Intimidad y protección de datos como derechos vertebradores en el uso de dispositivos de videovigilancia en el lugar de trabajo

Francisco A. González Díaz

Catedrático de Derecho del Trabajo y de la Seguridad Social.
Universidad de Murcia

Extracto

En la relación laboral es innegable la tensión conceptual entre privacidad y seguridad, lo que justifica que el presente trabajo analice el contexto jurídico en el que una empresa debe implantar los sistemas de videovigilancia de modo que se respeten los derechos a la intimidad y protección de datos de la persona trabajadora. En este contexto resulta fundamental aterrizar en los preceptos de la Constitución española, el Estatuto de los Trabajadores y la Ley orgánica de protección de datos y garantía de derechos digitales que tienen impacto y pueden amparar la videovigilancia encubierta como sistema específico de control de la actividad laboral.

Igualmente, y sobre todo teniendo en cuenta la disparidad –y evolución– de criterios judiciales sobre la materia, se analiza la doctrina del Tribunal Constitucional, Tribunal Supremo y Tribunal Europeo de Derechos Humanos en supuestos de videovigilancia encubierta. El estudio de la doctrina sentada por estos tribunales nos lleva a elaborar unas conclusiones que se enmarcan en legitimar el tratamiento de datos de la persona trabajadora como búsqueda de una mejora y eficiencia empresarial alejándose de un método de control injustificado e intrusivo en la vida privada de dicha persona.

Palabras clave: videovigilancia; intimidad; protección de datos; consentimiento; información.

Fecha de entrada: 17-06-2020 / Fecha de revisión: 15-07-2020 / Fecha de aceptación: 16-07-2020

Cómo citar: González Díaz, Francisco A. (2020). Intimidad y protección de datos como derechos vertebradores en el uso de dispositivos de videovigilancia en el lugar de trabajo. *Revista de Trabajo y Seguridad Social. CEF*, *451*, 149-184.

Privacy and data protection as fundamental rights in the use of surveillance systems in the workplace

Francisco A. González Díaz

Abstract

In labor relations, the conceptual tension between privacy and security is undeniable. That is why this work analyzes the legal context in which an employer must implement video surveillance systems in the company in a way that the rights to privacy and protection of worker data are guaranteed. In this context, it is essential to take into account the precepts of the Spanish Constitution, the Statute of Workers and the Organic Law on Data Protection and Guarantee of Digital Rights. All of them have an impact and can protect covert video surveillance as a specific system of control of labor activity.

Likewise, and especially taking into account the disparity –and evolution– of judicial criteria on the matter, the doctrine of the Constitutional Court, Supreme Court and European Court of Human Rights is analyzed in cases of covert video surveillance. The study of the doctrine established by these courts leads us to draw up conclusions that are framed in legitimizing the treatment of worker data as a search for business improvement and efficiency, staying away from an unjustified and intrusive method of control in the worker's private life.

Keywords: video surveillance; privacy; data protection; consent; information.

Citation: González Díaz, Francisco A. (2020). Privacy and data protection as fundamental rights in the use of surveillance systems in the workplace. *Revista de Trabajo y Seguridad Social. CEF, 451*, 149-184.

Sumario

Nota: estudio realizado en el marco del proyecto de investigación 20976/PI/18 titulado «El impacto de la Industria 4.0 en el trabajo: una visión interdisciplinar», financiado por la Fundación Séneca (Agencia de Ciencia y Tecnología de la Región de Murcia).

1. Introducción

Es bien conocido que la irrupción exponencial de sistemas de vigilancia en lugares públicos ha condicionado el comportamiento de la ciudadanía en estos espacios. Del mismo modo, una vigilancia de las personas trabajadoras modifica actitudes tan saludables como son las derivadas del ejercicio de sus derechos fundamentales (por ejemplo, reunión); presionando coercitivamente sobre los comportamientos de las personas trabajadoras y dificultando la detección de conductas empresariales anómalas. Sistemas de videovigilancia cada vez más frecuentes en el contexto de la relación laboral fruto del aumento de nuevas tecnologías que junto al bajo coste de su implementación han llevado a un nuevo escenario en el ejercicio del poder empresarial de vigilancia y control (art. 20 Estatuto de los Trabajadores –ET–) y a un marco en donde los riesgos de desprotección de las relaciones laborales crecen a medida que las nuevas tecnologías de la información y comunicación se apoderan de todas las facetas de nuestra vida (Molina Navarrete, 2018, p. 125).

De hecho, las nuevas tecnologías y los nuevos modelos de organización de la empresa, en opinión de Molina Navarrete y Olarte Encabo (1999):

> […] amplían extraordinariamente las diferentes prerrogativas empresariales de dirección y reintroducen el principio de autoridad en las relaciones laborales, por lo que la tutela o protección de los derechos de la persona del trabajador, en particular los derechos de libertad, privacidad y dignidad adquieren una renovada actualidad (p. 359),

en tanto que, no puede negarse el interés de la empresa en realizar un control de la utilización de las nuevas tecnologías por parte de las personas empleadas (Fernández Villazón, 2003, p. 136).

Sin embargo, este nuevo contexto obliga a que la empresa que opte por sistemas de videovigilancia configure una política de control de datos de manera que las personas trabajadoras puedan ser conscientes de la existencia y las consecuencias del control desarrollado, ya que este tipo de control presenta una muy intensa capacidad invasiva de la persona trabajadora con clara posibilidad de intromisión en su vertiente personal (Cruz Villalón, 2019, p. 16).

En este contexto, la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), tiene como eje común la

protección de las personas físicas dentro del marco constitucional en cuestiones relacionadas con el tratamiento de datos donde el propio artículo 18.4 de la Constitución española (CE) reconoce que la «ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos».

Reconocimiento que ha llevado al Tribunal Constitucional (TC) a señalar que la llamada libertad informática supone el derecho a controlar el uso de los datos insertos en un programa informático y alcanza la oposición de la ciudadanía a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención[1]. Por tanto, es necesario proteger los derechos de las personas frente al uso ilegítimo de la informática (Fernández Villazón, 1996).

Por ello, un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, no incluya garantías adecuadas frente a su uso potencialmente invasor de la vida privada de la ciudadanía vulneraría el derecho a la intimidad[2]. De modo que, el uso de datos suministrados a través de medios informatizados más allá de lo legalmente autorizado constituiría un grave atentado a los derechos fundamentales de la persona[3].

Todo lo anterior justifica que el artículo 18.4 de la CE no solo se ensalza como instrumento de protección de los derechos de la ciudadanía frente al uso malintencionado de la tecnología informática, sino que consagra un derecho fundamental que se traduce en el control de flujos de informaciones que conciernen a cada persona, tratando de evitar que la informatización-automatización de los datos personales ampare comportamientos discriminatorios[4].

Con base en lo anterior, el objeto de protección del derecho fundamental a la protección de datos no abarca, exclusivamente, datos íntimos de la persona, sino cualquier tipo de dato, sea o no íntimo, cuyo conocimiento o uso por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, protegida en virtud del artículo 18.1 de la CE, sino los datos de carácter personal[5].

Con esta idea, aunque la LOPDGDD dedica su cuerpo normativo, de forma mayoritaria y del mismo modo que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se

1 Sentencia del TC (STC) 254/1993, de 20 de julio (FJ 7.º).

2 STC 143/1994, de 9 de mayo (FJ 7.º).

3 Auto del TC 642/1996, de 23 de julio (FJ 3.º).

4 STC 94/1998, de 4 de mayo (FJ 6.º), que reconoce la utilización de un dato sensible que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta.

5 STC 292/2000, de 30 de noviembre (FJ 6.º).

deroga la Directiva 95/46/CE (Reglamento general de protección de datos –RGPD–), a cuestiones relacionadas con la protección de datos, transparencia, tratamientos específicos de datos; encontramos desde el punto de vista laboral, entre los diferentes derechos de la era digital, el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Ciertamente, este derecho encuentra su acomodo en la LOPDGDD en cuanto a que las imágenes no hacen más que transmitir unos datos. Por su parte, el artículo 4, apartado 1, del RGPD define «datos personales» como toda información sobre una persona física identificada o identificable, considerándose:

> […] persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica genética, psíquica, económica, cultural o social de dicha persona.

Junto a la anterior definición, resulta importante señalar que, por «tratamiento», según el artículo 4, apartado 2, debe entenderse «cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos automatizados o no». Por ello, de acuerdo con esta definición, la captación, y en su caso la grabación, de imágenes de personas constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa del RGPD[6].

Además, como nos recuerda la AEPD, la imagen de una persona es un dato personal y su tratamiento derivado de la captación, y, en su caso, la grabación, ha de ajustarse a la normativa sobre protección de datos de carácter personal[7]. Datos que requieren de una especial protección por la sensibilidad de que recogen la imagen de la persona trabajadora.

Quizá sea el momento de dejar definido que un sistema de videovigilancia comporta la captación de imágenes y sonidos que permiten su posterior tratamiento, ya sea mediante la reproducción, visualización o almacenamiento por tiempo determinado. Es, precisamente, este hecho sobre lo que se construye la idea de que estos sistemas no deben ser incorporados en el contexto de la relación laboral de forma genérica y arbitraria, sino respondiendo a una finalidad concreta y justificada que ponga por delante el derecho de las personas trabajadoras al respeto a su intimidad y dignidad; no obstante, como indica la profesora Gude Fernández (2015), esto se traduce en «la existencia de una cierta tensión conceptual entre privacidad y seguridad en el contexto laboral». En este contexto, la

[6] Agencia Española de Protección de Datos (AEPD), Informe jurídico 2016-0278, de 23 de diciembre, p. 2.

[7] AEPD, Informe jurídico 2017-0186, de 28 de noviembre.

AEPD determina que los sistemas de videovigilancia suponen un tratamiento de datos de carácter personal[8].

A través de este trabajo se pretende destacar los aspectos más relevantes que tras la entrada en vigor de la LOPDGDD y el RGPD han modificado la legislación española con relación a los derechos de las personas trabajadoras en materia de videovigilancia. Al mismo tiempo, se realiza un análisis de las sentencias más relevantes del TC y del Tribunal Europeo de Derechos Humanos (TEDH) sobre la interpretación de estas normas. Finalmente, el estudio se enriquece con la aportación de la doctrinal judicial emanada de nuestro Tribunal Supremo (TS).

2. El control de la videovigilancia y grabación de sonidos en la nueva LOPDGDD

La LOPDGDD regula en dos importantes artículos la protección que debe concederse a los datos obtenidos a través de la videovigilancia. Podríamos afirmar que nos encontramos ante dos medidas de protección distintas, pero complementarias. Una, más genérica en tanto que abarca a la persona responsable del fichero con independencia de que lo tratado sean datos con incidencia dentro de la relación laboral o no (art. 22 LOPDGDD). Y otra, más específica y dirigida, en esta ocasión, a la persona trabajadora cuyos datos se tratan, donde se pretende proteger uno de sus derechos fundamentales como es el derecho a su intimidad (art. 89 LOPDGDD). En opinión de Altés Tárrega (2020), los artículos 22 y 89 de la LOPDGDD junto con los artículos 20 y 20 bis del ET forman dos parejas de preceptos «cuyo alcance no está tan claro como *a priori* podría parecer».

