácter personal, así como la no utilización de estos datos para una finalidad diferente; la omisión de ese deber informativo será excepcional y circunscrita «exclusivamente a los supuestos en que concurre un imperativo preponderante relativo a la protección de los intereses públicos o privados importantes, como cuando existan sospechas fundadas de actos ilícitos graves»⁷.

III. PODER DE DIRECCIÓN EMPRESARIAL Y TUTELA DE LOS DATOS PERSONALES DE LA PERSONA TRABAJADORA EN LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL 160/2021, DE 4 DE OCTUBRE DE 2021

1. ANTECEDENTES DE HECHO

La STC 160/2021, de 4 de octubre, enjuicia un supuesto de control empresarial a través de la monitorización de las llamadas telefónicas recibidas y realizadas en el lugar de trabajo.

El procedimiento se inicia por un trabajador de la empresa Telefónica, encargado de atender telefónicamente a los clientes, en calidad de asesor comercial, al que la empresa notifica su despido el 6 de junio de 2014 por entender que ha cometido una falta muy grave, al amparo de lo dispuesto en el art. 212 i) y j) de la reglamentación laboral interna, en relación con el art. 54.2 b) y d) del ET (indisciplina o desobediencia y transgresión de la buena fe contractual). El despido fue justificado al comprobar la empresa que, durante diferentes días de los meses de marzo y abril de 2014, y hasta en un total de ocho ocasiones, se prestó a los clientes «una deficiente atención y una dilación injustificada en la resolución de los problemas que le planteaban, sin seguir los procedimientos establecidos para encauzar las incidencias, incluso

⁶ Con diferente perspectiva crítica, veáanse los comentarios a esta sentencia de Molina Navarrete, C. (2019: 336-343) y de Monereo Pérez, J. L. y Ortega Lozano P. G. (2019: 1-10).

⁷ Goñi Sein (2021: 4134-4135).

en algunos casos facilitándoles información errónea». Resulta probado que, en varias ocasiones, la empresa advierte al trabajador sobre la incorrección de su proceder, dándole las indicaciones pertinentes para una actuación adecuada.

El incumplimiento laboral fue constatado por el sistema de monitorización, continuado, general y permanente, de las llamadas telefónicas (captación y grabación de la voz) de los asesores comerciales, que la empresa venía haciendo en virtud de un pacto firmado con la representación de los trabajadores el 18 de noviembre de 2003. En dicho acuerdo, en relación con la grabación de las llamadas, se afirmaba que «la dirección de la empresa manifiesta que la finalidad del proyecto es la identificación de carencias formativas para la prestación de los servicios de atención y ventas, que permita la elaboración de planes individuales de formación y mejora de competencias capaces de superar las referidas carencias [...] asumiendo la empresa el compromiso de que la monitorización no tendrá en ningún caso como objetivo su utilización como un mecanismo disciplinario»⁸.

El trabajador impugnó el despido solicitando su nulidad por entender vulnerado su derecho a la protección de datos personales, al haber incumplido la empresa su compromiso de que la grabación de las conversaciones nunca tendría una finalidad disciplinaria.

En primera instancia, la sentencia 276/2015 del Juzgado de lo Social de Zaragoza, de 9 de junio de 2015, declaró la improcedencia del despido,

⁸ Previamente, desde 2001 y antes de la existencia del pacto firmado por la empresa con la representación de los trabajadores, un sistema similar de grabación de llamadas telefónicas y monitorización de los trabajadores de Telefónica motivó una demanda colectiva sindical solicitando la ilegalidad de las escuchas realizadas por la empresa por afectar a la intimidad de los trabajadores. En este caso, a diferencia del supuesto de hecho de la STC 160/2021, el control de las conversaciones de los asesores comerciales con los clientes no se realizaba de manera constante, sino de forma aleatoria, aunque sí permanentemente. El Tribunal Supremo, Sala de lo Social, en sentencia 7798/2003, de 5 de diciembre de 2003, entendió ajustado a la legalidad este control en la medida en que «el teléfono controlado se ha puesto a disposición de los trabajadores como herramienta de trabajo para que lleven a cabo sus funciones de telemarketing y a la vez disponen de otro teléfono para sus conversaciones particulares, si, como se ha apreciado, los trabajadores conocen que ese teléfono lo tienen sólo para trabajar y conocen igualmente que puede ser intervenido por la empresa, si además la empresa sólo controla las llamadas que recibe el trabajador y no las que hace, si ello lo realiza de forma aleatoria —un 0.25 %—, y con la finalidad exclusiva de controlar la buena realización del servicio para su posible mejora, la única conclusión razonable a la que se puede llegar es a la de que se trata de un control proporcionado a la finalidad que con el mismo se pretende»

dado que del contenido de las grabaciones no derivaba un incumplimiento grave de las obligaciones laborales del trabajador, pero desestimó su nulidad en razón de que la monitorización de las llamadas resultaba ser una medida proporcionada dentro de las facultades de control empresarial, de la que tenían perfecto conocimiento los asesores comerciales, afirmando que el pacto alcanzado en 2003 con la representación de los trabajadores «no excluye en modo alguno que la empresa pueda utilizar este soporte como medio de prueba en caso de constatar, no ya un defecto de formación en el trabajador sino un incumplimiento grave de sus deberes laborales».

La Sala de lo Social del Tribunal Superior de Justicia de Aragón, en sentencia 379/2016, de 27 de mayo de 2016, tomando como referencia la jurisprudencia del TS y la STC 39/2016, desestimó el recurso de suplicación, confirmando la validez de la prueba de las grabaciones por falta de lesión del derecho a la protección de datos del trabajador, al considerar que el compromiso asumido por la empresa en 2003 «en ningún caso puede traducirse en la inmunidad de los asesores frente al control empresarial de la actividad laboral que desempeñan, siempre que se realice en condiciones de respeto a su esfera íntima inatacable». Como se ha advertido⁹, «la tesis de los juzgadores es que aunque la empresa haya renunciado mediante pacto colectivo al uso del poder disciplinario ese pacto debe considerarse ineficaz (o nulo), dado que la empresa, aunque quiera y así lo manifieste en un acuerdo colectivo, no puede renunciar al poder disciplinario».

