# LAS FACULTADES DE CONTROL A DISTANCIA DEL TRABAJADOR: VIDEOVIGILANCIA Y GRABACIÓN DEL SONIDO

FEDERICO NAVARRO NIETO
*Catedrático de Derecho del Trabajo y de la Seguridad Social*
Universidad de Córdoba

**EXTRACTO** **Palabras Clave:** poder de control, intimidad, privacidad del trabajador, videovigilancia y grabación del sonido

El estudio se centra en el uso de dispositivos audiovisuales como medio de control empresarial de la actividad laboral en la empresa y el marco jurídico de tutela de la privacidad del trabajador. Se analiza el relevante papel de la jurisprudencia del TEDH y nuestra jurisprudencia interna en la construcción de dicho marco jurídico. Finalmente, se aborda el estudio del RGPD y las previsiones de la vigente LOPD sobre el uso de los dispositivos audiovisuales de control.

**ABSTRACT** **Key Words:** Geolocation, privacy, balancing trial, information rights

The study focuses on the use of audiovisual devices as a means of business control of the work activity in the company and the legal framework for the protection of the worker's privacy. It analyses the relevant role of the case-law of the ECHR and our internal case-law in the construction of that legal framework. Finally, the GDPR study and the current LOPD's forecasts on the use of audiovisual control devices are addressed.

 Recepción de original: 26.09.2019. Aceptación: 25.10.2019

## ÍNDICE



## 1. INTRODUCCIÓN

El uso de dispositivos audiovisuales como medio de control empresarial de la actividad laboral en la empresa contrapone el derecho empresarial de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales (art. 20.3 ET), como concreción del derecho empresarial de organización del trabajo en la empresa, amparado constitucionalmente por la libertad de empresa (art. 38 CE), con el derecho del trabajador al respeto de su intimidad (art. 18.1 CE), y, en el caso de las grabaciones de audio, con el derecho al secreto de las comunicaciones (art. 18.3 CE). De hecho, históricamente éste es uno de los primeros ámbitos de confrontación entre el poder de control empresarial mediante nuevas tecnologías y la esfera personal del trabajador. También está fuera de toda duda que las imágenes o sonidos grabados en un soporte físico constituyen un tratamiento de datos de carácter personal que queda integrado en la cobertura del art. 18.4 CE (STC 29/2013).

Es evidente, por otro lado, la imbricación entre el derecho a la intimidad y a la protección de datos. Es constatable con frecuencia la alegación ante los tribunales de ambos derechos frente a las prácticas empresariales de videovigilancia [1]. La imbricación de ambas perspectivas constitucionales se plasma de forma sintética en el nuevo art. 20 bis ET, que recoge el derecho de los trabajadores a "la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales". Actualmente, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD) contempla el tratamiento de datos a través de la videovigilancia mediante una regulación general recogida en el art. 22 LOPD, que se remite al art. 89 de la misma Ley para el

[1] Es un ejemplo la STEDH 9-1-2018, *asunto López Ribalda*, donde la demanda por videovigilancia irregular toma como fundamento el derecho al respeto de la vida privada, *ex* art. 8 CEDH, aunque en su fundamentación jurídica el TEDH tomará como referencia los apartados 1 y 4 del art. 18 CE y la normativa sobre protección de datos.

tratamiento por el empleador de datos del trabajador obtenidos a través de sistemas de cámaras o videocámaras. Aunque el art. 89 LOPD se refiere en su título a la protección del derecho a la intimidad, la norma arranca en su apartado 1º refiriéndose a la facultad empresarial de tratamiento de datos, remitiéndose en apartados posteriores a reglas y normas de protección del trabajador en este caso. Por tanto, un criterio sistemático que contemple las previsiones del ET y de la LOPD permite concluir que las garantías del art. 89 LOPD se refieren a la protección del derecho a la intimidad y a la protección de datos frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (lo que puede mantenerse también para los arts. 87 y 90 LOPD, por los mismos motivos). Nuestro TC ha observado, no obstante, que ambos derechos constitucionales tienen una distinta función, y por ello difieren también en objetos y contenidos[2].

## 2. EL TRATAMIENTO DE LOS SISTEMAS AUDIOVISUALES DE VIGILANCIA EN LA DOCTRINA CONSTITUCIONAL Y LA JURISPRUDENCIA ORDINARIA

Sobre los límites de la facultad empresarial de control de la conducta de los trabajadores a través de sistemas audiovisuales de vigilancia, la doctrina constitucional y la jurisprudencia ordinaria han sido vacilantes y están llenas de matices muy ligados a la casuística abordada.

En una primera fase la construcción doctrinal del TC se circunscribe al derecho a la intimidad, ex art. 18.1 CE, lo cual se explica porque en los asuntos abordados el apoyo de la demanda se limita a la referencia a dicha norma constitucional (SSTC 98/2000, 186/2000). Desde la perspectiva del derecho a la intimidad se asientan en esta fase algunas premisas básicas sobre los límites del control empresarial mediante la videovigilancia.

En primer lugar, subraya el TC que la mera invocación del interés empresarial no es suficiente para sacrificar el derecho fundamental del trabajador. El ejercicio de las facultades organizativas y disciplinarias del empleador no puede servir en ningún caso a la producción de resultados inconstitucionales, lesivos de los derechos fundamentales del trabajador (STC 98/2000, FJ 7). En segundo lugar, la instalación de tales medios en lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos "resulta, a fortiori, lesiva en todo caso del derecho a la

[2] Para el TC, la función del derecho fundamental a la intimidad del art. 18.1 CE "es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad". En cambio, el derecho fundamental a la protección de datos "persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" (STC 29/2013, FJ 7, con remisión a la STC 292/2000). El derecho a la protección de datos va más allá de los datos íntimos de la persona, abarcando el conjunto de datos de carácter personal (STC 292/2000, FJ 6).

intimidad de los trabajadores, sin más consideraciones" (STC 98/2000, FJ 6). Pero puntualizará el TC que el alcance del derecho a la intimidad de los trabajadores incluye también las zonas del centro de trabajo donde se desempeñan los cometidos propios de la actividad profesional, donde pueden producirse intromisiones ilegítimas por parte del empresario en el derecho a la intimidad de los trabajadores, como podría serlo la grabación de conversaciones entre un trabajador y un cliente, o entre los propios trabajadores, en las que se aborden cuestiones ajenas a la relación laboral (STC 98/2000, FJ 6) [3]. En tercer lugar, aunque el derecho a la intimidad no es absoluto, pudiendo ceder ante intereses constitucionalmente relevantes, es necesario que el recorte que aquél haya de experimentar se revele como "necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho" (STC 98/2000, FJ 5).

