El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización

Raquel Aguilera Izquierdo

Profesora titular de Derecho del Trabajo y de la Seguridad Social.
Universidad Complutense de Madrid

Extracto

Este estudio tiene por objeto analizar, desde el punto de vista laboral, los principios que regulan la protección de datos según la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, y 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. Asimismo, se analizan los problemas que se plantean en la práctica entre el derecho a la protección de datos y el control empresarial en los supuestos de uso de cámaras de videovigilancia y de sistemas de geolocalización, con especial atención a lo dispuesto sobre esta materia por la jurisprudencia.

Palabras clave: protección de datos; control empresarial; videovigilancia; geolocalización.

Fecha de entrada: 11-06-2019 / Fecha de revisión: 05-12-2019 / Fecha de aceptación: 05-12-2019

Cómo citar: Aguilera Izquierdo, R. (2020). El derecho a la protección de datos en el ámbito laboral. Los sistemas de videovigilancia y geolocalización. *Revista de Trabajo y Seguridad Social. CEF*, *442*, 93-134.

The right to data protection in the workplace. The video surveillance and geolocation systems

Raquel Aguilera Izquierdo

Abstract

The aim of this study is to analyze, from the labor point of view, the principles that regulate data protection according to the Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights, and the Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Likewise, the problems that arise in practice between the right to data protection and business control in the cases of use of video surveillance cameras and geolocation systems are analyzed, with special attention to the provisions on this matter by the jurisprudence.

Keywords: data protection; business control; video surveillance; geolocation.

Citation: Aguilera Izquierdo, R. (2020). The right to data protection in the workplace. The video surveillance and geolocation systems. *Revista de Trabajo y Seguridad Social. CEF*, *442*, 93-134.

Sumario

1. El ámbito de aplicación de la Ley orgánica de protección de datos y del Reglamento europeo 2016/679: los conceptos de fichero y de tratamiento y sus responsables

La protección de datos se concibe en nuestra Constitución como un instrumento de garantía de otros derechos fundamentales, la intimidad y el honor, pero también como un instituto que es en sí mismo un derecho o libertad fundamental[1]. Nos encontramos, por tanto, ante un derecho fundamental específico que coexiste con la función de garantía instrumental de otros derechos.

El contenido del derecho fundamental a la protección de datos:

> […] consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso (STC 292/2000, de 30 de noviembre, FJ 7.º).

En España:

> […] el proceso de construcción de un derecho fundamental a la protección de datos personales ha sido el resultado de la evolución de la doctrina constitucional que, en un juego sucesivo de adelantamientos sobre la acción legislativa, empieza a tutelar la protección frente al tratamiento automatizado de los datos al amparo del artículo 18.1 CE cuando el legislador no había cumplido, todavía, el mandato del artículo 18.4 CE, para luego adelantarse de nuevo a la acción legislativa proclamando un derecho fundamental específico en el año 2000 (Desdentado y Muñoz, 2012, p. 86).

Así, el derecho a la protección de datos se regula inicialmente por la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos. Como consecuencia de la aprobación de la Directiva 95/46/CE, la Ley 5/1992 fue derogada y sustituida por la Ley orgánica 15/1999, de 11 de diciembre, de protección de datos de carácter personal (LOPD/1999).

[1] Hasta la publicación de la Sentencia 254/1993, el Tribunal Constitucional (TC) concebía la protección de datos como una función exclusivamente de garantía del derecho a la intimidad (véanse, SSTC 110/1984 y 142/1993).

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos[2], ha sido derogada por 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 (RGPD). Este reglamento pretende superar, con su eficacia directa, los obstáculos que han impedido lograr la finalidad armonizadora de la Directiva 95/46/CE. En efecto, la trasposición de la directiva por los Estados miembros ha dado lugar a una variada regulación normativa que ha provocado un tratamiento fragmentado de la protección de datos en el territorio de la Unión. Con la finalidad de terminar con esa dispersión, el reglamento revisa las bases legales del modelo europeo de protección.

Este reglamento es directamente aplicable en cada Estado miembro desde el 25 de mayo de 2018. Ahora bien, el reglamento concede un cierto margen de maniobra a los Estados y en determinadas materias requiere una legislación nacional de aplicación. De este modo, en nuestro país, la adaptación al RGPD ha provocado la aprobación de una nueva ley orgánica de protección de datos, la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPD/2018) (BOE de 6 de diciembre de 2018). El objeto de la nueva ley orgánica de protección de datos, según señala su artículo 1, es doble: adaptar el ordenamiento jurídico español al RGPD y garantizar los que la norma denomina «derechos digitales de la ciudadanía» conforme al mandado establecido en el artículo 18.4 de la Constitución española (CE).

En consecuencia, el derecho a la protección de datos personales se ejercerá con arreglo a lo dispuesto en el RGPD y en esta ley orgánica. Así, a diferencia de la LOPD/1999, la nueva ley, al remitirse al reglamento comunitario, es mucho más concreta, de manera que, a efectos de definiciones o de determinar los principios rectores en esta materia, debemos remitirnos a lo dispuesto en dicho reglamento, pues la ley solo pretende completar sus disposiciones. Por otro lado, y como novedad, la ley incluye un capítulo específico, el capítulo X, dedicado a los denominados «derechos digitales», que fue introducido tras el debate a que durante más de 1 año fue sometido el proyecto de ley orgánica de protección de datos, de manera que en la primera versión del proyecto (publicada en el BOCG de 24 de noviembre de 2017) no se hacía ninguna referencia a dichos derechos. Este capítulo cobra una gran trascendencia desde el punto de vista laboral, pues, como analizaremos en el epígrafe 3, establece distintas reglas en relación con el control empresarial a través de las nuevas tecnologías, lo que venía siendo una demanda en los últimos años en búsqueda de una mayor seguridad jurídica en esta materia.

[2] La regulación europea se completa con el reconocimiento del derecho a la protección de datos de carácter personal en la Carta de los Derechos Fundamentales de la Unión Europea (art. 8).

El RGPD se aplica «al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero» (art. 2.1). Por datos de carácter personal se entiende cualquier información sobre una persona física identificada o identificable (art. 4.1). El concepto no puede ser más amplio y está integrado por dos elementos: a) el dato en sí, que es la información numérica, alfabética, gráfica… susceptible de recogida, registro, tratamiento o transmisión, y b) la relación del dato con la persona física «entendida dicha relación no como necesaria identificación actual, sino como una posibilidad real de identificación» (Vizcaíno, 2001, p. 72)[3]. En este sentido, señala el artículo 4.1 del RGPD que:

> […] se considerará 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.

El RGPD y la LOPD/2018, al igual que hacía la LOPD/1999, exigen para desplegar sus efectos protectores que estemos en presencia de datos de carácter personal. La jurisprudencia ha señalado que las opiniones y valoraciones que se realizan sobre una persona no son datos personales en el sentido expresado en la ley. Como se indica en la Sentencia de la Audiencia Nacional (SAN), Sala de lo Contencioso-Administrativo, de 22 de enero de 2010:

> El artículo 3 a) LOPD define los datos de carácter personal como «cualquier información concerniente a personas físicas identificadas o identificables» y por información hemos de entender la puesta en conocimiento de hechos de naturaleza objetiva referidos a una persona pero no las opiniones o juicios que puedan realizarse sobre ella ya que estas opiniones o juicios conllevan siempre una estimación subjetiva y por tanto cuestionable.

El registro en el que se recoge y almacena el conjunto de datos que integra la información es el fichero y, por su parte, el tratamiento de datos es «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no» (art. 4 RGPD).

Es, por tanto, necesario que el dato se haya incorporado a un fichero de datos personales y que sea susceptible de tratamiento. La existencia de un «tratamiento» junto a la existencia de un «fichero», sea automatizado o no, es condición inexcusable para la aplicación de los principios de protección contenidos en el RGPD.

[3] El artículo 3 a) de la LOPD/1999 entendía por datos de carácter personal cualquier información «concerniente a personas físicas identificadas o identificables», por tanto, las reflexiones que sobre este precepto han sido elaboradas por la doctrina siguen siendo válidas para la regulación actual.

No basta, sin embargo, la realización de una de las actuaciones señaladas en el reglamento en relación con datos personales para que esta norma despliegue sus efectos protectores y sus garantías y derechos del afectado. Es preciso algo más: que las actuaciones de recogida, estructuración, conservación, etc. se realicen de forma automatizada, o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a un fichero. Todo fichero de datos exige para tener esta consideración una estructura u organización con arreglo a criterios determinados[4]. Por ello, el mero acúmulo de datos sin criterio alguno no podrá tener la consideración de fichero a los efectos de la ley y del reglamento.

Junto a los conceptos de fichero y de tratamiento, resulta necesario, a los efectos de interpretar la LOPD/2018 y el RGPD, partir también de los conceptos de «responsable del tratamiento» y «encargado del tratamiento». La LOPD/1999 hablaba de responsable del fichero en lugar de responsable del tratamiento, pero en la práctica sus funciones son las mismas. El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento (art. 4 RGPD)[5]. Por su parte, encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (art. 4 RGPD).

La figura del responsable del tratamiento se conecta, pues, en la LOPD/2018 con el poder de decisión sobre la finalidad, contenido y uso del tratamiento. En el ámbito laboral, el empresario será, normalmente, el responsable del tratamiento, si bien pueden existir otros responsables, como los representantes de los trabajadores o los servicios de prevención (Desdentado y Muñoz, 2012, p. 95). El encargado del tratamiento será generalmente un tercero que tratará los datos personales siguiendo las instrucciones del responsable, en cuyo caso a dicho tercero le serán aplicables las reglas del artículo 28 de la LOPD/2018.

Por último, hay que tener en cuenta que otro criterio que determina el ámbito de aplicación de la LOPD/2018 es el ámbito territorial. La LOPD/1999 era aplicable al tratamiento de datos personales efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento cuando el establecimiento se encontraba ubicado en territorio español y el responsable del tratamiento tenía su domicilio social en otro Estado miembro (SAN, Sala de lo Contencioso-Administrativo, de 2 de diciembre de 2014).

[4] El artículo 4 del RGPD señala que se entenderá por fichero: «todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica».

[5] Según establecía el artículo 3 d) de la LOPD/1999, responsable del fichero es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

El RGPD ha ampliado el ámbito de aplicación territorial. Así, el ámbito de aplicación del nuevo reglamento afecta a cualquier empresa que gestione datos personales de ciudadanos de la Unión Europea (UE), y no solo a aquellas que forman parte de la UE. De esta manera, aunque la empresa no se encuentre ubicada en territorio español, si los trabajadores prestan servicios para dicha empresa desde España, será de aplicación lo dispuesto en el citado reglamento y en la normativa nacional a efectos de protección de datos.