Interpuesto recurso de casación para la unificación de doctrina por el demandante, resultó inadmitido por falta de contradicción. Contra este pronunciamiento, formulado mediante auto de la Sala de Social del TS de 18 de mayo de 2017, el trabajador interpuso recurso de amparo por considerar la «especial trascendencia constitucional» del asunto, permitiendo al Tribunal «aclarar la doctrina contenida en la STC 29/2013 con el fin de (i) concretar la amplitud del derecho a la intimidad personal a que se refiere el art. 18.4 CE en el puesto de trabajo, dadas las nuevas realidades sociales y el incremento de la vigilancia y control al través de medios informáticos y digitales, y (ii) el efecto sobre este derecho del incumplimiento empresarial del compromiso de no usar las grabaciones con fines disciplinarios».

En trámite de alegaciones, el Ministerio Fiscal interesó la desestimación del recurso de amparo, por considerar, a partir de los hechos probados, que la decisión empresarial no era inmotivada, arbitraria, o irrazonable y cumplía con los cánones requeridos por la jurisprudencia constitucional, considerando que el objeto del recurso solo de manera tangencial afectaba al derecho

⁹ Todolí Signes (2021b).

fundamental al estar centrado exclusivamente en dilucidar «el alcance del compromiso asumido por la empresa», referido a la renuncia empresarial a la utilización de las grabaciones con fines disciplinarios.

El TC admitió a trámite el recurso apreciando la concurrencia de una especial trascendencia constitucional (art. 50.1 LOTC), al afectar la resolución del conflicto «a una faceta de un derecho fundamental sobre el que no hay doctrina de este Tribunal». En concreto, considera que la jurisprudencia constitucional ha abordado la relevancia de grabaciones sonoras sobre los derechos fundamentales en el contexto de las relaciones laborales, pero solo desde la perspectiva del derecho a la intimidad (art. 18.1 CE), y no desde la protección de datos de carácter personal (art. 18.4 CE), o solo desde la óptica de la falta de conocimiento de la grabación de imágenes durante el desarrollo de la actividad laboral (STC 39/2016, de 3 de marzo), pero no en situaciones como la que plantea la singularidad del caso concreto, en el que «si bien los trabajadores —en este caso asesores comerciales de una compañía de telefonía— eran conocedores del hecho de la grabación, tenían un compromiso expreso de la empresa de que en ningún caso tendrían como objetivo su utilización como un mecanismo disciplinario. Por tanto, la trascendencia constitucional del asunto consiste en determinar la relevancia que para la configuración del derecho a la protección de datos del carácter personal (art. 18.4 CE) tienen las condiciones pactadas entre las partes respecto del uso de los datos de carácter personal obtenidos mediante estas grabaciones» (Fundamento jurídico 2).

2. DOCTRINA

Centrado el objeto del recurso en la determinación de la eventual vulneración del derecho a la protección de datos del trabajador por la utilización de las grabaciones sonoras para acreditar el incumplimiento laboral, pese al compromiso de la empresa de no utilizarlas como mecanismo disciplinario, el TC analiza por separado, en primer lugar, la incidencia de la monitorización del trabajo en el derecho a la protección de datos y, en segundo término, si el incumplimiento del compromiso asumido por la empresa de no utilizar las grabaciones con fines disciplinarios repercute en el derecho a la protección de datos.

2.1 *Inexistencia de afectación del derecho a la protección de datos por las grabaciones efectuadas a las personas trabajadoras*

A propósito de esta cuestión, el TC repasa la última jurisprudencia constitucional sobre el empleo de grabaciones de imágenes de las personas trabajadoras con fines disciplinarios, con especial mención de la STC 39/2016 y de la STEDH de 17 de octubre de 2019 («López Ribalda II»), si bien omite

cualquier referencia a la STC 29/2013 alegada por el recurrente para justificar la trascendencia constitucional de su demanda de amparo.

En este sentido considera como elementos relevantes, en cuanto a la afectación del derecho a la protección de datos de carácter personal por las grabaciones sonoras realizadas a los trabajadores, los siguientes:

1. Las grabaciones en un soporte físico que facilitan la identidad de una persona constituyen un dato de carácter personal protegido por el art. 18.4 CE.
2. El derecho fundamental a la protección de datos de carácter personal persigue garantizar un poder de control sobre los datos personales de la persona afectada, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, formando parte de este derecho fundamental «la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo».
3. En su proyección a las relaciones laborales, si bien el consentimiento del trabajador para la obtención de datos «se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes» (STC 39/2016), el deber de información sigue existiendo, ya que forma parte del contenido esencial del derecho a la protección de datos, en los términos establecidos en la STC 39/2016.

Aplicando esta doctrina, y la relativa al deber de información en materia de grabaciones a empleados del TEDH, el TC concluye simplemente afirmando que no se violó el derecho fundamental del trabajador a la protección de datos de carácter personal, en razón de los siguientes hechos no controvertidos:

(i) Los asesores comerciales telefónicos eran connotadores de que sus conversaciones con los clientes eran grabadas y de que entre las obligaciones de la coordinación del servicio estaba proceder a las escuchas de las conversaciones al objeto de comprobar cómo desarrollan su trabajo;

(ii) La empresa había firmado con la representación de los trabajadores un documento de desarrollo de compromisos en que, en relación con la monitorización de las llamadas de los asesores, «la dirección de la empresa manifiesta que la finalidad del proyecto es la identificación de carencias formativas para la prestación de los servicios de atención y ventas, que permita la elaboración de planes individuales de formación y mejora de competencias capaces de superar las referidas carencias [...] asumiendo la empresa el compromiso de que la monitorización no tendrá en ningún caso como objetivo su utilización como un mecanismo disciplinario»;

(iii) El recurrente, asesor comercial telefónico de una compañía de telefonía, fue despedido por la comisión de una falta muy grave con fundamento en que durante diferentes días de los meses de marzo y abril de 2014 y hasta en un total de ocho ocasiones se había constatado una deficiente atención y una dilación injustificada en la resolución de los problemas que le planteaban los clientes, sin seguir los procedimientos establecidos para encauzar las incidencias, incluso en algunos casos facilitándoles información errónea. El demandante de amparo, con fundamento en el contenido de esas grabaciones, fue advertido en varias ocasiones de la incorrección de su proceder, dándose las indicaciones para una actuación adecuada, a pesar de la cual se mantuvo en su actitud;