En este sentido, el artículo 22 de la LOPDGDD autoriza a que las personas físicas o jurídicas, públicas o privadas, puedan gestionar el tratamiento de imágenes obtenidas a través de sistemas de cámaras o videovigilancia con el objeto de preservar la seguridad de las personas y bienes, así como de sus instalaciones, sometiéndolas a una serie de requisitos, a saber:

- Una vez obtenidas estas imágenes, la persona propietaria de las mismas deberá proceder al borrado de los datos en el plazo de 1 mes desde su obtención.
- Este plazo no se tendrá en cuenta cuando de los datos obtenidos se desprenda la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, en cuyo caso, se pondrán a disposición de la autoridad competente en un plazo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

[8] AEPD, Informe jurídico 2017-0139, de 14 de septiembre.

- Información a la persona interesada que se contiene en los artículos 13 y 14 del RGPD y previendo el artículo 12 de la misma norma que esta obligación se entenderá cumplida, en relación con la videovigilancia, cuando se transmita mediante la «combinación de iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto».

A partir de lo regulado, a nivel general, por toda aquella persona que tenga la responsabilidad del tratamiento de datos obtenidos por videovigilancia, debemos centrarnos en la posibilidad de que estos datos se obtengan dentro del marco de una relación laboral, ya sea en el ámbito privado (personas trabajadoras por cuenta ajena) o público (personas empleadas públicas).

En este caso, la protección tiende a garantizar el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo y, concretamente, se dirige al tratamiento que de los datos pueda realizar la empresa. El punto de partida de la garantía de protección de la intimidad de la persona trabajadora obliga a que la empresa realice este tratamiento con la única finalidad de control de la actividad laboral. A partir de esa premisa, para el tratamiento de los datos se establecen una serie de exigencias:

- Información, con carácter previo, y de forma expresa, clara y concisa, a las personas trabajadoras o empleadas públicas y, en su caso, a su representación, acerca de esta medida. En este sentido, los profesores Desdentado Bonete y Muñoz Ruiz (2014) señalan que: «no debe confundirse la esfera de protección del art. 18.4 CE (el derecho fundamental a la protección de datos) con la garantía del deber de información a los representantes de los trabajadores sobre la implantación de sistemas de control del trabajo».

  Resulta interesante reflejar la enmienda número 13 (de modificación) del grupo parlamentario confederal de Unidas Podemos-En Comú Podem-En Marea, que proponía que «la instalación de cámaras de videovigilancia o de cualquier dispositivo que permita la captación de imágenes de los trabajadores» requiriera «siempre y sin excepción alguna que el empresario informe previamente de manera expresa, precisa, clara e inequívoca a los interesados y a sus representantes sobre la existencia, localización y características particulares de dichos sistemas»[9].

[9] BOCG. Congreso de los Diputados número A-13-3 de 18 de abril de 2018. Entiende el grupo parlamentario que la no aceptación de su enmienda supone una grave regresión en relación con la protección de los derechos de las personas trabajadoras apartándose, además, de la doctrina establecida por el TEDH en el caso López Ribalda (p. 13). Además, la admisión de esta enmienda supondrá, en palabras del grupo parlamentario mencionado, el fin a una configuración de los derechos fundamentales en la relación laboral, utilizada por el TC y muchas decisiones del orden social, en donde la intimidad y la vida privada se sacrificaban ante la existencia de un interés empresarial contrapuesto cuando se consideraba la medida idónea, necesaria y proporcionada (p. 15).

- Cuando la captación refleje la comisión flagrante de un acto ilícito por las personas trabajadoras y empleadas públicas, el deber de información se entenderá cumplido cuando exista un dispositivo informativo en lugar suficientemente visible en el que se identifique que se realizará tratamiento de las imágenes, la identidad de la persona responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD, principalmente, de acceso, rectificación, limitación, del tratamiento y supresión. Con objeto de aligerar el contenido del dispositivo, el artículo 22.4 de la LOPDGDD permite que se incorpore al propio dispositivo un código de conexión o dirección de internet que redirija a la información contenida en el RGPD.
- No admisión de instalación de sistemas de grabación de sonidos ni videovigilancia en los lugares destinados al descanso o esparcimiento de las personas trabajadoras. El artículo 89.2 de la LOPDGDD, a título ejemplificativo, señala vestuarios, aseos y comedores.
- Con carácter específico para la grabación de sonido, cualquier sistema utilizado, incluidos el sistema de cámara o videovigilancia, se admitirá 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. Se aplicarán las limitaciones previstas para las videoconferencias con especial referencia a los principios de proporcionalidad e intervención mínima. Esto incluye la supresión de los sonidos conservados en el plazo de 1 mes desde su obtención.

3. El control de la videovigilancia y grabación de sonidos en el ET

En el contexto de la relación laboral, la titularidad del poder de dirección queda atribuida a la empresa, que define los límites de la prestación laboral y tiene su principal derivada en el ejercicio del poder disciplinario y sancionador respecto a las personas trabajadoras que no operen con la diligencia debida y con la colaboración ordinaria, entendiendo que la prestación laboral debe regirse por la buena fe.

Para la labor de comprobación de la prestación laboral, bajo los parámetros expuestos en el párrafo anterior, resulta fundamental el artículo 20.3 del ET, que constituye el soporte legal de las facultades de fiscalización de la empresa (García-Perrote Escartín y Mercader Uguina, 2017, p. 8) y autoriza a la empresa a adoptar las medidas más oportunas de vigilancia y control para verificar el cumplimiento de las obligaciones y los deberes legales de las personas trabajadoras, de modo que la tutela de la intimidad se convierte en algo sacrificable en aras de permitir que la empresa pueda verificar el cumplimiento de las obligaciones laborales de la persona trabajadora (Goñi Sein, 2017, p. 20), generando no obstante una gran conflictividad (Molina Navarrete, 2019, p. 233).

Precisamente, entre esos medios de control se encuentra la videovigilancia (art. 20 bis ET), que autoriza a las personas empleadoras, en el marco de la LOPDGDD, así como cualquier otra legislación vigente, a realizar el tratamiento de las imágenes obtenidas a través de los sistemas de cámaras, con la limitación del respeto al derecho a la intimidad; lo que va a tener su aplicación práctica en el requisito de información a las personas trabajadoras y su representación, tal y como hemos señalado anteriormente, de manera previa y de forma expresa.

Lo anterior nos lleva a mantener que nuestro derecho, principalmente LOPDGDD y ET, permite el tratamiento de datos de las personas trabajadoras obtenidos por las cámaras de grabación bajo unos parámetros muy definidos, si bien el requisito de la información a las personas trabajadoras es susceptible de interpretaciones diversas; para unos se trata de una información muy genérica y para otros la información ha de ser clara y precisa.

En cualquier caso, este derecho de la empresa se condiciona a un ejercicio regular del mismo donde el límite de su actuación deriva del respeto a los derechos fundamentales y la dignidad de la persona trabajadora.

4. El control de la videovigilancia y grabación de sonidos en la AEPD

El Grupo de Trabajo del artículo 29, en su Dictamen 4/2004, referente al tratamiento de datos personales mediante videovigilancia, señaló que «se tomarán las medidas adecuadas para garantizar que la vigilancia por videocámara cumple los principios de la protección de datos, y se evitarán las referencias inadecuadas a la intimidad»[10].

Bajo esta premisa, la AEPD ha entendido que el artículo 20.3 del ET legitima a la persona empleadora para tratar las imágenes de las personas trabajadoras en el ámbito laboral con carácter general en la medida en que se cumplan todos los requisitos impuestos por la normativa de protección de datos[11], sin que esto implique que en el ámbito laboral tenga cabida cualquier tratamiento de datos para el control empresarial del cumplimiento de los deberes laborales de la persona trabajadora. Por tanto, la aplicación del artículo 20.3 del ET no legitima por sí sola el tratamiento de las imágenes, aun cuando sea posible sin

[10] El Grupo de Trabajo del artículo 29 era el órgano consultivo independiente de la Unión Europea cuya creación se sostiene en el propio artículo 29 de la Directiva 95/46/CE 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. Su labor se ha centrado en la protección de los datos y la vida privada y ha estado funcionando hasta el 25 de mayo de 2018, fecha de entrada en vigor del RGPD.

[11] AEPD, Informe jurídico 2014-0475, de 25 de noviembre, pp. 3 y 4.

contar con el consentimiento de la persona trabajadora siempre que haya sido debidamente informada de la existencia de sistemas de videovigilancia[12].

En este contexto, la AEPD, una vez que considera que el artículo 20.3 del ET es medio adecuado para el control de la actividad de la persona trabajadora, establece que estos sistemas de videovigilancia solo se adoptarán cuando se aprecie una relación de proporcionalidad entre la finalidad perseguida y el modo en el que se tratan las imágenes, en tanto no se contemple otra medida más idónea. Y una vez razonada la proporcionalidad, se tendrá en cuenta el derecho a la intimidad y a la propia imagen de las personas trabajadoras. De esta forma se dotará a los sistemas de vigilancia de la legitimidad necesaria.

Además, la AEPD, en las Fichas prácticas de videovigilancia VI, menciona los aspectos más importantes a tener en cuenta.

El primero de ellos alude al establecimiento del Registro de Actividades de Tratamiento. La puesta en funcionamiento de estos sistemas exige que, de manera previa, se elabore como documento interno un registro de actividades de ese tratamiento.

Con respecto al derecho de información, la AEPD exige la necesidad de información en todos los casos de la existencia de un sistema de videovigilancia. Esto obliga a la colocación de cartelería suficientemente visible en los accesos a las zonas sometidas a videovigilancia con una serie de información: identidad de la persona responsable de la instalación, a quién y a dónde dirigirse tanto para ejercer los derechos contemplados en la normativa de protección de datos, como para obtener más información relativa al tratamiento de los datos personales.

Esta información debe proporcionarse de manera personal a las personas trabajadoras y su representación, por cualquier medio que garantice su recepción.

Una vez informadas las personas trabajadoras o su representación, las cámaras solo captarán imágenes de los espacios indispensables para el control laboral, evitándose su ubicación en las zonas de vestuarios, baños y espacios de descanso de las personas trabajadoras. En el caso de utilización de cámaras orientables o *zoom*, con objeto de evitar captar imágenes de la vía pública, viviendas o cualquier otro espacio ajeno, será necesaria la instalación de máscaras de privacidad. En ningún caso, se registrarán conversaciones privadas.

Especial atención merecen las cuestiones relacionadas con el propio sistema de grabación y la visualización de las imágenes. En este contexto, la AEPD establece como ajustado a derecho un sistema de grabación, en un espacio de acceso restringido, en donde solo

[12] AEPD, Informe jurídico 2009-0495, de 27 de octubre, pp. 3 y 4.

acceda a las imágenes el personal autorizado[13]. El periodo de conservación será de como máximo 1 mes. Sin embargo, respecto a las imágenes sobre las que se basen posteriores denuncias o infracciones deberán acompañarse a la denuncia y conservarse para ser entregadas a las fuerzas o cuerpos de seguridad. Igualmente, las imágenes se pondrán a disposición, cuando así sea requerido, de los juzgados y tribunales que lo soliciten. Como garantía añadida a la protección de tratamiento de los datos obtenidos por los sistemas de videovigilancia, la petición de imágenes a las que estamos haciendo referencia se realizará siempre en el marco de actuaciones policiales o judiciales.

