Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Facultad de Derecho

PCEO DERECHO-ADE

TRABAJO FIN DE GRADO

VIDEOVIGILANCIA LABORAL Y PROTECCIÓN DE DATOS PERSONALES

Alumno: Alba Martínez Rubio

Convocatoria: Extraordinaria, julio de 2020

RESUMEN

En el presente trabajo se analiza la videovigilancia empresarial en torno a las novedades que plantea la normativa de protección de datos. El desarrollo de nuevas tecnologías ha permitido a las empresas utilizar de manera generalizada estos medios de control de los trabajadores. En este sentido, la instalación de videocámaras y la grabación de sonidos ha generado mucha controversia por la compleja ponderación de los intereses empresariales frente a los derechos fundamentales de los trabajadores.

Los derechos fundamentales afectados por la videovigilancia están regulados, principalmente, en el artículo 18 de la Constitución. Así, se habla del derecho a la intimidad, a la propia imagen, al secreto de las comunicaciones y al derecho a la protección de datos, entre otros.

La dificultad del estudio se ve incrementada por la ausencia de una legislación específica de protección de datos en el ámbito laboral y sobre videovigilancia empresarial. En este contexto, como veremos, adquiere gran importancia la labor interpretativa de los Tribunales (tanto nacionales como europeos).

ABSTRACT

The following research analyses the video surveillance in relation to the current regulation on data protection. Brand new technologies have allowed companies to use these control methods in an extensive way. This has caused a lot of controversy due to the complex balance between business interests and workers' rights.

The 18th article of the Constitution establishes the fundamental rights affected by video surveillance. Those rights include the right to privacy, self-image, secrecy of communications and data protection, among others.

The complexity of the study has increased because of the absence of a specific legislation on data protection and video surveillance in the workplace. In this context, the interpretative work of the Courts has acquired great importance (both national and supranational Courts).

PALABRAS CLAVE: video vigilancia, protección de datos, intimidad, derechos fundamentales.

KEY-WORDS: video surveillance, data protection, privacy, fundamental rights.

ACRÓNIMOS Y ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
Art.	Artículo
CE	Constitución Española de 27 de diciembre de 1978
CEDH	Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente.
DPD	Delegado de Protección de Datos
ET	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
GTA 29	Grupo de Trabajo del Artículo 29 creado por la Directiva 95/46/ CE
LOPD	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LPRL	Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales.
núm.	Número
OIT	Organización Internacional del Trabajo
RPGD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016
TC	Tribunal Constitucional
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnología de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
TSJ	Tribunal Superior de Justicia

ÍNDICE

INTRODUCCIÓN

La videovigilancia es un medio de control empresarial cada vez más habitual en el entorno laboral. Su desarrollo ha evolucionado mucho a lo largo de los años a raíz de la aparición de las tecnologías de la información (TIC) y al aumento de las transacciones económicas. En este sentido, se puede afirmar que las nuevas tecnologías han transformado los centros de trabajo, desde los sistemas organizativos hasta las relaciones laborales.

Los cambios tecnológicos tienen muchos aspectos positivos, pero también vienen de la mano de nuevas amenazas relacionadas con la vulneración de derechos fundamentales de los trabajadores. No cabe duda, que los medios de control tecnológico han incrementado los poderes de dirección y control del empresario sobre los trabajadores, y han contribuido a difuminar la línea de separación entre la vida personal y la vida profesional.

La importancia del estudio de los sistemas de videovigilancia actuales se debe a que han acrecentado los conflictos entre los intereses empresariales y los derechos fundamentales relativos a la intimidad, a la propia imagen, y a la protección de datos personales de los empleados, entre otros.

A la complejidad que supone ponderar los denominados “derechos de la personalidad” de los trabajadores frente a los poderes empresariales, se añade la ausencia de una regulación clara y específica en materia laboral.

Para el estudio de esta problemática es preciso adentrarse en la nueva normativa de protección de datos, tanto a nivel nacional como europeo; en el Estatuto de los Trabajadores y en la labor interpretativa de los Tribunales.

Con el propósito de situar en contexto la materia objeto de estudio, se debe hacer una breve mención a la definición de dato personal y su implicación. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, lo delimita como “*toda información sobre una persona física identificada o identificable*” (art. 4). La jurisprudencia, asimismo, ha ido precisando qué tipo de información merece una especial protección de esta normativa, quedando fuera la protección de datos de las personas jurídicas.

Las imágenes y sonidos captados por videocámaras son datos personales cuando identifican o permiten identificar a las personas[1]. Además, pueden considerarse como

[1] RD 1332/1994, de 20 de junio.

datos especialmente sensibles cuando posibilitan el conocimiento del origen racial o étnico, la religión, las creencias…de un trabajador. Por todo ello, la normativa de protección de datos ha realizado un esfuerzo por establecer mayores garantías.

A fin de ofrecer una visión de los aspectos controvertidos de esta temática, el trabajo se ha estructurado en tres partes. En primer lugar, se hace una breve alusión a los antecedentes y marco normativo en materia de protección de datos. Seguidamente, se trata tanto los poderes empresariales, como la finalidad, medios y medidas de seguridad en relación a la videovigilancia empresarial. Por último, se abordan los límites a las facultades empresariales, es decir, se analizan los derechos fundamentales de los trabajadores afectados por la videovigilancia.

1. ANTECEDENTES Y MARCO NORMATIVO

La normativa de protección de datos personales contiene reglas generales que están pensadas para todo tipo de relaciones sociales. Actualmente, no existe una normativa específica que regule la protección de datos personales en el ámbito laboral, aunque no se descarta que en un futuro cercano pueda elaborarse.

La protección de datos personales tiene su origen en el Convenio núm. 108 aprobado por el Consejo de Europa el 28 de enero de 1981. Esta norma internacional no hacía ninguna mención expresa al ámbito laboral y estaba orientada al tratamiento de datos automatizados en relación con el derecho fundamental a la vida privada.

En 1995 se aprobó a nivel europeo la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, convirtiéndose en el primer instrumento legislativo con alcance general que incluía alguna referencia al ámbito laboral. Su objetivo era la armonización de la normativa de protección de datos personales y la libre circulación de estos con las oportunas garantías. A partir de este momento, el tratamiento de datos personales ya no era concebido solo como un aspecto social sino también como una cuestión esencial para las transacciones económicas[2].

Los nuevos desafíos tecnológicos y la existencia de una normativa fragmentada dejaron al descubierto las carencias que arrastraba la Directiva 95/46/CE. En este contexto, se aprobó el Reglamento Europeo 2016/679, de 27 de abril de 2016 (en adelante RGPD),

[2] 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*", Nueva Revista Española de Derecho del Trabajo*, nº 216, 2019, (versión digital), págs. 1 y ss.

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. Sin embargo, no entró en vigor hasta el 25 de mayo de 2018 para posibilitar que los Estados europeos y organizaciones fueran conociendo su contenido y adaptándose a la nueva normativa.

A diferencia de la Directiva de 1995, que fue transpuesta de manera desigual, el RGPD es de eficacia y aplicación directa en todos los Estados Miembros. De esta forma, deja poco margen a los Estados para que legislen sobre esta materia, consiguiendo así sentar las bases y unificar la normativa.

El Reglamento Europeo deroga la Directiva anterior y moderniza la normativa sobre protección de datos. Entre sus novedades destaca la inclusión de tres nuevos conceptos que forman parte de la definición de "dato personal": los datos genéticos, los datos biométricos y los datos relativos a la salud. Incorpora también nuevos derechos, como el derecho al olvido, el derecho a la portabilidad de datos y el derecho a la transparencia de información, entre otros. Y amplía el deber de información a los interesados, traduciéndose en un mayor control sobre sus datos personales[3].

Por otra parte, el RGPD habilita a los Estados Miembros a regular sobre determinadas materias específicas, entre las que se encuentra el ámbito laboral (art. 88 RGPD). Igualmente, permite que las empresas elaboren códigos de conducta, acuerdos de empresa, convenios colectivos, etc., para el tratamiento de datos personales de sus trabajadores.

Pese a que el Reglamento reconoce la importancia del tratamiento de datos en el ámbito laboral y autoriza a los Estados a la concreción de su contenido, la nueva normativa española apenas hace referencia a las relaciones laborales. Así, el 6 de diciembre de 2018 se publicó la Ley Orgánica 3/2018, de 5 de noviembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDPGDD).

Esta Ley derogó formalmente la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y modificó (disposiciones finales 13ª y 14ª) el Estatuto de los Trabajadores (art. 20 bis ET) y el Estatuto Básico del Empleado Público (art. 14.j. bis). En esencia, se ha limitado a la adaptación del ordenamiento jurídico interno al Reglamento Europeo y a garantizar los denominados "derechos digitales" en relación al art. 18.4 CE.

[3] Se crea la figura del Delegado de Protección de Datos (DPD) para asesorar a las empresas acerca de la normativa de protección de datos personales. Se suprime el deber de notificación a la AEPD sobre la creación de ficheros. Asimismo, se establece la obligación de realizar evaluaciones sobre el impacto en la protección de los datos personales, etc.

La LO 3/2018 hace mención al ámbito laboral, exclusivamente, en los artículos 22, 24, 87, 88, 89 y en las disposiciones finales decimotercera y decimocuarta. No crea, por tanto, una regulación específica en materia laboral. Resulta paradójico, además, que, de los siete preceptos mencionados, cuatro se refieran a los dispositivos de videovigilancia, de forma, que se convierte en la primera ley que aborda la videovigilancia empresarial. No obstante, estas escasas referencias no permiten hablar tampoco de un régimen jurídico propio[4].