Por su parte, el artículo 19 de la vigente LOPD considera lícito el tratamiento de los datos de contacto y, en su caso, los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica, siempre que se cumplan los siguientes requisitos: que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional y que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios. La LOPD/2018 se refiere, por tanto, a los datos necesarios para su localización profesional, esto es, los destinados –específicamente– a la actividad profesional del trabajador y que han de ser los proporcionados por la empresa para el desarrollo de la actividad laboral del empleado; no los particulares de que los trabajadores pudieran disponer.

2. Principios de la protección de datos y derechos de las personas con especial incidencia en el ámbito laboral

El capítulo II del RGPD y el título II de la LOPD regulan los principios de protección de datos. De entre los principios enumerados, desde un punto de vista laboral, gozan de especial relevancia el relativo a la exactitud de los datos y al consentimiento para el tratamiento de los datos. Directamente relacionado con el consentimiento está el deber de información, pues sin información no puede haber consentimiento. La LOPD/1999 recogía el deber de información entre los principios de la protección de datos, sin embargo, la LOPD/2018, siguiendo lo dispuesto en el RGPD, no lo enumera entre los principios, sino que regula este deber en el título III de la ley relativo a los derechos de las personas.

2.1. La exactitud de los datos

El RGPD, en su artículo 5, señala que los datos personales serán tratados de manera lícita, leal y transparente; recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; y exactos y, si fuera necesario, actualizados. El artículo 4 de la LOPD/2018 se remite a dicho precepto. Por su parte, la LOPD/1999, para referirse a este principio, utilizaba la denominación genérica de «calidad de los datos» (art. 4).

La aplicación de los datos a la finalidad para la que fueron pedidos constituye un principio básico de la protección de datos, y así lo ha señalado el TC en su Sentencia 39/2016, de 6 de marzo. Como recuerda la citada sentencia:

> […] debe existir […] una relación directa entre la finalidad que justifica el fichero y los datos personales que se recaban y que afectan a los derechos de las personas. Además, de conformidad con el apartado 2 del citado artículo 4 LOPD, «los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos». La utilización de un fichero para finalidades incompatibles representa una vulneración del principio de calidad, así como del principio de consentimiento e información (FJ 3.º).

En el artículo 5 del RGPD se señala bajo qué condiciones y en qué supuestos específicos pueden ser recogidos y sometidos a tratamiento los datos de carácter personal, estableciéndose las características que han de reunir la recogida y el tratamiento de los mismos. Los datos de carácter personal recogidos deben ser adecuados y pertinentes, como ya señalaba la LOPD/1999. Para la doctrina judicial, el principio de pertinencia:

> […] exige que los datos sean apropiados, estén relacionados con el fin perseguido, por lo que deben ser «adecuados» y no exceder de los fines para los que se han registrado, es decir, deben «servir» o ser relevantes para la finalidad para la que se obtienen, de forma que exista una clara conexión entre la información que se recaba y el objetivo para el que se solicitó (Sentencia del Tribunal Superior de Justicia –STSJ– de Asturias, Sala de lo Contencioso-Administrativo, de 12 de septiembre de 2005, rec. 393/1999).

Como hemos señalado, el artículo 5 del RGPD, reproduciendo la Directiva 95/46/CE y tal y como ya señalaba el artículo 4.2 de la LOPD/1999, prevé que los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. El RGPD, como la LOPD/1999, habla de finalidades incompatibles y no de finalidades distintas como hacía la Ley orgánica de protección de datos de 1992. Esta diferencia provocó en su momento distintas interpretaciones doctrinales. La norma dice que los datos no pueden utilizarse para finalidades incompatibles, con lo que queda la duda de si pueden utilizarse para finalidades distintas o diferentes, pero no necesariamente incompatibles (Troncoso, 2010, p. 328; Vizcaíno, 2001, p. 93). Estas dudas han sido resueltas por la doctrina judicial al entender que la norma utiliza el término «incompatibles» como sinónimo de «distintas» o «diferentes»[6].

[6] SAN, Sala de lo Contencioso-Administrativo, de 11 de febrero de 2004 (rec. 119/2002). En el mismo sentido, SAN, Sala de lo Contencioso-Administrativo, de 16 de junio de 2011 (rec. 314/2010).

En el ámbito laboral, la STC 11/1998[7] declaró que vulneraba el artículo 28.1 de la CE en relación con el artículo 18.4 de la CE la conducta empresarial consistente en utilizar los datos de afiliación de los trabajadores para una finalidad distinta de aquella para la que dichos datos habían sido facilitados. La afiliación del trabajador recurrente a determinado sindicato se facilitó con la única y exclusiva finalidad lícita de que la empresa descontara de la retribución la cuota sindical y la transfiriera al sindicato, de acuerdo con lo establecido en el artículo 11.2 de la Ley orgánica de libertad sindical. Sin embargo, el dato fue objeto de tratamiento automatizado y se hizo uso de la correspondiente clave informática para un propósito radicalmente distinto: retener la parte proporcional del salario relativa al periodo de huelga.

En este mismo sentido, se ha considerado que vulnera el derecho a la protección de datos la aportación por la empresa como prueba documental de un listado de afiliados a un sindicato, sin estar autorizada a ello, y del que disponía con la finalidad de proceder al descuento de la cuota sindical[8].

Por lo que se refiere a la adecuación y pertinencia de los datos a la que alude el RGPD, como también lo hacía la LOPD/1999, estas exigencias se refieren a la idoneidad del dato para lograr la finalidad para la que ha sido recogido, por ello el reglamento europeo señala con claridad que los datos solicitados deben ser limitados a lo necesario en relación con los fines para los que son tratados. La aplicación de este principio puede apreciarse con claridad en el Auto del TC (ATC) 29/2008, que analiza la negativa de la Tesorería General de la Seguridad Social al envío masivo de datos solicitados por el sindicato CC. OO., que consideraba necesario disponer de los mismos para el mejor desenvolvimiento de su labor de defensa de los derechos e intereses legítimos de los funcionarios públicos. Para el TC, al denegar la cesión de los datos personales que les fueron solicitados, los poderes públicos han satisfecho la obligación que recae sobre ellos de proceder al tratamiento de los datos personales contenidos en los ficheros públicos con las debidas garantías. Como se indica en el ATC 29/2008:

> La solicitud formulada no solo era desproporcionada y no contemplada por el legislador, sino que además tampoco la petición cursada había obedecido a una necesidad debidamente justificada sobre la que sustentar un pedido que llegara a recabar tal conocimiento masivo de los datos como el interesado, para el ejercicio del derecho de actividad sindical, que tampoco se había especificado en qué sentido pretendía llevarse a efecto (FJ 6.º).

[7] A esta sentencia siguieron las SSTC 33/1998, 35/1998, 45/1998, 60/1998, 77/1998, 94/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 125/1998, 126/1998, 158/1998, 198/1998, 223/1998 y 44/1999.

[8] Sentencia del Tribunal Supremo (STS) de 8 de abril de 2014 (rec. 19/2013).

2.2. El consentimiento y el deber de información

El principio clave en materia de protección de datos es el consentimiento del afectado. De conformidad con el artículo 4.11 del RGPD, reproducido en el artículo 6 de la LOPD/2018, se entiende por consentimiento del afectado «toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen».

La novedad del RGPD frente a la LOPD/1999 es que especifica solo dos formas de expresar el consentimiento, mediante una declaración o mediante una acción afirmativa. Por lo tanto, no cabe el llamado consentimiento tácito (Adsuara, 2016, p. 152)[9]. Ahora bien, la propia norma prevé una serie de excepciones a este deber y, por lo que al ámbito laboral se refiere, el artículo 6 del RGPD señala que el tratamiento será lícito, sin necesidad de consentimiento, si «es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales»[10]. En este sentido, puede afirmarse, como hace el TS en su Sentencia de 10 de abril de 2019 (rec. 227/2017), que la nueva normativa flexibiliza y hace más clara la aplicación del principio de consentimiento del interesado.

En el ámbito laboral, como indica la STC 39/2016:

> […] el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes. […]
>
> La dispensa del consentimiento se refiere, así, a los datos necesarios para el mantenimiento y cumplimiento de la relación laboral, lo que abarca, sin duda, las obligaciones derivadas del contrato de trabajo. Por ello un tratamiento de datos dirigido al control de la relación laboral debe entenderse amparado por la excepción citada, pues está dirigido al cumplimiento de la misma. Por el contrario, el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato (FJ 3.º).

La excepción abarca, por tanto, según la jurisprudencia constitucional, el mantenimiento, desarrollo o control de la relación laboral.

[9] El consentimiento se definía por la LOPD/1999, artículo 3 h), como «toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen».

[10] El artículo 6.2 de la LOPD/1999 ya establecía que no será preciso el consentimiento cuando los datos se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

La utilización de un fichero para finalidades incompatibles representa una vulneración del principio de exactitud de los datos, pero también del principio de consentimiento e información. De hecho, como recuerda la STC 39/2016:

> […] el Real Decreto 1720/2007 regula expresamente la solicitud del consentimiento del interesado para el tratamiento de sus datos personales en el marco de una relación contractual para fines no relacionados directamente con la misma. Así, se establece que «si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos» (art. 15). Por lo tanto, solo cuando la finalidad del tratamiento de datos no sea el mantenimiento, desarrollo y control de la relación contractual se necesita consentimiento del afectado (FJ 3.º).

Por lo que se refiere al deber de información, como ya hemos señalado, la LOPD/1999 lo consideraba un principio de la protección de datos, sin embargo, el RGPD y la LOPD/2018 lo incluyen entre lo que denominan «derechos de las personas». En cualquier caso, a pesar de esta diferente consideración del deber de información en la nueva regulación, hay que entender que el deber de información sigue formando parte del contenido esencial del derecho a la protección de datos independientemente de que se requiera o no el consentimiento del afectado. Como señala el TC, aunque no sea necesario el consentimiento:

> […] el deber de información sigue existiendo, pues este deber permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o, en su caso, del representante. El deber de información previa forma parte del contenido esencial del derecho a la protección de datos, pues resulta un complemento indispensable de la necesidad de consentimiento del afectado (STC 39/2016, FJ 3.º).

El deber de información ha planteado numerosos problemas prácticos en materia laboral desde el punto de vista del control empresarial a los que haremos referencia en el epígrafe correspondiente.