En definitiva, la AEPD da validez jurídica al tratamiento de datos proporcionados a través de sistemas de videovigilancia bajo las premisas de legitimidad (interés legítimo) e información. Cuestiones que se abordarán en los epígrafes siguientes de acuerdo a la doctrina de los tribunales internacionales y españoles.

5. Legitimidad en el tratamiento de datos obtenidos a través de sistemas de videovigilancia

El tratamiento de los datos de las personas trabajadoras obtenidos por videovigilancia sin límites comporta que el interés legítimo de la empresa en estos datos se aleje de la búsqueda de una mejora y eficiencia empresarial y se acerque a un modo de control injustificado e intrusivo en la vida privada de la persona trabajadora.

Resulta importante determinar que los sistemas de videovigilancia cuya finalidad sea el control empresarial encuentran amparo jurídico en la medida en que se aprecie proporcionalidad entre la finalidad perseguida y el modo en el que se tratan las imágenes, y siempre teniendo en cuenta que no existan otras medidas más idóneas. En definitiva, la videovigilancia debe realizarse en tanto sea proporcional.

La consecuencia práctica de apreciarse la legitimidad de la medida no es baladí, puesto que excepcionaría la necesidad de consentimiento de la persona interesada, siempre y cuando en un ejercicio de ponderación entre el «interés legítimo y los derechos fundamentales de los afectados prevalezca el primero sobre el segundo»[14]. Por ello, es necesario aplicar la regla de proporcionalidad que valorará en cada caso concreto si prevalece un interés legítimo por parte de la persona responsable del tratamiento o prevalecen los derechos fundamentales de las personas interesadas a las que se refiera el tratamiento.

[13] Este requisito obliga a que, si el acceso se realiza con conexión a internet, deberá contar con un código de usuario y una contraseña puestos a disposición de las personas autorizadas para acceder a dichas imágenes que deberán cambiarse una vez instalado el sistema y no ser fácilmente deducibles.

[14] AEPD, Informe jurídico 2016-0278, de 23 de diciembre, p. 6.

Como punto de partida debemos situarnos ante el considerando 47 del RGPD, que establece que el interés legítimo de una persona responsable del tratamiento o una tercera persona puede ser base jurídica suficiente para realizar el tratamiento de datos, en tanto no se sitúen en un plano de protección mayor los intereses o los derechos y libertades de la persona interesada, «teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable».

Este interés legítimo, continúa señalando el considerando 47 del RGPD, requiere de una evaluación meticulosa con independencia de que la persona interesada pueda prever de forma razonable que se vaya a efectuar una recogida y tratamiento de sus datos. Y, concretamente, los intereses y derechos de la persona interesada pueden anteponerse a los de la persona responsable del tratamiento cuando los datos personales tratados se hubieran producido, de manera posterior, en circunstancias no esperadas razonablemente por la persona interesada.

De manera más específica, el artículo 6.1 f) del RGPD justifica la licitud de un tratamiento de datos tras un proceso de valoración entre la satisfacción de los intereses legítimos perseguidos por la persona responsable del tratamiento y los intereses o los derechos y libertades fundamentales de la persona interesada; de tal forma que la licitud dependerá de que el interés de la persona responsable del tratamiento prevalezca sobre el interés del sujeto tratado.

Por tanto, el primer paso para justificar la legitimidad de un tratamiento, en el contexto de la relación laboral, pasa por el análisis de estos requisitos:

- Relación de subordinación, en este caso de la persona trabajadora frente a la empresa.
- Evaluación meticulosa, sometida al examen de la proporcionalidad de la medida.
- Prevalencia al derecho de la persona trabajadora frente al interés de la empresa en tanto el tratamiento realizado sobre los datos no fuera el esperado por la persona trabajadora.

En cualquier caso, la invocación del interés legítimo para justificar la implantación de un sistema de videovigilancia aconseja la existencia de medidas específicas de mitigación, con el fin de realizar una adecuada ponderación entre el interés de la empresa y los derechos y libertades fundamentales de la persona trabajadora (Grupo de Trabajo del artículo 29, 2017, p. 8).

Aterrizando en nuestra norma interna, la LOPDGDD, respecto a la videovigilancia, señala la existencia de una presunción *iuris tantum* del interés legítimo de la empresa en la medida en que se ponderen una serie de requisitos, lo que no supone carta blanca alguna a la

empresa para establecer estos sistemas de vigilancia por cuanto se apreciará la ilicitud del tratamiento de los datos obtenidos por estos sistemas si no cumplen estrictamente con la legislación establecida.

Este interés legítimo se establece claramente en la LOPDGDD, dentro del título IV (art. 22), respecto a tratamientos concretos como la videovigilancia. Sería discutible si esta base legitimadora, es decir, el interés legítimo que autoriza el tratamiento, resulta extrapolable a los derechos digitales del título IX, y, concretamente, al artículo 89, «Derecho a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo».

En este sentido, debemos afirmar que tanto el artículo 22 como el 89 de la LOPDGDD elevan a la máxima protección el tratamiento de una serie de datos que afecta directa, o indirectamente, a la intimidad, por tanto, debe extenderse el interés legítimo que justifica el tratamiento en el artículo 22 de la LOPDGDD al artículo 89, y la empresa se encuentra obligada a realizar una ponderación con carácter previo al tratamiento que desee realizar de los datos obtenidos de las personas trabajadoras a través de dispositivos de videovigilancia. Solo esta forma de actuación empresarial –ponderación y proporcionalidad– servirá de base jurídica y legal para que la empresa pueda demostrar una base legitimadora en el tratamiento de estos datos.

Tras realizar esta equiparación, no cabe duda de que el interés legítimo de la empresa puede invocarse como justificación jurídica del tratamiento en cuanto persiga un fin legítimo y cumpla con el principio de proporcionalidad.

Esta prueba de proporcionalidad constituye el primer paso con carácter previo a la instalación de cualquier sistema de videovigilancia con objeto de determinar la necesidad de los datos y la subordinación del derecho a la intimidad a los intereses generales de la empresa. De tal modo que, como señala la AEPD, cualquier medida que se adopte debe superar el juicio de proporcionalidad, lo que nos conducirá a entender que nos encontramos frente a una medida adecuada, necesaria y equilibrada. En caso contrario, debe considerarse desproporcionada y, en consecuencia, contraria a la normativa de protección de datos[15].

Y, de manera específica, respecto a la instalación de sistemas de videovigilancia, el respeto al principio de la proporcionalidad se basa, fundamentalmente, en el análisis de la existencia de otros medios menos intrusivos de vigilancia de la prestación laboral de las personas trabajadoras con el fin de evitar ataques injustificados a los derechos y libertades fundamentales de las mismas.

[15] AEPD, Informe jurídico 2017-0186, de 28 de noviembre, pp. 2 y 3.

6. Enfoque del TC sobre la consideración de los datos proporcionados a través de sistema de vigilancia

El TC ha dedicado varias sentencias a distinguir entre derecho a la intimidad versus derecho a la protección de datos. Esta distinción es fundamental en cuanto a que, dependiendo del enfoque que se le aplique a un caso concreto, los parámetros de proporcionalidad pueden resultar afectados.

El TC considera que el derecho fundamental a la intimidad protege a la persona trabajadora de cualquier invasión que puede realizarse en su vida privada, estableciéndose un ámbito reservado de su vida frente a la acción y conocimiento de terceras personas, de modo que le garantiza un poder jurídico sobre la información relativa a su persona, estando los poderes públicos obligados a adoptar cuantas medidas fueran necesarias para hacer efectivo ese poder de disposición. No obstante, lo que garantiza el artículo 18.1 de la CE no es la intimidad sin más, sino el derecho a poseerla, lo que obligará a establecer unos límites, pero con un minucioso respeto del contenido esencial de este derecho[16].

Frente a este derecho a la intimidad, el derecho a la protección de datos se construye sobre el derecho de la persona trabajadora de asegurar un poder de control sobre sus datos personales, su obtención y tratamiento, con objeto de no permitir su tráfico. Este control se escapa en la medida en que la persona trabajadora desconozca los datos que se poseen, quién los posee y con qué fin.

Por ello, el TC reconoce que el objeto del derecho a la protección de datos es más amplio que el del derecho a la intimidad, ya que no se limita a lo constitucionalmente protegido por el artículo 18.1 de la CE, sino que responde a un conjunto de bienes jurídicamente protegidos, sean o no constitucionales, que caen dentro del ámbito de la vida privada de la persona trabajadora; de modo que derecho a la intimidad y derecho a la protección de datos son categorías diferentes, aunque relacionadas (Chacartegui Jávega, 2018, p. 122). Así pues:

> […] el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal[17].

[16] STC 144/1999, de 22 de julio (FJ 8.º).

[17] STC 292/2000, de 30 de noviembre (FJ 6.º).

Ahondando en esta idea, la STC 292/2000, de 30 de noviembre, diferencia entre derecho a la intimidad versus derecho de protección de datos; este otorga a su titular un conjunto de facultades cuyo ejercicio (previo consentimiento, acceso, rectificación, cancelación) imponen a terceras personas deberes jurídicos, que no se encuentran contenidos en el derecho a la intimidad y que garantizan a la persona un poder de control sobre sus datos. Todo esto garantiza a la persona trabajadora el pleno poder de disposición y control sobre sus datos y se traduce en la facultad que tiene una persona trabajadora para decidir cuáles de estos desea proporcionar a una tercera o cuáles puede esta tercera recabar. Además, permite a la persona trabajadora tener conocimiento de quién posee sus datos personales y para qué, pudiendo oponerse a su posesión y uso.

En cualquier caso, derecho a la intimidad o derecho a la protección de datos, el TC tiene perfectamente asentada, desde hace años, la doctrina de la plena efectividad de los derechos fundamentales de la persona trabajadora en el marco de la relación laboral, en tanto que esta no puede implicar la privación de tales derechos para quienes prestan servicios en las organizaciones productivas, que no son ajenas a los principios y derechos constitucionales que informan el sistema de relaciones laborales[18]. El ejercicio de tales derechos únicamente admite limitaciones o sacrificios en la medida en que se desenvuelve en el seno de una organización que refleja otros derechos reconocidos constitucionalmente en los artículos 38 y 33 de la CE. Además, surge un límite adicional en el ejercicio de los respectivos derechos constitucionales, impuesto por la relación laboral, que se deriva del principio de buena fe entre las partes en el contrato de trabajo y al que estas han de ajustar su comportamiento mutuo[19].

No obstante, la relación empresa-persona trabajadora ha de ser contextualizada de una forma real, lo que obliga al reforzamiento de la esfera de los intereses de la persona trabajadora, puesto que, si la relación laboral tiene como efecto típico la sumisión de ciertos aspectos de la vida humana a los poderes empresariales y a los requerimientos de la organización productiva, resulta necesario algo más que la sola afirmación del interés empresarial como justificación de la limitación de los derechos fundamentales de la persona trabajadora dada la posición prevalente que estos alcanzan en nuestro ordenamiento jurídico[20].

En este sentido, todo lo que la empresa pudiera argumentar para justificar una restricción de los derechos fundamentales de las personas trabajadoras debe construirse sobre razones de necesidad estricta, acreditándose que no es posible otra forma de alcanzar el

[18] STC 90/1997, de 6 de mayo (FJ 4.º) y las allí citadas.