En todo caso, las lagunas que existen en nuestro ordenamiento jurídico en relación con el ámbito laboral y, más concretamente, con la videovigilancia empresarial, van cubriéndose con el esfuerzo interpretativo de los Tribunales, tanto nacionales como europeos.

2. EL USO DE DISPOSITIVOS DE GRABACIÓN DE IMAGEN Y/O SONIDO EN EL TRABAJO

El control de videovigilancia viene definido en el artículo 42 de la Ley 5/2014, de 4 de abril, de Seguridad Privada, como "*el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas*."

Por descontado, las imágenes y sonidos captados son datos personales siempre que, como se deduce del Reglamento Europeo 2016/679 de protección de datos, determinen o permitan determinar la identidad de una persona física[5], otorgándose una especial protección a los mismos.

El desarrollo tecnológico ha venido a sustituir las formas de videovigilancia personal por sistemas de vigilancia audiovisual que se extienden tanto en el ámbito público como en el ámbito privado de la empresa (siendo este último el que se va a tratar). Estos medios posibilitan un control más amplio de la actividad laboral, permitiendo al empresario visionar y/o escuchar las grabaciones en un momento posterior, y crear bases de datos.

[4] ALTÉS TARREGA J.A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la SETDH López Ribalda (II)", *Revista General del Derecho del Trabajo y de la Seguridad Social*, nº 55, 2020, págs. 328 y ss.

[5] Así, fue declarado en la STEDH núm. 42409/98, de 21 de febrero de 2002 (Caso Schüssel vs. Austria), la sentencia núm. 59320/00 (Caso Von Hannover vs Germany) y más recientemente en la STC 39/2016, de 3 de marzo.

El objeto de controversia sobre el que se ahondará en el presente trabajo será, precisamente, el poder empresarial frente a los derechos de los trabajadores, expresado a través de sistemas de videovigilancia.

2.1. EL PODER DE DIRECCIÓN DEL EMPRESARIO: VIGILANCIA, CONTROL Y POLICÍA

El artículo 20 del Estatuto de los Trabajadores regula el poder de dirección y control de la actividad laboral, que se configura como una de las manifestaciones de la libertad empresarial (art. 38 CE). El empresario está facultado para organizar la empresa, dar órdenes e instrucciones (poder de dirección), vigilar (poder de control) y sancionar (poder disciplinario) a los trabajadores, etc.

Para llevar a cabo sus funciones puede valerse de diversos mecanismos de vigilancia y control. El artículo 20.3 ET no prohíbe la utilización de ninguno, pero si establece dos límites: que los medios de control estén dirigidos a vigilar y controlar las obligaciones y deberes laborales de los trabajadores, y que respeten su dignidad. Asimismo, se incluye como garantía la participación de los representantes de los trabajadores (art. 64.5 f) ET)[6].

El primer límite tiene como objetivo evitar que el empresario extienda sus poderes de control a la esfera privada de los trabajadores o a cuestiones no vinculadas con el desarrollo de la actividad laboral. No obstante, en la práctica no es tan fácil delimitar qué pertenece a la actividad laboral y qué no. Las nuevas tecnologías y sistemas de organización del trabajo han desdibujado aún más la separación entre la vida privada y la vida laboral.

Entre los poderes que ostenta el empresario está el "poder de policía" que le permite preservar el patrimonio empresarial y le obliga a proteger a los trabajadores y/o terceros vinculados con la empresa. En este sentido, el empleador puede acceder a los objetos personales del trabajador (facultad de registro), conforme a lo establecido en el artículo 18 ET.

El poder de control y vigilancia no solo alcanza, por tanto, a supervisar que los trabajadores cumplen específicamente las ordenes empresariales, sino a vigilar que cumplen todo tipo de obligaciones, incluidas las no contractuales[7]. Sin embargo, esto

[6]ARRÚE MENDIZÁBAL M., *El derecho a la propia imagen de los trabajadores*, Aranzadi, Cizur Menor (Navarra), 2019, Capítulo IV, págs. 345 y ss.

[7] El poder de vigilancia y control es independiente del poder directivo (que ordena y dirige la actividad laboral). La facultad de vigilancia puede ir más lejos de la actividad laboral, abarca controles extralaborales, tales como la supervisión de bienes, personas e instalaciones de la empresa.

último se corresponde con un poder extraordinario o excepcional y solo debería ejercitarse ante sospechas de incumplimientos muy graves por parte de los trabajadores ("*que puedan perjudicar los legítimos intereses de la empresa*"[8]).

El segundo límite versa sobre el respeto a la dignidad de los trabajadores durante la vigencia de las medidas de control empresarial. La dignidad humana alude al respeto de los derechos y libertades de los trabajadores, y se configura como un valor o principio fundamental.

Los sistemas de videovigilancia y los mecanismos de control tecnológicos aumentan el riesgo de que no se respete la dignidad de los trabajadores, debido a su mayor capacidad de intromisión frente a otros medios más tradicionales. No obstante, los derechos fundamentales no son límites absolutos al poder empresarial, a la vez que tampoco el poder empresarial es ilimitado. La doctrina constitucional intenta lograr un equilibrio entre ambas posiciones a través del juicio de proporcionalidad, que se tratará más adelante.

En último lugar, es preciso hacer una mención a la participación de los representantes de los trabajadores en el poder de dirección empresarial. El artículo 64.5. f) del ET dispone que su intervención constituye una garantía añadida a la protección de los derechos de los trabajadores. En concreto, el "*comité de empresa tendrá derecho a emitir un informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre la implantación y revisión de sistemas de organización y control del trabajo".*

Ahora bien, se trata de una participación limitada, porque el informe emitido por el comité de empresa no es preceptivo y tampoco se requiere que el empresario llegue a un acuerdo con los representantes de los trabajadores. Al mismo tiempo, la normativa no es clara respecto a los efectos jurídicos que supondría el incumplimiento de esta formalidad.

La jurisprudencia, en la misma línea, ha minimizado la importancia de esta garantía, convirtiéndola en un mero trámite ajeno al objeto de los conflictos suscitados en torno a los sistemas de videovigilancia[9].

[8] ARRÚE MENDIZÁBAL M., *El derecho a la propia imagen de los trabajadores*, Aranzadi, Cizur Menor (Navarra), 2019, Capítulo IV, págs. 347 y ss.
[9] STC 186/2000, de 10 de julio.

2.2. FINALIDAD Y ALCANCE DE TRATAMIENTO DE IMÁGENES Y SONIDOS

El Reglamento (UE) 2016/679, de protección de datos, dispone en su artículo 5.b) que los datos "*serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines*".

La nueva Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, regula en los artículos 22 y 89 el objetivo perseguido y la finalidad de tratamiento de los datos obtenidos a través de sistemas de videocámaras en el centro de trabajo.

Las empresas hacen uso de estos sistemas con dos objetivos claros: controlar la actividad laboral de su personal (art. 89 LOPDPGDD) y/o, garantizar; la seguridad de sus instalaciones, incluidos los bienes y personas que se encuentran en las mismas (art. 22 LOPDPGDD). En esta misma línea, se exige a los responsables de tratamiento de datos personales, especificar, de manera clara, la finalidad de utilización de los datos captados. Estos datos solo pueden emplearse para el objetivo perseguido y no para otro distinto, es decir, se exige que exista una conexión entre la finalidad y la recogida y tratamiento de datos posterior [10].

Los empleadores tienen permitido el uso de estos sistemas, conforme a lo estipulado en el artículo 20.3 del Estatuto de los Trabajadores, que establece las facultades de control y dirección empresarial. No obstante, se les exige que en su actuación respeten la dignidad de los trabajadores y actúen conforme a los límites dispuestos en la normativa de protección de datos, tal y como resalta el art. 89 de la LOPDPGDD.

Los sistemas de videovigilancia no pueden emplearse para el control directo y sin criterio de la actividad laboral. En este sentido, el *Grupo de Trabajo sobre protección de datos del artículo 29*[11]*,* estableció en su Dictamen 4/2004, de 11 de febrero, que "*los sistemas de vigilancia por videocámara, cuyo objetivo es controlar la calidad y cantidad de las actividades laborales y, por tanto, implican el tratamiento de datos personales en este contexto, por regla general no deberán estar permitidos*". En resumen, no son

[10] En cuyo caso, las imágenes y sonidos captados se considerarían ilegítimos (STC 29/2013, de 11 de febrero).

[11] El Grupo de Trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo europeo independiente en materia de protección de datos y privacidad. Está formado por la Comisión Europea, el Supervisor Europeo de Protección de Datos y las Autoridades de Protección de Datos de todos los Estados Miembros. La AEPD también se integra en el mismo desde 1997. Emite dictámenes, informes, recomendaciones…sobre protección de datos, de carácter no vinculante. Ha dejado de funcionar con la entrada en vigor del RGPD.

adecuados aquellos sistemas de vigilancia cuya finalidad es el seguimiento continuo del cumplimiento de la actividad laboral de los trabajadores[12].

Al hilo del argumento anterior, algunos autores consideran que el control laboral solo debería ser admitido para comprobar la existencia de un ilícito mediante el uso de cámaras ocultas o bien cuando se descubren incumplimientos de forma accidental[13].

En relación con las grabaciones de sonido, La Agencia Española de Protección de Datos recoge en su Informe núm. 497/2007, que también constituyen datos personales, conforme a lo establecido en la propia Ley de Protección de Datos y, en la medida que faciliten la identificación de una persona con cierta facilidad[14]. No obstante, la actual Ley Orgánica de Protección de Datos Personales, en el apartado tercero del artículo 89, limita su uso a aquellos casos en los que se aprecie un riesgo notable para la seguridad en el espacio de trabajo, y exige respetar los "*principios de proporcionalidad, intervención mínima y las garantías previstas*"[15].