(iv) En vía judicial se consideró que no existió nulidad del despedido por vulneración del art. 18.4 CE, aunque sí improcedencia ante la falta de constatación de un incumplimiento muy grave, con el argumento de que (i) la monitorización de las llamadas era una medida proporcionada dentro de las facultades de control empresarial de la que tienen perfecto conocimiento los asesores comerciales y (ii) lo acordado entre la empresa y los representantes de los trabajadores no excluye la utilización de las grabaciones como forma de comprobación del cumplimiento de la prestación de trabajo por parte de los asesores y, por tanto, el incumplimiento grave de sus deberes laborales que puedan llevar al ejercicio del poder disciplinario de la empresa.

No entra el máximo intérprete constitucional en el análisis concreto del cumplimiento de la garantía de transparencia, que exige proporcionar una información previa y útil que incorpore la finalidad de vigilancia empresarial, con la salvedad de los criterios que, según el TEDH, legitimarían el control tecnológico oculto o, según nuestro legislador actual, la menor intensidad de la información proporcionada en «el supuesto de que se haya captado la comisión flagrante de un acto ilícito» (art. 89.1, párr. 2º, LOPDGDD). Por el contrario, a juicio del TC, el empleador dio cumplimiento a las exigencias de información previa sobre la posibilidad y efectiva existencia de las observaciones y grabaciones de las conversaciones telefónicas, aun cuando la finalidad informada no coincidiese con los fines de control laboral. Tampoco lo hace en cuanto a la proporcionalidad de la medida consistente en la monitorización telefónica permanente, general y continua de todas las llamadas en relación con la finalidad de control laboral *ex* art. 22.3 ET, limitándose a reproducir los hechos probados y las argumentaciones esgrimidas en sede judicial laboral en orden a la consideración de la monitorización de las llamadas como una medida proporcionada y al hecho de que el pacto entre empresa y representantes

de los trabajadores no excluye la utilización de las grabaciones con fines de control empresarial¹⁰.

2.2. No afectación del derecho fundamental a la protección de datos por el incumplimiento del compromiso pactado con la representación de los trabajadores de no utilizar las grabaciones con fines disciplinarios

Descartado que la utilización por el empleador de las grabaciones de las llamadas con fines de control laboral y disciplinario exceda los límites requeridos por la jurisprudencia constitucional, el TC considera que el problema, desde la perspectiva del derecho a la protección de datos de carácter personal (art. 18.4 CE), «queda limitado a determinar la afectación que sobre este derecho tiene el supuesto incumplimiento del empleador de su compromiso con los representantes de los trabajadores de que la medida de observación y grabación del desarrollo laboral de esta categoría profesional “no tendrá en ningún caso como objetivo su utilización como un mecanismo disciplinario”».

A tal efecto, el TC constata que el empleador dio estricto cumplimiento a las exigencias de información previa respecto de la posibilidad y efectiva existencia de las observaciones y grabaciones de las conversaciones telefónicas, así como que las grabaciones fueron utilizadas en primera instancia con los fines de calidad de servicio y formativos a los que se comprometió la empleadora, siendo el demandante de amparo «advertido en varias ocasiones de la incorrección de su proceder —fines de calidad de servicio—, dándose las indicaciones para una actuación adecuada —fines formativos—», siendo la actitud reacia del trabajador a corregir su proceder la que posteriormente determinó el ejercicio de acciones disciplinarias y el despido del demandante de amparo.

En este aspecto concluye el Tribunal, siguiendo la línea ya planteada por el Ministerio Fiscal, que la interpretación, ante la reticencia del trabajador a seguir las indicaciones laborales, de si la cláusula pactada con los representantes de los trabajadores supone o no la renuncia al control empresarial a través de monitorización de las llamadas con fines disciplinarios, es una cuestión que corresponde decidir a los órganos judiciales, ajena al derecho fundamental a la protección de datos personales, por lo que desestima el recurso.

¹⁰ Como se ha indicado (Rojo Torrecilla, E. (2021)), «cabe plantear la duda, a efecto de debate, de si el Tribunal Constitucional ha hecho la adecuada valoración constitucional cuando está en juego un derecho recogido en la Constitución Española y para el que no debe servir únicamente la valoración efectuada en sede judicial».

IV. NOTAS A PROPÓSITO DE LOS RAZONAMIENTOS JURÍDICOS DEL FALLO

1. CONTROL TECNOLÓGICO LABORAL Y CUMPLIMIENTO NORMATIVO: NO SOLO LA TRANSPARENCIA, LOS PRINCIPIOS DE MINIMIZACIÓN Y LIMITACIÓN DE LA FINALIDAD COMO PARTE DEL NÚCLEO ESENCIAL DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Partiendo de que, con carácter general, en el ámbito de las relaciones laborales, la base jurídica que legitima el tratamiento de datos personales de las personas trabajadoras con finalidades de control del cumplimiento de sus obligaciones por las personas trabajadoras vendrá determinada por la existencia de una relación contractual conforme a lo señalado en el art. 6.1.b) del RGPD¹¹, la legitimidad de los sistemas de supervisión empresarial llevada a cabo por medios tecnológicos requerirá, por norma, el cumplimiento de todos los principios configuradores del derecho fundamental; principios jurídicos que constituyen deberes para el responsable del tratamiento y derechos para los interesados.