El sacrificio del derecho a la intimidad, por tanto, se somete al juicio de proporcionalidad, que incluye tres exigencias. En primer lugar, debe tratarse de una medida justificada en las facultades empresariales de control de la actividad laboral, particularmente porque existan razonables sospechas de la comisión por parte del trabajador de graves irregularidades en su puesto de trabajo. En segundo lugar, debe ser idónea para la finalidad pretendida por la empresa (el control de la actividad laboral y en su caso verificar si el trabajador cometía efectivamente las irregularidades sospechadas) y ser estrictamente necesaria para la satisfacción del interés empresarial. En tercer lugar, debe ser equilibrada o proporcional en sentido estricto. A estos efectos habrá que atender a las circunstancias concurrentes en el supuesto concreto para determinar si existe o no vulneración del art. 18.1 CE (STC 98/2000, FJ 6): i) el lugar del centro del trabajo en que se instalan por la empresa sistemas audiovisuales de control. Concretamente si la grabación se limita a la zona del puesto de trabajo; ii) si la instalación se hace o no indiscriminadamente y limitada o no en el tiempo; iii) si los sistemas son visibles o han sido instalados subrepticiamente; iv) la finalidad real perseguida con la instalación de tales sistemas; v) si existen razones de seguridad, por el tipo de actividad que se desarrolla en el centro de trabajo de que se trate, que justifique la implantación de tales medios de control.

En un segundo momento temporal, el enjuiciamiento constitucional hace entrar en juego también las garantías del art. 18.4 CE (SSTC 29/2013 y 39/2016). Subraya el TC que estamos "dentro del núcleo esencial del derecho fundamental del art. 18.4 CE, que se actualiza aún de modo más notorio cuando nos adentramos en un ámbito —el de la video-vigilancia— que ofrece múltiples medios de tratamiento de los datos" (STC 29/2013, FJ 5).

Con este nuevo enfoque constitucional será fundamental como requisito para la

[3] Importante doctrina que supondrá una corrección a la doctrina de suplicación de los años anteriores. Cfr. Desdentado Bonete, A. y Muñoz Ruiz, A.B., *Control informático, videovigilancia y protección de datos en el trabajo*, Valladolid, Lex Nova, 2012 págs. 19-21.

licitud del tratamiento de datos la información previa del afectado [4]. Nos dirá el TC que forma parte del "núcleo esencial" de la definición constitucional del art. 18.4 CE "el derecho del afectado a ser informado de quién posee los datos personales y con qué fin" (STC 29/2013, FJ 7). En esta temática la doctrina constitucional impone un giro en el tratamiento judicial de la cuestión, dado que hasta ese momento la cuestión del derecho de información no tiene atribuida relevancia constitucional [5]. Ese derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, "pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento" (STC 29/2013, FJ 7). Por otra parte, el deber de información a cargo de la empresa debe concretarse necesariamente en una información previa a la puesta en marcha de los controles (SSTC 29/2013, 39/2016).

El debate constitucional a partir de aquí se centra en el contenido y la forma de dicha información previa y, en relación con ello, la posibilidad de controles con medios audiovisuales ocultos.

La STC 29/2013, dictada por la Sala 1ª, está referida a un supuesto donde las cámaras de videovigilancia instaladas en el recinto universitario reprodujeron la imagen del trabajador en sus entradas y salidas del mismo y permitieron verificar el incumplimiento de su jornada de trabajo. En el caso, la Sentencia estima que la debida información previa no queda solventada por la existencia de distintivos anunciando la instalación de cámaras y captación de imágenes en zonas de acceso y de paso públicos, ni porque se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos. Concluye el TC en esta sentencia que "era 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". Esa información debe concretar las características y el alcance del tratamiento de datos que se va a realizar, 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" (FJ 8).

Sin embargo, el Pleno del Tribunal, en la sentencia 39/2016, matiza sustancial-

[4] Hay que advertir que el consentimiento del afectado es uno de los elementos definidores del sistema de protección de datos de carácter personal (art. 6 LOPD). Ahora bien, en el ámbito laboral el consentimiento del trabajador "pasa como regla general a un segundo plano pues el consentimiento 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. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato" (STC 39/2016, FJ 3). De esta forma el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 ET (STC 39/2016, FJ 4).

[5] Cfr. Desdentado Bonete, A. y Muñoz Ruiz, A.B., op. cit. págs. 66-67

mente este criterio. En el caso, constatada las existencias de descuadres contables en una caja registradora, se instalan cámaras de videovigilancia para la observación del espacio en el que se ubicaba la caja, constando en el escaparate del establecimiento, en un lugar visible, el distintivo informativo de la existencia de sistemas de videovigilancia. En esta sentencia se indica que el caso permite al Tribunal "perfilar o aclarar su doctrina en relación con el uso de cámaras de videovigilancia en la empresa", y en concreto "aclarar el alcance de la información a facilitar a los trabajadores sobre la finalidad del uso de la videovigilancia en la empresa: si es suficiente la información general o, por el contrario, debe existir una información específica (tal como se había pronunciado la STC 29/2013, de 11 de febrero)" (FJ 1). Para esta sentencia, en caso de instalación de sistemas de videovigilancia por sospechas de incumplimientos laborales, se flexibilizan las exigencias de información previa (que no debe ser expresa, ni precisa), aunque se mantiene la exigencia de un juicio de proporcionalidad.

Esta sentencia considera que, en el asunto abordado, se respeta el derecho de información, porque "en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo exigido por la instrucción 1/2006" de la AEPD. De manera que la trabajadora "podía conocer la existencia de las cámaras y la finalidad para la que habían sido instaladas", estimando que con ello se satisfacía el derecho de información previa que forma parte del derecho fundamental a la protección de datos (FJ 4).