2.3. EL DEBER DE INFORMACIÓN. REFERENCIA AL CONSENTIMIENTO

La licitud de las medidas de videovigilancia se basa, principalmente, en el deber de informar a los trabajadores y a sus representantes sobre las mismas. Tal información debe ser previa, y hacerse de manera "*expresa, clara y concisa",* de acuerdo al artículo 89.1. de la LOPDPGDD.

El deber y derecho de información ha sido uno de los elementos más problemáticos a la hora de establecer estos sistemas de control en el ámbito laboral. No obstante, antes de entrar en la materia, es preciso hacer referencia al consentimiento.

No es necesario el consentimiento explícito del trabajador, porque se sobreentiende que se produce un consentimiento implícito o tácito en el momento de la firma de un contrato de trabajo[16]. En otras palabras, los trabajadores, mediante la celebración del contrato,

---

[12] GOÑI SEIN, J. L., *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa,* Bomarzo, Albacete, 2018, págs. 67 y ss.

[13] ALTÉS TARREGA J.A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la SETDH López Ribalda (II)", *Revista General del Derecho del Trabajo y de la Seguridad Social*, nº 55, 2020, págs. 328 y ss.

[14] Agencia Española de Protección de Datos, Informe jurídico 497/2007.

[15] ORELLANA CANO, A. M. *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores.* Aranzadi, Cizur Menor (Navarra), 2019, págs. 136-145.

[16] ARRÚE MENDIZÁBAL M.*, El derecho a la propia imagen de los trabajadores*, Aranzadi, Cizur Menor (Navarra), 2019, Capítulo IV, págs. 350 y ss.

aceptan el uso de estos sistemas como parte del poder de dirección y control empresarial recogido en el artículo 20.3 ET; y para el cumplimiento de la finalidad de seguridad. Así lo ha dejado patente la STC 39/2016, de 3 de marzo, que, además, añade que, "*aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de información"*.

No obstante, los medios de control empresarial, como la instalación de videocámaras, deben estar justificados y ser legítimos para que puedan limitar los derechos fundamentales de los empleados (arts. 5 y 6 RGPD). En otras palabras, la ausencia de consentimiento por parte de los trabajadores no autoriza a los empresarios a ejercitar poderes de vigilancia y control desproporcionados o exorbitantes.

Por otro lado, en caso de que los empleadores exigiesen un consentimiento expreso por parte de sus empleados, se consideraría un consentimiento condicionado, debido a que no se encuentran en igualdad de condiciones a la hora de contratar. En este sentido se ha pronunciado el Grupo de Trabajo Sobre Protección de Datos del artículo 29 en el Dictamen 2/2017, al sostener que "*los trabajadores casi nunca están en condiciones de dar, denegar o revocar el consentimiento libremente, habida cuenta de la dependencia que resulta de la relación empresario/trabajador. Dado el desequilibrio de poder, los trabajadores solo pueden dar su libre consentimiento en circunstancias excepcionales, cuando la aceptación o el rechazo de una oferta no tiene consecuencias."*

De otro lado, el deber fundamental de información está muy ligado al consentimiento, tanto es así, que, en ocasiones, se llega a hablar de la necesidad de un "consentimiento informado". La información cobra un mayor interés en este terreno, porque la dispensa del consentimiento, la convierte en el único medio que tiene el trabajador para la protección y control de sus datos personales. Sin ella, el trabajador no puede ejercitar otros derechos como el derecho de oposición, rectificación, acceso, supresión y limitación del tratamiento, entre otros.

El Reglamento (UE) 2016/679 ha reforzado el deber informativo, exigiendo una mayor transparencia y rigor en la información que se suministra a los empleados. Así el Considerando (39) dispone que "*debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro."*

Para el cumplimiento del deber de información, la Agencia Española de Protección de Datos[17] exige incorporar carteles informativos claros y visibles en las zonas videovigiladas. Los rótulos deberán incluir: 1) La legislación aplicable, 2) El propósito de su colocación ("*debe referirse a que es una zona videovigilada*"), y 3) La determinación del responsable del tratamiento, fundamentalmente (art. 13 RGPD).

No es necesario que tales distintivos informativos se coloquen próximos a las cámaras y tampoco que se especifique si graban, además de imágenes, sonidos. Si será preciso que tales carteles estén presentes tanto en la entrada del centro de trabajo como en aquellas áreas donde estén colocadas las cámaras. En definitiva, la finalidad de los distintivos informativos es que el empleado tenga constancia de que está siendo grabado de manera lícita y como parte de la facultad de control y dirección del empresario.

Por el contrario, ha habido varios giros jurisprudenciales acerca de si es esencial la información previa e individualizada a los trabajadores, además, de la presencia de estos carteles. Se hace referencia tanto a la información dispuesta en el contrato de trabajo como a la información adicional que se proporciona al interesado en un momento posterior. Dicha información debería alcanzar a la identidad del responsable del tratamiento, la finalidad de tratamiento, sus destinatarios, sus efectos, y los derechos que pueden ejercitar los trabajadores (art. 11 LOPDGDD). Sin embargo, la normativa aplicable no dispone cuánta información ni cómo debe proporcionarse (la forma); y tampoco es clara acerca de las consecuencias que se derivan de su incumplimiento.

Ahora bien, si las cámaras captan la "*comisión flagrante de un acto ilícito por los trabajadores*", el deber de información se entiende cumplido con la "*colocación de un dispositivo informativo en un lugar suficientemente visible (…)*" (arts. 22.4 y 89.1. LOPDGDD). Esta salvedad tampoco clarifica a qué tipo de actos ilícitos se refiere la ley, pero se vienen interpretando jurisprudencialmente como incumplimientos laborales (habitualmente son hurtos, sustracción de dinero, etc.).

La instalación de estos sistemas de control se debe notificar a los representantes de los trabajadores, tal y como dispone el artículo 64 del ET, el artículo 89 de la LOPDGDD y el Informe Jurídico, núm. 0006/2009 de la AEPD.

Además, es aconsejable consultar previamente a los representantes de los trabajadores sobre la implantación de mecanismos de control para garantizar una mejor protección

[17] Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD, págs.. 21 y ss. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf (Fecha de consulta: 1 de junio de 2020)

de sus derechos[18]. En concreto, este método sería útil cuando no se informa previamente a los empleados porque existen indicios de que se están produciendo infracciones durante el periodo de trabajo (es el supuesto de las cámaras ocultas).

No se requiere el consentimiento expreso de los representantes de los trabajadores, sino que bastaría con su conocimiento y, en el supuesto de que no se cumpla el deber de información, no conllevaría la ilicitud del tratamiento de datos, pero sí que podrían derivarse sanciones administrativas.

En la práctica, los Tribunales han ido cambiando de criterio respecto de la importancia del deber de información[19]. Así, en la STC 186/2000, de 10 de julio, el Tribunal concluyó que el deber de información del empresario no era esencial, porque se pretendía descubrir a un trabajador cometiendo incumplimientos graves y no existían otros medios menos perjudiciales.

En cambio, en la STC 29/2013, de 11 de febrero, se establece la necesidad de proporcionar al trabajador una información "*previa y expresa, precisa, clara e inequívoca sobre la finalidad de control de la actividad laboral",* no siendo suficiente con el cartel informativo de "zona videovigilada".

Nuevamente, en la STC 39/2016, de 3 de marzo, se modifica el criterio anterior. El Tribunal sostiene que el deber de información se entiende cumplido con los carteles informativos de "zona videovigilada". Asimismo, reconoce que "el *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*", por tanto, se constituye como un deber residual.

Por último, están las recientes SSTEDH en el caso López Ribalda I y II[20]. La STEDH de 9 de enero de 2018 (Caso López Ribalda contra España I) reconoce la obligación del empresario de informar previamente a los trabajadores sobre el tratamiento y finalidad de la recogida de datos (recogido en el art. 5 LOPD 1999 y el art. 3 de la Instrucción 1/2006 de la AEPD), que en este caso se incumplió.

El Estado español recurre la STEDH de 9 de enero 2018 (Caso López Ribalda contra España I) ante la Gran Sala. Por el contrario, la STEDH de 17 de octubre de 2019 (Caso

[18]ORELLANA CANO, A. M., *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores,* Aranzadi, Cizur Menor (Navarra), 2019, pág. 190.

[19] Todas estas sentencias se analizarán más detalladamente en el apartado 4 del trabajo (Sentencias ejemplares: casos y reglas).

[20] GARCÍA SALAS A.I., "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2019", *Revista de Información Laboral*, nº 2, 2018 (versión digital), págs. 1 y ss.

López Ribalda contra España II) dictaminó, que la falta de información previa a los trabajadores estaba justificada por las sospechas fundadas de que se estaban cometiendo irregularidades muy graves (en el mismo sentido que la STC 186/2000, de 10 de julio). El deber de información se configura como un requisito adicional (y no como un criterio independiente) a la hora de examinar si un sistema de videovigilancia cumple el juicio de proporcionalidad. En conclusión, podría decirse que es un requisito necesario, pero no suficiente para examinar si las medidas de control empresarial suponen o no una intromisión en los derechos fundamentales de los trabajadores.

2.4. TIPOLOGÍA Y UBICACIÓN DE LAS CÁMARAS

La instalación de sistemas de videovigilancia empresarial como medida de seguridad y/o control de la actividad laboral está supeditada a ciertos límites, en aras a preservar el derecho a la intimidad de los trabajadores. Por esta razón, no todos los emplazamientos de una empresa pueden ser videovigilados.

En cualquier caso, es obligatorio, en principio, que aquellas áreas de la empresa en las que se vayan a implantar cámaras contengan el preceptivo cartel informativo advirtiendo sobre su presencia.