Estos principios, que forman parte del contenido esencial del derecho fundamental¹², y que cualquier responsable de un tratamiento de datos personales debe estar en condiciones de demostrar su cumplimiento (responsabilidad proactiva), se encuentran actualmente recogidos en el art. 5 RGPD, a saber: a) Licitud (el tratamiento debe encontrar justificación en alguna de las razones legales establecidas en los arts. 6 y 9 RGPD), lealtad (impide recabar

¹¹ Como ha advertido la AEPD en su Informe Jurídico 2020-0073 (accesible en <https://bit.ly/3ffgCVe>), este nuevo régimen exige, respecto contenido en la derogada Ley Orgánica de Protección de Datos de 1999, «un cambio de perspectiva en lo que respecta a los principios articuladores del derecho fundamental a la protección de datos de carácter personal y, en particular, a aquél que hacía del «principio de consentimiento» el eje central del derecho a la protección de datos», advirtiendo que «en las relaciones entre empleador y trabajador se viene considerando que la base jurídica del tratamiento no puede ser el consentimiento, dada la situación de desigualdad que se produce, lo que impide considerar que el mismo sea libre..., sino que con carácter general, en el ámbito de las relaciones laborales, dicha base jurídica vendrá determinada por la existencia de una relación contractual conforme a lo señalado en el art. 6.1.b) del RGPD: el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales».

¹² Sobre el contenido esencial del derecho a la protección de datos, A. Troncoso Reigada (2010: 111-168 y 2021: 847-907).

datos personales por medios fraudulentos, desleales o ilícitos e implica el reconocimiento de las expectativas razonables de privacidad del interesado) y transparencia (mediante la articulación de medidas para facilitar al interesado toda la información relativa al tratamiento y al uso de su información personal); b) Limitación de la finalidad, debiendo realizarse el tratamiento para fines determinados, explícitos y legítimos y proscribiéndose un tratamiento ulterior de los datos que sea incompatible con la finalidad original; c) Minimización, de modo que solo se realizará un tratamiento de datos personales cuando la finalidad pretendida no pueda realizarse por otros medios y, en tal caso, solo se utilizarán los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; d) Exactitud de los datos, debiendo adoptarse todas las medidas razonables para la supresión o rectificación sin dilación de los datos inexactos con respecto a los fines para los que se tratan; e) Limitación del plazo de conservación, no manteniendo los datos durante más tiempo del necesario para los fines del tratamiento; y f) Integridad y confidencialidad, garantizando la seguridad de los datos, de manera que queden protegidos contra el acceso, uso, modificación o difusión, no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

En el ámbito del control tecnológico empresarial, la garantía de la transparencia es la que ha venido suscitando la mayor conflictividad, en buena medida tras el devaluado cumplimiento del deber de información exigido por la doctrina constitucional tras la STC 39/2016; línea jurisprudencial controvertida que en la actualidad ha quedado circunscrita a aquel supuesto en el que la utilización de dispositivos de videovigilancia «haya captado la comisión flagrante de un acto ilícito por los trabajadores o empleados públicos», en cuyo caso «se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el art. 22.4 de esta Ley orgánica» (art. 89.1, segundo párrafo, LOPDGDD)¹³, es decir, la información genérica facilitada a través de «un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los arts. 15 a 22 del Reglamento 2016/679», pudiendo incluirse también en el propio dispositivo «un código de conexión o dirección de internet a esta información»¹⁴. Con

¹³ Véase López Balaguer, M. (2020: 364).

¹⁴ Norma que debilita el deber de transparencia en el ámbito laboral, respecto de la que se afirma su falta de compatibilidad con el RGPD, véase, en este sentido, la sentencia del Juzgado de lo Social núm 3 de Pamplona/Iruña de 18 de febrero de 2021 (Rec. 754/2020) y, previamente, del mismo Juzgado la sentencia de 18 de febrero de 2019 (Rec. 875/2018); esta última comentada por Romero Ródenas, M. J. y Moraru,

carácter general, sin embargo, como se indica en la propia norma, la licitud de la videovigilancia con finalidad de control laboral requerirá «informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida»¹⁵.

Pero, abundando en el pronunciamiento del TC, lo significativo es que en el caso enjuiciado entran en juego, no solo la garantía de transparencia y consiguiente derecho a recibir información previa, sino otros principios vigentes en la legislación aplicable a los hechos, encuadrados en el anterior parámetro de «calidad de los datos» previsto en la Ley Orgánica 15/1999, que forman parte del contenido esencial del derecho fundamental, pero parecen resultar irrelevantes para el intérprete constitucional.

Recordemos que, no solo en el actual régimen normativo de protección de datos, sino también en el aplicable a los hechos enjuiciados, los datos personales solo podrán ser objeto de tratamiento cuando sean «adecuados,

G. -F., 2019: 1-8. En la doctrina, véanse, entre otros, Fernández Villazón, L. A. (2020: 215-225); Herranz Ortiz, A. I. (2021: 52-56) y García Rubio, M. A. (2022: 33-39).

¹⁵ No obstante, la reciente STS 692/2022, Sala de lo Social, de 22 julio 2022, admite la omisión del deber de transparencia más allá de las prescripciones del actual art. 89 LOPDGDD en atención a las circunstancias singulares que concurren en el supuesto enjuiciado, reconociendo la validez excepcional de un control laboral oculto de carácter defensivo. En concreto, el TS estima el recurso de casación para unificación de doctrina interpuesto contra la STSJ Asturias 1762/2020, de 20 de octubre de 2020, por la empleadora demandada que, encontrándose en grave situación de vulnerabilidad (tetrapléjica), utilizó un sistema de videovigilancia encubierta en su hogar familiar para aportar pruebas en el proceso ante la fundada creencia de la sustracción de importantes cantidades de dinero y de joyas por su empleada doméstica. Con apoyo en la STC 39/2016, de 3 de marzo de 2016, el TS afirma que «no todo incumplimiento del deber de información previa, en nuestro caso, del art. 89.1 de la Ley Orgánica 3/2018, conlleva una vulneración del derecho fundamental a la protección de datos del art. 18.4 CE. Una ponderación de la proporcionalidad de la medida adoptada puede excluir la vulneración de este derecho fundamental»; y, con base en la STEDH de 17 de octubre de 2019 («López Ribalda II»), considera que «una imperativa protección de intereses privados —y aquí puede entenderse concurrente— puede justificar la ausencia de información previa», haciendo especial mención a la conocida «excepción doméstica» del art. 2.2 c) RGPD que, aun cuando para ser aplicada debe estar desconectada de una actividad profesional (considerando 18 RGPD), revela «que el ámbito doméstico es un lugar bien específico y singular desde la perspectiva de la protección de datos personales. Y ciertamente en el hogar familiar su titular y quienes con él conviven ejercen derechos fundamentales de especial importancia y reforzada tutela».

pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido» (arts. 4.1 de la derogada Ley Orgánica 15/1999 y 5.1.c RGPD). Además, deben ser recogidos para fines «determinados, explícitos y legítimos», quedando, como regla, prohibido su tratamiento posterior «de manera incompatible con dichos fines» (arts. 4.1 y 4.2 de la derogada Ley Orgánica 15/1999 y art. 5.1.b RGPD). El RGPD explicita algo más que la legislación derogada y ofrece algunos criterios en orden a determinar la posible compatibilidad entre finalidades diferentes. Al efecto, señala el art. 6.4 RGPD que «se tendrá en cuenta, entre otras cosas: a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento; c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el art. 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el art. 10; d) las posibles consecuencias para los interesados del tratamiento ulterior previsto; e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización». La evaluación de la compatibilidad entre los fines es, por tanto, una pieza clave para la legitimidad de un tratamiento ulterior de los datos personales.

Pues bien, en relación con ambas piedras angulares del derecho fundamental a la protección de datos, llama la atención que el TC, en la sentencia objeto de este comentario, no haya tomado en consideración a la incidencia que sobre la validez del sistema de control empresarial pueda tener un déficit de su cumplimiento. En otros términos, cabría entrar a valorar si la inobservancia parcial o total del régimen normativo en materia de protección de datos comporta una infracción constitucional del derecho a la protección de datos y, consecuentemente, la nulidad de la prueba así obtenida.

El principio de limitación de la finalidad es una garantía que refuerza el control sobre la propia información, al estar estrechamente vinculado con la transparencia del tratamiento, y facilita el efectivo ejercicio de sus derechos por los interesados. El interesado debe ser informado siempre de «los fines del tratamiento a que se destinan los datos personales» (arts. 13.1.c y 14.1.c RGPD) e, incluso, cuando se proyecte un tratamiento ulterior de datos personales para un fin distinto al que se recogieron, debe facilitarse al interesado, con anterioridad a dicho tratamiento ulterior, «información sobre ese otro fin» (arts. 13.3 y 14.4 RGPD). Significativo, en este sentido, es que la regulación actual contenida en LOPDGDD sobre la videovigilancia tome como eje conductor la finalidad del tratamiento, difiriendo el régimen aplicable según

se realice con fines de seguridad de las personas, bienes o instalaciones (art. 22) o con finalidades de control laboral (art. 89)¹⁶.

¹⁶ En este sentido, vid. STSJ 1178/2021, Sala de lo Social, de 15 de febrero de 2021, en la que se advierte que en la vigente normativa «se deducen dos marcos habilitantes de la videovigilancia en el trabajo, sometidos cada uno a diferentes exigencias: «-Uno de ellos se refiere a la que podríamos denominar videovigilancia laboral específica, que obliga al empleador al cumplimiento de las exigencias establecidas en la legislación laboral (art. 20.3 del ET, art. 18 de la CE y art. 8 del Convenio Europeo de Derechos Humanos, de ahí la exigencia de superar, para la legitimidad de la restricción de los derechos fundamentales de la persona trabajadora, un juicio de proporcionalidad basado en los tres subjuicios de idoneidad, necesidad y proporcionalidad en sentido estricto) y a que informe con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida. Lo que no exige la norma es comunicar la ubicación exacta de las cámaras, con lo cual se habilita para la colocación de cámaras ocultas siempre que se cumplan las exigencias de idoneidad, necesidad y proporcionalidad en sentido estricto. El otro marco regulador presupone la existencia de una video vigilancia implementada por personas físicas o jurídicas, públicas o privadas, con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones (art. 22 de la LOPD), esto es de carácter no laboral y en cuya ejecución aparece un hallazgo casual relacionado con la actividad laboral del personal al servicio de la empleadora, esto es «en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores», sin limitar el acto ilícito al delito penal, con lo cual entraría un ilícito solo laboral. Basta en este caso para cumplir con el deber de información, con la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos ARCO reforzados según aparecen regulados en los arts. 15 a 22 del RGPD (acceso, rectificación, cancelación y oposición + derecho al olvido, la limitación del tratamiento y la portabilidad de los datos). Tampoco aquí se exige informar de la ubicación de las cámaras, pues aunque sea muy habitual colocar el dispositivo informativo debajo de la cámara, es suficiente con colocarlo en un lugar visible en que las personas interesadas puedan leerlo antes de que se las grabe y, por tanto, puedan decidir si seguir adelante y ser grabadas, o por el contrario no entrar en la zona videovigilada. Lo que no contemplan estas normas es la video vigilancia sin una información, más o menos amplia, a las personas interesadas (lo que constituiría una cámara secreta), salvo (y esto abriría la posibilidad de un tercer marco legal habilitante de la video vigilancia) si esa video vigilancia está permitida por una norma en ámbitos en que no resulta aplicable la normativa sobre tratamiento de protección de datos personales (el ejemplo más evidente: el tratamiento por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención; véanse art. 2 Reglamento (UE) 2016/679 y art. 2 de la LOPD)».

En el supuesto enjuiciado debería haberse entrado a valorar el cumplimiento de este principio, pues siendo la finalidad de la recogida de datos formativa, pactada con la representación de los trabajadores y comunicada a estos, las grabaciones de voz han sido posteriormente tratadas con fines de control laboral. Es por ello que hubiera sido deseable el cuestionamiento y una toma de posición por parte del TC sobre la compatibilidad entre ambos fines, máxime teniendo en cuenta el contexto laboral de la recogida, la situación de desequilibrio entre responsable del tratamiento (empresa) e interesado (persona trabajadora), las expectativas derivadas de la existencia del pacto colectivo¹⁷, y las consecuencias perjudiciales que para la persona trabajadora tiene ese tratamiento posterior con fines de control y disciplinario.

Lo mismo puede indicarse respecto del principio de minimización, estrechamente relacionado con el de limitación de la finalidad, en cuanto que debe existir una relación directa entre los fines del tratamiento y la adecuación y pertinencia de los datos personales tratados para alcanzarlos, que deben ser los menores posibles («no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido», según el tenor del art. 4.1 Ley Orgánica 15/1999, o «limitados a lo necesario en relación con los fines para los que son tratados», en términos del art. 5.1.c RGPD).