Pero el TC en esta sentencia no sólo "aclara" el alcance de la exigencia de información como obligación empresarial. También introduce un importante matiz en su canon de razonamiento con respecto a la STC 29/2013, estimando que el incumplimiento del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada. Indica el TC, en este sentido, que "la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE" (FJ 4). De esta argumentación se puede extraer la importante conclusión de la admisión de controles ocultos, que quedarían únicamente sometidos al juicio de proporcionalidad, lo que, como veremos, ha sido avalado por la más reciente doctrina del TEDH.

El principio de proporcionalidad, como hemos visto, es un canon de razonamiento ya asentado con la STC 98/2000. En el caso de la sentencia 39/2016, se concluye que la medida de instalación de cámaras de seguridad se considera justificada porque existen razonables sospechas de que alguno de los trabajadores que prestan servicios en determinadas cajas de cobros se esta apropiando de di-

nero y dicha instalación controla la zona de caja donde la trabajadora desempeña actividad laboral; es una medida idónea y necesaria para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); y equilibrada (pues la grabación de imágenes se limita a la zona de la caja y han sido tratadas las imágenes captadas para el control de la relación laboral), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.

Sobre esta construcción doctrinal del TC (deber de información y juicio de proporcionalidad) se monta la jurisprudencia del TS (SSTS 31-1-2017, rec. 3331/15, 1-2-2017, rec. 3262/15, y 15-1-2019, rec. 341/17) y la doctrina de suplicación. Lo que se percibe es que las contradicciones en la doctrina constitucional más reciente se reflejan en una doctrina dubitativa de la jurisdicción ordinaria. Los problemas se centran en el uso con fines de control laboral de un sistema de videovigilancia general y en la instalación de un sistema de videovigilancia oculto.

Ya en la STS 7-7-2016, rec. 3233/14, el TS considera que las SSTC 29/2013 y 39/2016 se refieren a supuestos diferentes que requieren distintas soluciones, justificando con ello la similitud del supuesto abordado con el referido en la STC 39/16, cuya doctrina aplica [6]. Y esta misma premisa sirve a las SSTS 31-1-2017 y 1-2-2017, donde se debate la instalación de sistemas de videovigilancia por motivos de vigilancia y seguridad del establecimiento (por actos de clientes, de empleados, de terceros, y por los riesgos más diversos en las instalaciones empresariales), y el uso como prueba de las imágenes grabadas sin informar a los trabajadores de cuál sería el uso que se les daría a efectos disciplinarios (igualmente, STS 2-2-2017, rec. 554/16, acogiéndose también a la doctrina de la STC 39/2016). Las sentencias toman como referencia la doctrina de la STC 39/2016, "donde [se] ha rebajado -indica el TS- las exigencias informativas que debe facilitar la empresa al trabajador cuando instala un sistema de video-vigilancia". El TS concluye que se supera el juicio de proporcionalidad y "los trabajadores estaban informados, expresamente, de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad, expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo". No obstante, puntualiza el TS que esta finalidad genérica "excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc. etc..". De forma que en estos casos cabe entender que debe informarse al trabajador expresamente de la finalidad de control laboral de los sistemas de videovigilancia. En pronunciamientos posteriores el TS matiza esta doctrina, pero a partir de un

[6] En el caso, el uso de la videovigilancia del centro de trabajo -almacén-, conocido por los trabajadores y donde existen carteles indicadores, para acreditar el consumo irregular por la trabajadora de productos de la empresa.

dato que ratifica: que la prueba obtenida de la videovigilancia es lícita porque el trabajador está informado de la instalación del sistema por razones de seguridad (ATS 18-9-2018, rec. 1092/18; STS 15-1-2019, rec. 341/17) [7].

En suplicación se asume el enfoque flexibilizador de la STC 39/2016 y la doctrina del TS descrita en relación con el deber de información al trabajador. De esta forma, la obligación de información previa se entiende cubierta con el cumplimiento de los requisitos específicos de información a través del distintivo, de acuerdo con la Instrucción 1/2006, sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control, justificando el uso de la videovigilancia de seguridad con fines laborales cuando existan distintivos generales de información y sospechas de ilícitos laborales [8]. El juicio de proporcionalidad tiene su utilidad esencialmente de cara a la legitimación de la videovigilancia encubierta, por tanto, sin información previa a los trabajadores y sus representantes. En el caso de cámaras ocultas se considera que la instalación debe obedecer a un concreto designio de investigación, de forma que no se respeta el principio de proporcionalidad en sentido estricto cuando la instalación de cámaras es indiscriminada, esto es, general y prolongada [9]. Aunque también en suplicación se matiza esta orientación flexibilizadora en algunos casos, en el sentido de considerar inexcusable el deber de información, que no se subsana por el hecho de que la videovigilancia esté justificada por el comportamiento irregular del trabajador y la proporcionalidad de la medida adoptada por la empresa [10].

[7] Como decimos, el TS matiza su doctrina en la STS 15-1-2019. La cuestión suscitada en el recurso de casación para la unificación de doctrina se centra en determinar si debe admitirse como prueba de los hechos imputados en la carta de despido la grabación obtenida por cámaras de videovigilancia que la empresa había instalado, con conocimiento de los trabajadores, pero sin que éstos fueran informados del destino que le iba a dar al control obtenido por medio de la grabación, que además era general y prolongada en el tiempo. Considera el TS, en primer lugar, que los dispositivos de información deben respetar las disposiciones normativas vigentes. En cierta forma abunda el TS en la idea de que debe existir una información expresa a los trabajadores del uso de la videovigilancia como medio de control laboral. En segundo lugar, debe respetarse el principio de proporcionalidad, lo que no ocurre cuando no existe justificación de la videovigilancia (en el asunto abordado era una instalación general y por años, con mucha antelación a su uso con fines laborales) y cuando la videovigilancia es indiscriminada (la instalación de cámaras era general, prolongada y sin conocerse su objetivo).