El artículo 89. 2 de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales dispone 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."* No es posible, por tanto, ubicar sistemas de videovigilancia en lugares privados o áreas en las que no se desarrolla la actividad laboral y que pueda afectar a la intimidad y la imagen de los empleados.

La Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de Videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, puede complementar la normativa laboral, y fija en su artículo 6 los principios de utilización de las videocámaras. El apartado quinto de dicho artículo recoge la prohibición de grabar "…*en los lugares donde se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia.*" Por consiguiente, todo contenido audiovisual obtenido de manera fortuita deberá ser eliminado por el responsable o encargado de tratamiento de datos.

Por norma, no se permite la instalación de cámaras ni en vestuarios ni en taquillas, pero se admite su colocación en sus alrededores, cuando estén orientadas, exclusivamente, a las entradas y salidas de esas áreas. En consecuencia, son nulas y carecen de valor probatorio las grabaciones que registren incumplimientos de los trabajadores obtenidas en zonas privadas.

Cabe la posibilidad de que las cámaras sean de baja resolución y no permitan la identificación de los empleados. En estos casos, lo captado no se considerará como dato personal, sin perjuicio de que las cámaras sean susceptibles de producir injerencias en el derecho a la intimidad de los trabajadores (u otros derechos como el derecho al secreto de las comunicaciones).

Existe gran diversidad de cámaras y no todas conllevan el mismo grado de intromisión en la vida privada de los empleados. La primera distinción se hace entre cámaras analógicas y cámaras digitales[21]. Las cámaras analógicas son las cámaras tradicionales que requieren de cables para la transmisión de los videos a otros soportes (por ejemplo, a DVR). En cambio, las cámaras digitales pueden enviar vídeos, imágenes… sin cable, directamente a la red. Las segundas, por tanto, comportan un mayor riesgo de que se quebrante la seguridad de los datos captados y almacenados.

Por otro lado, están las cámaras fijas y las cámaras orientables o con "zoom", siendo estas últimas las que permiten grabar áreas más extensas de la empresa. Las cámaras con "zoom" requieren mayores cautelas, en la medida que pueden filmar espacios considerados como privados.

No obstante, son las cámaras ocultas las que generan los mayores conflictos, porque chocan directamente con el preceptivo deber de información que tienen los empresarios con sus trabajadores. La finalidad de estas cámaras es captar incumplimientos de los empleados cuando se tienen sospechas fundadas sobre los mismos. Debe ser una medida excepcional y proporcionada, y, en todo caso, es imprescindible la existencia del cartel informativo, aunque no señale la exacta ubicación de la cámara. En estos casos, para evitar conflictos mayores con los empleados, sería útil informar, al menos, a los representantes de los trabajadores[22].

En último lugar se encuentran las cámaras que no graban, es decir, aquellas cámaras que no guardan los datos personales de los trabajadores. Este tipo de sistema solo

[21] BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018, págs. 191 y ss.

[22] Se permite la instalación de cámaras ocultas en casos excepcionales tal y como recoge la STEDH de 17 de octubre de 2019 (Caso López Ribalda contra España II).

reproduce en “tiempo real” lo que está sucediendo en una determinada zona de la empresa. El Informe núm. 0070/2010, del Gabinete Jurídico de la Agencia Española de Protección de Datos dispone que el cartel informativo sigue siendo pertinente en estos casos para “*garantizar el derecho fundamental de protección de datos*”. No obstante, como las datos no son almacenadas en ningún soporte no es necesario informar a acerca de los derechos sobre las imágenes (derechos de acceso, rectificación, supresión…).

La AEPD ha confirmado que este tipo de cámaras, aunque no conservan o archivan los datos personales, con la grabación de imágenes y sonidos es suficiente para que se pueda considerar que tiene lugar un tratamiento de datos y se la aplica igualmente la normativa pertinente.

2.5. MEDIDAS ESPECIALES DE SEGURIDAD

A la hora de visualizar imágenes y sonidos captados por videocámaras es necesario establecer una serie de medidas de seguridad para evitar que terceros tengan acceso a las mismas. El Informe Jurídico núm. 0475/2014 de la Agencia Española de Protección de Datos precisa que son necesarias las medidas de seguridad tanto en el visionado preliminar de las imágenes como en “los posibles accesos posteriores a las grabaciones”. Los responsables o encargados del tratamiento, o sus representantes son los únicos que tienen permitido visionar el contenido de las cámaras y deberán hacerlo en estancias cerradas con códigos de acceso para reforzar la seguridad de los datos personales.

El responsable del tratamiento “*aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario*” (artículo 24.1. del RGPD). Un ejemplo de medida de seguridad es la seudonimización que consiste en tratar los datos personales sin incluir los datos identificativos de los trabajadores[23].

Todo el contenido captado debe transferirse a un fichero que permita su organización e identificación. Se utilizan mecanismos de clasificación que fijan qué datos son considerados como sensibles para aplicarles sistemas de seguridad más específicos.

[23] 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*”, Nueva Revista Española de Derecho del Trabajo*, nº 216, 2019 (versión digital), págs. 1 y ss.

Igualmente, las copias del contenido audiovisual deben conservarse en soportes informáticos seguros o salas cerradas que impidan su sustracción.

Las medidas especiales de seguridad sugieren la realización de copias de seguridad una vez por semana, el establecimiento de procesos de recuperación del material captado en caso de destrucción y la previsión de fallos o ataques cibernéticos que puedan comprometer los datos personales recopilados.

Los procedimientos de seguridad tienen que adaptarse a la tipología de las videocámaras utilizadas, dado que es más fácil acceder a los datos personales contenidos en cámaras digitales, por su transmisión a la red, que en otro tipo de cámaras.

Las imágenes, videos y/o sonidos solo deben conservarse durante el tiempo imprescindible para impedir que la empresa obtenga más datos personales de los necesarios en relación con el fin de tratamiento de datos elegido[24]. No obstante, el artículo 5 e) del RGPD subraya que los datos "…*podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos…".* Dejando a un lado estas excepciones, el RGPD exige la supresión de los datos personales prohibiendo su conservación por más tiempo del necesario.

En este sentido, tanto la LOPDGDD (artículo 22.3) como la Instrucción 1/2006 sobre videovigilancia (artículo 6) disponen que el plazo máximo de conservación de los datos personales será de un mes. Una vez transcurrido este plazo los datos serán suprimidos (no cancelados como establecía la Instrucción 1/2006), es decir, que las imágenes y videos serán eliminados directamente. Si bien, no serán destruidos "*cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones*". En este último caso, serán los organismos públicos los encargados de conservar las grabaciones hasta que tales actos ilícitos prescriban.

2.6. DERECHOS DE LOS TRABAJADORES SOBRE LAS IMÁGENES Y SONIDOS

Los artículos 13 a 18 de la LOPDGDD y los artículos 15 a 22 del RGPD comprenden los derechos que tienen los trabajadores (o interesados) sobre el tratamiento de sus datos personales. En general, los trabajadores tienen derecho de acceso, rectificación,

[24] GOÑI SEIN J. L., *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa,* Bomarzo*,* Albacete, 2018, págs. 77 y ss.

oposición, supresión, limitación del tratamiento y derecho a la portabilidad de los datos personales. Pese a todo, en el ámbito de la videovigilancia no siempre pueden ejercitarse estos derechos y en ocasiones están sometidos a limitaciones.

El derecho de acceso concede al trabajador la posibilidad de pedir información sobre la grabación de sus imágenes y sonidos, y su exhibición. Además, se extiende a otro tipo de información como el origen, la finalidad, los destinatarios, las categorías de datos personales, el plazo de conservación, etc. Es una potestad decisiva para que el trabajador pueda ejercitar otros derechos como el derecho de supresión, rectificación u oposición.

Sin embargo, debido a que durante el acceso al contenido puede resultar complicado aislar las imágenes del interesado de las del resto de empleados, se establecen una serie de herramientas de pixelado que evitan la identificación de terceros[25]. En definitiva, no es un derecho absoluto y se limita en aquellos casos en que su ejercicio pueda vulnerar derechos de otras personas, así como en los casos que "*exista un peligro para la defensa del Estado y la seguridad pública o por la necesidad de la investigación que se está realizando*".

El derecho a la supresión de datos personales se extiende a más circunstancias de las que englobaba el derecho a la cancelación. Está recogido en el artículo 17.1. del RGPD y dispone que "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*

a) *Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;*
b) *El interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;*
c) *El interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;*
d) *Los datos personales hayan sido tratados ilícitamente;*

[25] BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018, págs. 195 y ss.

e) *Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;*
f) *Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información".*

El derecho de cancelación comportaba el bloqueo de datos personales y su entrega a las Administraciones Públicas, el Ministerio Fiscal, Jueces y Tribunales. Aunque este derecho ha sido sustituido por el derecho de supresión (y derecho al olvido) aparece recogido en el artículo 32 de la LOPDGDD bajo la rúbrica "*Bloqueo de los datos*".

Una vez ejercitado por el interesado el derecho de supresión el responsable del tratamiento tiene un plazo máximo de un mes para proceder a la eliminación de los datos personales[26]. No obstante, el empresario debe suprimir los datos personales de oficio en caso de que tales datos "*ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo y cuando hayan sido tratados ilícitamente"* (art. 32.1 apartados a) y d) LOPDGDD).

Cuando no se esté cumpliendo la normativa de protección de datos los trabajadores también tienen derecho a pedir la rectificación de las imágenes[27]. Sin embargo, tanto el derecho de supresión como el de rectificación no tienen cabida en sistemas de videovigilancia de circuito cerrado porque no se archiva el contenido audiovisual.