Un supuesto particular, relacionado con el deber de consentimiento y el deber de información, que merece una mención especial por la trascendencia práctica que tiene en el ámbito laboral, es la comunicación o cesión de datos a un tercero.

Constituye cesión o comunicación de datos toda revelación de datos realizada a una persona distinta del interesado. El artículo 11 de la LOPD/1999 exigía dos condiciones para que la comunicación de datos a un tercero se pudiese llevar a cabo: en primer lugar, que se tratase del cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario y, en segundo lugar, que contase con el previo consentimiento

del interesado. El artículo 11 de la LOPD/1999 ha sido uno de los preceptos de la ley que se ha prestado a mayores dudas interpretativas.

La LOPD/2018 no contiene ningún precepto que se refiera expresamente a la cesión de datos a un tercero, pero de lo dispuesto en el RGPD parece derivarse que en la actualidad ya no es necesario el consentimiento del interesado para ceder datos a un tercero, pero sí el deber de información, del que indirectamente deriva el consentimiento. En efecto, el artículo 6.1 f) del RGPD señala que el tratamiento de datos será lícito si «el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero». Por su parte, el artículo 14 del RGPD prevé la información que debe facilitarse al interesado cuando los datos personales no se hayan obtenido directamente de él, es decir, cuando se hayan obtenido de un tercero. Por lo tanto, el deber de información se exige en estos casos. Y, por último, el artículo 21.1 del RGPD señala que el interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6.1 f).

De este modo, en la regulación actual, cabe la cesión de datos a un tercero debiendo el responsable del tratamiento informar al interesado de los fines del tratamiento a que se destinan los datos personales. No es necesario el consentimiento expreso de este, que se entenderá concedido si no ejerce su derecho de oposición.

En materia laboral son muy variados los supuestos en los que la jurisprudencia se ha planteado si la cesión o comunicación de datos a un tercero constituye una vulneración de los principios de la protección de datos. Entre dichos supuestos podemos destacar, a modo de ejemplo, los siguientes:

1. El primero –SAN de 15 de junio de 2017 (rec. 137/2017) y STS de 10 de abril de 2019 (rec. 227/2017) que casa y anula la anterior– resuelve el conflicto colectivo planteado por varios sindicatos contra la empresa Unisono, empresa de *contact center*, que en sus contratos de trabajo incluye habitualmente una cláusula tipo que dice lo siguiente:

> El trabajador consiente expresamente, conforme a la LO 1/1982, de 5 de mayo, RD 1720/2007 de protección de datos de carácter personal y Ley orgánica 3/1985, de 29 de mayo, la cesión de su imagen, tomada mediante cámara web o cualquier otro medio, siempre con el fin de desarrollar una actividad propia de *telemarketing* y cumplir, por tanto, con el objeto del presente contrato y los requerimientos del contrato mercantil del cliente.

La empresa demandada defiende la generalización de la cláusula controvertida en los contratos de trabajo, porque la captación de imágenes de los trabajadores es absolutamente imprescindible para la ejecución de sus contratos de tra-

bajo, cuando los clientes requieren servicios de videollamada, que es uno de los supuestos reflejados en el ámbito funcional del convenio, en el que se contempla como herramienta para contactar con terceros en entornos multimedia, lo cual, a su juicio, les exime, incluso, de requerir ningún tipo de consentimiento.

Para la SAN de 15 de junio de 2017, es totalmente legítimo que la empresa exija a sus trabajadores la realización de servicios de videollamada, cuando el servicio pactado con el cliente lo requiera, lo cual comportará necesariamente que entre en juego la imagen de los trabajadores afectados, puesto que, si no cedieran su imagen, no podría activarse la videollamada con terceros. «Ahora bien, el hecho de que sea necesaria la cesión de la imagen de los trabajadores para la realización de este tipo de servicios no exime del consentimiento expreso de los trabajadores, puesto que los servicios de videollamada» resultan excepcionales en la empresa. La AN considera que cuando la empresa destine a sus trabajadores a la realización de servicios de videollamada, porque lo requiera así el contrato mercantil con el cliente, deberá solicitar, en ese momento, el consentimiento del trabajador, que deberá ajustarse de manera precisa y clara a los requerimientos de cada contrato, sin que sea admisible la utilización de cláusulas tipo de contenido genérico, que no vayan asociadas a servicios concretos, requeridos por contratos específicos, por cuanto dicha generalización deja sin contenido real el derecho a la propia imagen de los trabajadores, que queda anulado en la práctica, aunque se diera consentimiento genérico al formalizar el contrato.

Contra esta sentencia interpuso recurso de casación la empresa, que fue estimado por la STS (Sala de lo Social) de 10 de abril de 2019. Para el TS, la actividad de quienes son contratados para prestar los servicios de *contact center* incluye las videollamadas, cuando ello sea necesario para la prestación de un mejor servicio o por exigencias del cliente:

> Consiguientemente, si se trata de la realización de funciones propias del objeto del contrato celebrado, aunque no sean las habituales, es lo cierto que la cláusula controvertida se limita a advertir al nuevo contratado de la posibilidad de tener que realizar una de las funciones propias del contrato que suscribe y, a la par que el mismo queda advertido de ello, presta, expresamente, su consentimiento a la cesión de su imagen, pero con una salvaguarda: «siempre con el fin de desarrollar una actividad propia de *telemarketing* y cumplir, por tanto, con el objeto del presente contrato», esto es que la cesión de la imagen, el dato, venga condicionada a que su fin sea cumplir con el objeto del contrato (FJ 2.º 3).

De este modo, concluye que la cláusula controvertida no es abusiva, sino, más bien, informativa, y a la vez receptora de un consentimiento expreso que no era preciso requerir, conforme a lo dispuesto en los artículos 6.1 b), 7 y 9.2 b) del RGPD. Para el TS, estos preceptos nos muestran que el consentimiento no es

necesario prestarlo hoy día, ni tampoco lo era conforme a la normativa anterior, cuando los datos, la imagen, se ceden en el marco del cumplimiento de un contrato de trabajo cuyo objeto lo requiere.

2. La segunda sentencia –SAN de 11 de diciembre de 2017– hace referencia a un supuesto de cesión de datos a terceros autorizado por la ley en materia de planes y fondos de pensiones. Se plantea en dicha sentencia si vulnera o no el derecho a la protección de datos la obligación de la empresa de entregar a la comisión de control del plan de pensiones el fichero mensual con las aportaciones de los partícipes, en el que se incluya el NIF de los partícipes junto con los datos salariales de los mismos, como única forma de llevar a cabo por la misma la supervisión y control a la que viene obligada por la Ley de planes y fondos de pensiones.

   La protección de datos alcanza a la protección de los datos relativos a la retribución, como ha señalado el ATC 29/2008, y al DNI, en virtud de lo previsto en el artículo 3 a) de la LOPD/1999. La revelación de estos datos supone una comunicación de datos a una persona distinta del interesado y, por tanto, según el artículo 11.1 de la LOPD/1999, se exige su consentimiento. Ahora bien, la cesión de información a la comisión de control está autorizada por la ley, de manera que no será necesario el consentimiento. La comisión de control puede ser usuario autorizado para acceder a la información necesaria para el ejercicio de sus funciones, si bien la cesión de datos debe realizarse estrictamente para el desempeño de la función supervisora, quedando obligados sus miembros al deber de confidencialidad.

3. Asimismo, se ha declarado que no constituye vulneración del derecho a la protección de datos ni del derecho a la intimidad la cesión de datos al perito externo a la mutua cuando se trata de datos correspondientes a la evolución de la lesión de un trabajador, pues la mutua debe hacerse cargo de las consecuencias derivadas del accidente de trabajo –STSJ de Andalucía de 1 de julio de 2013, rec. 375/2013–.

4. Sobre la cesión de datos a terceros se ha pronunciado también la STS, Sala de lo Social, de 7 de febrero de 2018 (rec. 78/2017). La controversia resuelta por esta sentencia gira en torno a la interpretación y aplicación del Acuerdo de la CIVEA de 21 de diciembre de 2000, según el cual, aprobadas las relaciones de puestos de trabajo (RPT), los centros gestores deberán elaborar un informe anual de ocupación de los puestos, en el que se deberá contener:

   > […] la relación individualizada de la totalidad de puestos de trabajo de su respectivo ámbito con expresión del código de puesto de trabajo de la RPT, apellidos y nombre del titular del puesto, en su caso, y el domicilio del centro de trabajo al que esté adscrito el puesto (FJ 1.º).

   La Administración se niega a proporcionar los listados de ocupación porque en estos figura el nombre y apellidos de los trabajadores.

Para el TS:

> […] la necesidad de identificación de los trabajadores que ocupan cada uno de los puestos que en la RPT se relacionan no resulta baladí, pues los elementos personales guardan relación con aspectos tales como la formación, titulación, y especialización, siendo también necesarios para delimitar las circunstancias de las vacantes, su cobertura, orden de prioridades, sistemas de sustitución y de promoción, etc.
>
> En suma, parece evidente que el cumplimiento de aquellas funciones de las representaciones sindicales justifica el acceso a tal dato y, por ello, no se produce un acceso indebido a datos personales que contravenga el derecho a la protección de tales datos (FJ 3.º).

Ahora bien, no hay que olvidar que los sindicatos deben limitar el uso estricto de los datos cedidos por la empresa «a la finalidad para la que se considera legítima la cesión, pues lo contrario sí sería susceptible de constituir una lesión del derecho de los trabajadores».

3. Control empresarial y protección de datos

Son muchos los problemas que el control empresarial viene planteando desde el punto de vista del derecho a la protección de datos. Aunque tradicionalmente nuestros tribunales han venido enfocando los problemas derivados del control empresarial a través de las nuevas tecnologías como una cuestión que afecta al derecho a la intimidad, no puede obviarse, como indica Thibault:

> […] la circunstancia de que existe diferencia sustancial entre las nuevas tecnologías y los anteriores medios de control a distancia, cual es la aparición y definición de un nuevo y sofisticado tipo de control que consiste en la reconstrucción del perfil del trabajador, a través del almacenamiento y la reelaboración de una serie de datos aparentemente anodinos, una amenaza potencial antes desconocida (2009, p. 215).