[8] SSTSJ Andalucía, 15-2-2017, rec. 952/16, y 10-10-2018, rec. 2260/17; STSJ País Vasco 11-12-2018, rec. 2292/18; STSJ Madrid 22-5-2017, rec. 384/17; STSJ Madrid 25-1-2019, rec. 971/18; STSJ Castilla y León 22-6-2017, rec. 384/17; STSJ Castilla La Mancha 12-1-2018, rec. 1416/17; STJ Cataluña 8-1-2019, rec. 6190/18.

[9] STS 15-1-2019, rec. 341/17; SSTSJ Andalucía 22-2-2017, rec. 1203/16, 22-3-2017, rec. 1461/16, 7-6-2017, rec. 2091/16, 17-1-2018, rec. 1878/17; STSJ Castilla La mancha 12-1-2018, rec. 1416/17; STSJ País Vasco 27-2-2018, rec. 226/18; STSJ Madrid 4-6-2018, rec. 217/18; STSJ Islas Canarias 27-3-2017, rec. 934/16; STSJ Madrid 13-9-2018, rec. 417/18; SSJS Sevilla 26-7-2018, JUR 2018/2107, y 3-9-2018, JUR 2018/260395.

[10] STSJ Cataluña 9-3-2017, rec. 39/17; STSJ Castilla y León 11-4-2018, rec. 407/18. Las SSTSJ Madrid 13-9-2018, rec. 417/18, y 28-9-2018, rec. 275/18, estiman que el trabajador de seguridad debería haber sido informado previamente que el sistema de video vigilancia general de los accesos de entrada al recinto ferial en el que opera su empresa podía ser utilizado a los efectos de control de su actividad laboral, porque así lo imponía la normativa vigente en ese momento (art. 5 LO 15/1999). Aun estimando que el sistema de video vigilancia era conocido por el trabajador por evidente y notorio, su finalidad

## 3. LA STEDH (GRAN SALA) 17-10-2019, *ASUNTO LÓPEZ RIBALDA*

En el ámbito doctrinal y judicial se ha extendido la convicción de que la sentencia dictada por la Sección 3ª del TEDH de 9-1-2018, *Asunto López Ribalda y otros* (Asuntos nº 1874/13 y 8567/13) cuestiona claramente la orientación doctrinal del TC y del TS, que hemos expuesto[11]. En la sentencia, el TEDH declara la violación del art. 8 del CEDH por considerar que la vigilancia encubierta o secreta de las cajeras de un supermercado español vulneró su derecho a la vida privada, en las concretas circunstancias en que se produjo. El caso abordado se refiere a la instalación de videovigilancia consistente en cámaras tanto visibles como ocultas y que "(l)os empleados solo tenían conocimiento de la existencia de las cámaras visibles que enfocaban las salidas del supermercado, y no fueron informados de la instalación de cámaras enfocadas a las cajas" (ap. 58). Para la sentencia no se han respetado los principios de trasparencia (información previa, clara y específica -no genérica- en cuanto a la naturaleza del control empresarial) y de proporcionalidad (sospecha justificada, vigilancia individualizada y limitada espacial y temporalmente).

Considera el TEDH que, a pesar de haberse colocado en el establecimiento distintivos informativos de carácter general, la empresa desatendió "la obligación mencionada anteriormente de informar previamente a los interesados de modo expreso, preciso e inequívoco sobre la existencia y características particulares de un sistema de recogida de datos de carácter personal". Y concluye en el asunto abordado que, a diferencia del *asunto Köpke*, la videovigilancia encubierta no era la consecuencia de una sospecha justificada contra las demandantes y, en consecuencia, no iba dirigida específicamente a ellas, sino a todo el personal que trabajaba en las cajas registradoras, durante semanas, sin límite de tiempo y durante todas las horas del trabajo; la decisión de adoptar medidas de vigilancia se basó en una sospecha general contra todo el personal en vista de las irregularidades que habían sido previamente detectadas por el encargado de la tienda. (ap. 68). Esta comparación con el *asunto Köpke* era llamativa, porque implícitamente se alinea con la doctrina de la STC 39/2016 en la admisión, en determinadas circunstancias, de una videovigilancia encubierta.

En cualquier caso, la STEDH (Gran Sala) 17-10-2019, dictada en el mismo asunto, rectifica la doctrina de la Sentencia de la Sección 3ª y declara que en el asunto no se ha producido una violación del art. 8 del CEDH, alineándose claramente con la más reciente y cuestionada doctrina del TC y del TS.

no era la de control de la actividad laboral de los trabajadores de la contratista, sino la de control de acceso general al recinto ferial. Por otro lado, su uso específicamente como medio de control singular de determinados trabajadores por existencia de sospechas en su comportamiento laboral debería superar el juicio de proporcionalidad, lo que no se justifica en ninguna de las dos sentencias.

[11] Expresamente así lo interpretan algunas sentencias en suplicación (STSJ País Vasco 27-2-2018, rec 226/18, STSJ Castilla y León 11-4-2018, rec. 407/18).

La Gran Sala ratifica en esta sentencia su doctrina sobre la noción de "vida privada" tutelada por el art. 8 CEDH, y su extensión al ámbito de la actividad laboral, particularmente frente a la videovigilancia en el lugar de trabajo (apdos. 87-95). También se acoge, *mutatis mutandis*, al canon de garantías perfilado en la STEDH 5-10-2010, *asunto Köpke*, y completado y sistematizado en la STEDH 5-9-2017 (Gran Sala), *asunto Barbulescu* (ap. 116).

De esta forma, la Sentencia dirige el test de legitimidad diseñado en esta última sentencia a enjuiciar la conformidad de la actuación de los tribunales nacionales con el Convenio. A partir de los siguientes factores: i) si ha existido información previa sobre la videovigilancia; ii) las características de las medidas empresariales y el grado de injerencia en la vida privada del trabajador; iii) la existencia de motivos legítimos; iv) si era posible o no medidas menos intrusivas para alcanzar dicho fin; v) la coherencia del uso que el empresario ha hecho del uso de la videovigilancia respecto de la finalidad que la justificó; vi) la existencia de garantías adecuadas, como la información ofrecida, la traslación de la información a un organismo independiente o la posibilidad de reclamaciones.