3. DERECHOS FUNDAMENTALES AFECTADOS POR LA VIDEOVIGILANCIA

Los derechos fundamentales son inherentes a toda persona y conservan su vigencia en las relaciones laborales. En otras palabras, el trabajador mantiene la titularidad sobre estos derechos, aunque se someta al poder de organización y dirección del empresario. Asimismo, los derechos de los trabajadores son modulables, porque coexisten con los intereses y derechos del empleador, quien ostenta la posición de contratante fuerte en la relación laboral[28].

[26] GOÑI SEIN, J. L., *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa,* Bomarzo, Albacete, 2018, págs. 121 y ss.
[27] BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018, págs. 195 y ss.

[28] GARCÍA MURCIA, J., "Derechos fundamentales y contrato de trabajo: algunos puntos críticos*".* Primera Ponencia de la Jornada de estudio *"Derechos fundamentales y contrato de trabajo*", Oviedo, 28 de octubre de 2016.

No se puede hablar de un listado único de derechos fundamentales en el marco de las relaciones laborales, porque existe un catálogo de derechos constitucionales, y diversos catálogos de derechos de la personalidad o de ciudadanía recogidos en textos internacionales.

En relación con la videovigilancia laboral pueden resultar comprometidos diversos derechos, como el derecho a la intimidad, a la propia imagen y a la protección de datos personales, fundamentalmente. En general, son derechos relativos a la esfera privada, a la dignidad y a la libertad de las personas, y por ello merecen especial atención.

La implantación de cámaras en la empresa permite vigilar a los trabajadores a distancia y reproducir tales imágenes y sonidos en cualquier momento. Esto puede traducirse en una intromisión exorbitante en la vida privada de los empleados. Además, existe el riesgo de que el contenido audiovisual pueda compartirse a terceros, vulnerando en mayor medida los derechos fundamentales[29].

Estos derechos colisionan con otro derecho constitucional: la libertad de empresa (artículo 38 de la CE)[30]. Este derecho se manifiesta en las facultades de control y dirección del empresario que le permiten, entre otras cosas, "*adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales*" (art. 20.3. ET).

3.1. EL DERECHO A LA INTIMIDAD

El derecho a la intimidad está reconocido en el artículo 18.1. de la Constitución junto al derecho al honor y el derecho a la propia imagen. Ha sido el Tribunal Constitucional el encargado de delimitar su contenido, si bien, el concepto de intimidad ha ido evolucionando para adaptarse a los cambios tecnológicos y sociales.

La intimidad hace referencia al ámbito privado del trabajador y a la facultad de este para decidir qué información proporciona a terceros (en este caso al empresario) impidiendo que sin su conformidad adquieran tal conocimiento. Es un derecho autónomo y está interconectado o interrelacionado con el derecho a la protección de datos. Engloba las

[29]ARRÚE MENDIZÁBAL M., *El derecho a la propia imagen de los trabajadores*, Aranzadi, Cizur Menor (Navarra), 2019, capítulo IV.

[30] BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018, págs. 37 y ss.

relaciones personales, la salud, las relaciones familiares, creencias religiosas, relaciones afectivas, etc.[31]

En un primer momento, la doctrina constitucional[32] dejó fuera de la esfera de intimidad cualquier hecho que tuviese lugar durante el desarrollo de la actividad laboral o, que estuviese relacionado con la vida profesional. El centro de trabajo formaba parte del ámbito público y, por este motivo, las empresas utilizaban, sin apenas restricciones, sistemas de videovigilancia u otro tipo de tecnologías de control laboral.

Se produce un cambio de criterio a partir de la STC 98/2000, de 10 de abril y la STC 186/2000, de 10 de julio, que reconocen que el centro de trabajo constituye un espacio en el que se ejerce el derecho a la intimidad de los trabajadores. Concretamente la STC 98/2000, de 10 de abril concluye que " *no puede descartarse que también en aquellos lugares de la empresa en los que se desarrolla la actividad laboral puedan 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*". En consecuencia, los trabajadores pueden tener una expectativa razonable de intimidad en el desarrollo de su actividad laboral.

El derecho a la intimidad aparece recogido de manera general en el artículo 4.2. e) y de manera más específica en el artículo 20 bis, del Estatuto de los Trabajadores. Concretamente, el artículo 20 bis establece que "los *trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización*".

Por otro lado, el Estatuto de los Trabajadores no especifica cuáles son los límites a la libertad empresarial, teniendo que acudir a la jurisprudencia para que resuelva los conflictos que surjan entre las facultades empresariales y los derechos fundamentales de los trabajadores. De esta forma, la STC 186/2000[33], de 10 de julio elaboró un "test o juicio de proporcionalidad" que permite comprobar si el control empresarial es legítimo.

---

[31] GOÑI SEIN J.L., "Intimidad del trabajador y poderes de vigilancia y control empresarial*".* Segunda Ponencia de la Jornada de estudio "*Derechos fundamentales y contrato de trabajo*", Oviedo, 28 de octubre de 2016.

[32] Un ejemplo es la STC 142/1993, de 22 de abril.

[33] La STC 186/ 2000, de 10 de julio, versa sobre una empresa que implantó una serie de cámaras en las cajas de cobro para vigilar a sus trabajadores ante sospechas fundadas de que se estaban cometiendo irregularidades y descuadres de caja. Las sospechas fueron confirmadas y la empresa procedió a despedir a los infractores. El tribunal concluyó que la medida utilizada era la única forma de comprobar si se estaban produciendo tales incumplimientos. Cumplía, asimismo, el juicio de idoneidad y era proporcionada porque

Para constatar que los mecanismos de control utilizados por el empresario, como los sistemas de videovigilancia, están justificados, deben cumplirse tres requisitos:

a) "*Si es susceptible de conseguir el objetivo propuesto*". Esta primera condición hace referencia al juicio de idoneidad que examina si la medida de control se ajusta a la finalidad establecida.
b) "*Si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia*". El juicio de necesidad analiza si existen mecanismos menos lesivos con los derechos de los trabajadores. En otras palabras, se busca que la medida de control utilizada sea la única para alcanzar los objetivos propuestos y que, en base al principio de intervención mínima, la vulneración de los derechos fundamentales sea la estrictamente necesaria[34].
c) "*Si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto*". Una vez que se cumplen las condiciones anteriores se realiza el juicio de proporcionalidad para evaluar las ventajas y desventajas de la medida de control.

El test de proporcionalidad se ha convertido en el "canon de enjuiciamiento" de toda aquella medida que conlleve una intromisión ilegítima en los derechos fundamentales de los trabajadores. Las medidas de control empresarial superarán el juicio de proporcionalidad si son adecuadas, necesarias y proporcionadas.

En la misma línea, el *Grupo de Trabajo sobre protección de datos del artículo 29* ha emitido el Dictamen 2/2017 resumiendo una serie de pautas a cumplir por los empresarios:

i) "*Asegurarse que el tratamiento de los datos de sus trabajadores se hace de acuerdo a un propósito legítimo y específico que sea a la vez proporcionado y necesario*
ii) *Tomar en consideración los principios de minimización del tratamiento de los datos personales, de forma que se haga uso de dichos datos de modo adecuado relevante y no excesivo de acuerdo con la finalidad perseguida.*
iii) *Aplicar los principios de proporcionalidad y subsidiariedad.*

se limitó su uso a un corto periodo de tiempo y la cámaras estaban orientadas exclusivamente a la cajas registradoras (solo se podían apreciar las manos de los empleados).

[34] BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018, págs. 39 y ss.

iv) Utilizar procedimientos transparentes en el uso de las nuevas tecnologías.

v) *Permitir a los trabajadores ejercer sus derechos sobre el tratamiento de sus datos personales y mantener dicho tratamiento solo durante el tiempo imprescindible*"

Como reflexión final a este epígrafe es conveniente hacer una precisión acerca de la proporcionalidad y licitud de las medidas de control empresarial. La normativa laboral no excluye la utilización de ningún mecanismo de control, siempre que respete los límites establecidos en art. 20.3 ET. Asimismo, el art. 20 bis ET (introducido por la nueva normativa de protección de datos) hace referencia a los sistemas de videovigilancia y a otros medios de supervisión laboral. Por ello, para determinar si se ha producido una intromisión en los derechos de los trabajadores se debe analizar, en cada caso concreto, si las conductas empresariales son proporcionadas, y no únicamente si los medios son legítimos.

3.2. EL DERECHO A LA PROPIA IMAGEN

El derecho a la propia imagen se regula en el artículo 18.1. CE, junto al derecho a la intimidad y el derecho al honor, pero se configura como un derecho autónomo. El uso de sistemas de videovigilancia por terceros sin el consentimiento del interesado comporta una injerencia ilegítima en el derecho a la propia imagen, conforme a lo dispuesto en el art. 7.5 de Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El Tribunal Constitucional, en la Sentencia 156/2001, de 2 de julio, delimita el contenido propio y específico del derecho a la propia imagen separado del derecho a la intimidad y el derecho al honor. En concreto, determina que "*mediante la captación y reproducción gráfica de una determinada imagen de una persona se puede vulnerar su derecho a la intimidad sin lesionar el derecho a la propia imagen, lo que sucederá en los casos en los que mediante las mismas se invada la intimidad pero la persona afectada no resulte identificada a través de sus rasgos físicos; en segundo lugar, también puede vulnerarse el derecho a la propia imagen sin conculcar el derecho a la intimidad, supuesto éste que se producirá cuando las imágenes permitan la identificación de la persona fotografiada, pero no entrañen una intromisión en su intimidad; y, finalmente, puede suceder que una imagen lesione al mismo tiempo ambos derechos, lo que ocurriría en los casos en los que revele la intimidad personal y familiar y permita identificar a la persona fotografiada*".

Se define como un derecho de la personalidad que permite decidir sobre la imagen propia tanto en espacios privados como públicos, incluyéndose, por tanto, el ámbito laboral. No es un derecho absoluto y, por ello, el consentimiento de los trabajadores

para la captación y utilización de imágenes por parte del empresario podría resultar irrelevante[35].