[19] STC 106/1996, de 12 de junio (FJ 5.º).

[20] STC 6/1995, de 10 de enero (FJ 2.º).

legítimo objetivo perseguido, porque no existe medio razonable para lograr una adecuación entre el interés de la persona trabajadora y el de la empresa donde presta sus servicios[21].

Esto nos conduce a que el centro de trabajo es un espacio en el que no puede obviarse el derecho a la intimidad de las personas trabajadoras, de tal manera que lo que suceda en el mismo debe estar amparado por el artículo 18.1 de la CE, si bien mediante un análisis detallado y conjunto de los hechos sería posible atemperar el derecho a la intimidad de la persona trabajadora.

Así, la limitación del derecho fundamental a la intimidad por parte de la empresa solo encontrará amparo en la medida en que la propia naturaleza del trabajo comprometido implique restricción del derecho o bien cuando quede acreditada una determinada necesidad o un interés empresarial, sin que sea suficiente su mera afirmación de esa necesidad o interés para sacrificar el derecho fundamental de la persona trabajadora[22].

Por tanto, las limitaciones o modulaciones tienen que ser las estrictamente necesarias para satisfacer un interés empresarial; de modo que, si se encuentran otras vías para satisfacer el mencionado interés que afecten de manera menos agresiva al derecho fundamental en cuestión, habrá que emplearlas frente a otras más agresivas.

El TC, en la Sentencia 98/2000, de 10 de abril, analiza un caso en el que la empresa decidió instalar aparatos de grabación, de modo que la captación de las imágenes a través de CCTV proporcionaba a la empresa mayor seguridad para hacer frente a las reclamaciones de la clientela y posibles fraudes de su personal. La sentencia recurrida ante el TC considera la medida justificada en la proporción en que se instalaba en puntos concretos, conocidos por las personas trabajadoras y atendiendo a una finalidad legítima. Sin embargo, el propio TC, en aplicación del principio de proporcionalidad, considera que la mera utilidad o conveniencia de la empresa, sin más, no legitima la instalación de aparatos de audio y grabación, habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audio pretende complementar[23].

Por tanto, la empresa no justifica la necesidad de la medida, sino más bien la presenta como algo complementario al modelo de vigilancia que se estaba utilizando, no acreditándose la indispensabilidad de la medida para la «seguridad y el buen funcionamiento de la empresa».

El TC aborda la resolución de este caso desde la perspectiva del derecho a la intimidad y con un resultado, en opinión de Álvarez Alonso (2013), «en buena sintonía con

[21] STC 99/1994, de 11 de abril (FJ 7.º).

[22] STC 136/1996, de 23 de julio (FJ 7.º).

[23] STC 98/2000, de 10 de abril (FF. JJ. 7.º, 8.º y 9.º).

la jurisprudencia internacional y comunitaria» (p. 360). Así, el hecho de que se pueda permitir la captación indiscriminada y prolongada en el tiempo de conversaciones de personas trabajadoras y clientela sobrepasa las facultades de la empresa contempladas en el artículo 20.3 del ET suponiendo una intromisión en el derecho a la intimidad, ya que no se han respetado los principios de proporcionalidad e intervención mínima que sirven para modular los derechos fundamentales frente al requerimiento del interés empresarial.

En la STC 186/2000, de 10 de julio, la decisión del TC parte de que el análisis de cualquier medida restrictiva de derechos fundamentales debe justificarse en el cumplimiento del principio de proporcionalidad. En este caso, se sometía al control constitucional la instalación de un circuito cerrado de televisión que grababa la zona de caja de una trabajadora ante la sospecha de que estuviera cometiendo graves irregularidades en su puesto de trabajo. El TC, con base en el principio de proporcionalidad, analiza si la medida era justificada, idónea, necesaria y equilibrada.

La medida se considera justificada, por las sospechas razonables de la comisión de graves irregularidades por parte de la trabajadora; idónea, para la finalidad pretendida por la empresa en la medida en que se dirigiría a comprobar si, efectivamente, se estaban cometiendo esas irregularidades de cara a establecer la correspondiente sanción; necesaria, en cuanto a que la grabación era el único medio de prueba para demostrar las irregularidades; y equilibrada, en la medida en que la grabación se limitó a la zona de caja de la trabajadora investigada y se prolongó por tiempo determinado (exclusivamente, el suficiente para comprobar que no se trataba de una confusión o hecho aislado).

La aplicación de este juicio de proporcionalidad, enfocada sobre la posible lesión del derecho fundamental a la intimidad, lleva a afirmar al TC que no se produce una agresión a la intimidad de la trabajadora por el hecho de realizar grabaciones de cómo ejecutaba su trabajo, puesto que esta decisión no es arbitraria y no pretende divulgar lo captado en ningún otro foro, sino obtener datos sobre una realidad sospechada de irregularidades cometidas en su puesto de trabajo que contravenían el principio de buena fe[24].

A diferencia de la sentencia expuesta anteriormente, se descarta la vulneración del derecho a la intimidad sobre la base de que la vigilancia no se produce con un propósito genérico en el cumplimiento de las obligaciones de las personas trabajadoras, sino sobre determinada zona de caja tras advertir comportamientos irregulares de las personas trabajadoras.

[24] STC 186/2000, de 10 de julio (FJ 7.º).

Por último, el TC considera que carece de trascendencia desde la perspectiva constitucional el hecho de no llevar a cabo el trámite de que la instalación del sistema de videovigilancia fuera comunicada a la representación de las personas trabajadoras. Este incumplimiento empresarial parece oportuno en la medida en que pretende evitar filtraciones a las personas trabajadoras y garantizar la efectividad de la medida, pero, en cualquier caso, se trata de una cuestión de legalidad ordinaria.

En la STC 29/2013, de 11 de febrero, la constitucionalidad de la instalación de sistema de videovigilancia se analiza desde la perspectiva del derecho a la protección de datos (art. 18.4 CE) y no de la intimidad (art. 18.1 CE), que es el caso de las dos sentencias constitucionales referidas con anterioridad. Esto tiene un efecto inmediato en que lo que se somete a revisión constitucional es «el derecho fundamental a la autotutela informativa».

El supuesto enjuiciado en esta sentencia se refiere a un trabajador de la Universidad de Sevilla al que, con objeto de verificar el cumplimiento de su jornada laboral, se somete a un control a través de las cámaras de videovigilancia instaladas en el recinto universitario para el control de acceso de las personas de la comunidad universitaria y sobre el que se habían adoptado las medidas impuestas por la AEPD de información a través de carteles visibles.

En primer lugar, el tribunal considera que las imágenes grabadas y que se almacenan en un soporte físico constituyen un dato de carácter personal que queda amparado dentro del artículo 18.4 de la CE en la medida en que el derecho fundamental acoge los supuestos en los que se traten datos que identifiquen a la persona.

Se trata, pues, de analizar la constitucionalidad de una medida en la que, a diferencia de la STC 98/2000 (puesto de trabajo concreto) o la STC 186/2000 (fin concreto de controlar posibles infracciones laborales), se utilizan imágenes para un fin distinto del expresamente divulgado y tomadas en vestíbulos y lugares públicos de paso fuera de las dependencias laborales de la persona trabajadora. En este contexto, el análisis del artículo 18.4 resulta totalmente decisivo.

Así, para el TC, una interpretación de este precepto 18.4 de la CE se traduce en el derecho fundamental de la persona trabajadora a conocer en todo momento quién dispone de los datos y la finalidad de su tratamiento. En este sentido, la brecha constitucional se produce ante la falta de información de la persona afectada sobre quién posee los datos y la finalidad que va a aplicar a los mismos. De hecho, Arrabal Platero (2015) manifiesta que «el TC se ha servido del prisma de la protección de datos para censurar las grabaciones de videovigilancia como prueba en el proceso laboral».

Ahora bien, este derecho a la información, como exigencia previa, a la grabación de imágenes puede amparar limitaciones y no ser absoluto, siendo posible admitir limitaciones por

razones constitucionalmente admisibles y legalmente previstas que deberán estar contempladas en norma con rango de ley, ya que nos encontramos ante la limitación de un derecho constitucional[25].

Sobre esta base, el TC levanta nueva doctrina para indicar que «no hay habilitación legal expresa sobre la que justificar la omisión del derecho a la información sobre el tratamiento de los datos personales en el ámbito de las relaciones laborales». Por ello, el mero interés de la persona empleadora resulta insuficiente para justificar que el tratamiento de los datos de la persona trabajadora sea empleado en su contra sin al menos realizar una labor informativa previa sobre el control laboral puesto en práctica con el sistema de videovigilancia, vulnerándose la efectividad del derecho fundamental.

Esto obliga a que la empresa distinga entre la legitimidad del fin, control empresarial vía artículo 20.3 del ET, y la constitucionalidad del acto, basado en la exigencia de información previa, contenida en el artículo 13 del actual RGPD. Admitir la legitimidad de la medida en ningún caso supone carta abierta para lesionar el derecho constitucional del artículo 18.4 de la CE, que quedaría vulnerado si esa medida de control se realiza con medios encubiertos que evitan que la persona trabajadora disponga de la información exigible.

Por ello, en la STC 29/2013, el tribunal entiende que se vulnera el artículo 18.4 de la CE en tanto las cámaras de vigilancia de la universidad captaron la imagen –dato personal– de una de sus personas trabajadoras, siendo utilizada con fines de control de su jornada de trabajo, sin que la persona responsable del tratamiento hubiera informado a la persona trabajadora de que esas capturas de imagen se dirigirían a la supervisión de su actividad laboral. Además, la finalidad de la instalación de las cámaras fue declarada ante la AEPD como medida de seguridad pública y no contenía una mención expresa a un fin declarado y específico de control de la actividad laboral.

Esta nueva doctrina, que cuanto menos pone en cuarentena la posibilidad de emplear sistemas de videovigilancia –sobre la base del poder de control empresarial del art. 20.3 ET– con cierta garantía de éxito, en opinión de la doctrina laboralista, supone el establecimiento de «un canon de control constitucional más rígido que el que la jurisprudencia constitucional venía aplicando respecto a los derechos fundamentales a cuyo servicio se sitúa la garantía prevista» en el artículo 18.4 de la CE (García Rubio, 2016).

Debido a ello, es fácilmente entendible el voto particular que presenta la sentencia, en el que el magistrado pone de relieve la total ausencia de ponderación. Indirectamente se ha realizado una ponderación abstracta en la que la protección de los datos personales prima

[25] Y tal y como señala la STC 29/2013, de 11 de febrero, en su fundamento jurídico séptimo, exigiendo además que el recorte «sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, respetuoso con el contenido esencial del derecho fundamental restringido».

sobre las medidas empresariales. Ponderación que hubiera resultado más problemática si se hubiera producido entre el derecho a la intimidad y el derecho a la protección de datos en cuanto que aquel acaba confiriendo relevancia a este.