En primer lugar, se estima la justificación que los tribunales españoles otorgan a la videovigilancia (el interés legítimo empresarial en identificar a los responsables de las importantes pérdidas detectadas y sancionarles). El Tribunal destaca que en el análisis de la proporcionalidad de una medida de videovigilancia es necesario considerar el ámbito al que se dirige, y subraya que las garantías al respecto se atenúan en espacios visibles o accesibles a los compañeros o a un público amplio (ap. 125). En concreto, considera razonables las medidas de videovigilancia adoptadas, limitadas en el espacio y en los trabajadores afectados (las cámaras se circunscriben a las cajas que parecen estar en el origen de las pérdidas) (ap. 123 y 124), y limitadas temporalmente (ap. 126). Por otro lado, los resultados de la videovigilancia han sido utilizados para el fin que la justificó (identificar a los causantes de las irregularidades y sancionarles) (ap. 127).

Es llamativo que, en aplicación del test de legitimidad, la sentencia de la Sección 3ª y de la Gran Sala lleguen a conclusiones encontradas en todos los criterios (al igual que el voto particular frente al criterio de la mayoría en ésta última). Como ya observé en otro lugar [12], el test de legitimidad plasmado en la STEDH 5-9-2017, *asunto Barbulescu*, supone un avance en la clarificación de criterios a tener en cuenta en la aplicación del art. 8 CEDH, pero su valor se relativiza teniendo en cuenta que el TEDH considera necesario valorar las decisiones impugnadas a la luz del conjunto de la causa y respetar el margen de apreciación del que disponen los tribunales nacionales, bastando al Tribunal con que la argumentación de los mismos sea pertinente y suficiente (STEDH 22-2-2018, *asunto Libert contra Francia*).

Respecto del carácter oculto de la videovigilancia, que es el principal motivo

[12] "*El alcance del derecho al respeto de la correspondencia del trabajador ex art. 8 CEDH en la jurisprudencia del TEDH*", en *Temas Laborales*, núm. 145/2018, pág. 191.

de las demandas planteadas, entiende el Tribunal que la medida se justifica al no existir otra medida adecuada a la finalidad pretendida, ya que "informar a cualquier integrante del personal podía comprometer efectivamente la finalidad de la videovigilancia" (128). El Tribunal recuerda que "la exigencia de trasparencia y el derecho a la información que se deriva del mismo reviste un carácter fundamental" e implica, en principio, la necesidad de informar previamente y con claridad; pero entiende el TEDH que es posible justificar la ausencia de información previa cuando exista "un imperativo preponderante relativo a la protección de intereses públicos o privados importantes" (ap. 133). El supuesto de hecho de la sentencia encaja para el TEDH en este criterio: sospechas de graves irregularidades cometidas por la acción concertada de un grupo de trabajadores que afecta al buen funcionamiento de la empresa (ap. 134) [13].

Por otro lado, entiende la Gran Sala que el canon de razonamiento a seguir implica que "la información ofrecida a la persona sometida a la vigilancia y su amplitud no es sino uno de los criterios a tener en cuenta para apreciar la proporcionalidad de tal medida" (ap. 131), de manera que "si la información falta, las garantías derivadas de otros criterios serán más relevantes" [14]. Esta doctrina es coincidente con la mantenida en la STC 39/2016, estimando que el incumplimiento del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada. Es más, el Tribunal indica que los criterios de proporcionalidad establecidos por la jurisprudencia del TC y aplicados en el asunto "son próximos a los que él [el TEDH] ha mantenido en su jurisprudencia", debiéndose concluir que "las jurisdicciones internas han verificado si un motivo legítimo justificaba la medida de la videovigilancia y si las medidas adoptadas a este fin eran adecuadas y proporcionadas, habiendo constatado en particular que el fin legítimo perseguido por el empleador no podía ser alcanzado con medidas menos intrusivas para los derechos de las recurrentes" (ap. 132).

También resulta de interés la observación de la sentencia, referida al uso judicial de las pruebas obtenidas mediante la videovigilancia, que "el Tribunal no

[13] El voto particular de tres magistrados que acompaña la sentencia discrepa de la mayoría de la Sala. Parten del dato, que estiman determinante, de la exigencia de la normativa española de una información previa a las medidas de videovigilancia (art. 5 LOPD 15/99), sin que esta exigencia, para dichos magistrados, tenga en derecho español ninguna excepción (ap. 4 a 6). Por otro lado, entienden que los tribunales españoles no verificaron el criterio de la existencia de medios menos intrusivos que el adoptado por la empresa (ap. 8), ni consideran que la vigilancia haya sido limitada en el espacio y en los trabajadores afectados (como en el *asunto Kopke*) (ap. 11). Por otro lado, consideran que el interés empresarial en aclarar la situación irregular no permite a la empresa una videovigilancia oculta, pudiendo y debiendo la empresa poner en conocimiento de la policía lo que puede considerarse un ilícito penal (ap. 9). En definitiva, en este caso serían necesarias garantías procedimentales complementarias, al igual que la convención impone en la videovigilancia secreta en materia penal (ap. 10).

[14] El voto particular discrepa de este planteamiento porque considera que dicho canon de razonamiento se aparta del criterio tradicional que distingue la exigencia de legalidad de la medida y posteriormente el juicio de proporcionalidad (ap. 7).

observa ningún elemento que ponga en duda su autenticidad o fiabilidad. Considera por ello que tratándose de pruebas sólidas no existiría necesidad de ser corroboradas por otros elementos" (ap. 156). Aunque en el caso el Tribunal toma en consideración otros elementos de prueba (ap. 157).

## 4. EL TRATAMIENTO DE LOS SISTEMAS AUDIOVISUALES DE VIGILANCIA LABORAL EN EL RGPD DE 2016 Y EN LA LOPD DE 2018

La videovigilancia cuenta ya con un marco legal de regulación específica, dando por cerrada una etapa donde la protección del derecho a la intimidad se limitaba al art. 20.3 ET y a una doctrina judicial que facilitaba espacios de inseguridad jurídica, y desde la perspectiva de la protección de datos se circunscribía al marco general de la Directiva 95/46, la LOPD 15/99 y el RD 1720/2007 (con una adaptación, eso sí relevante, al ámbito laboral por medio de las instrucciones y resoluciones de la AEPD).