No tiene un normativa propia en el ámbito laboral, pero el Estatuto de los Trabajadores hace referencia indirecta al mismo en diversos preceptos (art. 4.2 e), art 20, art 20 bis). La ausencia de desarrollo legal dificulta su protección como derecho fundamental y entraña un mayor desequilibrio entre los poderes empresariales y los derechos de los trabajadores[36].

Como regla general, el trabajador tiene el deber de cumplir las órdenes e instrucciones del empresario en el ejercicio de sus facultades (artículo 5. c) ET). No obstante, el trabajador puede desobedecer las órdenes que sean manifiestamente contrarias a derechos fundamentales irrenunciables (como el derecho a la propia imagen) o impropias a la relación laboral (STC 99/1994, de 11 de abril).

En todo caso, es la jurisprudencia la encargada de ponderar los intereses empresariales y los derechos fundamentales de los trabajadores para dar una solución adaptada a cada supuesto. Los tribunales deben comprobar si se lesionó el derecho a la propia imagen a través de las condiciones del juicio de proporcionalidad, al igual que se hacía con el derecho a la intimidad. En definitiva, la medida de control empresarial (sistema de videovigilancia) debe ser idónea, necesaria y proporcionada.

3.3. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

El derecho a la protección de datos personales, también denominado derecho a la privacidad[37], viene reflejado en el artículo 18.4 de la Constitución, reconocido por el Tribunal Constitucional en la Sentencia 94/1998, de 4 de mayo. Está estrechamente vinculado con el derecho a la intimidad, pero comprende un derecho más amplio y genérico que este último y se configura como un derecho autónomo.

El derecho a la privacidad abarca la protección de los datos íntimos de la persona, así como, la facultad *para "consentir la recogida, obtención y acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero"* (STC 292/200, de 30 de noviembre). Por datos personales, se entiende todo tipo de datos, sean privados o no. En general, son datos que identifican o permiten

[35]ARRÚE MENDIZÁBAL M., *El derecho a la propia imagen de los trabajadores*, Aranzadi, Cizur Menor (Navarra), 2019, capítulo IV.

[36] CRISTOBAL RONCERO R., "Protección del derecho a la propia imagen en el trabajo*", Nueva Revista Española de Derecho del Trabajo*, nº 199, 2017 (versión digital), págs. 1 y ss.

[37] GOÑI SEIN J.L., "Intimidad del trabajador y poderes de vigilancia y control empresarial". Segunda Ponencia de la Jornada de estudio "*Derechos fundamentales y contrato de trabajo*", Oviedo, 28 de octubre de 2016.

identificar a una persona y merecen una especial protección para evitar que sean utilizados con finalidades distintas a las permitidas y afecten a otros derechos y libertades[38].

De igual forma que el derecho a la intimidad, al honor y a la propia imagen, el derecho a la protección de datos personales no es un derecho absoluto y puede colisionar con el control empresarial. Además, es muy común en la práctica que una misma circunstancia pueda llevar a la lesión de varios derechos fundamentales.

En relación con su tratamiento jurisprudencial se produce un cambio de criterio con la STC 29/2013, del 11 de febrero. El tribunal argumentó que se vulneró el art. 18.4 CE (derecho a la protección de datos) y no el art 18.1 CE (derecho a la intimidad), porque el núcleo esencial de este precepto es "*el derecho del afectado a ser informado de quién posee los datos personales y con qué fin*". El derecho a la protección de datos se presenta, por tanto, como el más idóneo y el que tiene un ámbito de protección más amplio.

No obstante, a diferencia de lo que ocurre en la STC 186/2000, de 10 de julio, el Tribunal no comprueba, mediante el juicio de proporcionalidad, si la medida de control es adecuada, idónea y equilibrada.

Por el contrario, en la Sentencia 39/2016, de 3 de marzo, el Tribunal Constitucional si examinó las tres condiciones del juicio de proporcionalidad y concluyó que la medida era idónea para el objetivo o finalidad propuesta, estaba justificada porque existían sospechas de irregularidades y, era proporcionada porque se empleó durante un plazo de tiempo razonable, limitándose exclusivamente a la zona donde se produjeron las infracciones.

En principio, es fundamental que la finalidad del medio de control sea la misma durante todo el tratamiento de los datos personales. Por consiguiente, si la finalidad de la instalación de las cámaras es la seguridad del establecimiento mercantil, no debería aprovecharse para controlar el desarrollo de la actividad laboral de los trabajadores (finalidad posterior). Esta condición no es absoluta, y tanto el TC como la Organización Internacional del Trabajo (OIT)[39] han admitido que se flexibilice en aquellos casos donde no sea posible utilizar otros mecanismos para vigilar a los trabajadores. Esta

[38] BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018, págs. 38 y ss.
[39] Repertorio de Recomendaciones Prácticas de la OIT, de octubre de 1996, sobre protección de los datos personales de los trabajadores.

misma solución se extiende a los casos en que el empresario averigua, de manera accidental, incumplimientos por parte de los trabajadores[40].

La normativa de protección de datos recomienda, no obstante, que las empresas informen sobre las distintas finalidades de los medios empleados. No es preceptivo, pero facilita la protección de derechos fundamentales y la utilización de las grabaciones como prueba.

Para finalizar con el estudio del derecho a la protección de datos se presentan dos sentencias recientes sobre videovigilancia oculta: la STEDH de 9 de enero de 2018 (Caso López Ribalda y otros vs. España) y la STEDH de 17 de octubre de 2019 (Caso López Ribalda contra España II).

En un primer momento, el TEDH estimó que las medios adoptados por el empresario no fueron proporcionales y, por tanto, las pruebas audiovisuales aportadas fueron consideradas nulas.

Posteriormente, la Gran Sala cambia de criterio en la STEDH de 17 de octubre de 2019 (*Caso López Ribalda contra España II)* y comparte la decisión adoptada por los Tribunales españoles*.* Para ello, trae a colación el Test Barbulescu que consiste en una serie de requisitos mínimos que tienen que tener en cuenta los tribunales nacionales a la hora de valorar los derechos en conflicto. Teniendo en cuenta tanto los criterios utilizados por los tribunales españoles como los requisitos del Test Barbulescu (que son muy parecidos), la Sala concluyó que el sistema de videovigilancia era idóneo, necesario y proporcionado; no apreciando la vulneración del art. 8 CEDH[41].

3.4. OTROS DERECHOS EN CONFLICTO

En el artículo 18.3 CE se reconoce el derecho al secreto de las comunicaciones y, aunque también está vinculado al derecho al honor, a la intimidad y a la propia imagen. es un derecho independiente. Su propósito es proteger la libertad de las comunicaciones frente a terceros, es decir, evitar que otras personas intercepten datos personales no consentidos.

---

[40] BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018, págs. 44 y ss.

[41] Artículo 8.- Derecho al respeto a la vida privada y familiar.

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."

Se plantea la vulneración de este derecho cuando en los sistemas de videovigilancia se incorporan mecanismos de escucha y grabación de sonidos y que permiten a la empresa archivar tales conversaciones (STC 98/2000, de 10 de abril). En definitiva, se aplica cuando se utilizan sistemas de videovigilancia de circuito cerrado (o cualquier medio de circuito cerrado) que permiten el control microfónico y cuando las comunicaciones objeto de protección se realizan a distancia.

La disposición constitucional solo hace referencia al secreto de comunicaciones vía "*postales, telegráficas y telefónicas*". No obstante, se interpreta como un numerus apertus de modalidades entre las que se incluye el correo electrónico, videoconferencias, servicios de mensajería interna de la empresa, etc. Por otro lado, las comunicaciones que tienen lugar en canales abiertos como la televisión no estarían protegidas bajo el derecho al secreto de las comunicaciones[42].

Es aconsejable que las empresas elaboren una guía de buenas prácticas en la que se detallen los mecanismos de comunicación empresariales y así prevenir la lesión del derecho al secreto de las comunicaciones, o cualquier otro derecho. En relación con la instalación de sistemas de videovigilancia se recomienda que no graben sonidos para no vulnerar este derecho.

En la práctica, sin embargo, las imágenes y sonidos captados por sistemas de videovigilancia empresarial se conciben como datos personales amparados por el derecho a la intimidad (art. 18.1 CE) y/o el derecho a la protección de datos personales (art. 18.4 CE).

4. SENTENCIAS EJEMPLARES: CASOS Y REGLAS

- *STC 186/2000, de 10 de julio*

El Tribunal Constitucional examinó la implantación de un sistema de videocámaras en los cajeros de un establecimiento comercial ante la sospecha fundada de que se estaban produciendo descuadres contables. Las grabaciones constataron la comisión de actos ilícitos por parte de uno de los trabajadores lo que se tradujo en su despido inmediato. El trabajador acude al Tribunal Constitucional alegando, entre otras cosas, que la instalación del sistema de videovigilancia no fue notificada ni a los trabajadores ni al Comité de empresa, conforme a lo exigido en el Estatuto de los Trabajadores.

[42]ARRÚE MENDIZÁBAL M., *El derecho a la propia imagen de los trabajadores*, Aranzadi, Cizur Menor (Navarra), 2019, capítulo IV.

El TC estimó que la comunicación al Comité de Empresa y a los trabajadores era una "mera legalidad ordinaria que carecía de trascendencia". Asimismo, consideró que prevalecían las facultades de control del empresario sobre el derecho a la información de los trabajadores porque, en caso contrario, no hubiera sido posible descubrir al trabajador cometiendo tales infracciones[43]. En otras palabras, el Tribunal una vez analizado que el sistema de control utilizado cumplía con los estándares del *test de proporcionalidad* (era necesario, proporcionado e idóneo), concluyó que era la única manera de comprobar el carácter ilegal del comportamiento del empleado.