La nueva LOPD/2018 ha tratado de dar respuesta a algunos de esos problemas, pues la aplicación al ámbito laboral de una normativa que estaba pensada para otras cuestiones ha provocado una situación de gran inseguridad jurídica. En efecto, la LOPD/1999 no contenía ninguna referencia específica al ámbito laboral, por lo que ha sido la jurisprudencia quien ha ido interpretando la normativa en materia de protección de datos tratando de ajustarla a las peculiaridades laborales. La aprobación del RGPD ha supuesto un cambio en esta materia al contener una referencia expresa a la normativa laboral (Rodríguez, 2019, p. 2). Así, el artículo 88 del RGPD prevé que:

> Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

Pues bien, el legislador español ha hecho uso de esta posibilidad y, en el título X de la LOPD/2018, ha recogido un elenco de derechos digitales de los ciudadanos, entre los que cobran una gran importancia los ceñidos al ámbito de la empresa y la relación de trabajo (Orellana, 2019).

Como ha señalado la doctrina:

> […] no siempre es fácil discernir la relación, ni la línea de separación, entre lo que ese texto legal ha llamado «derechos digitales» y lo que implica más bien protección de datos personales. En verdad, muchos de los derechos digitales reconocidos con carácter general en la Ley orgánica 3/2018 (neutralidad de internet, acceso universal a internet, rectificación en internet o educación digital) carecen de una relación directa con la protección de datos personales y se conectan más bien con otros derechos básicos o fundamentales de las personas, como la igualdad y no discriminación, la libertad de expresión, la intimidad, el honor o la dignidad (García y Rodríguez, 2019, p. 31).

Por lo que se refiere a los derechos digitales específicamente laborales, se aprecian esas mismas dificultades de delimitación, pues no siempre está en juego el derecho a la protección de datos. En efecto, dentro del elenco de derechos digitales enumerados en el título X de la LOPD/2018, los específicamente laborales son los siguientes: el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87), el derecho a la desconexión digital en el ámbito laboral (art. 88), el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89) y el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (art. 90).

De estos derechos, solo respecto de los dos últimos contiene la norma referencias expresas a la protección de datos, pues en los dos primeros se garantizan otros derechos fundamentales, principalmente, la intimidad.

Así, en relación con el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87), señala la norma que el empresario podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de con-

trolar el cumplimiento de las obligaciones laborales o estatutarias y garantizar la integridad de dichos dispositivos. Para ello, los empresarios deberán establecer criterios de utilización de estos dispositivos respetando, en todo caso, su derecho a la intimidad. Cuando el empresario haya admitido el uso de dispositivos digitales con fines privados, para que este pueda acceder a su contenido deberá especificar de modo preciso los usos autorizados y establecer garantías para preservar la intimidad de los trabajadores.

Como puede comprobarse, el precepto establece determinadas garantías con la finalidad de proteger el derecho a la intimidad y no el derecho a la protección de datos.

Es cierto, como ya hemos señalado, que los problemas que desde el punto de vista de los derechos fundamentales plantea el control empresarial del uso de dispositivos digitales se han abordado tradicionalmente desde la perspectiva del derecho a la intimidad y no del derecho a la protección de datos. En este sentido, hay que tener en cuenta que solo estaremos en el ámbito de la LOPD cuando el control empresarial del uso del ordenador puesto a disposición de los trabajadores suponga el acceso a datos personales incluidos en un fichero[11]. Ahora bien, respecto de este supuesto, ninguna garantía específica prevé el artículo 87 de la LOPD/2018.

Por lo que se refiere al derecho a la desconexión digital en el ámbito laboral (art. 88), señala el precepto que los trabajadores y empleados públicos tendrán derecho a la desconexión tecnológica, a fin de garantizar, fuera del tiempo de trabajo, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar. Las modalidades de ejercicio de este derecho se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores. Por su parte, la empresa elaborará una política interna dirigida a los trabajadores en esta materia.

Este derecho se conecta en la LOPD/2018 con el derecho a la intimidad y con el derecho a la conciliación de la vida personal, familiar y laboral. El derecho a la protección de datos no está tampoco garantizado en este precepto.

[11] En este sentido, el Tribunal Europeo de Derechos Humanos (TEDH) en Sentencia de 22 de febrero de 2018 (caso Libert contra Francia) ha incluido el control empresarial del ordenador de un trabajador en el derecho a la protección de datos porque el empresario en dicho control accede a archivos del trabajador. El demandante se queja de una violación de su derecho al respeto de su vida privada como resultado del hecho de que el empresario abrió, en su ausencia, archivos personales almacenados en el disco duro de su ordenador profesional. El tribunal declara que el derecho positivo francés contiene un principio dirigido a la protección de la privacidad. El principio es que, si bien el empresario puede abrir los archivos profesionales almacenados en el disco duro de los ordenadores que pone a disposición de sus empleados para el desempeño de sus funciones, no puede, «excepto riesgo o acontecimiento especial», abrir archivos subrepticiamente identificados como personales. Únicamente podrá proceder a la apertura de los archivos en presencia de los empleados afectados o después de que hayan sido debidamente informados. Sin embargo, en este caso considera el tribunal que el empresario pudo abrir los archivos informáticos sin vulnerar su derecho al respeto a la vida privada porque estos no habían sido debidamente identificados, al ser archivados por el trabajador, como de carácter privado.

De este modo, de los derechos digitales específicamente laborales, el derecho a la protección de datos trata de garantizarse solo en los artículos 89 y 90 de la LOPD/2018, relativos, respectivamente, al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo y a la utilización de sistemas de geolocalización en el ámbito laboral. En efecto, es en materia de control de la prestación de trabajo a través de las técnicas de reproducción de la imagen y el sonido donde el derecho a la protección de datos está planteando mayores problemas y esa circunstancia ha tenido reflejo en los artículos 89 y 90 de la LOPD/2018.

En todo caso, y aunque entre los derechos digitales específicamente laborales contenidos en la LOPD/2018 solo se recojan garantías específicas en relación con el derecho a la protección de datos personales en los dos supuestos señalados, hay que tener en cuenta que desde hace tiempo la doctrina jurisprudencial lo que está haciendo es aplicar las reglas propias de la protección de datos al derecho a la intimidad, de manera que, como gráficamente se ha dicho, la protección de datos se está comiendo a la intimidad (García-Perrote y Mercader, 2017). «La protección de datos, si bien nació tímidamente, se ha convertido en un agujero negro que lo absorbe todo y no deja escapar nada a su entorno», de manera que:

> […] a la luz de los amplios conceptos de datos personales y tratamiento, cualquier acto de comunicación basado en medios automáticos, como las telecomunicaciones, el correo electrónico o las redes sociales, relativo a una persona física, constituye una interferencia putativa tal de este derecho fundamental que requiere de justificación (Córdoba y Díez-Picazo, 2016, p. 109).

La jurisprudencia se muestra muy estricta «con la relevancia que se asigna, en el terreno de la toma de decisiones empresariales, al efectivo cumplimiento de las reglas generales sobre protección de datos» (Goerlich, 2016, p. 146). La regla general parece ser la necesidad de información previa respecto del sistema de control que se va a utilizar. De este modo, a la hora de adoptar una medida de control informático que comporte un tratamiento de datos personales, debe aplicarse el principio de proporcionalidad y cumplirse con el deber de información a los trabajadores recogido en la LOPD.

3.1. Videovigilancia y protección de datos

3.1.1. Información general sobre la existencia de cámaras de videovigilancia. Situación anterior a la entrada en vigor de la LOPD/2018

El control mediante la captación o grabación de la imagen durante la ejecución del contrato ha dado lugar a una extensa doctrina jurisprudencial y a un interesante debate en la doctrina constitucional y la del TEDH (Gude, 2014).

La imagen de una persona constituye un dato personal y la captación de imágenes con fines de vigilancia y control se encuentra sometida a la LOPD en la medida en que dicha imagen sea objeto de tratamiento.

Los problemas que desde el punto de vista del control empresarial se han planteado en materia de videovigilancia fueron resueltos inicialmente desde la perspectiva únicamente del derecho a la intimidad, pero sin analizar la posible vulneración del derecho a la protección de datos (art. 18.4 CE), quizás porque este derecho se concibió inicialmente como una función de garantía del derecho a la intimidad y no como un derecho fundamental propio. Esto sucedió, por ejemplo, en la conocida STC 98/2000, de 10 de abril, sobre la instalación de micrófonos en determinadas dependencias del Casino de La Toja, en la que el derecho fundamental alegado por el recurrente y, por tanto, el único analizado por el TC fue el derecho a la intimidad; o en la STC 186/2000, en la que se alega vulneración del artículo 18.1 de la CE por haberse admitido como prueba de cargo en el proceso por despido las grabaciones de vídeo presentadas por la empresa.

Sin embargo, poco a poco, los problemas que provoca el control empresarial a través de sistemas de videovigilancia han sido abordados por los órganos judiciales y por el TC no solo desde la perspectiva del derecho a la intimidad, sino también a la protección de datos. En efecto, el TC, en su Sentencia 29/2013, de 11 de febrero, se pronunció por primera vez sobre la vulneración del artículo 18.4 de la CE en un supuesto de control empresarial a través de un sistema de videovigilancia. En esta sentencia, el TC declaró vulnerado el derecho a la protección de datos de carácter personal (art. 18.4 CE) de un trabajador de la Universidad de Sevilla que fue sancionado por incumplimientos en su jornada de trabajo que fueron detectados por las cámaras de videovigilancia instaladas en el recinto universitario sin haber sido informado el trabajador sobre esa utilidad de supervisión laboral asociada a las capturas de su imagen.

Recuerda la sentencia que es complemento indispensable del derecho fundamental del artículo 18.4 de la CE:

> […] la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo. […] Ese derecho de información opera también cuando existe habilitación legal para recabar los datos sin necesidad de consentimiento, pues es patente que una cosa es la necesidad o no de autorización del afectado y otra, diferente, el deber de informarle sobre su poseedor y el propósito del tratamiento (FJ 7.º).

Afirma el TC que no hay en el ámbito laboral una razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental del artículo 18.4 de la CE.

> Por tanto, no será suficiente que el tratamiento de datos resulte en principio lícito, por estar amparado por la ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar even-

> tualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa (FJ 7.º).

En el supuesto resuelto por la citada sentencia, las cámaras de videovigilancia instaladas en el recinto universitario reprodujeron la imagen del recurrente y permitieron el control de su jornada de trabajo sin haber sido informado el trabajador de que las imágenes capturadas por las cámaras podían ser utilizadas para el control laboral, por lo que se declara vulnerado el artículo 18.4 de la CE. Señala la sentencia que la ilegalidad de la conducta empresarial no desaparece por el hecho de que la existencia de las cámaras fuera apreciable a simple vista.

> No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la AEPD; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo (FJ 8.º).