Actualmente, el Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y la LOPD constituyen el marco regulador de referencia respecto a la protección del trabajador frente a la videovigilancia empresarial [15]. Se puede decir que este marco regulador parte de la legitimación del poder de videovigilancia empresarial en las relaciones laborales, dentro de un marco normativo apoyado en los principios de legitimidad de fines, transparencia en la información y proporcionalidad en los métodos de videovigilancia.

El RGPD no establece una regulación específica de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral. Se limita en este sentido a facultar a los Estados miembros, a través de disposiciones legislativas o de convenios colectivos, para establecer "normas más específicas" (art. 88), con la importante puntualización de que el objetivo debe ser "garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral". Especifica que las normas estatales "incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos

[15] Cfr., sobre este marco jurídico, Goñi Sein, J.L., "*Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento europeo de protección de datos de 2016*", *RDS*, nº 78, 2018; García Murcia, J. y Rodríguez Cardo, I.A., "*La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo*", en REDT, nº 216, enero, 2019; Rodríguez Escanciano, S., "*Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales*", en *Diario La Ley*, nº 9328, 2-1-2019; Preciados Domenech C.H., *Los derechos digitales de las personas trabajadoras,* Th.R. Aranzadi, 2019; Orellana Cano, A.M. *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores,* Th.R. Aranzadi, 2019; Baz Rodríguez, J., "*La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático*", en *Trabajo y Derecho*, nº 54, junio, 2019,

fundamentales", con especial atención "a la transparencia del tratamiento,… y a los sistemas de supervisión en el lugar de trabajo" (art. 88.2). Por otra parte, el Reglamento fija los principios que deben regir el tratamiento de datos personales (art. 5 del Reglamento), también vinculantes en el ámbito laboral, siendo particularmente relevantes, como veremos, los principios de legitimación de la finalidad, trasparencia y proporcionalidad y minimización en el tratamiento de datos.

La LOPD da respuesta a este mandato del Reglamento comunitario mediante su Título X, referido a la "Garantía de los derechos digitales" (art. 79 y sigs.), donde se incluye el precepto de nuestro interés, el art. 89 [16]. Esta norma reconoce el derecho empresarial al control de la actividad laboral mediante video y audiovigilancia. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 ET y en la legislación de función pública, "siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo" (89.1, pár. 1 LOPD).

El art. 89.2 LOPD, por su parte, prevé que "en ningún caso se admitirá" la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos [17]. No obstante, aquí cabe distinguir espacios más sensibles a la intimidad y lugares de esparcimiento de los trabajadores que pueden estar abiertos al público (cafeterías, comedores) [18]. En este último caso puede justificarse una videovigilancia por objetivos de seguridad de las instalaciones de la empresa [19]. Recordemos que el TEDH considera que las garantías de la vida privada ex art. 8 CEDH requiere tomar en consideración el ámbito al que se dirigen las medidas de videovigilancia (STEDH (Gran Sala) 17-10-2019).

Por otra parte, y respecto del control empresarial en los espacios de trabajo, la instalación de sistemas de videovigilancia no es posible sin respetar el principio de legitimidad de fines, el derecho de información previa y el principio de proporcionalidad y de intervención mínima de la videovigilancia. Vamos a referirnos a estos requisitos.

[16] La especialidad de la problemática de la videovigilancia en el ámbito laboral, acreditada con la problemática jurisprudencial expuesta, puede ser la razón del tratamiento separado de la videovigilancia general en espacios públicos (art. 22 LGPD), que en el Proyecto de LOPD de 10 de noviembre de 2017 se incluía como apartado 5º del art. 22 del mismo.

[17] Como hemos visto, la doctrina constitucional ya era clara en la prohibición contenida en el art. 89.2 LOPD (STC 98/2000, FJ 6). Así lo prevé, igualmente, la Recomendación CM/Rec (2015)5 del Comité de Ministros de los Estados miembros del Consejo de Europa, apartado 15.2.

[18] Cfr. Desdentado Bonete, A. y Muñoz Ruiz, A.B., op. cit. págs. 58-59.

[19] Cfr. Desdentado Bonete, A. y Muñoz Ruiz, A.B., op. cit. págs. 31-33.

1. El principio de legitimidad de fines

Ciertamente, el empresario está legitimado para establecer una videovigilancia con el fin de controlar la actividad laboral del trabajador. Pero el RGPD recoge entre los principios básicos en la protección de datos que los mismos deben ser recogidos "con fines determinados, explícitos y legítimos", y que serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" (art. 5.1 b) y c) RGPD). De esta forma la legitimación del control empresarial no puede justificar una videovigilancia indiscriminada y permanente [20]. La legitimidad de fines está estrechamente vinculada al principio de proporcionalidad, como veremos.

2. El deber de información previa

En el ámbito laboral el tratamiento de datos se justificará legalmente por ser necesario para la ejecución de un contrato y por la existencia de un interés legítimo empresarial (art. 6.1 b) y f) RGPD). De manera que el fundamento de dicho tratamiento queda al margen del consentimiento del trabajador. La exigencia de una información previa inherente a una garantía de trasparencia ya es subrayada en diversos documentos relevantes en este terreno [21]. Destaquemos que, actualmente, el RGPR sitúa como concepto clave del tratamiento de datos la trasparencia de la información para asegurar la expectativa razonable de privacidad del afectado [22]. En este sentido, el art. 5.1 a) indica que los datos personales serán tratados "de manera lícita, leal y transparente en relación con el interesado". El art. 12.1 dis-

[20] La Recomendación CM/Rec (2015)5 del Comité de Ministros de los Estados miembros del Consejo de Europa, sobre el tratamiento de datos personales en el contexto del empleo, apartado 15, indica que "la introducción y utilización de sistemas y tecnologías de la información que tengan por finalidad directa y principal el control de la actividad y el comportamiento de los trabajadores no deben ser permitidos". Es posible que pueda existir "un control indirecto" de la actividad laboral "por otras finalidades, tales como la protección de la producción, de la salud, de la seguridad o la gestión eficaz de una organización".