En este sentido correspondía a los tribunales determinar, en cada caso concreto, si era más relevante el objeto perseguido o los derechos de los trabajadores.

- *STC 29/2013, de 11 de febrero*

En esta sentencia se produjo un cambio de orientación de la jurisprudencia. El tribunal resolvió un supuesto en el que, un sistema de cámaras de videovigilancia instaladas en los accesos de la Universidad de Sevilla grabó a un empleado incumpliendo su jornada laboral. Las imágenes captadas confirmaron las sospechas y se sancionó al trabajador con una suspensión de empleo y sueldo. La Universidad de Sevilla no informó previamente al trabajador, provocando su desconocimiento acerca de la finalidad y utilidad de las videocámaras (más allá de como medida de seguridad).

Para la anterior STC 186/2000, de 10 de julio, el derecho de información era una "mera cuestión de legalidad ordinaria", pasando a convertirse en un factor esencial del contenido del derecho fundamental del art 18.4 CE[44]. De esta manera, el tribunal recoge que "*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 … Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin*."

De igual modo, establece que no será suficiente con la implantación de carteles distintivos de zona videovigilada (información general), sino que será preciso que se proporcione al trabajador una información "*previa y expresa, precisa, clara e inequívoca*

[43] TALÉNS VISCONTI E.E., "Vídeo-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros", *Revista Internacional y Comparada de relaciones laborales y derecho del empleo*, Volumen 6, nº 3, 2018, págs. 3 y ss.

[44] ALTÉS TARREGA J.A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la SETDH López Ribalda (II)", *Revista General del Derecho del Trabajo y de la Seguridad Social*, nº 55, 2020, págs. 328 y ss.

sobre la finalidad de control de la actividad laboral ". Recalca, por tanto, la exigencia de la preceptiva información y alienta a que la finalidad de tratamiento sea lícita y adecuada.

Lo característico de esta resolución es que el tribunal se pronuncia de manera opuesta a la doctrina anterior (STC 186/2000, de 10 de julio). No solo pasa a considerar el derecho a la protección de datos personales como el derecho afectado, sino que tampoco examina si la medida de control empresarial resulta proporcionada (juicio de proporcionalidad).

La sentencia concluyó que se había vulnerado el derecho fundamental del art 18.4 CE y, consiguientemente, declaró nulas las sanciones que se le impusieron al recurrente. Dispone, no obstante, de un voto particular que reprocha que no se hubiese contemplado a la hora de resolver, el juicio de proporcionalidad ni las facultades de control del empresario[45].

- *STC 39/2016, de 3 de marzo*

El Tribunal rectifica con esta sentencia la doctrina anterior (STC 29/2013, de 11 de febrero). Se presenta, nuevamente, un supuesto de despido fundado en imágenes extraídas de un sistema de videocámaras instalado en la cajas registradoras de un local comercial. El establecimiento de las cámaras se hizo sin comunicación previa a los trabajadores, aunque si existían carteles informativos de zona videovigilada. En las imágenes captadas se comprobó que el trabajador se apoderaba del dinero de la caja durante su actividad laboral y se procedió a su despido.

El TC resuelve de manera contraria a la doctrina anterior, considerando el deber de información previa como un requisito puramente formal (no esencial). Por ende, señala que el deber de información (previa) se cumple con los carteles informativos ubicados en la empresa, de acuerdo a lo establecido en la Instrucción 1/2006 de la AEPD y no se estaría vulnerando, por tanto, el derecho fundamental del artículo 18.4. CE (protección de datos personales). Del mismo modo, el sistema de videovigilancia se ajusta al juicio de proporcionalidad y al derecho a la intimidad de los trabajadores (art. 18.1 CE) por lo que el despido es procedente[46].

[45] La citada sentencia no logró unificar criterios en los restantes tribunales ordinarios. De este modo, las sentencias del TSJ de Cataluña de 25 de junio de 2014, (rec. 2007/2014) y del TSJ de Cataluña de 24 de noviembre de 2014, (rec. 4131/2014) optaron por seguir la línea de la STC 186/2000, de 10 de julio. Por el contrario, las sentencias del TSJ de Asturias de 23 de mayo de 2014, (rec. 797/2014), del TSJ del País Vasco de 18 de junio de 2013 (rec. 1039/2013) y STS de 13 de mayo de 2014, (rec. 1685/2012) adoptaron la doctrina posterior (STC 29/2013, de 11 de febrero).

[46] ALTÉS TARREGA J.A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la SETDH López Ribalda (II)", *Revista General del Derecho del Trabajo y de la Seguridad Social*, nº 55, 2020, págs. 328 y ss.

El giro jurisprudencial generó dos votos particulares reprochando la falta de consistencia del cambio de criterios. El primer voto argumentaba que no se podía reducir libremente el contenido fundamental del derecho a la protección de datos personales en relación con el deber de información. Mientras que, el segundo magistrado disidente destacó, que no era equiparable el "hallazgo casual de una infracción" mediante el uso de sistemas de videovigilancia, y la colocación de estos sistemas ante una sospecha de que se están produciendo incumplimientos.

- Las SSTEDH en el caso López Ribalda I y II[47]

La STEDH de 9 de enero de 2018 (Caso López Ribalda contra España I) resuelve un supuesto de videovigilancia oculta en un supermercado. La empresa sospechaba que se estaban produciendo disparidades entre las ventas y el nivel de stock que tenía el supermercado y, por ello, instaló varias cámaras, unas ocultas y otras visibles. La empresa únicamente informó a los trabajadores de las cámaras que eran visibles.

El sistema de videocámaras captó a trabajadores y clientes hurtando determinados artículos del supermercado, corroborando así, las sospechas de la empresa. En consecuencia, se utilizaron esas imágenes para fundamentar los despidos alegando "*transgresión de la buena fe contractual y abuso de confianza (art 54.2 ET)".*

La jurisdicción ordinaria resolvió el asunto en la misma línea que la STC 186/2000, de 10 de julio (anteriormente analizada), y, finalmente, la cuestión se llevó hasta el Tribunal Europeo de Derechos Humanos (TEDH).

El argumento central de los trabajadores despedidos se basa en la inobservancia del artículo 8 de la Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en adelante CEDH)[48].

El TEDH reconoce que los sistemas de cámaras ocultos suponen una intrusión en la vida privada de los trabajadores y lo compara con la STEDH de 5 de octubre de 2010 (*Caso Köpke*). La principal diferencia con el *Caso Köpke* es que en el presente caso existía una legislación nacional que contaba con previsiones sobre protección de datos: concretamente, sobre la obligación del empresario de informar a los trabajadores sobre el tratamiento y finalidad de la recogida de datos (art. 5 LOPD 1999 y el art. 3 de la Instrucción 1/2006 de la AEPD), que se incumplió.

[47] GARCÍA SALAS A.I., "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2019", *Revista de Información Laboral*, nº 2, 2018 (versión digital), págs. 1 y ss.

[48] Artículo 8.1. del CEDH. Derecho al respeto a la vida privada y familiar. "*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*"

Asimismo, consideró que los tribunales españoles no ponderaron de forma correcta los intereses empresariales y los derechos de los trabajadores, vulnerando el art. 8 CEDH. En este sentido, el Tribunal entendió que la videovigilancia oculta no se dirigió específicamente a aquellos trabajadores de los que se sospechaba, sino que se extendió a todos los empleados que trabajaban en la caja sin límite temporal y durante toda la jornada laboral; dando la razón a los trabajadores.

El Estado español recurre la STEDH de 9 de enero 2018 (Caso López Ribalda contra España I) ante la Gran Sala, que, inesperadamente, rectifica su postura. La STEDH de 17 de octubre de 2019 (Caso López Ribalda contra España II) dictaminó que se cumplía el test de proporcionalidad, que no existía vulneración del art. 8 del CEDH y que, por tanto, la utilización de cámaras ocultas se ajustaba a derecho.

El Tribunal toma como base la STEDH de 5 de septiembre de 2017 (Caso Barbulescu vs Rumanía II) que elaboró un *Test* acerca de las "expectativas de privacidad" de los empleados en el ámbito de control del correo electrónico (pero se extiende, también, a la videovigilancia)[49].

El *Test* establecía que áreas de la empresa tenían una mayor y menor "expectativa de privacidad" para los trabajadores, y reglas sobre la información previa, medidas alternativas, garantías, etc. los parámetros de proporcionalidad que venían utilizando los Tribunales españoles son muy parecidos al Test de Barbulescu.

[49] Estas seis condiciones son:

"(*i) Si el trabajador ha sido informado de la posibilidad de que el empleador adopte medidas de vídeo vigilancia y del implementación de tales medidas. Si bien en la práctica los trabajadores pueden ser informados de varias maneras, dependiendo de las circunstancias fácticas particulares de cada caso, la notificación normalmente debe ser clara sobre la naturaleza del vídeo vigilancia y debe darse anterior a su aplicación.*

(ii) El alcance de la vídeo vigilancia por parte del empleador y el grado de intrusión en la privacidad del empleado. En este sentido, se debe tener en cuenta el nivel de privacidad en el área que se está vigilando, junto con las limitaciones de tiempo y espacio y la cantidad de personas que tienen acceso a los resultados.

(iii) Si el empleador ha proporcionado razones legítimas para justificar la vídeo vigilancia y el alcance de la misma. Cuanto más intrusivo sea la vídeo vigilancia, mayor será la justificación que se requerirá.

(iv) Si hubiera sido posible establecer un sistema de vídeo vigilancia basado en métodos y medidas menos intrusivos. A este respecto, debe haber una evaluación a la luz de las circunstancias particulares de cada caso en cuanto a si el objetivo perseguido por el empleador podría haberse logrado a través de un menor grado de interferencia con la privacidad del empleado.