Posteriormente, y sobre la base de la discrepancia de la sentencia de 2013, el TC pronunció la Sentencia 39/2016, tampoco exenta de intenso debate dentro del tribunal, con tres votos particulares, en la que se define un nuevo enfoque al conflicto entre la videovigilancia de las personas trabajadoras y los derechos a la protección de datos y a la intimidad, y cuya detallada explicación de los votos particulares puede consultarse en Valdés Dal-Ré (2017, pp. 24 y ss.). El supuesto de hecho parte del despido de una trabajadora al apropiarse dinero de la caja mediante operaciones falsas de devolución de venta de prendas y habiendo sido obtenida la prueba mediante un sistema de videovigilancia cuya instalación para la labor expresa de vigilancia desconocía la trabajadora, aunque sí se encontraba colocado en el escaparate del establecimiento el distintivo informativo que indicaba que se estaba en una zona sometida a videovigilancia.

Respecto al derecho a la protección de datos, *ex* artículo 18.4 de la CE, el tribunal refuerza su doctrina de que nos encontramos ante un dato personal. Ello obliga a dos acciones frente a la persona trabajadora, por un lado, a solicitar el consentimiento sobre la recogida y uso de sus datos y, por otro, como modo de hacer efectivo el consentimiento surge el derecho a ser informada.

Partiendo del consentimiento como elemento definidor del sistema de protección de datos de carácter personal, el artículo 6.1 de la Ley orgánica 15/1999, de protección de datos –actual art. 6, apdos. 1 y 3, LOPDGDD, requiere el consentimiento inequívoco de la persona afectada salvo una serie de supuestos como los relativos a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, abarcando las obligaciones derivadas del contrato; concretamente, la profesora Rodríguez Escanciano (2018) se refiere a «excepciones de interés en el marco de las relaciones laborales» (p. 29). Por ello, entiende el tribunal que un tratamiento de datos que tiene como objeto el control de la actividad laboral tiene cabida en la excepción al previo consentimiento de la persona trabajadora. Sin embargo, la supresión del consentimiento previo no anula el deber de información que tiene la persona titular del tratamiento. Para un sector doctrinal, en la STC 39/2016 se produce una banalización del derecho a la información al entender cumplido este derecho con la colocación de un distintivo (Gallardo Moya, 2017, p. 151).

En cualquier caso, el deber de requerimiento del consentimiento para el tratamiento de los datos o el deber de información previa requiere de una ponderación de la proporcionalidad de la medida adoptada. La no apreciación de la proporcionalidad supondrá una vulneración del derecho a la protección de datos. Es esta premisa, aplicación del juicio de

proporcionalidad en el tratamiento de datos, lo que supone un giro en la doctrina constitucional en relación con la STC 29/2013.

En este sentido, el TC pondera entre necesidad del consentimiento expreso, o no, de la interesada para el tratamiento de sus datos. Y teniendo en cuenta que dentro de la finalidad legítima que se exige a todo tratamiento estarían las facultades de control empresarial en tanto no lesionen derechos fundamentales, la empresa no necesitará 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»[26].

Con relación al deber de información, la ausencia del mismo a la trabajadora por parte de la empresa requiere del adecuado juicio de proporcionalidad. Por ello, el TC en casos de falta de información del tratamiento debe ponderar la falta de información sobre el tratamiento de datos versus la facultad de empresa de vigilar y controlar la actividad laboral reconocida en el artículo 20.3 del ET en conexión con los artículos 33 y 38 de la CE. Juicio de ponderación que el tribunal resuelve a favor de la teoría empresarial sobre la base de la información previa de la que disponía la trabajadora, a través del correspondiente distintivo informativo exigido, la Instrucción 1/2006, de 8 de noviembre, de la AEPD, se considera suficiente y cumple con la exigencia de la normativa de protección de datos con relación a la información, si bien un sector doctrinal considera que se produce una relajación en el deber de información (Lahera Forteza, 2016, p. 494), considerando que el medio informativo es de una entidad tal que se ha tocado fondo (Terradillos Ormaetxea, 2017, p. 157) y hasta el punto de disentir de que el distintivo informativo, fruto de una mera instrucción de un organismo público, sea fuente formal o material del derecho como elemento sustitutivo, sin más, del derecho a la información (Sepúlveda Gómez, 2016, p. 234).

Junto al examen constitucional del tratamiento de datos, la STC 39/2016 examina la vulneración del derecho a la intimidad, reiterando la doctrina establecida por el mismo respecto de la que cualquier medida restrictiva de derechos fundamentales debe evaluarse desde el minucioso análisis del principio de proporcionalidad. En definitiva, someter la medida a un juicio de idoneidad (si la medida es susceptible de conseguir el objetivo propuesto, en este caso verificar si alguna de las personas trabajadoras cometía las irregularidades sospechadas), juicio de necesidad (si la medida es necesaria, en el sentido de que no exista otra más moderada para la consecución del tal propósito con igual eficacia. Ciertamente la grabación servía de prueba de las irregularidades) y juicio de proporcionalidad en sentido estricto (si la medida es ponderada o equilibrada por derivarse de ella más beneficios que ventajas para el interés general que prejuicios sobre otros bienes o valores en conflicto, lo que ocurre en este caso al limitarse la grabación a la zona de cajas).

[26] STC 39/2016, de 3 de marzo (FJ 4.º).

Por tanto, en esta sentencia, el TC aplica el principio de la proporcionalidad para resolver dos conflictos:

- Conflicto entre intimidad de la persona trabajadora y control empresarial.
- Conflicto entre derecho de información de la persona trabajadora como elemento del derecho de protección de datos y control empresarial.

Sobre este último conflicto, un sector doctrinal opina que, teniendo en cuenta que el deber de información es una falta leve en la normativa de protección de datos de 1999, elevar esa falta de información a vulneración del derecho de protección de datos supone una sanción constitucional más estricta que la diseñada por el propio legislador. Así debería excluirse el deber de información del contenido esencial del derecho a protección de datos (Pascual Caballero, 2017, p. 13).

Sin embargo, esta consideración del deber de información no hace más que constituirlo como un elemento paralelo al derecho a la intimidad y, efectivamente, la realidad de la ausencia de información deja a la persona trabajadora desnuda frente a posibles abusos empresariales. No debemos focalizar el discurso jurídico tanto en la calificación de la infracción administrativa como en las consecuencias prácticas que la ausencia del derecho a la información causa en la persona trabajadora y su traducción práctica en una vulneración de su intimidad. Por ello, consideramos necesario que esa labor de información forme parte del derecho a la protección de datos (art. 18.4 CE), que no es más que un desarrollo del derecho a la intimidad (art. 18.1 CE).

7. Aplicación de la doctrina constitucional por el TS

Partiendo de la doctrina sentada por la STC 39/2016, de 3 de marzo, se han analizado las sentencias emitidas con posterioridad al 8 de abril de 2016. No obstante, se procede a indicar un grupo de resoluciones en las que no se aprecia contradicción, por lo que el TS no entra en el análisis jurídico, pero que contienen importantes manifestaciones:

- Auto del TS (ATS) 14014/2019, de 12 de diciembre (proc. núm. 1317/2019). No se aprecia contradicción en cuanto a que en la sentencia recurrida no consta si la cámara que captó a la trabajadora estaba oculta, del mismo modo que no consta que la empresa hubiera informado a la trabajadora. Sin embargo, en la sentencia de referencia se acredita que la trabajadora fue informada del sistema de videovigilancia.
- ATS 12010/2019, de 23 de octubre (proc. núm. 3958/2018). El trabajador recurre en casación para la unificación de la doctrina con objeto de declarar la nulidad del acuerdo transaccional –reconociendo los hechos–, puesto que dicho documento

se firmó tras visionar el trabajador una grabación donde se ponían de manifiesto determinadas irregularidades. Para ello, invoca como sentencia de contraste la Sentencia del TEDH (STEDH) de 9 de enero de 2018 (asunto López Ribalda). Entiende el TS que dicha sentencia no puede aportarse como contraste, puesto que no nos encontramos frente a una sentencia firme a los efectos de lo exigido en el artículo 224.3, en relación con el artículo 219.2 de la Ley reguladora de la jurisdicción social[27].

- ATS 8912/2019, de 12 de septiembre (proc. núm. 2465/2018). Se declara la inadmisión del recurso por cuanto en la sentencia de contraste se ordena la grabación de imágenes sin que existieran previamente sospechas de actuaciones ilícitas de las personas trabajadoras. Sin embargo, en la sentencia recurrida, la empresa acude a la contratación de un detective privado que realiza un seguimiento durante 2 días ante las irregularidades detectadas por la empresa.
- ATS 8293/2019, de 26 de junio (proc. núm. 3472/2018). No puede apreciarse contradicción en la medida en que en la sentencia recurrida la empresa no ofreció previa información a las personas trabajadoras sobre la posibilidad de ser grabadas, mientras que en la de referencia, que declara la licitud de la prueba, el trabajador conocía –por motivos de seguridad– la existencia de cámaras y su ubicación.

Dentro de la doctrina judicial del TS, la admisión de la validez de los sistemas de videovigilancia debe someterse a una verdadera justificación de la medida acreditada mediante el correspondiente juicio de proporcionalidad.

Presencia de cámaras en la mayor parte del centro de trabajo. En la Sentencia del TS (STS) de 7 de julio de 2016 (rec. 3233/2014) se analiza un caso en el que la empresa realiza una instalación masiva de las cámaras en el centro de trabajo que tiene como finalidad la protección del patrimonio empresarial posibilitando la grabación de conductas que atenten contra esa finalidad, y todo esto con base en el detonante de cuantiosas pérdidas sufridas. Por tanto, se produce una situación en la que todas las personas trabajadoras se convierten en sospechosas. Queda acreditada la voluntad de la empresa de solventar el estado de las cosas, puesto que la instalación se produce tras la generación de la situación de desconfianza.

[27] Considera el auto del TS que la declaración de inadmisión del recurso de casación para la unificación de la doctrina no puede quedar desvirtuada por el hecho de que la sentencia del TEDH se hubiera publicado «en la página del Ministerio de Justicia, lo que induce a pensar en la firmeza de la misma». El TS entiende que no puede acogerse indefensión porque:

> […] en la propia página del Tribunal Europeo de Derechos Humanos, consta que la misma está elevada a Gran Sala, página que es pública y oficial, siendo así que en la página del ministerio aparecen sentencias a modo ilustrativo, por lo que la parte tuvo capacidad de conocer que la sentencia no era firme.

Las grabaciones muestran que en la zona de «reserva», de acceso exclusivo para las personas empleadas, se detecta a una trabajadora que consume productos de la empresa sin abonarlos. La sentencia insiste en que la trabajadora era conocedora de la existencia de las cámaras no solo por ser de común conocimiento, sino también por la existencia de carteles indicadores, si bien no había sido informada expresa e inequívocamente de que tales filmaciones pudieran ser utilizadas con fines disciplinarios.

Además, el área donde se produce la grabación es una zona de almacén que mucho dista de un lugar que pudiera calificarse como área de privacidad. Por ello, semejante relato específico «excluye el factor sorpresa y muestra claramente la situación de riesgo asumido por [la trabajadora] y por cualquier otro responsable de conductas análogas». Todo esto conduce a un juicio de proporcionalidad en el que no se localizan otras medidas más idóneas para averiguar el origen de las pérdidas ni más moderadas en la consecución de tal propósito; por lo que la referida sentencia alcanza la conclusión de un uso apropiado de la videovigilancia implantada y que la consecución de su objetivo se ha ajustado a las exigencias «razonables de respeto a la intimidad de la persona»[28].