En el caso enjuiciado, no se trata de que los datos recogidos (las grabaciones de voz) no resulten adecuados y pertinentes para la finalidad de control laboral, el problema se encuentra en lo innecesario de la acumulación de datos para alcanzar esta finalidad al producirse una monitorización constante y permanente de toda la actividad laboral, lo que puede hacer que el tratamiento no respete el principio de minimización o resulte excesivo¹⁸.

¹⁷ Como se ha indicado (Álvarez Del Cuervo, A. (2020: 292)), «las expectativas de privacidad pueden ser diferentes en función del uso que se haga de la información obtenida; así, por ejemplo, puede ser que un espacio físico o virtual no sea particularmente «privado» —en la medida en que los titulares del poder de dirección pueden acceder directamente a él sin ningún condicionamiento material o simbólico—, pero que, aun así, existan limitaciones respecto a la recopilación sistemática de datos personales del trabajador y al tratamiento que se haga de estos datos».

¹⁸ Así lo resalta la AEPD en su Informe Jurídico 2020-0073: «En definitiva, el control laboral como causa legitimadora para el tratamiento de datos personales no implica, que quepa todo tratamiento de datos amparado en dicha finalidad, sino que dicho tratamiento deberá ser proporcional, cumpliendo igualmente con el resto de principios que se establecen en el art. 5 del RGPD. Con carácter general, esta Agencia ha venido manifestando que no cabe una monitorización del trabajador durante toda su jornada en el lugar de trabajo que supondría una medida intrusiva y probablemente

No obstante, la decisión final del TC pudiera ser indicativa de que el incumplimiento de estos principios no comporta afectación constitucional del derecho a la protección de datos del trabajador, siempre que se supere el juicio de proporcionalidad como apunta la línea jurisprudencial derivada de la STC 39/2016 en relación con la garantía de transparencia y consiguiente deber información. En consecuencia, a efectos de valorar la proporcionalidad del tratamiento objeto del litigio principal, es necesario medir la gravedad de la injerencia en el derecho fundamental a la protección de datos de carácter personal y determinar si la importancia del objetivo de interés general perseguido por el tratamiento es proporcionada a la gravedad de la injerencia.

La cuestión es que, así las cosas, el máximo intérprete constitucional da por superado ese juicio o canon interpretativo de proporcionalidad, asumiendo la valoración realizada en las sentencias de los órganos judiciales ordinarios que «parecen admitir todas ellas que la monitorización constante de todas, y cada una de las llamadas, es completamente «necesario y proporcional»»¹⁹.

En este sentido, cabe lamentar la ausencia del recurso al método ponderativo y de una valoración del justo equilibrio entre los derechos en colisión por parte del TC, máxime cuando el juicio constitucional de proporcionalidad en el ámbito del derecho fundamental a la protección de datos personales, en buena medida, debe realizarse en conjunción con los principios expuestos de «calidad de los datos», pues, por una parte, el subjuicio de idoneidad exige la adecuación y pertinencia de los datos en relación con lo fines para los que son tratados, así como, por otra, el enjuiciamiento de la necesidad implica respetar el principio de limitación a lo necesario en relación con los fines, a lo que debe sumarse el test de proporcionalidad en sentido estricto²⁰.

desproporcionada en relación con la finalidad perseguida, sin ser una respuesta proporcionada ante riesgos potenciales o concretos. En este sentido se pronunciaba, igualmente, el Grupo de Trabajo sobre protección de datos del art. 29 en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017 (WP 249), «La rápida adopción de las nuevas tecnologías de la información en el lugar de trabajo, en términos de infraestructura, aplicaciones y dispositivos inteligentes, permite nuevos tipos de tratamiento de datos sistemáticos y potencialmente invasivos».

¹⁹ Así, Todoli Signes, A. (2021b).

²⁰ Coincidentemente Mercader Uguina, J. R. (2022a: 18 y 2022b: 175-176), quien advierte: «Los fines para los que son recabados u obtenidos los datos son la pauta de la proporcionalidad en su tratamiento, pues la idoneidad, necesidad y proporcionalidad se miden en función del fin para el que se han obtenido, como ha entendido el Tribunal de Justicia de la Unión Europea reiteradamente, entre otras en el STJUE 24 de noviembre de 2011, C-468/10 y C-469/10, ASNEF. No era pues, a nuestro juicio,

Pero incluso, yendo más allá de la utilización de las grabaciones sonoras con finalidad de control laboral, y siendo preceptivo en cualquier tratamiento de datos personales el cumplimiento de estos principios rectores y garantías legales, en el caso concreto enjuiciado por el TC, se ha eludido probablemente el problema constitucional más relevante: la propia legitimidad de un sistema de monitorización de la actividad laboral continuo, constante y permanente implementado vía convenio colectivo, aun siendo conocido e informado a las personas trabajadoras²¹.

2. LA ESPECIAL TRASCENDENCIA CONSTITUCIONAL: INCIDENCIA DE LA NEGOCIACIÓN COLECTIVA EN EL DERECHO FUNDAMENTAL, ¿CUESTIÓN DE LEGALIDAD ORDINARIA?

Como se ha señalado anteriormente, la STC 160/2021 sitúa la especial trascendencia constitucional del caso enjuiciado en la cuestión relativa a la incidencia que pueda tener la negociación colectiva en el tratamiento de los datos de las personas trabajadoras, para concluir que carece de trascendencia desde la perspectiva constitucional, por tratarse de una cuestión de mera legalidad ordinaria, ajena al derecho fundamental a la protección de datos personales.

Cabe dudar razonablemente de que la conclusión alcanzada en este punto por el TC guarde, como se ha advertido²², coherencia en relación con el requisito de admisión de las demandas de amparo relativo al concepto de especial trascendencia constitucional (arts. arts. 49.1, 50.1 y 50.3 Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional —LOT—); especial trascendencia que, según reza el art. 50.1.b) LOTC, se apreciará por la importancia del recurso para la interpretación de la Constitución, para su aplicación o general eficacia, y para la determinación del contenido y alcance de los derechos fundamentales, y se vincula con una decisión sobre el fondo.