La STC 29/2013 pone, por tanto, el énfasis en la necesidad de que el interesado conozca de antemano el destino específico de sus datos personales, y de ello deriva que la falta de información al trabajador, en el caso examinado, de que las grabaciones de la cámara de seguridad podrían ser utilizadas en su contra para controlar el cumplimiento de sus obligaciones laborales determina la nulidad de la prueba.

Esta sentencia dio lugar a diferentes interpretaciones por los órganos judiciales. Así, algunas sentencias entendieron que no puede recibir el mismo tratamiento el caso de cámaras destinadas a un uso genérico como el control de accesos y cuyas imágenes son aprovechadas *a posteriori* por la empresa para realizar un control de cumplimiento de la jornada laboral que el de las cámaras de videovigilancia:

> […] específicamente instaladas para controlar la actividad en la caja registradora o TPV, siendo ello un hecho perfectamente conocido por los trabajadores, aunque no se haya sujetado la transmisión de la información a las exigencias derivadas de la Instrucción 1/2006, pero que hace que los empleados sean plenamente conscientes de la finalidad y utilidad de dichas cámaras (STSJ de Cataluña de 1 de julio de 2013, rec. 1804/2013).

No tratándose de una instalación oculta y siendo público y notorio el objetivo y finalidad de la cámara, no puede apreciarse la vulneración de derecho fundamental que vicie de nulidad la prueba de grabación aportada por la empresa.

Sin embargo, para otras sentencias no es válida la prueba consistente en las imágenes grabadas por las cámaras de videovigilancia que hay, por ejemplo, en un supermercado y a través de las cuales se comprueba que un trabajador está cometiendo irregularidades en el cobro de productos a sus clientes apropiándose de determinadas cantidades de dinero. Consideran que el trabajador debería haber sido informado sobre esa utilidad de supervisión laboral. Aunque la finalidad de la instalación de las cámaras pueda ser la prevención de hurtos y similares, lo cierto es que se usó con la indicada y distinta finalidad de controlar la actividad de la trabajadora y luego para sancionar a la misma con el despido, por lo que se declara no lícita la prueba de grabación de imágenes y su utilización para acreditar los hechos constitutivos del despido (STSJ del País Vasco de 18 de junio de 2013, rec. 1039/2013).

La existencia de distintas posturas en la doctrina judicial dio lugar a que el TS se pronunciara en unificación de doctrina (STS de 13 de mayo de 2014, rec. 1685/2013) sobre esta cuestión en relación con una cajera de un supermercado a la que las cámaras de seguridad captaron evitando en la caja el escaneo de diversos productos en beneficio de su pareja. En aplicación de la doctrina sentada por la STC 29/2013, el TS llega a la conclusión de que se ha vulnerado el derecho a la protección de datos porque la empresa no dio información previa a la trabajadora de la posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras instaladas permanentemente, ni tampoco se informó, con carácter previo ni posterior a la instalación, a la representación de los trabajadores de las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, ni explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo. Insiste el TS en señalar que la ilegalidad de la conducta empresarial no desaparece por el hecho de que la existencia de las cámaras fuera apreciable a simple vista y añade que:

> […] el mero hecho de la instalación y del conocimiento de la existencia de tales cámaras no puede comportar la consecuencia de entender acreditado el que existiera evidencia de que podían utilizarse aquellas para el control de la actividad laboral y para la imposición de sanciones disciplinarias por incumplimientos contractuales, puesto que expresamente, como hemos indicado, en el presente caso la representación empresarial, tras la instalación de la cámaras, comunicó a la representación de los trabajadores que la finalidad exclusiva era la de evitar robos por parte de clientes y que no se trataba de un sistema de vigilancia laboral (FJ 6.º 4).

Es cierto que la aplicación de la doctrina sentada por la STC 29/2013, sin matizaciones en supuestos en los que el trabajador ha cometido una infracción que puede ser castigada penalmente, puede llevar a situaciones absurdas. Así, podríamos preguntarnos: ¿qué pasa

si la cámara visiona casualmente un delito cometido por un empleado?; ¿estamos ante una prueba ilícita y el trabajador será absuelto del delito?; ¿o las imágenes obtenidas podrían servir como medio de prueba en un proceso penal, pero no en un proceso laboral para despedir al trabajador que ha cometido la correspondiente infracción por no haber sido informado de la posible utilidad de supervisión laboral asociada a las capturas de su imagen?

Ante las distintas dudas que en la práctica plantea la aplicación de la doctrina de la STC 29/2013, el TC modificó su doctrina en la STC 39/2016, de 3 de marzo. Esta sentencia pretende aclarar su doctrina en relación con el uso de cámaras de videovigilancia en la empresa y, en concreto:

> […] aclarar el alcance de la información a facilitar a los trabajadores sobre la finalidad del uso de la videovigilancia en la empresa: si es suficiente la información general o, por el contrario, debe existir una información específica (tal como se había pronunciado la STC 29/2013, de 11 de febrero) (FJ 1.º).

En el supuesto resuelto por la citada STC 39/2016, la recurrente en amparo consideró vulnerado el artículo 18.4 de la CE porque no había sido informada previamente de la instalación de cámaras de videovigilancia en el puesto de trabajo. Las cámaras de videovigilancia instaladas en la tienda donde prestaba sus servicios la recurrente en amparo captaron su imagen apropiándose de dinero y realizando, para ocultar dicha apropiación, operaciones falsas de devoluciones de venta de prendas. Ante estos hechos, la trabajadora fue despedida.

La cámara estaba situada en el lugar donde se desarrollaba la prestación laboral, enfocando directamente a la caja, y en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo exigido por la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos (AEPD), sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. Como recuerda la STC 39/2016:

> La necesidad de adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos ha llevado a la AEPD, en ejercicio de la competencia que le atribuye el artículo 37.1 c) de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, a dictar la citada instrucción para adecuar los tratamientos de imágenes con fines de vigilancia a los principios de dicha ley orgánica y garantizar los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos. Esta instrucción, en su artículo 3, exige a los responsables que cuenten con sistemas de videovigilancia cumplir con el deber de información previsto en el artículo 5 de la Ley orgánica 15/1999, y a tal fin deberán «colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados» y «tener a disposición de los/las interesados impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley orgánica 15/1999». El con-

> tenido y el diseño del distintivo informativo se ajustará a lo previsto en el anexo de esta instrucción, según el cual el distintivo deberá incluir una referencia a la Ley orgánica 15/1999, de protección de datos, una mención a la finalidad para la se tratan los datos («Zona videovigilada») y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley orgánica 15/1999 (FJ 4.º).

La sentencia considera que la empresa cumplió con la obligación de información previa:

> […] pues basta a estos efectos con el cumplimiento de los requisitos específicos de información a través del distintivo, de acuerdo con la Instrucción 1/2006. El trabajador conocía que en la empresa se había instalado 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. Lo importante será determinar si el dato obtenido se ha utilizado para la finalidad de control de la relación laboral o para una finalidad ajena al cumplimiento del contrato, porque solo si la finalidad del tratamiento de datos no guarda relación directa con el mantenimiento, desarrollo o control de la relación contractual, el empresario estaría obligado a solicitar el consentimiento de los trabajadores afectados (FJ 4.º).

En efecto, afirma el TC que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el artículo 20.3 del Estatuto de los Trabajadores (ET).

> Si la dispensa del consentimiento prevista en el artículo 6 LOPD se refiere a los datos necesarios para el mantenimiento y el cumplimiento de la relación laboral, la excepción abarca sin duda el tratamiento de datos personales obtenidos por el empresario para velar por el cumplimiento de las obligaciones derivadas del contrato de trabajo. El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario (FJ 4.º).

Ahora bien, aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de información del artículo 5 de la LOPD, pero para que el incumplimiento de este deber por parte del empresario implique una vulneración del artículo 18.4 de la CE debe valorarse la observancia o no del principio de proporcionalidad.

> Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el

> artículo 20.3 ET, en conexión con los artículos 33 y 38 CE. En efecto, la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva (FJ 4.º).

Obviamente, el sometimiento de la falta o insuficiencia de información al reiterado juicio de proporcionalidad requerirá determinar en cada supuesto, con carácter previo, si se ha producido o no la indicada omisión de la información debida. Y, en este sentido, el TC estima que la trabajadora tiene información previa de la instalación de las cámaras de videovigilancia a través del correspondiente distintivo informativo, sin que sea necesaria una información específica acerca de que las cámaras pueden ser utilizadas también para detectar posibles incumplimientos laborales.

De este modo, el tribunal modifica su doctrina anterior sobre el control empresarial a través de cámaras de videovigilancia, al entender que basta con que exista una información general sobre su existencia.

El TC opta por dictar una doctrina general sobre el control empresarial a través de cámaras de videovigilancia en lugar de centrarse en las diferencias que existen entre el supuesto de hecho que dio lugar a la STC 29/2013 y el que da lugar a la STC 39/2016. La diferencia entre ambos supuestos radica, a mi juicio, en el hecho de que, en este segundo asunto, la grabación no se destinó a un uso distinto a su finalidad. La acción captada es un ilícito laboral que afecta a la seguridad, que es precisamente la finalidad para la que fueron instaladas las cámaras.

En efecto, la cámara estaba situada en el lugar donde se desarrollaba la prestación laboral, enfocando directamente a la caja, y en el escaparate del establecimiento, en un lugar visible, se colocó el distintivo informativo exigido por la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. La finalidad de la vigilancia a través de cámaras no aparece reflejada de modo expreso en el distintivo exigido en estos casos por la AEPD, que solo exige que aparezca la expresión «Zona videovigilada», al entenderse con esta expresión que el propósito de la vigilancia a través de cámaras, que tienen como destino un colectivo indeterminado de personas, no es otro que establecer un control general de seguridad.

Pues bien, el sistema de videovigilancia captó la apropiación de efectivo de la caja de la tienda por parte de la recurrente, que por este motivo fue despedida disciplinariamente. Por tanto, a diferencia del asunto enjuiciado en la STC 29/2013, donde la grabación fue utilizada para una finalidad distinta a la de seguridad para la que habían sido instaladas las cámaras –en concreto, para controlar el horario de trabajo–, en el segundo caso, la grabación realizada fue destinada a la finalidad para la que las cámaras habían sido instaladas, que no era otra que la de controlar la seguridad en la empresa.

Este es un dato importante a tener en cuenta, pues resulta muy curioso que, detectado por las cámaras de videovigilancia un incumplimiento de un trabajador que puede constituir un delito, el empresario no pueda utilizar esta grabación como medio de prueba para despedir a su trabajador porque previamente no ha sido informado de que las cámaras instaladas pueden utilizarse para el control de la actividad laboral.