Presencia de las cámaras hacia una persona trabajadora concreta. La STS de 2 de febrero de 2017 (rec. 554/2016) considera adecuada la videovigilancia focalizada en una persona trabajadora concreta en tanto que las quejas de los compañeros y las compañeras sobre el trabajador despedido acerca de su conducta y el incumplimiento de las obligaciones laborales le hacían acreedor de una mayor atención respecto del conjunto de sus deberes como persona trabajadora, sin que quepa practicar controles aleatorios que afecten a quienes nunca habían participado en las conductas bajo sospecha (Preciado Domènech, 2017, p. 180). Por ello, la instalación de la cámara debe calificarse como razonable y proporcionada a su objeto en la medida en que era conocedor de que su conducta estaba siendo grabada.

Información suficiente. La STS de 31 de enero de 2017 (rec. 3331/2015) se refiere a la información que deben recibir las personas trabajadoras sobre la finalidad del sistema de videovigilancia y hasta qué punto resulta importante que esta información se refiera a la finalidad de la medida. En la mencionada sentencia se acredita que las personas trabajadoras conocían la instalación del sistema de seguridad y la ubicación de las cámaras por razones de seguridad, por lo que se deduce que estas personas trabajadoras eran conocedoras de que se producía una vigilancia de los actos ilícitos de las personas empleadas y de terceras personas. Además, la sentencia resalta la justificación de la medida por razones de seguridad (controlar hechos ilícitos), idónea para el fin mencionado (control de caja y cobros) y necesaria y proporcionada al fin perseguido.

[28] La sentencia apunta que no se genera una situación de indefensión a la trabajadora en cuanto que los actos por los que se sanciona tienen lugar en un marco de riesgo asumido, «el de actuar a ciencia y paciencia de una observación llevada a cabo por medios tecnológicos y cuya finalidad, conocida, es combatir las actividades generadoras de pérdidas».

En este sentido, en la STS de 2 de febrero de 2017 (rec. 554/2016) se declara probado que las cámaras se encuentran ubicadas en la entrada y espacios públicos del gimnasio, estando solo autorizado al visionado de las mismas el jefe de seguridad. Respecto al uso destinado, es cierto que no consta en la autorización de la Agencia de Protección de Datos que se incluyera el control horario laboral ni la utilización disciplinaria para las personas trabajadoras que, además, no habían sido advertidas de esta posibilidad, si bien eran conocedoras de la instalación de las cámaras en la entrada y demás espacios públicos del local, salvo vestuarios y aseos, y la posibilidad de ser destinadas al control de cualquier irregularidad, especialmente en la entrada. Junto a lo anterior, debe excluirse la afectación sorpresiva del trabajador por cuanto conocía el despido de otro trabajador con idéntica causa (colar a personas en el gimnasio utilizando la pulsera del trabajador para activar el torno de entrada) y ocupaba un puesto de dirección.

Sobre esta base, la sentencia del Alto Tribunal considera cumplido el deber de información previa cuando la persona trabajadora conozca la existencia de la instalación en la empresa de un sistema de control por videovigilancia «sin que haya que especificar, más allá de la mera vigilancia, la finalidad exacta que se le ha asignado a ese control».

Y los pronunciamientos anteriores nos llevan a la conclusión de que no se pueden emplear estos sistemas de videovigilancia para otras finalidades ajenas a la seguridad laboral como la efectividad del trabajo, las ausencias del puesto de trabajo o las conversaciones entre compañeros y compañeras.

En la STS de 21 de enero de 2019 (rec. 341/2017) no se analiza el motivo de recurso, pero consideramos acertado referenciar la Sentencia del Tribunal Superior de Justicia de Madrid de 18 de noviembre de 2016 recurrida y en la que los magistrados consideran que una cosa es que la empresa informe, en el propio contrato, a las personas trabajadoras de la implantación de medidas de seguridad de índole técnica y organizativa y otra que esa actuación sea equiparable al deber de información sobre recogida de datos, su objeto y finalidad. En tanto que esto no se puede admitir y que la empresa no tuviera los distintivos informativos correspondientes, por mucho que las cámaras estuvieran a la vista no se puede admitir cumplido el requisito constitucional de información a la trabajadora para proceder a la licitud del despido.

Finalidad de la videovigilancia. La prueba obtenida por videovigilancia no puede desvirtuarse por el hecho de que la persona trabajadora sea, o no, advertida expresamente de la finalidad de control de la actividad laboral y del destino que se le puedan dar a las grabaciones, siempre y cuando quede acreditado que la persona trabajadora conocía la existencia de las cámaras y la ubicación[29].

[29] ATS de 18 de septiembre de 2018 (proc. núm. 1092/2018).

Sobre la validez de la prueba resulta interesante el ATS de 5 de mayo de 2018 (proc. núm. 3202/2017), en el que se obtienen pruebas del maltrato hacia personas discapacitadas psíquicas en el cuarto de baño de una residencia tras la instalación de cámaras, si bien no se colocaron carteles informativos. El auto tiene en cuenta la reunión informativa realizada con las personas trabajadoras debido a las sospechas fundadas de maltratos por alguna de las personas cuidadoras, siendo la única forma posible para su comprobación, teniendo en cuenta que las directamente perjudicadas por dicha conducta nunca habrían podido denunciarla al tratarse de personas discapacitadas psíquicas.

El ATS de 14 de junio de 2017 (proc. núm. 4200/2016) se refiere a la validez de la prueba consistente en la reproducción de imágenes y sonidos siempre que la persona trabajadora conozca la instalación de las cámaras y su ubicación por motivos de seguridad, de manera que resulta intrascendente si la persona trabajadora ha sido, o no, advertida expresamente de la finalidad de control de la actividad laboral.

En la STS de 1 de febrero de 2017 (rec. 3262/2015), la cuestión controvertida se basa en determinar si cabe apreciar vulneración de derechos fundamentales cuando la prueba del despido se sustenta en grabaciones de vídeo realizadas por una cámara de seguridad instalada para la previsión de robos y otros delitos en la empresa y, aun así, se emplea para acreditar incumplimientos laborales; es decir, admitir como prueba las imágenes grabadas sin señalar cuál sería el uso que les daría a efectos disciplinarios. Desde luego resulta necesario que las personas trabajadoras conocieran de la existencia del sistema (bien por recibir información expresamente, bien por resultar público y notorio al no estar ocultas), siendo indiferente que la empresa las hubiera advertido sobre el destino que pudiera darles a las grabaciones o que las pudiera utilizar en su contra.

Así, argumenta la STS de 1 de febrero de 2017 que lo importante será la determinación de si los datos obtenidos se han utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al contrato, porque si la finalidad del tratamiento de los datos no guarda relación directa con el «mantenimiento, desarrollo o control de la relación contractual, el empresario estará obligado a solicitar el consentimiento de los trabajadores afectados». Esto conduce a que en estos casos donde no hay una información directa de la finalidad del control de la cámara se deba considerar la grabación como prueba lícita en tanto se trata de una medida justificada por razones de seguridad (el control de hechos ilícitos por personas empleadas, clientela o terceras personas), idónea (en este caso el fin perseguido es de control de cobros) y necesaria y proporcionada al fin perseguido, «razón por la que estaba justificada la limitación de derechos fundamentales en juego, máxime cuando los trabajadores estaban informados, expresamente, de la instalación del sistema de vigilancia, de la ubicación de las cámaras por razones de seguridad».

En esta línea, el ATS de 18 de octubre de 2016 (proc. núm. 2645/2015) se refiere a un supuesto en el que la instalación de las cámaras en la caseta de control se llevó a cabo por la empresa principal que contrató la prestación del servicio de vigilancia y seguridad y cuya finalidad era la de garantizar la seguridad de las personas y los bienes que allí se encontraban.

El vigilante era conocedor del sistema de vigilancia por cuanto se encargaba de controlar su correcto funcionamiento. Ante las quejas sobre él de varios usuarios, la empresa principal examinó las grabaciones y se constató que el vigilante se durmió en reiteradas ocasiones. Todo ello desembocó en el despido disciplinario del trabajador ajustado a derecho.

Vigilancia oculta. Por último, y que irá en conexión con lo tratado en el epígrafe siguiente, el TS en su Sentencia de 21 de julio de 2016 se refiere a la legalidad de la prueba obtenida mediante un sistema de videovigilancia oculta ante la sospecha de actividades irregulares de la trabajadora y, por tanto, sin previo conocimiento de que se estuvieran produciendo grabaciones en su puesto de trabajo. Debe advertirse que las grabaciones se realizan sobre un periodo limitado de tiempo. El TS considera que la sentencia de suplicación se acoge a la doctrina emanada de la STC 186/2000, de 11 de agosto. Además, advierte que la validez de la grabación de comportamientos irregulares sin conocimiento ni consentimiento de las personas trabajadoras afectadas depende de las circunstancias de cada caso. En este sentido, el TC ha arbitrado una doctrina en la que nos dice que la grabación es ajustada a derecho cuando concurren determinadas circunstancias y se convierte en ilícita cuando esa actuación empresarial se produce en otras condiciones diferentes.

Por todo lo anterior, desde la doctrina se entiende que debe restringirse al máximo el uso de las cámaras ocultas, relegando su uso para situaciones de gravedad y excepcionalidad (Berlanga de la Pascua, 2018).

8. La doctrina del TEDH sobre el control de las personas trabajadoras mediante sistemas de videovigilancia

En opinión de Fernández Villazón (2016), «la normativa sobre protección de datos se ha convertido en un símbolo de los altos estándares de calidad del derecho europeo y de su capacidad para imponerlos en el ámbito internacional». Ahora bien, tan importante como la existencia de esta normativa es la aplicación que se realiza de la misma por los órganos judiciales europeos. Con independencia de la existencia de numerosas sentencias emanadas del TEDH sobre la materia, consideramos hacer referencia a dos de ellas, puesto que van ligadas a la decisión de un tribunal español, suponen un cambio de criterio entre una y otra y, en definitiva, una de ellas contiene la actual doctrina del TEDH sobre el empleo de sistemas de videovigilancia para sancionar comportamientos de las personas trabajadoras.

Las circunstancias del caso se resumen en que una cadena de supermercados, con el fin de investigar y acabar con las pérdidas económicas, instala un sistema de videovigilancia compuesto por cámaras tanto visibles como ocultas. De las primeras se avisa a las trabajadoras y al comité de empresa, de las segundas no, pues enfocaban directamente sobre las cajas registradoras y con la finalidad de controlar posibles robos de personas empleadas. Tras el visionado de las cámaras ocultas se comprueba que varias cajeras habían

participado en la apropiación de diferentes productos, para ellas o terceras personas, sin pagar la mercancía, por lo que se procede a su despido. La profesora García Salas (2018) se refiere a estas cámaras ocultas como «control extraordinario».

Las trabajadoras articularon un procedimiento ante el TEDH en el que argumentaron que el empleo de sistemas de videovigilancia sin haber sido previamente informadas suponía una vulneración a su derecho a la intimidad que tienen reconocido en virtud del artículo 8 del Convenio europeo para la protección de los derechos humanos y libertades fundamentales. Además, reclamaron que el proceso había sido ilegal, puesto que la grabación constituía la prueba esencial para justificar la legalidad de los despidos.