[21] El Protocolo de revisión de 2018 del Convenio nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, destaca en la nueva versión del art. 5 del convenio la relevancia del principio de trasparencia en el tratamiento de datos personales, que se concreta en una ampliación de las obligaciones empresariales de información (deber de información sobre las bases legales y los fines del tratamiento de datos, sobre el catálogo de datos objeto de tratamiento y los derechos del afectado al respecto) (art. 8). También se refieren a dicho principio de trasparencia la Recomendación CM/Rec(2015)5 del Comité de Ministros de los Estados miembros del Consejo de Europa (apartado 14.1 y el apartado 21 a)) y los dictámenes del Grupo de Trabajo 29 (art. 29 Working Party) en interpretación de la derogada Directiva 95/46/CE. Así, el Informe 2/2017 GT29 recomienda que se comunique efectivamente a los trabajadores cualquier control que se lleve a cabo, sus fines y circunstancias, y que las políticas y normas relativas al control legítimo sean claras y de fácil acceso.

[22] J. Muñoz Ontier, "*Disposiciones generales (arts. 1-5*)", en *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, López Calvo (Coord.), Wolters Kluwer, 2018, pág. 348.

pone, además, que el responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información relativa al tratamiento de datos "en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo".

Situados ya en el ámbito laboral, se puede observar como regla general que el art. 89 LOPD cierra el paso a las practicas extendidas en nuestras relaciones laborales de una video vigilancia empresarial sin conocimiento de los trabajadores y de sus representantes. Recordemos que un aspecto que no ofrece dudas en la jurisprudencia constitucional es la exigencia de una información previa de la instalación de sistemas de videovigilancia (SSTC 29/2013 y 39/2016).

Dicho esto, el art. 89.1 LOPD diferencia de manera implícita el deber de información según se refiera a una videovigilancia específica de control laboral o a una videovigilancia de seguridad general (de personas, bienes e instalaciones). En el primer caso, como supuesto típico de la norma, los empleadores habrán de informar "con carácter previo, y de forma expresa, clara y concisa", a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. (89.1, pár. 1 LOPD). El alcance del derecho de información debería incluir algunos aspectos de la información básica del art 11.1 de la Ley, en concreto "la finalidad del tratamiento" y "la posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679" [23]. Por analogía, es trasladable a este supuesto el contenido de la información exigida para los dispositivos de geolocalización por el art. 90.2 de la Ley, concretamente, "la existencia y características de estos dispositivos" y "el posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión" (son derechos a los que se refieren los artículos 15 a 22 del RGPD). Sólo de esta manera el trabajador puede tutelar su privacidad en la empresa y, por ejemplo, hacer uso del derecho de supresión («el derecho al olvido»), cuando los datos personales hayan sido tratados ilícitamente (art. 17.1 d) RGPD).

A la vista de estas reglas, en el caso de la videovigilancia específica de control laboral no será suficiente con la colocación de un dispositivo informativo ex 22.4 LOPD, porque así lo dispone expresamente el art. 89.1, pár. 1º y porque en otro caso carece de sentido el supuesto singular del pár. 2º de esta norma, que comentamos a continuación. En suma, los trabajadores deben ser informados previamente a la instalación de los sistemas de videovigilancia de que éstos tienen una específica función de control laboral y de sanción disciplinaria, en su caso, y de sus características.

El segundo supuesto, la videovigilancia de seguridad de instalaciones, sólo

[23] Estas reglas deben completarse con la previsión sobre un deber de trasparencia del art. 12.1 RGPD, que prevé que "la información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos"; la comunicación de forma verbal sólo se admite "cuando lo solicite el interesado".

puede utilizarse con fines laborales en el supuesto de captación de actos ilícitos del trabajador. En este caso, se entenderá cumplido el deber de información previa cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de la LOPD (89.1, pár. 2), es decir, mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando la existencia del sistema de videovigilancia. Esta previsión legislativa supone la admisión del uso con fines laborales de un sistema de videovigilancia general [24].

La previsión del art. 89.1, pár. 2 LOPD parece tomar como referencia la doctrina de la STC 39/2016, y, particularmente, la doctrina de las SSTS 31-1-2017 y 1-2-2017, ya comentadas. Recordemos que en estas sentencias del TS lo que se debate es el uso con fines laborales de sistemas de videovigilancia por motivos de seguridad del establecimiento. El TS concluye que se supera el juicio de proporcionalidad y "los trabajadores estaban informados, expresamente, de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad, *expresión amplia que incluye la vigilancia de actos ilícitos de los empleados y de terceros y en definitiva de la seguridad del centro de trabajo*" (cursivas nuestras); en estos asuntos se consideran actos ilícitos actuaciones irregulares en el uso de cajas registradoras, con sustracción de dinero (que justificará el despido por transgresión de la buena fe contractual y abuso de confianza).

Ahora bien, puntualiza el TS que esta finalidad genérica del sistema de vigilancia "excluye otro tipo de control laboral que sea ajeno a la seguridad, esto es, el de la efectividad en el trabajo, las ausencias del puesto de trabajo, las conversaciones con compañeros, etc. etc..". De manera que no podría hacerse un uso laboral de cámaras de videovigilancia de seguridad general para registrar el cumplimiento de horarios laborales (como fue el caso de la STC 29/2013), pero sí en el caso de captación de grave manipulado de cajas registradoras (el caso de la STC 39/2016) o sustracción de productos (el caso de la STS 7-7-2016, rec. 3233/14). Es decir, las pruebas extraídas de la videovigilancia general pueden ser utilizadas legítimamente cuando la actuación del trabajador afecte a la integridad de las instalaciones, bienes y personas en la empresa, pero no cabe servirse de este tipo de videovigilancia para el control del cumplimiento de las obligaciones laborales. Creo que este esquema argumental del TS es el que ha encontrado acogida en el art. 89.1, pár. 2º LOPD. Es el mismo planteamiento recogido expresamente en el art. 89.3 LOPD para la utilización de sistemas de audiovigilancia en el lugar de trabajo.