Una valoración mucho más acorde con la apreciación realizada sobre la trascendencia constitucional del asunto consistente, a juicio del Tribunal, «en

una mera cuestión de legalidad ordinaria la que estaba en juego sino, antes bien, un elemento directamente conectado con el contenido esencial del derecho a la protección de datos personales que hubiera requerido de una respuesta más fundada por nuestro Tribunal Constitucional».

²¹ Véanse, en este sentido, las consideraciones realizadas por Molina Navarrete, C. (2021: 117-118).

²² Véase Molina Navarrete, C. (2021: 115).

determinar la relevancia que para la configuración del derecho a la protección de datos del carácter personal (art. 18.4 CE) tienen las condiciones pactadas entre las partes respecto del uso de los datos de carácter personal obtenidos mediante estas grabaciones», y aun teniendo claro que «la especial trascendencia constitucional no predetermina el sentido estimatorio del fallo, desde una perspectiva material», debería haber conducido al TC a entrar en el fondo del asunto «que no ha sido resuelto con anterioridad, sobre el que la doctrina constitucional es insuficiente (más que inexistente) o que ofrece una posibilidad de modificar o aclarar una doctrina preexistente»²³.

La cuestión relativa a la consideración que debe otorgarse a la introducción de garantías adicionales vía autonomía colectiva en los derechos fundamentales de las personas trabajadoras, y las consecuencias que la vulneración o infracción de tales garantías deba ocasionar, dista, a nuestro juicio, de ser eludida dejándola en manos de la jurisdicción ordinaria y reduciendo así el ámbito de protección de los derechos fundamentales de las personas trabajadoras. La aplicación del principio de interpretación más favorable a la efectividad de los derechos fundamentales (SSTC 17/1985, de 9 de febrero y 200/2014, de 15 de diciembre) también militaría a favor de conceder relevancia constitucional a esta cuestión. Más aún cuando, aunque no sea de aplicación a los hechos, no puede obviarse por completo la nueva realidad normativa de la protección de datos en el contexto laboral. Tanto el legislador europeo como el nacional han dado entrada a la negociación colectiva, peculiar fuente normativa del Derecho laboral, en la regulación del derecho fundamental a la protección de datos²⁴.

En concreto, el RGPD reconoce dos ámbitos en los que el convenio colectivo puede jugar un papel fundamental en la delimitación del derecho a la protección de datos personales. En primer lugar, realiza una llamada a la negociación colectiva para incorporar excepciones a la prohibición de tratamiento de datos de categorías especiales de los trabajadores, siempre que se establezcan «garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado» (art. 9.2. b RGPD). Tal sería el caso de la utilización de datos biométricos con finalidades de control de la jornada laboral autorizada en el marco de un convenio colectivo²⁵. En segundo lugar, habilita al convenio colectivo para establecer normas específicas relativas al tratamiento

²³ Véase González Beilfuss, M. (2016: 356).

²⁴ Sobre este nuevo régimen, ampliamente, Calvo Gallego, F. J. (2021: 4225-4270).

²⁵ Véase, en este sentido, el Dictamen CNS 2/2022 de la Autoridad Catalana de Protección de Datos sobre dispositivos de control de presencia en el trabajo mediante reconocimiento facial (accesible en <https://bit.ly/3DFLebP>).

de datos personales de los trabajadores en el ámbito laboral, «en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral» (considerando 155 y art. 88²⁶).

El legislador español recoge la negociación colectiva en la regulación del derecho a la desconexión digital (art. 88) y, en general, para establecer «garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral» (art. 91 LOPDGDD). No se contempla expresamente la posibilidad de regular por vía convencional aspectos de la protección de categorías especiales de datos de los trabajadores, aunque es una posibilidad derivada directamente del RGPD y que encaja en los amplios términos de la norma nacional.

La negociación colectiva es, pues, reconocida formalmente como fuente normativa en el establecimiento de garantías adicionales a las previstas legalmente siempre que exista afectación de los derechos fundamentales de las personas trabajadoras por el tratamiento de sus datos personales²⁷.

Por tanto, ante este nuevo régimen legal, cabe plantearse si será posible seguir aplicando el criterio jurisprudencial sobre el papel y alcance de la negociación colectiva en la configuración del derecho a la protección de datos que, con relación a hechos anteriores a la LOPDGDD, ha mantenido el TC en esta sentencia. Sigue siendo una cuestión abierta, a nuestro juicio, delimitar si las garantías adicionales a las previstas por el legislador introducidas vía convenio colectivo se integran en el contenido esencial del derecho a la protección de datos personales de las personas trabajadoras

²⁶ Como se ha advertido (Pérez de los Cobos Orihuel, F. (2019: 29)): «Los márgenes que el precepto reconoce a la legislación y negociaciones colectivas internas son amplísimos, por ello resulta del mayor interés leer el parco artículo de la Ley española a la luz del mismo: desde el punto de vista de su alcance, las normas «más específicas» pueden abarcar cualquier secuencia de la relación laboral, desde la contratación hasta la extinción del contrato; desde la perspectiva de contenido, deben contener medidas que preserven la dignidad humana, los derechos fundamentales e intereses legítimos de los trabajadores».

²⁷ Ampliamente sobre esta cuestión, Sierra Hernaiz, E. (2020: 129-136).

o, por ser ajenas al mismo, constituyen una cuestión de mera legalidad ordinaria²⁸.