El TEDH consideró en la Sentencia de 9 de enero de 2018 (asunto López Ribalda y otros vs. España) que la medida no era proporcional con relación a la finalidad legítima de proteger los intereses patrimoniales de la empresa, dando lugar a una revisión de la doctrina de nuestro TC en materia de videovigilancia en el trabajo (Preciado Domènech, 2018). Se rompe la proporcionalidad en cuanto a que la vigilancia se extiende durante un periodo prolongado, abarca a todas las personas trabajadoras y sin información, por lo que no se logra un equilibrio equitativo entre el derecho de las trabajadoras al respeto de su vida privada (art. 8 Convenio europeo) y el interés de la empresa en la protección de sus derechos patrimoniales. No obstante, la sentencia incorpora un voto particular que considera que el «comportamiento ofensivo es incompatible con el derecho a la vida privada en virtud del convenio», por lo que debe prevalecer el interés público de la sociedad siempre que no se realice una injerencia abusiva. En este sentido, la considera abusiva, puesto que debe prevalecer el principio general de que «no se debe permitir que los demandantes se beneficien legalmente de sus propios actos ilícitos». Se aprecia una gran similitud entre este voto particular y la fundamentación de la STC 39/2016 (Rojo Torrecilla, 2018).

La doctrina de esta sentencia de la Sección 3.ª se rectifica por la STEDH (Gran Sala) de 17 de octubre de 2019, alineándose claramente con la doctrina actual de nuestro TC (Navarro Nieto, 2019, p. 79). La Gran Sala comparte que la especificidad de las relaciones de empleo y el desarrollo de nuevas tecnologías ocasiona que se adopten medidas que a veces pueden ser intrusivas en la vida privada de las personas trabajadoras. Para evitar esto, las medidas de videovigilancia deben ser proporcionales, lo que se justifica en el análisis de una serie de factores. A saber, notificación a la persona empleada de las medidas de videovigilancia y las garantías puestas a su disposición, existencia de razones legítimas que justifiquen la videovigilancia, posibilidad de establecer medidas menos intrusivas y consecuencias de la vigilancia para la persona trabajadora sometida a ella.

El TEDH en la sentencia dictada por la Gran Sala constata la proporcionalidad de la medida en cuanto a que:

- Estaba limitada en lo que respecta a las áreas y al personal que estaba supervisando (la grabación solo al personal de caja y la grabación de las otras dos trabajadoras implicadas se produce en una zona de paso común de personas empleadas y

clientela). En este sentido, el tribunal considera que es necesario distinguir entre lugares donde la expectativa de intimidad es muy alta por ser privados (aseos) o zonas de trabajo cerradas (oficinas) y lugares donde no concurre la expectativa de intimidad.

- Respecto al tiempo, el tribunal aprecia que una duración de 10 días no es excesiva, sobre todo si finaliza en cuanto se produce la identificación de las autoras de los actos ilícitos contra el patrimonio de la empresa.
- Con relación a las consecuencias de la videovigilancia es cierto que se emplearon para el despido de las trabajadoras, pero no fueron utilizadas por la empresa para fines distintos a la localización de las responsables de las pérdidas.
- Se constata la inexistencia de otros medios para cumplir el objetivo legítimo perseguido, lo que conduce a que los sistemas de videovigilancia se consideren como necesarios.
- Respecto a la información de la instalación del sistema de vigilancia, el TEDH da por válida la existencia de carteles informadores que alertaban sobre la instalación de circuitos cerrados de televisión, y, en cualquier caso, esta información es solo uno de los criterios a tener en cuenta para evaluar la proporcionalidad de la medida. Este razonamiento supone una estrecha alineación con la doctrina establecida en la STC 39/2016, en la que el deber de información previa será considerado como vulneración del derecho fundamental a la protección de datos tras realizar el juicio de proporcionalidad al sistema de videovigilancia en el caso concreto.

En definitiva, el TEDH se mueve en un escenario conservador en la medida en que no puede aceptar que la más mínima sospecha de apropiación indebida u otras acciones ilegales por parte de las personas empleadas puede justificar la instalación de sistemas de videovigilancia, pero sí se justifica esta instalación ante la existencia de una sospecha razonable de la comisión de una falta grave o pérdidas de cantidades importantes en el volumen del negocio. Por tanto, se justifica la grabación con cámaras ocultas en el centro de trabajo por la existencia debidamente acreditada de sospechas razonables de irregularidades graves (Monereo Pérez y Ortega Lozano, 2019).

9. Conclusiones

9.1. Licitud de la prueba

Debemos admitir la licitud de la prueba siempre que la persona trabajadora conozca la instalación de las cámaras y su ubicación por motivos de seguridad. Por tanto, es importante definir que implica la responsabilidad y obligación de la empresa de garantizar la «seguridad en el centro de trabajo». Efectivamente, nos encontramos ante una expresión amplia que

incluye la posibilidad de vigilar actos ilícitos de terceras personas y de las propias personas trabajadoras, pero no puede justificarse «la seguridad» para el control de comportamientos estrictamente laborales como las ausencias del puesto, la efectividad en el trabajo o incluso las conversaciones que pudieran intercambiarse con los compañeros y compañeras de trabajo.

Esta conclusión se sostiene, además de en la doctrina judicial que la aplica, en el artículo 42.4 de la Ley 5/2014, de 4 de abril, de seguridad privada, que establece que las grabaciones realizadas por los sistemas de videovigilancia no podrán destinarse a un uso distinto del de su finalidad. Así, la finalidad es la seguridad en los términos expresados en el párrafo anterior.

La finalidad legítima en el tratamiento de datos prevista en la LOPD (art. 4.1 antigua) se apoya, en el caso de la videovigilancia laboral, en las facultades de control empresarial reconocidas en el artículo 20.3 del ET, en tanto no lleven aparejada la lesión de derechos fundamentales de las personas trabajadoras. En este sentido se permitirá la instalación de cámaras puntuales y ocultas cuando existan indicios de comportamientos antijurídicos y con base en las exigencias de la proporcionalidad, de manera que nos encontremos con una medida idónea, necesaria, proporcionada en sentido estricto y de carácter temporal. En definitiva, la utilización de estos sistemas de control se reserva a situaciones graves o muy graves y, aunque por la doctrina se sugiere que debe tratarse de delitos (Toscani Giménez, 2019), en ningún caso debe restringirse solo a la dimensión penal (Miñarro Yanini, 2019, p. 10).

9.2. Consentimiento

La imagen que se pueda captar a través de los sistemas de videovigilancia establecidos por la empresa debe considerarse como un dato personal (dato propio de la identidad de la persona); esto obliga a dar una protección sobre la base del artículo 18.4 de la CE.

Partiendo de la anterior premisa, en cuanto a dato personal, la captación y tratamiento de imágenes requiere del consentimiento de la persona interesada que se enarbola como requisito esencial de la protección (Fernández Villazón, 1994, p. 518). Sin embargo, consideramos que, en el marco de la relación laboral, no resulta necesario contar con el consentimiento de la persona trabajadora de manera previa al tratamiento o captación. Por un lado, el artículo 6.1 b) del RGPD señala que el tratamiento será válido, entre otras razones, cuando sea necesario «para la ejecución de un contrato en que el interesado es parte, una vez acordada su licitud». Por otro, la LOPDGDD, en su artículo 6.2, especifica que «no será preciso el consentimiento cuando los datos se refieran a las partes de un contrato de una relación laboral y sean necesarios para su mantenimiento o cumplimiento». De este modo queda autorizada la posibilidad de instalación de sistemas de videovigilancia y sin necesidad del consentimiento expreso de la persona trabajadora dentro del marco de obligaciones y derechos del contrato de trabajo, basándonos en los artículos mencionados en conexión con el artículo 20.3 del ET.

Debe advertirse que no resulta adecuado utilizar el artículo 9.2 b) del RGPD para justificar la ausencia de consentimiento expreso de la persona trabajadora para el tratamiento de sus datos, en la línea que realizan determinadas sentencias del TS[30]. El artículo 9 se refiere a la imposibilidad de tratamiento de determinadas categorías especiales de datos personales como aquellos que revelen información, entre otros aspectos, relativa al origen étnico, la afiliación sindical o los datos relativos a la salud. Solo podrían ser tratados, y es cierto que, sin necesidad de contar con el consentimiento de la persona trabajadora, en la medida en que sea necesario para el cumplimiento y el ejercicio de derechos específicos de la empresa o de la persona trabajadora en el ámbito del derecho laboral y de la seguridad y protección social. Explicado de una manera práctica, la empresa no tendrá derecho a tratar el dato de que una persona trabajadora está afiliada a un sindicato salvo que de su nómina se detraiga una cantidad directa en concepto de afiliación sindical. Una empresa, o mejor dicho su servicio de prevención, no tendrá derecho a saber que una persona trabajadora padece una cardiopatía salvo que el puesto de trabajo requiera de un esfuerzo extraordinario.

Y lo señalado no tiene nada que ver con el tratamiento de unos datos genéricos, no especialmente protegidos, que son el resultado de los aportados por los sistemas de videovigilancia y creados como consecuencia de la conveniencia, o no, de evaluar la decisión respecto a mantener una relación laboral en función de grado de cumplimiento de una de las partes. Si bien es cierto que, en un caso como en el otro, está justificado no contar con el consentimiento expreso de la persona trabajadora.

En definitiva, respecto al consentimiento, la persona trabajadora no está en condiciones de darlo o revocarlo, dada su posición, en la relación laboral, de dependencia frente a la empresa.

9.3. Información

El deber de información sobre la instalación y tratamiento de datos proporcionados a través de sistemas de videovigilancia forma parte esencial del derecho a la protección de datos. De este modo, se establece como el complemento indispensable vinculado a la necesidad del consentimiento de la persona trabajadora, sobre todo en los casos en los que no se haya requerido el consentimiento expreso. Por ello debe atenderse, ante una posible vulneración del artículo 18.4 de la CE, a la concurrencia de información legalmente exigible y al juicio de ponderación. El hecho de no haber dispuesto de información legalmente exigible se traducirá en las correspondientes infracciones administrativas. El hecho de no haber informado a la persona trabajadora sobre la instalación de sistemas de videovigilancia y utilizar los datos requerirá una justificación basada en la observancia del principio de proporcionalidad que se traducirá en una ponderación entre el derecho a la protección de datos y las limitaciones al mismo justificadas en el marco del cumplimiento de las

[30] STS 304/2019, de 10 de abril.

obligaciones laborales y el derecho de la empresa al ejercicio de las facultades empresariales de control y vigilancia reconocidas en el artículo 20.3 del ET.

Como consecuencia del sometimiento de la falta de información a un juicio de proporcionalidad en cada caso concreto, y en virtud de las circunstancias alegadas, nos indicará si se ha producido la omisión de la información debida. Esto dificultará la elaboración de patrones y la posibilidad de ofrecer respuestas uniformes. Lo que en la práctica se traduce en mayor conflictividad judicial esperando que cada tribunal realice una interpretación acorde a las pretensiones de una de las partes.