(v) Las consecuencias de la vídeo vigilancia para el trabajador sujeto a él. Debe tenerse en cuenta, en particular, el uso que hace el empleador de los resultados de la supervisión y si dichos resultados se han utilizado para lograr el objetivo declarado de la medida.

(vi) Si el trabajador ha recibido las garantías apropiadas, especialmente cuando las operaciones vídeo vigilancia del empleador son de naturaleza intrusiva. Dichas garantías pueden tomar la forma, entre otras, de proporcionar información a los empleados interesados o a los representantes del personal en cuanto a la instalación y el alcance de la vídeo vigilancia, o una declaración de tal medida a un organismo independiente o la posibilidad de presentar una queja".

La Sala consideró (siguiendo la doctrina de la STC 186/2000, de 10 de julio) que la falta de información previa a los trabajadores acerca de las cámaras no visibles estaba justificada por las sospechas fundadas de que se estaban cometiendo irregularidades graves en las cajas y no existían medios menos lesivos para comprobarlo. En este sentido, el tribunal mantiene que la información previa es necesaria, pero sería modulable en función de las circunstancias en las que nos encontremos. No obstante, recalca que la utilización de cámaras ocultas solo será válida cuando se dan estas condiciones y no otras (no siendo válida su utilización ante mínimas sospechas).

El Tribunal valoró, asimismo, la escasa duración del sistema de videocámaras (solo grabaron durante 10 días), su suspensión una vez identificados a los infractores, la pertinencia del medio utilizado y el limitado número de personas que tuvieron acceso al contenido audiovisual.

En conclusión, esta nueva resolución abre la posibilidad de utilizar cámaras ocultas en circunstancias excepcionales y establece que la inobservancia de la normativa de protección de datos es, por sí misma, insuficiente para determinar que el uso de sistemas de videovigilancia conculcan los derechos fundamentales.

CONCLUSIONES

La realidad siempre va dos pasos por delante del Derecho y los nuevos sistemas de videovigilancia laboral son un ejemplo de ello. Es de vital importancia, por tanto, que las leyes se modernicen para adaptarse a todo tipo de cambios, especialmente a los cambios tecnológicos.

En respuesta a los nuevos desafíos de la “Era digital” se aprobó el Reglamento Europeo 2016/679, de protección de datos y, para adaptarse al mismo, se promulgó a nivel nacional la Ley Orgánica 3/2018. En general, dieron respuesta a muchas lagunas jurídicas que existían hasta entonces, pero el ámbito laboral no ha tenido la misma suerte.

Una de las principales dificultades en la práctica es preservar los derechos fundamentales de los trabajadores (art. 18 CE) sin olvidar las facultades de dirección y control que ostenta el empresario (art. 20.3 ET). Las nuevas tecnologías han permitido a la empresa incrementar su poder empresarial y han desdibujado la línea de separación entre la vida privada y la vida laboral de los trabajadores. En este escenario, el derecho a la protección de datos es fundamental para proteger la esfera íntima de los empleados en el ámbito laboral.

La ausencia de una legislación específica en materia laboral ha sido cubierta, en cierto modo, por los Tribunales. Entre sus aportaciones destaca el "juicio o test de proporcionalidad" que permite valorar cuando una medida de vigilancia empresarial es idónea, necesaria y equilibrada. Han determinado, también, que no es necesario el consentimiento del trabajador para el tratamiento de sus datos, salvo excepciones. No obstante, en mi opinión, no han sabido establecer unas pautas claras acerca del deber de información previa del empresario sobre el tratamiento de datos personales de sus empleados.

El deber de información representa el núcleo central del derecho a la protección de datos personales y su omisión imposibilita al trabajador para el ejercicio de otros derechos (derecho de acceso, derecho de supresión de datos, etc.). En general, la doctrina actual entiende que la obligación se cumple mediante la colocación de carteles informativos visibles de "*zona videovigilada*", sin necesidad de que exista una "*información previa, precisa y clara" (*artículo 89.1. LOPDGDD). Tampoco es obligatorio informar a los representantes de los trabajadores, aunque sí es recomendable.

Los Tribunales han permitido, asimismo, la validez de cámaras ocultas cuando existan sospechas razonables de que se están produciendo incumplimientos graves por parte de los trabajadores y no existan medios menos lesivos. De esta forma, cabe la posibilidad de omitir el deber de información en casos excepcionales.

En definitiva, el deber de información se configura como un criterio complementario a la proporcionalidad de la medida de control y pasa a un segundo plano. Esto se traduce en una mayor protección de los intereses empresariales en detrimento de los derechos de los trabajadores.

Resulta paradójica la importancia que da la legislación europea a la necesidad de una legislación en materia laboral específica para cada Estado, en contraposición con la escasa trascendencia que ha tenido en la práctica. En consecuencia, las lagunas legales han generado mucha inseguridad jurídica.

Desde mi punto de vista, la legislación debería incorporar las pautas establecidas por los tribunales o, bien, otras más precisas, para lograr un equilibrio razonable entre los derechos de los trabajadores y del empresario. Una buena forma de garantizar ambos intereses podría ser convirtiendo en obligatorio la colaboración entre el empresario y los representantes de los trabajadores a la hora de establecer medios de control laboral.

BIBLIOGRAFÍA

1. MONOGRAFÍAS

ARRÚE MENDIZÁBAL M., *El derecho a la propia imagen de los trabajadores,* Aranzadi, Cizur Menor (Navarra), 2019.

BLÁZQUEZ AGUDO E.M., *Aplicación práctica de la protección de datos en las relaciones laborales,* CISS-Wolters Kluwer, Madrid, 2018.

GOÑI SEIN J.L., *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa,* Bomarzo, Albacete, 2018.

ORELLANA CANO A.M., *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores,* Aranzadi, Cizur Menor (Navarra), 2019.

2. ARTÍCULOS

ALTÉS TARREGA J.A., "La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la SETDH López Ribalda (II)", *Revista General del Derecho del Trabajo y de la Seguridad Social*, nº 55, 2020.

CRISTOBAL RONCERO R., "Protección del derecho a la propia imagen en el trabajo", *Nueva Revista Española de Derecho del Trabajo*, nº 199, 2017 (versión digital).

GARCÍA MURCIA, J., "Derechos fundamentales y contrato de trabajo: algunos puntos críticos". Primera Ponencia de la Jornada de estudio *"Derechos fundamentales y contrato de trabajo*", Oviedo, 28 de octubre de 2016.

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", *Nueva Revista Española de Derecho del Trabajo*, nº 216, 2019, (versión digital).

GARCÍA SALAS A.I., "El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2019", *Revista de Información Laboral*, nº 2, 2018 (versión digital).

GOÑI SEIN J.L., "Intimidad del trabajador y poderes de vigilancia y control empresarial". Segunda Ponencia de la Jornada de estudio *"Derechos fundamentales y contrato de trabajo"*, Oviedo, 28 de octubre de 2016.

TALÉNS VISCONTI E.E., "Vídeo-vigilancia y protección de datos en el ámbito laboral: una sucesión de desencuentros", *Revista Internacional y Comparada de relaciones laborales y derecho del empleo*, Volumen 6, nº 3, 2018 (versión digital).

3. PÁGINAS WEB CONSULTADAS

Agencia Española de Protección de Datos, Informe Jurídico núm. 0006/2009. Disponible en: https://www.aepd.es/es/documento/2009-0006.pdf (Fecha de consulta: 3 de junio de 2020)

Agencia Española de Protección de Datos, Informe Jurídico núm. 0070/2010. Disponible en: www.electrovision.es › app › download › 2010-0070 ... (Fecha de consulta: 14 de abril de 2020)

Agencia Española de Protección de Datos, Informe Jurídico núm. 0475/2014. Disponible en: https://www.aepd.es/es/documento/2014-0475.pdf (Fecha de consulta: 15 de abril de 2020)

Agencia Española de Protección de Datos, Informe jurídico núm. 497/2007. Disponible en: https://www.aepd.es/es/documento/2007-0497.pdf (Fecha de consulta: 27 de mayo de 2020)

Guías Jurídicas Wolters Kluwer: "Tratamiento de Datos con fines de videovigilancia". Disponible en: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkNjSxMLE7Wy1KLizPw8WyMDQwtDIwOwQGZapUt-ckhlQaptWmJOcSoApCkmQzUAAAA=WKE (Fecha de consulta: 6 de junio de 2020)

Guía sobre el uso de videocámaras para seguridad y otras finalidades de la AEPD. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-videovigilancia.pdf (Fecha de consulta: 1 de junio de 2020)

Grupo de Trabajo sobre protección de datos del artículo 29, Dictamen 4/2004, de 11 de febrero. Disponible en: https://www.apda.ad/sites/default/files/2018-10/wp89_es.pdf (Fecha de consulta: 3 de junio de 2020)

Noticias jurídicas: "Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras". Disponible en: http://noticias.juridicas.com/base_datos/Admin/i1-2006-apd.html (Fecha de consulta: 16 de abril de 2020).

Noticias jurídicas: "El TC aclara su doctrina en relación con el uso de cámaras de videovigilancia en la empresa". Disponible en: http://noticias.juridicas.com/actualidad/jurisprudencia/10962-el-tc-aclara-su-doctrina-

en-relacion-con-el-uso-de-camaras-de-videovigilancia-en-la-empresa/ (Fecha de consulta: 12 de junio de 2020)

Recomendaciones Prácticas de la OIT, de octubre de 1996, sobre protección de los datos personales de los trabajadores. Disponible en: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf (Fecha de consulta: 6 de junio de 2020)