Pero, aunque ciertamente el TC podría haberse limitado a establecer esa diferencia entre ambos supuestos y resolver exclusivamente el problema que se plantea cuando las cámaras, instaladas con una finalidad de seguridad en la empresa, detectan que el trabajador está cometiendo un robo o cualquier otra conducta que puede ser tipificada como delito o falta desde el punto de vista penal (por ejemplo, una agresión física o sexual a un compañero de trabajo o a un cliente), optó por establecer una doctrina con carácter general en los supuestos de control empresarial a través de cámaras de videovigilancia. La doctrina del TC deja claro que lo importante es que el trabajador conozca la existencia de las cámaras, que esté informado de su presencia, pero sin que sea necesario informar de la finalidad que se le ha asignado a ese control. La cámara puede haberse instalado por razones de seguridad en la empresa y si de un modo accidental registra un incumplimiento laboral, no se vulnera el derecho a la protección de datos porque no se cumpla con la finalidad inicialmente asignada al medio de control. El trabajador sabe que está siendo controlado porque conoce la existencia de las cámaras y no es necesario que conozca la finalidad principal asignada a las mismas.

3.1.2. Cámaras ocultas

La doctrina constitucional expuesta no resuelve expresamente el problema de la videovigilancia a través de cámaras ocultas, si bien deja claro que, en todo caso, para que el incumplimiento del deber de información por parte del empresario implique una vulneración del artículo 18.4 de la CE, es necesario valorar la observancia o no del principio de proporcionalidad.

> Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el artículo 20.3 ET, en conexión con los artículos 33 y 38 CE. En efecto, la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los artículos 33 y 38 CE y que, como se ha visto, en lo que ahora interesa se concreta en la previsión legal *ex* artículo 20.3 ET que expresamente faculta al empresario a adoptar medidas de

> vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones laborales (SSTC 186/2000, de 10 de julio, FJ 5.º; 170/2013, de 7 de octubre, FJ 3.º). Esta facultad general de control prevista en la ley legitima el control empresarial del cumplimiento por los trabajadores de sus tareas profesionales (STC 170/2013, de 7 de octubre; STEDH de 12 de enero de 2016, caso Bărbulescu v. Rumanía), sin perjuicio de que serán las circunstancias de cada caso las que finalmente determinen si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego (FJ 4.º).

Por lo tanto, es necesario comprobar si la medida restrictiva del derecho fundamental supera el juicio de proporcionalidad, para lo cual es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

Los órganos judiciales[12] vienen entendiendo que la omisión de toda información previa de la existencia de videovigilancia solamente sería admisible cuando, en los términos del Repertorio de recomendaciones prácticas de la Organización Internacional del Trabajo sobre protección de datos de los trabajadores, lo permita la normativa nacional o existan sospechas suficientes de actividad delictiva y/u otras infracciones graves (punto 6.14.2). En este sentido, la STC 186/2000, de 10 de julio, pero en relación con el derecho a la intimidad y no a la protección de datos, no apreció vulneración del artículo 18.1 de la CE por el hecho de

[12] STSJ de Andalucía de 13 de junio de 2016 (rec. 1820/2015):

> En el caso concreto de autos existían indicios, que ya no solo sospechas, de que alguno de los trabajadores se estaba apropiando de víveres, por lo que la medida de instalar unas cámaras enfocando a las dos salidas y entrada trasera del edificio y en la despensa, como en el pasillo de acceso a las dependencias del despacho del jefe de cocina y en el pasillo del vestuario y en el exterior del recinto de la cocina resulta justificada pues se pretendía verificar si algún trabajador cometía irregularidades y adoptar medidas disciplinarias en ese caso, por lo que la medida es idónea para dicha finalidad; la grabación servía de prueba de tales irregularidades, por lo que la medida resulta necesaria; y la grabación de imágenes se limitó a las zonas en las que se podían sacar los víveres, por lo que la medida parece equilibrada pues con arreglo a la STC 186/2000 (RTC 2000, 186) concurría la situación precisa para el control oculto, esto es sin notificar expresamente la colocación de la cámara a los trabajadores, porque era, en principio, el único medio posible dicho control para satisfacer el interés empresarial de saber fehacientemente quién estaba realizando los actos defraudatorios de los que indiciariamente ya se tenían conocimiento. La empresa adoptó la medida cuestionada no sobre sospechas sino sobre indicios que había en curso un fraude.

En el mismo sentido, la STSJ de Canarias de 27 de marzo de 2017 (rec. 934/2016).

haberse instalado un circuito cerrado de televisión que controlaba la zona donde el demandante de amparo desempeñaba su actividad laboral, pese a que el mismo no había sido informado de tal instalación, porque «existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo».

Sobre la utilización de cámaras ocultas y la posible vulneración del derecho a la protección de datos, se ha pronunciado el TEDH en su Sentencia de 9 de enero de 2018 (caso López Ribalda y otros contra España) (Rojo, 2018; Chacartegui, 2018). El asunto tiene su origen en varias demandas dirigidas contra España por cinco trabajadoras, cajeras de un supermercado, que fueron despedidas por robo. El empresario fue informado de ciertas irregularidades entre la mercancía almacenada existente en el supermercado y las ventas reales diarias. Concretamente, el supervisor de la tienda identificó pérdidas en exceso por importe de 7.780 euros en febrero, 17.917 euros en marzo, 13.936 euros en abril, 18.009 euros en mayo y 24.614 euros en junio de 2009. Con el fin de investigar lo que estaba sucediendo, el empresario instaló cámaras de vigilancia tanto visibles como ocultas. El propósito de las cámaras visibles era grabar los posibles robos de los clientes y estaban colocadas en las entradas y salidas del supermercado. El propósito de las cámaras ocultas era grabar y controlar los posibles robos de los empleados y enfocaban a las cajas registradoras, cubriendo el área detrás de la caja. La empresa comunicó a sus trabajadores previamente la instalación de las cámaras visibles, pero no fueron informados de las cámaras ocultas.

Las demandantes fueron despedidas por motivos disciplinarios, porque habían sido captadas por vídeo ayudando a otros compañeros de trabajo y a clientes a robar productos y robándolos ellas mismas. Según sus cartas de despido, habían sido grabadas escaneando productos de la cesta de la compra de los clientes y otros compañeros de trabajo para después cancelar las compras. Las cámaras de seguridad también las grabaron permitiendo a los clientes y otros compañeros abandonar el supermercado con productos por los que no habían pagado.

En la misma fecha en la que se produjeron los despidos, casi todas las trabajadoras firmaron diversos acuerdos transaccionales en atención a los cuales declaraban que en la carta de despido se recogen una serie de hurtos de productos que la trabajadora reconoce como ciertos, solicitándose por parte de la trabajadora un acuerdo por el cual se convalide la decisión empresarial y la empresa no interponga acciones penales contra la trabajadora, acordando la rescisión del contrato laboral que los unía y teniendo por saldada y finiquitada la relación laboral.

Las trabajadoras interpusieron las correspondientes demandas alegando vulneración del derecho a la protección de su privacidad por el uso de la videovigilancia encubierta. El juzgado de lo social declaró que el uso de la videovigilancia encubierta en el lugar de trabajo sin una comunicación previa es conforme con el artículo 20 del ET. Para el juzgado de lo social, siguiendo la doctrina judicial en esta materia, en casos donde existan fundadas sospechas de robos, las especiales circunstancias justifican la injerencia en el derecho del

trabajador a la privacidad. De este modo, desestimó las demandas por considerar procedente el despido en uno de los casos y en los restantes por considerar que existía «falta de acción» por haber firmado las trabajadoras un «documento de saldo y finiquito plenamente válido, eficaz y liberatorio para la empresa».

Frente a estas resoluciones, las trabajadoras interpusieron dos recursos de suplicación que fueron desestimados por SSTSJ de Cataluña de 28 de enero y 24 de febrero de 2011. Para el TSJ de Cataluña, reconociendo que es posible que el empresario podría enfrentarse a una sanción administrativa por no informar a sus empleados y al comité de empresa antes de la instalación de las cámaras, ese solo hecho carece de importancia desde el punto de vista constitucional, ya que desde esta perspectiva la videovigilancia encubierta estaba justificada –dado que existían sospechas razonables de robo–, adecuada al objetivo legítimo perseguido, necesaria y proporcionada. Por ello, declaró los despidos procedentes.

Las recurrentes interpusieron recursos de casación para unificación de doctrina, que fueron inadmitidos por falta de contradicción por los AATS de 5 de octubre de 2011 y 7 de febrero de 2012.

Finalmente, las recurrentes interpusieron dos recursos de amparo ante el TC, que fueron inadmitidos por providencias de 27 de junio y 18 de julio de 2012, por inexistencia de la vulneración denunciada.

Las recurrentes en amparo interpusieron demanda ante el TEDH alegando, por lo que aquí interesa, vulneración del artículo 8 del Convenio para la protección de los derechos humanos y de las libertades fundamentales, porque la videovigilancia encubierta de su lugar de trabajo interfirió gravemente en su derecho a la privacidad.

Por lo que se refiere, en primer lugar, a la vulneración del derecho a la privacidad al amparo del artículo 8 del convenio, señala el TEDH que el presente asunto difiere del asunto Köpke contra Alemania (núm. 420/07, de 5 de octubre de 2010), y ello porque en ese caso, cuando el empresario llevó a efecto la videovigilancia encubierta tras las sospechas de robo contra dos empleadas, todavía no se habían establecido en el estatuto las condiciones en las que un empresario podía utilizar la videovigilancia de un empleado para investigar un delito. Sin embargo, considera el tribunal que la legislación española vigente en el momento de los hechos claramente establece que debe informarse a los interesados de la recogida de datos, de la existencia de medios de recogida y del tratamiento de sus datos de carácter personal (art. 5 LOPD). Por lo tanto, las demandantes tenían una expectativa razonable de respeto a su privacidad.

Además, a diferencia también de Köpke, en este caso la videovigilancia encubierta no era la consecuencia de una sospecha justificada contra las trabajadoras y, en consecuencia, no iba dirigida específicamente a ellas, sino a todo el personal que trabajaba en las cajas registradoras, sin límite de tiempo y durante todas las horas de trabajo. En Köpke, la

medida de vigilancia estuvo limitada en el tiempo (2 semanas) y solo dos empleados fueron el objetivo de la medida. En el presente caso, por el contrario, la decisión de adoptar medidas de vigilancia se basó en una sospecha general contra todo el personal ante las irregularidades que se habían detectado en el supermercado.