El conocimiento por parte de las personas trabajadoras de la ubicación de las cámaras de seguridad instaladas por «razones de seguridad» debe interpretarse como que las personas trabajadoras, así como clientela y terceras personas, se encuentran informadas sobre la vigilancia de actos ilícitos que se pueda estar produciendo en su puesto de trabajo. No obstante, esta ausencia de información no justifica otro control de las personas trabajadoras que no sea el estrictamente derivado de la seguridad laboral; rechazándose el control sobre la efectividad en el puesto de trabajo o las ausencias o de las conversaciones entre compañeros y compañeras.

En las sentencias del TS mencionadas se observa una flexibilización de la doctrina sobre la información que debe tener la persona trabajadora del sistema de videovigilancia establecida en la STC 29/2013 a raíz de la publicación de la STC 39/2016. Así es posible el uso de cámaras fijas con la finalidad de sancionar a las personas trabajadoras sin información previa en tanto la empresa justifique pérdidas.

Desde la aprobación de la LOPDGDD, nuestros tribunales no prestan atención a que el artículo 89.1 de la LOPDGDD señala, en el marco de sistemas de videovigilancia no ocultos, que, cuando se produzca la captación de un ilícito por el sistema de videovigilancia instalado por la empresa, la obligación de información se limita a la existencia del cartel informativo al que hace referencia el artículo 22.4 de la LOPDGDD; relajando significativamente la obligación de información sobre el sistema de videovigilancia.

Respecto a los defectos informativos de los sistemas de videovigilancia que pudieran alegar las personas trabajadoras que, conociendo la ubicación de las cámaras, no tenían una información expresa del control, cabe bien solicitar más información a la empresa o bien denunciar ante la AEPD, que será la responsable de sancionar por las infracciones que aprecie.

9.4. Otras cuestiones

En la instalación de estos sistemas de videovigilancia, la empresa, como responsable del fichero, no puede olvidar que la norma europea –art. 5 RGPD– la hace responsable del cumplimiento de una serie de principios (licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación e integridad

y confidencialidad), debiendo mostrar una responsabilidad proactiva que se concreta, fundamentalmente, en la necesidad de configurar el registro de la actividad de tratamiento vinculada a la autorización de las videocámaras con el contenido del artículo 30.1 del RGPD y el artículo 31 de la LOPDGDD, y de dar cumplimiento al derecho de información en los términos expresados en el artículo 13 del RGPD y el artículo 11 de la LOPDGDD.

Debe ponerse en valor el papel de los convenios colectivos que ayuden al establecimiento de normas más específicas, como reconoce el artículo 88 del RGPD, para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de las personas trabajadoras en el ámbito laboral.

Finalmente, no puede resultarnos ajeno que los sistemas de videovigilancia no son más que la versión moderna de la clásica tensión, existente desde los orígenes del derecho del trabajo, entre poder de dirección de la empresa y los derechos de las personas trabajadoras. En este contexto, la aprobación de normas e interpretaciones judiciales de las mismas serán los factores moduladores de tracción entre las partes de la relación laboral. Y solo así se verán reforzados los derechos de las personas trabajadoras y se garantizará que las medidas de control empleadas por la empresa se usen con plena garantía de licitud en cuanto que respetarán los derechos fundamentales de las personas trabajadoras. No se trata de que el artículo 20.3 del ET se use de manera torticera para limitar los derechos fundamentales de las personas trabajadoras ni de que la aplicación de la LOPDGDD permita que las personas trabajadoras encuentren amparo para la comisión de actos ilícitos.

Referencias bibliográficas

Altés Tárrega, Juan Antonio. (2020). La videovigilancia encubierta en la nueva regulación sobre derechos digitales laborales y la incidencia de la STEDH López Ribalda II. *Revista General de Derecho del Trabajo y de la Seguridad Social*, *55*.

Álvarez Alonso, Diego. (2013). Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: Sentencia TC 98/2000, de 10 de abril. En Joaquín García Murcia (Dir.), *Derecho del trabajador y libertad de empresa. 20 casos de jurisprudencia constitucional* (1.ª ed., pp. 338-378). Thomson Reuters Aranzadi.

Arrabal Platero, Paloma. (2015). La videovigilancia laboral cómo prueba en el proceso. *Revista General de Derecho Procesal*, *37*.

Berlanga de la Pascua, Carlos. (25 de septiembre de 2018). Los límites de la videovigilancia laboral. *ElDerecho.com*. https://elderecho.com/los-limites-la-videovigilancia-laboral.

Chacartegui Jávega, Consuelo. (2018). Videovigilancia en el lugar de trabajo y «expectativa razonable de privacidad» según el Tribunal Europeo de Derechos Humanos. Comentario a la Sentencia de 9 de enero de 2018 (caso López Ribalda contra España). *Revista de Derecho Social*, *83*, 119-132.

Cruz Villalón, Jesús. (2019). Las facultades de control del empleador ante los cambios organizativos y tecnológicos. *Temas Laborales. Revista Andaluza de Trabajo y Bienestar Social*, *150*, 13-44.

Desdentado Bonete, Aurelio y Muñoz Ruiz, Ana Belén. (2014). Trabajo, videovigilancia y controles informáticos: un recorrido por la jurisprudencia. *Revista General de Derecho del Trabajo y de la Seguridad Social*, *39*.

Fernández Villazón, Luis Antonio. (1994). Tratamiento automatizado de datos personales en los procesos de selección de trabajadores. *Relaciones Laborales. Revista Crítica de Teoría y Práctica*, *1*, 510-538.

Fernández Villazón, Luis Antonio. (1996). Los derechos de los trabajadores frente al tratamiento de datos personales. Comentario a la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. *Relaciones Laborales. Revista Crítica de Teoría y Práctica*, *2*, 1.178-1.209.

Fernández Villazón, Luis Antonio. (2003). *Las facultades empresariales de control de la actividad laboral*. (1.ª ed.). Thomson Reuters Aranzadi.

Fernández Villazón, Luis Antonio. (2016). El nuevo Reglamento Europeo de Protección de Datos. *Foro. Revista de Ciencias Jurídicas y Sociales*, *1*, 395-411.

Gallardo Moya, Rosario. (2017). Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Bărbulescu II c. Rumania. *Revista de Derecho Social*, *79*, 141-156.

García Rubio, María Amparo. (17 de junio de 2016). Nueva doctrina constitucional sobre videovigilancia laboral y protección de datos personales. *ElDerecho.com*. https://elderecho.com/nueva-doctrina-constitucional-sobre-videovigilancia-laboral-y-proteccion-de-datos-personales.

García Salas, Ana Isabel. (2018). El deber empresarial de informar acerca de la videovigilancia ejercida sobre los trabajadores. Comentario a la STEDH de 9 de enero de 2018. *Revista de Información Laboral*, *2*, 117-147.

García-Perrote Escartín, Ignacio y Mercader Uguina, Jesús Rafael. (2017). La protección de datos se come a la intimidad: la doctrina de la Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Bărbulescu v. Rumania; n.º 61496/08; Gran Sala). *Revista de Información Laboral*, *10*, 7-12.

Goñi Sein, José Luis. (2017). Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016. *Revista de Derecho Social*, *78*, 15-42.

Grupo de Trabajo del artículo 29. (2017). Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de 8 de junio. WP249/17.

Gude Fernández, Ana María. (2015). La videovigilancia en el ámbito laboral y el derecho a la intimidad. *Revista General de Derecho Constitucional*, *20*.

Lahera Forteza, Jesús. (2016). Nueva jurisprudencia constitucional en la videovigilancia laboral. Valoración crítica (STC 39/2016, 3 de marzo). *Derecho de las Relaciones Laborales*, *5*, 494-499.

Miñarro Yanini, Margarita. (2019). La «Carta de derechos digitales» de los trabajadores ya es ley: menos claros que oscuros en la regulación. *Revista de Trabajo y Seguridad Social. CEF*, *430*, 5-14.

Molina Navarrete, Cristóbal. (2018). De «Bărbulescu II» a «López Ribalda»: ¿qué hay de nuevo en la protección de datos de los trabajadores? Comentario a la Sentencia del Tribunal Europeo de Derechos

Humanos de 9 de enero de 2018, caso López Ribalda «et alii» vs. España (Demandas acumuladas 1874/13 y 8567/13). *Revista de Trabajo y Seguridad Social. CEF*, *419*, 125-135.

Molina Navarrete, Cristóbal. (2019). Control tecnológico del empleador y derecho probatorio: efectos de la prueba digital lesiva de derechos fundamentales. *Temas Laborales. Revista Andaluza de Trabajo y Bienestar Social*, *150*, 331-354.

Molina Navarrete, Cristóbal y Olarte Encabo, Sofía. (1999). Los derechos de la persona del trabajador en la jurisprudencia del Tribunal Constitucional. *Relaciones Laborales. Revista Crítica de Teoría y Práctica*, *2*, 359-386.

Monereo Pérez, José Luis y Ortega Lozano, Pompeyo Gabriel. (2019). Se justifica la grabación con cámaras ocultas en el centro de trabajo por la existencia debidamente acreditada de sospechas razonables de irregularidades graves. STEDH (Gran Sala) de 17 de octubre de 2019 (números 1874/13 y 8567/13) (asunto López Ribalda II). *Revista de Jurisprudencia Laboral*, *8*.

Navarro Nieto, Federico. (2019). Las facultades de control a distancia del trabajador: videovigilancia y grabación del sonido. *Temas Laborales. Revista Andaluza de Trabajo y Bienestar Social*, *150*, 71-89.

Pascual Caballero, Juan. (2017). El uso de las cámaras de videovigilancia a través de la jurisprudencia: una sistematización necesaria para delimitar el canon constitucional requerido para su validez. *Foro Español de Laboralistas (FORELAB).* https://forelab.com/wp-content/uploads/videovigilancia-juan-pascual-caballero.pdf.

Preciado Domènech, Carlos Hugo. (2017). La vídeo vigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal. ¿Es acorde la doctrina del TC y del TS con el Derecho de la UE? *Revista de Derecho Social*, *77*, 175-194.

Preciado Domènech, Carlos Hugo. (2018). Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalta y otras c. España. *Revista de Información Laboral*, *1*, 41-53.

Rodríguez Escanciano, Susana. (2018). El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679. *Revista de Trabajo y Seguridad Social. CEF*, *423*, 19-62.

Rojo Torrecilla, Eduardo. (2018). Derecho del trabajador a la privacidad en la empresa y límites a su control por cámaras de vigilancia. Estudio del caso López Ribalda y otras contra España (a propósito de la Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018). *Derecho de las Relaciones Laborales*, *2*, 135-152.

Sepúlveda Gómez, María. (2016). Poder de control empresarial mediante cámaras de videovigilancia y derecho de los trabajadores a la protección de datos personales. *Temas Laborales. Revista Andaluza de Trabajo y Bienestar Social*, *133*, 219-235.

Terradillos Ormaetxea, Miren Edurne. (2017). El principio de proporcionalidad como referencia garantista de los derechos de los trabajadores en las últimas sentencias del TEDH dictadas en materia de ciberderechos: un contraste con la doctrina del Tribunal Constitucional español. *Revista de Derecho Social*, *80*, 139-162.

Toscani Giménez, Daniel. (2019). La videovigilancia de los trabajadores con cámaras ocultas o clandestinas. *Trabajo y Derecho. Nueva Revista de Actualidad y Relaciones Laborales*, *60*, 69-74.

Valdés Dal-Ré, Fernando. (2017). Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa. *Revista de Derecho Social*, *79*, 15-35.