La cuestión ahora es si, con este marco jurídico, cabe la existencia de dispositivos específicos ocultos para verificar sospechas de ilícitos laborales. El supuesto no es abordado en el art. 89 LOPD. Es significativo que en la tramitación parla-

[24] Esta posibilidad ha sido cuestionada en sentencias de instancia por estimarse que contradice la doctrina de la sentencia de la Sección 3ª del TEDH de 9-1-2018, *asunto López Ribalda* (SJS nº 3 Pamplona 18-2-2919, nº 52/2919; SJS nº 3 Bilbao 4-4-2019, nº 128/2019), y aunque, en mi opinión, era compatible con dicha sentencia, la posterior STEDH (Gran Sala) cierra cualquier posible polémica al respecto.

mentaria del proyecto de LOPD no se admitieron enmiendas (las núms. 81 y 265) que amparaban la colocación de videovigilancia sin necesidad de información a los trabajadores, siempre que existiesen sospechas fundadas y se respetase el principio de proporcionalidad. Sin embargo, la doctrina de la STEDH (Gran Sala) 17-10-2019, *asunto López Ribalda,* avala, en mi opinión, esta posibilidad, siempre que se verifiquen los concretos factores que constituyen el canon de razonamiento de la sentencia. Recordemos que en esta sentencia el TEDH parte de la existencia de una regulación en España que impone la necesidad de informar con claridad y con carácter previo de una medida de videovigilancia. Sin embargo, ello no ha sido obstáculo para admitir dicha práctica si se respeta un principio de proporcionalidad.

### 3. El límite del juicio de proporcionalidad y de intervención mínima

La instalación de sistemas de videovigilancia debe respetar el principio de proporcionalidad y de intervención mínima, porque, aunque no se recoja expresamente (tal como ocurre para la grabación de sonidos ex art. 89.3 LOPD), el poder de control empresarial deberá ejercerse "con los límites inherentes al mismo" (89.1, pár. 1 LOPD). No hay que olvidar que el RGPD recoge entre los principios básicos en la protección de datos que los mismos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" (art. 5.1 b) y c) RGPD). Ya hemos referido que se trata de un canon de razonamiento asentado en la jurisprudencia constitucional y que ahora cuenta con un canon de garantías delimitado con claridad en la STEDH (Gran Sala) 17-10-2019, *asunto López Ribalda*.

El régimen del uso de sistemas de audiovigilancia en el lugar de trabajo se contiene en el art. 89.3 LOPD. Conforme al mismo, la utilización de sistemas de audiovigilancia en el lugar de trabajo "se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo". La finalidad del control constituye la singularidad de su régimen jurídico con respecto a la videovigilancia, cuyo fundamento está en el interés legítimo de la empresa (art. 6.1 f) RGPD). Pero no cabe excluir el supuesto en que la grabación de sonidos sea estrictamente necesaria para la ejecución del contrato (art. 6.1 b) RGPD), como es el caso del telemarketing telefónico, donde la jurisprudencia admite esta posibilidad (STS 5-12-2003, rec. 52/2003).

Por otro lado, se establece expresamente que dicha audiovigilancia debe respetar el principio de proporcionalidad y el de intervención mínima, que como hemos indicado son también aplicables al supuesto de videovigilancia. Además, deben respetarse las garantías previstas en los apartados anteriores del art. 89 LOPD, es decir, una información específica previa, y el respeto de los espacios de privacidad del trabajador en las instalaciones empresariales. De esta norma, el legislador re-

quiere el cumplimiento del deber de información también en supuestos de riesgos relevantes para el interés empresarial. Finalmente, se dispone que la supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 LOPD [25].

## 5. EL PAPEL REGULADOR DE LA NEGOCIACIÓN COLECTIVA Y EL DERECHO DE INFORMACIÓN Y CONSULTA DE LOS REPRESENTANTES DE LOS TRABAJADORES

Tanto el RGPD como la LOPD contemplan un papel regulador para la negociación colectiva en la materia. El art. 88.1 RGPD indica que los Estados miembros podrán establecer "normas específicas" de adaptación de la regulación europea a través de disposiciones legislativas e igualmente mediante convenios colectivos [26]. Por su parte, el artículo 91 LOPD dispone que los convenios colectivos podrán 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. Entendemos que la negociación podrá adaptar la regulación prevista en la LOPD, respetando en todo caso sus prescripciones.

El derecho de información y consulta de los representantes de los trabajadores sobre los medios de tratamiento de datos previstos por la empresa en el plano laboral es subrayado en diversos documentos internacionales relevantes en este terreno [27]. La Ley española contempla el protagonismo de los representantes de los trabajadores en la efectividad de las garantías de los derechos digitales de los trabajadores, como se refleja en diversos preceptos (art. 87.3, 88.3 LOPD). Por su

[25] Recordemos que la STC 98/2000 estima contrario al principio de proporcionalidad las grabaciones indiscriminadas de voz y conversaciones de los trabajadores en el lugar de trabajo, al margen de que en el caso la empresa informara previamente a los trabajadores de dicho sistema de control. Considera especialmente relevante que la audiovigilancia permite captar comentarios privados, "ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal" (FJ 9). Para el TC no se cumple el juicio de necesidad (dentro del test de proporcionalidad) porque no queda acreditado en el caso que la audiograbación fuera imprescindible para la seguridad de la empresa. Precisamente, apoyándose en esta doctrina de la STC 98/2000, la jurisdicción ordinaria valora los supuestos de telemarketing telefónico, estimando que en estos casos se verifica el cumplimiento del juicio de proporcionalidad (STS 5-12-2003, rec. 52/2003; STSJ País Vasco, 10-5-2011, rec. 727/11; STSJ Andalucía 4-9-2014, rec. 1330/14): el teléfono como herramienta de trabajo, con información previa del posible control empresarial, control referido a las llamadas entrantes con un objetivo de control de calidad del servicio, salvaguardando la intimidad del trabajador mediante la habilitación de teléfonos o líneas de uso personal y no profesional.

[26] El considerando 155 del RGPD puntualiza que la referencia a los convenios colectivos, incluye también los «convenios de empresa».

[27] Recomendación CM/Rec(2015)5 del Comité de Ministros de los Estados miembros del Consejo de Europa (apartado 21 c)), e Informe 2/2017 del Grupo de Trabajo 29 (art. 29 Working Party) en interpretación de la derogada Directiva 95/46/CE.