De este modo, el tribunal deja claro que se aparta de la sentencia Köpke por las dos razones señaladas, y a continuación afirma que la videovigilancia llevada a cabo por el empresario no cumplía los requisitos establecidos en el artículo 5 de la LOPD, al no haber informado a los trabajadores «de modo expreso, preciso e inequívoco sobre la existencia y características particulares de un sistema de recogida de datos de carácter personal». El tribunal afirma que los derechos del empresario podrían haber sido protegidos por otros medios, «en especial, informando previamente a los demandantes, incluso de una manera general, sobre la instalación de un sistema de videovigilancia y dotándolos de la información establecida en la LOPD».

Por lo tanto, para el TEDH hubiera bastado con una información general sobre la instalación de un sistema de videovigilancia. En este caso, el empresario informó de la existencia de las cámaras visibles que enfocaban las salidas del supermercado, pero no de las cámaras ocultas. Sin embargo, para el tribunal, el empresario debería también haber informado a sus trabajadores de la existencia de cámaras ocultas, bastando con una información general sobre su existencia. El TEDH no pondera, por tanto, si existían sospechas razonables para instalar dichas cámaras y considera que el deber de información exigido por la LOPD debe aplicarse sin excepciones. Así, parece que los trabajadores no tienen por qué saber dónde están colocadas las cámaras, pero deben saber que las cámaras existen y que la zona está siendo videovigilada.

A mi juicio, esta doctrina del TEDH no resulta contraria a la doctrina constitucional dictada en la STC de 3 de marzo de 2016. En esta sentencia, como hemos señalado, el TC consideró suficiente una información general sobre la existencia de cámaras de videovigilancia, al entender que basta con el distintivo informativo de zona videovigilada que exige la Instrucción 1/2006 de la AEPD. Y esta misma postura parece mantener el TEDH en Sentencia de 9 de enero de 2018, pues no exige que exista una información concreta y específica, sino que considera suficiente una información general que en el caso de las cámaras ocultas no se ha dado. Los trabajadores tenían conocimiento de la existencia de las cámaras visibles, pero no de las cámaras ocultas, y lo que dice el TEDH es que deberían haber sido informados de su existencia, siendo suficiente para ello con una información general.

Esta doctrina, que sin duda hacía imposible que los empresarios pudieran utilizar cámaras ocultas, al exigir un deber de información general sobre su existencia, ha sido matizada, con buen criterio, en la Sentencia de la Gran Sala del TEDH de 17 de octubre de 2019 en este mismo asunto (caso López Ribalda contra España) (Navarro, 2019). En efecto, en virtud del artículo 43 del Convenio de protección de derechos y libertades fundamentales de 1999, el Gobierno solicitó la remisión del asunto ante la Gran Sala que ha dictado la señalada sentencia que

modifica la doctrina sentada en la de 9 de enero de 2018 y supone un acercamiento a la posición que venían manteniendo nuestros tribunales en relación con el uso de cámaras ocultas. El TEDH insiste en que es necesario informar sobre la instalación de sistemas de videovigilancia, pero pueden existir razones importantes que justifiquen la ausencia de información previa. Para el TEDH, la existencia de sospechas razonables de que se han cometido graves irregularidades y el alcance de los robos constatados pueden ser razones suficientes que justifican la falta de información. No basta, por tanto, con una mera sospecha de robos u otras irregularidades, sino que debe tratarse de una sospecha razonable.

3.1.3. El uso de dispositivos de videovigilancia y grabación en la LOPD/2018

El artículo 89 de la LOPD/2018 señala que:

> Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

El precepto admite, por tanto, el control empresarial a través de sistemas de videovigilancia, siempre y cuando el empresario informe de esta medida a sus trabajadores. No basta, en principio, con una información genérica acerca de la existencia de cámaras de videovigilancia, sino que es precisa una información específica sobre la posibilidad de que dichas cámaras sean utilizadas para el control laboral. La información será previa, expresa, clara y concisa.

Ahora bien, el precepto establece una excepción a esta regla general para el supuesto de que las cámaras de videovigilancia hayan captado la comisión flagrante de un acto ilícito por los trabajadores. En este caso, se entenderá cumplido el deber de información cuando exista al menos un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos de acceso, rectificación, supresión u oposición previstos legalmente. Se trata así de salvar la situación absurda, a la que hemos hecho referencia en el epígrafe anterior, a la que se puede llegar si por falta de una información específica al trabajador sobre la posibilidad de control de su actividad laboral no pudiera utilizarse como medio de prueba válido la grabación en la que el trabajador es captado cometiendo un acto ilícito. De este modo, en el caso de la STC 39/2016 anteriormente comentada, en el que una trabajadora es captada por las cámaras de seguridad apropiándose de dinero de la caja, la solución a

la que se llega con la normativa actual es la misma a la que llegó el TC: basta en este caso con una información general sobre la existencia de cámaras, información que se entiende cumplida cuando existe un dispositivo informativo en lugar suficientemente visible. Parece así existir una clara sintonía entre el artículo 89 de la LOPD/2018 y la STC 39/2016.

El precepto no establece ninguna excepción al deber de información en los supuestos de cámaras ocultas. El artículo 89 de la LOPD/2018 da así respuesta al problema que se plantea *a posteriori*, es decir, cuando el acto ilícito se ha cometido y es captado por las cámaras de videovigilancia instaladas con una finalidad genérica de seguridad en la empresa, y no para el control específico de los trabajadores. Pero el precepto no da ninguna solución para el supuesto de que el empresario tenga claras sospechas de que se ha cometido una infracción y quiera llevar a cabo un control, que podemos denominar «sorpresivo». Aunque una aplicación literal del precepto pudiera llevarnos a entender que el deber de información debe existir siempre y, por tanto, no cabe la instalación de cámaras ocultas, la doctrina sentada por el TEDH, que coincide, como hemos señalado, con la que ya venían aplicando nuestros tribunales, debe llevarnos a la conclusión de que cabe la instalación de un sistema de videovigilancia encubierto por parte del empresario, cuando existan sospechas razonables de que se están cometiendo graves irregularidades. Qué se entienda por sospechas razonables o por graves irregularidades es algo que los tribunales irán fijando según las circunstancias de cada caso.

En contra de esta postura podemos citar la Sentencia del Juzgado de lo Social núm. 3 de Pamplona de 18 de febrero de 2019 (rec. 875/2018) que considera que la LOPD/2018 no está respetando el derecho a la privacidad y a la protección de datos personales, pues el RGPD no establece ningún tipo de excepción al deber de información en las relaciones laborales. Por otra parte, señala dicha sentencia que:

> […] en la hipótesis de sospechas de la comisión de hurtos o de otras conductas delictivas parece que lo más razonable es impetrar el auxilio judicial, de modo que el empresario debería interponer la correspondiente denuncia y solicitar las medidas de investigación del delito adecuadas, incluida la videovigilancia, que podrá acordarse si resulta eficaz a los fines de la instrucción penal y si concurren los requisitos legales, salvaguardando así los derechos del empleador, solo que con el amparo y debido control judicial (FJ 2.º).

Junto a la protección de datos de carácter personal, el artículo 89 de la LOPD/2018 protege también la intimidad de los trabajadores en los supuestos de uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Así, en primer lugar, el artículo 89.2 señala que «en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos». En este sentido, el precepto no hace sino recoger una doctrina constitucional y jurisprudencial clara sobre la vulneración del derecho a la intimidad en estos casos. Como afirmó

la STC 98/2000, de 10 de abril (FJ 6.º), la instalación de medios de vigilancia y control «en lugares de descanso o esparcimiento, vestuarios, aseos, comedores y análogos resulta, *a fortiori*, lesiva en todo caso del derecho a la intimidad de los trabajadores, sin más consideraciones, por razones obvias».

Y, en segundo lugar, los sistemas de grabación de sonidos en el lugar de trabajo se admitirán únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, de intervención mínima y las garantías previstas en los apartados anteriores (art. 89.3 LOPD/2018). Como ha señalado la doctrina:

> […] las exigencias son en apariencia bastante más estrictas para la captación de sonidos que para la captación de imágenes, puesto que para la instalación de sistemas de videovigilancia el precepto únicamente establece como requisito específico el de «informar con carácter previo, y de forma expresa, clara y precisa», a los trabajadores y en su caso a sus representantes, mientras que para la captación de sonidos se imponen, además de ese deber de información, aquellos otros límites (García y Rodríguez, 2019, p. 36).

Es decir, además del deber de información hay que respetar el principio de proporcionalidad y de intervención mínima.

Parece así recoger este precepto la doctrina constitucional contenida en la STC 98/2000, de 10 de abril, en el caso del Casino de la Toja. En esta sentencia se planteó si la instalación de micrófonos que permitían grabar las conversaciones de trabajadores y clientes en determinadas zonas del casino se ajustaba a las exigencias indispensables del respeto del derecho a la intimidad. La sentencia concluyó que:

> […] la implantación del sistema de audición y grabación no ha sido en este caso conforme con los principios de proporcionalidad e intervención mínima que rigen la modulación de los derechos fundamentales por los requerimientos propios del interés de la organización empresarial, pues la finalidad que se persigue (dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes) resulta desproporcionada para el sacrificio que implica del derecho a la intimidad de los trabajadores (e incluso de los clientes del casino).
>
> Este sistema permite captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios ajenos por completo al interés empresarial y por tanto irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y

> grabados por la empresa. Se trata, en suma, de una intromisión ilegítima en el derecho a la intimidad consagrado en el artículo 18.1 CE, pues no existe argumento definitivo que autorice a la empresa a escuchar y grabar las conversaciones privadas que los trabajadores del casino mantengan entre sí o con los clientes (FJ 9.º).

De este modo, el empresario, antes de instalar sistemas de grabación de sonidos, deberá no solo informar a sus trabajadores, sino valorar si la finalidad que se persigue con esa medida resulta proporcionada a la limitación del derecho a la intimidad de los trabajadores, teniendo en cuenta que la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación.

En todo caso, no parece que sea admisible, como regla general, una videovigilancia y grabación de sonidos genérica y permanente con finalidad de control laboral, aunque se haga la oportuna advertencia a los trabajadores. En este sentido, ya señaló la reiterada STC 98/2000 que:

> […] el uso de un sistema que permite la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores, como de los clientes del casino, constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el artículo 20.3 LET y supone, en definitiva, una intromisión ilegítima en el derecho a la intimidad consagrado en el artículo 18.1 CE (FJ 9.º).