Bibliografía

- Álvarez Del Cuvillo, A. (2020). La delimitación del derecho a la intimidad de los trabajadores en los nuevos escenarios digitales. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social*, 151, 275-292. Disponible en: <https://bit.ly/3SKnhEB>.
- Calvo Gallego, F. J. (2021). Derechos digitales en la negociación colectiva (Comentario al artículo 91 LOPDGDD). En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 4225-4270). Cizur Menor: Thomson Reuters Aranzadi.
- Fernández Villazón, L. A. (2020). Protección de datos y derechos digitales de los trabajadores. En L. A. Fernández Villazón (coord.). *Derecho y nuevas tecnologías* (pp. 205-237). Cizur Menor: Civitas Thomson Reuters.
- García Rubio, M. A. (2022). Control tecnológico empresarial y nuevos problemas aplicativos tras la L.O. 3/2018. Una mirada desde el deber de información previa. *Labos*, 1, 21-46. Disponible en: <https://doi.org/10.20318/labos.2022.6845>.
- González Beilfuss, M. (2016). La especial trascendencia constitucional de las demandas de amparo. Análisis de la doctrina del Tribunal Constitucional sobre un concepto etéreo. *Revista Española de Derecho Constitucional*, 107, 333-367. Disponible en: <https://doi.org/10.18042/cepc/redc.107.10>.
- Goñi Sein, J. L. (2021). El derecho a la privacidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (Comentario al artículo 89 LOPDGDD). En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 4127-4161). Cizur Menor: Thomson Reuters Aranzadi.
- Herranz Ortiz, A. I. (2021). Transformación digital de las relaciones laborales y derechos fundamentales: videovigilancia laboral, tutela informativa del trabajador y derecho a la protección de datos personales. En M. L. Rodríguez Fernández (dir.). *Tecnología y trabajo: el impacto de la revolución digital en los derechos laborales y la protección social* (pp. 19-56). Cizur Menor: Thomson Reuters Aranzadi.

²⁸ En este mismo sentido, vid. Rivas Vallejo, P. (2021: 7). En favor de la integración de estas garantías adicionales pactadas formen parte del derecho fundamental a la protección de datos, Muñoz Ruiz, A. B. (2022: 16-19).

- López Balaguer, M. (2020). El control empresarial por videovigilancia en la LOPD. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social*, 151, 357-372. Disponible en: <https://bit.ly/3TRxsIY>.
- Mercader Uguina, J. R. (2022a). Nuevas señales y paradojas de la protección de datos en la reciente doctrina de los Tribunales y de la Agencia Española de Protección de Datos. *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, 85, 1-24.
- (2022b). *Algoritmos e inteligencia artificial en el derecho digital del trabajo*. Valencia: Tirant lo Blanch.
- Molina Navarrete, C. (2019). Control tecnológico del empleador y derecho probatorio: Efectos de la prueba digital lesiva de derechos fundamentales. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social*, 150, 331-354. Disponible en: <https://bit.ly/3FoCF6p>.
- (2021). Eficacia de gestión versus protección de datos: ¿reactividad jurisdiccional a la «inflación de derechos humanos» (en el trabajo)? Comentario a la Sentencia del Tribunal Constitucional 160/2021, de 4 de octubre. *Revista de Trabajo y Seguridad Social CEF*, 465, 109-122. Disponible en: <https://doi.org/10.51302/rtss.2021.2564>.
- Monereo Pérez, J. L. y Ortega Lozano P. G. (2019). Se justifica la grabación con cámaras ocultas en el centro de trabajo por la existencia debidamente acreditada de sospechas razonables de irregularidades graves. STEDH (Gran Sala) de 17 de octubre de 2019 (números 1874/13 y 8567/13) (asunto López Ribalda II). *Revista de Jurisprudencia Laboral*, 8, 1-10. Disponible en: https://doi.org/10.55104/RJL_00088.
- Muñoz Ruiz, A. B. (2022). Grabación de las conversaciones de los trabajadores y derecho fundamental de protección de datos de carácter personal. Comentario a la STC 160/2021. *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, 88, 1-16.
- Pérez de los Cobos Orihuel, F. (2019). Poderes del empresario y derechos digitales del trabajador. *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, 59, 16-29.
- Rivas Vallejo, P. (2021). Derecho a la protección de datos y monitorización del trabajo: juego de incumplimientos. *Revista de Jurisprudencia Laboral*, 10, 1-7. Disponible en: https://doi.org/10.55104/RJL_00294.
- Rojo Torrecilla, E. (2021). Monitorización de la actividad laboral. Para el TC no existe vulneración del derecho constitucional a la protección de datos. Notas a propósito de la sentencia de 4 de octubre de 2021 (caso Telefónica España S.A.U.). *El nuevo y cambiante mundo del trabajo. una mirada abierta y crítica a las nuevas realidades laborales* [blog], 31-10-2021. Disponible en: <https://bit.ly/3zjRwv6>.
- Romero Ródenas, M. J. y Moraru, G. F. (2019). El deber informativo previo sobre el alcance de las medidas empresariales de videovigilancia. *Revista de Jurisprudencia Laboral*, 2, 1-8. Disponible en: https://doi.org/10.55104/RJL_00027.

- Sierra Hernaiz, E. (2020). El papel de la negociación colectiva en el tratamiento de los datos personales de los trabajadores. *Temas Laborales. Revista andaluza de trabajo y bienestar social*, 152, 115-138. Disponible en: <https://bit.ly/3gQMIAu>.
- Todolí Signes, A. (2021a). Nulidad o improcedencia en caso de vulneración de derechos fundamentales en la adquisición de la prueba, pero siempre una indemnización adicional. *Revista de Trabajo y Seguridad Social. CEF*, 459, 237-244. Disponible en: <https://doi.org/10.51302/rtss.2021.2408>.
- (2021b). Los Tribunales niegan la eficacia de la negociación colectiva en materia de Protección de Datos. Comentario a la STC de 160/2021, de 4 de octubre. *Argumentos en Derecho Laboral* [blog], 11-11-2021. Disponible en: <https://bit.ly/3DdWOtb>.
- Troncoso Reigada, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant lo Blanch.
- (2021). Los principios relativos al tratamiento (comentario al artículo 5 RGPD y al artículo 4 LOPDGDD). En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales* (pp. 847-907). Cizur Menor: Thomson Reuters Aranzadi.
- Valle Muñoz, F. A. (2021). Las cámaras de videovigilancia en la empresa como medio de prueba en el proceso laboral. *IUSLabor. Revista d'anàlisi de Dret del Treball*, 3, 31-59. Disponible en: <https://doi.org/10.31009/IUSLabor.2021.i03.02>.
- (2022). Control tecnológico empresarial y licitud de la prueba en el proceso laboral. *Trabajo y Derecho: nueva revista de actualidad y relaciones laborales*, 87, 1-30.