Por último, hay que tener en cuenta que, según señala el artículo 89.3 de la LOPD/2018, «la supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley». De este modo, los sonidos serán suprimidos en el plazo máximo de 1 mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

4. Protección de datos y sistemas de geolocalización

Cada vez más empresas utilizan los avances tecnológicos para controlar las herramientas de trabajo facilitadas a sus trabajadores. Entre esas tecnologías adquieren importancia las herramientas de geolocalización con las que el empresario puede conocer la localización tanto de bienes propiedad de la empresa, como de trabajadores (Fernández, 2010; Goñi, 2009).

La instalación del sistema de geolocalización por la empresa supone el tratamiento de datos personales por afectar a personas identificables.

La AEPD ya en su Informe 0613/2009 determinó que resulta aplicable a estos supuestos la LOPD y su normativa de desarrollo, habida cuenta de que los datos de localización

se refieren siempre a una persona física identificada o identificable, por lo que constituyen datos personales.

El Grupo de Trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo 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, en el Dictamen 5/2005, sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido, estableció una serie de pautas o recomendaciones a tener en cuenta en relación con el tratamiento de datos de localización relativos a empleados.

Así, señaló que en estos casos el tratamiento de datos ha de corresponder a:

> […] una necesidad específica de la empresa que guarde relación con su actividad. El tratamiento de los datos de localización puede estar justificado si se lleva a cabo formando parte del control del transporte de personas o bienes o de la mejora de la distribución de los recursos para servicios en puntos remotos (por ejemplo, la planificación de operaciones en tiempo real) o cuando se trate de lograr un objetivo de seguridad en relación con el propio empleado o con los bienes o vehículos a su cargo. Por el contrario, el Grupo considera que el tratamiento de datos es excesivo en el caso de que los empleados puedan organizar libremente sus planes de viaje o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios. En estos dos casos, su finalidad no justifica el uso de un tratamiento que, por el tipo de datos recogidos, supone una innegable intromisión.

Si la empresa cede al trabajador un vehículo para ser usado por el mismo en el ejercicio de las funciones propias de su trabajo, los datos que se conecten a su manejo, así como a sus desplazamientos y ubicaciones a lo largo de la jornada laboral, vendrán a reflejar la forma de proceder del trabajador como conductor del vehículo, permitiendo de ese modo, como se indica en la STSJ de Madrid de 21 de marzo de 2014 (rec. 1952/2013), el permanente:

> […] conocimiento de parcelas de la vida del trabajador que por muy imbricadas que estén en el desarrollo de la relación laboral con la empresa inciden potencialmente en la esfera de su derecho a la intimidad personal y, de ser objeto de tratamiento como aquí sucede, del que igualmente le asiste a la protección de datos de tal carácter (FJ 16.º).

La cuestión, por tanto, a resolver en estos supuestos queda centrada en la determinación de los requisitos a los que debe ajustarse la posible instalación por la empresa de un sistema de vigilancia como el GPS, a fin de salvaguardar el derecho fundamental que, de conformidad con el artículo 18.4 de la CE, asiste al trabajador.

El artículo 90 de la LOPD/2018 reconoce el derecho de los empleadores a tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de funciones de control de los trabajadores previstas en el artículo 20.3 del ET, «siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». Para llevar a cabo este tratamiento de datos, el artículo 90.2 de la LOPD/2018 prevé que:

> Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Se da, así, un tratamiento muy similar al del uso de dispositivos de videovigilancia, pues se exige la información expresa, clara e inequívoca a los trabajadores. En todo caso, esta venía siendo la postura mantenida por la jurisprudencia en estos supuestos, pues, aunque no siempre se exigía el consentimiento de los trabajadores, sí que se exigía el deber de información sobre la utilización de estos sistemas de geolocalización.

En este sentido, se ha entendido que el empresario puede establecer esta medida de control sin el consentimiento de los trabajadores afectados siempre y cuando la medida se considere necesaria para el mantenimiento y ejecución del contrato de trabajo. Así, por ejemplo, la AEPD (Informe 0090/2009) ha considerado que no es necesario el consentimiento en el supuesto de una empresa de seguridad que proporciona a sus empleados en tareas de escolta un teléfono que dispone de localizador GPS. El tratamiento de los datos de localización del escolta durante la prestación del servicio y, como consecuencia, de la persona escoltada, así como los relativos al inicio o fin del servicio o las incidencias ocurridas durante su prestación, responde a la necesidad de garantizar la seguridad del escoltado y forma parte de la prestación del servicio de protección a la persona escoltada, por lo que el tratamiento de dicho dato vendría amparado en lo dispuesto en el artículo 6.2 de la LOPD/1999.

En este sentido, se ha considerado que no es necesario el consentimiento de los trabajadores cuando el sistema de geolocalización instalado por la empresa en los vehículos que pone a disposición de sus trabajadores tiene una finalidad de control del cumplimiento de las funciones y obligaciones de los conductores durante la jornada laboral. «La finalidad de control alegada por la empresa está justificada y permite que dada la existencia de una relación laboral entre en juego la excepción (del art. 6.2 LOPD) durante la jornada de trabajo»[13].

[13] STSJ de Asturias de 27 de diciembre de 2018 (rec. 2241/2017):

> La utilización de los vehículos de motor para desplazarse a los diferentes domicilios de los clientes, en toda la comunidad autonómica asturiana, consume una buena parte de la jornada y es un medio fundamental en la prestación de servicios y en la actividad empresarial de

Sin embargo, aunque en determinados supuestos no sea necesario el consentimiento del trabajador, lo que ha resultado exigible por la jurisprudencia, con carácter general, es cumplir con el deber informativo que impone la LOPD. Ahora bien, es cierto que en algún supuesto la doctrina judicial no ha considerado necesario que el empresario haya informado expresamente al empleado de su instalación.

A título de ejemplo, podemos citar la STSJ de Cataluña de 5 de marzo de 2012 (rec. 5194/2011). En este caso, el trabajador había sido advertido de que podían adoptarse las medidas más oportunas de vigilancia y control para verificar el cumplimiento de sus obligaciones laborales, pero no específicamente de la instalación del GPS en el vehículo de empresa que tenía a su disposición. La empresa tuvo noticias, a través de comentarios de empleados y de otros encargados de obras, de que el trabajador incumplía gravemente su jornada y su horario de trabajo, no realizando el total de la misma y no visitando las obras en determinados momentos, por lo que decidió instalar un dispositivo de GPS en su vehículo de empresa para tener localizado el vehículo todo el tiempo y conocer los sitios que visitaba durante su jornada laboral. Al trabajador se le remitió una carta en la que se le recordaba su deber de cumplir con las obligaciones concretas de su puesto de trabajo, y se le advertía que el empresario podría adoptar las medidas que estime más oportunas de vigilancia y control. En sentido similar, la STSJ de Valencia de 2 de mayo de 2017 (rec. 3689/2016) consideró que, a pesar de no haber sido informados expresamente por el empresario de su instalación, los trabajadores conocían la existencia del GPS, porque emitía un sonido cuando se abría el vehículo que se apagaba al introducir la llave. E incluso en algún supuesto, a pesar de no existir ningún tipo de advertencia por parte del empresario, se ha considerado que no hay vulneración, pues, como señala la STSJ de Galicia de 6 de junio de 2014 (rec. 903/2014), no parece razonable que la empresa, ante la comisión de faltas laborales, desvele las medidas de control y de seguridad tendentes a prevenir o a disuadir a posibles infractores, cuando se refieren a vigilancia sobre mercancías, que pueden ser sustraídas, o localización de vehículos en sus rutas laborales en un ámbito que no se puede considerar de intimidad o privacidad o de estricto control de una persona con un fin ilegal.

Por tanto, parece que, aunque la regla general ha sido el deber de información al trabajador acerca de la instalación de los correspondientes dispositivos de geolocalización, no faltan sentencias que han considerado posible eludir el deber de información cuando el dispositivo se instala ante las sospechas razonables que tiene el empresario de que el trabajador está incumpliendo con sus obligaciones laborales.

instalar y mantener servicios de telecomunicaciones de la sociedad Telecable. La instalación de los dispositivos GPS y el uso de la información transmitida contribuye de forma importante a la supervisión del cumplimiento eficiente de la prestación de servicios, a corregir deficiencias en la confección y ejecución de las diferentes rutas y a mejorar la capacidad de respuesta ante los acontecimientos imprevistos (una solicitud urgente de un cliente, una avería de un vehículo, etc.) (FJ 4.º).

Esta situación cambia con la entrada en vigor de la LOPD/2018, pues la ley exige el deber de información con carácter previo sin ningún tipo de excepción.

Ahora bien, una duda que se planteaba ya antes de la entrada en vigor de la nueva LOPD, y que esta no resuelve, es si resulta necesario que el empresario indique expresamente que la instalación del correspondiente dispositivo GPS servirá para verificar el cumplimiento por parte de los trabajadores de las obligaciones y deberes laborales o si basta simplemente con que el trabajador tenga conocimiento de su instalación.

Si el sistema GPS se instala para controlar la posición del trabajador durante la jornada laboral, a mi juicio, basta con que el trabajador tenga conocimiento de que se ha instalado el citado dispositivo, pues la finalidad de control resulta implícita en su instalación. Si el sistema GPS se instala en el vehículo asignado, en el teléfono móvil, en la tableta o en cualquier otro instrumento de trabajo puesto a disposición de los trabajadores por la empresa para el desarrollo del servicio y la localización del trabajador, resulta difícil separar el control de la posición de tales instrumentos de trabajo del cumplimiento de las obligaciones laborales de los trabajadores. Como señala la STSJ de Castilla-La Mancha de 31 de marzo de 2015 (rec. 19/2015):

> […] si el sistema GPS se instala en el vehículo asignado precisamente para el desarrollo del servicio y para poder realizar las rutas de vigilancia, entonces no acertamos a discernir cómo puede separarse conceptualmente el control de posición de tal vehículo de la comprobación del cumplimiento de sus obligaciones por parte del trabajador (FJ 4.º).

De este modo, en estos casos, aunque el trabajador solo haya sido informado de la instalación del correspondiente sistema de geolocalización, pero no de que puede ser utilizado para el control de sus obligaciones laborales, a mi juicio, no se plantea ninguna duda en relación con si resulta o no exigible el deber de información.

Por el contrario, cuando el dispositivo se implanta con la función de proteger bienes empresariales (por ejemplo, vehículo de empresa), pero a la vez permite conocer la ubicación y los movimientos del trabajador, resulta dudoso si el empresario puede utilizar los datos obtenidos con una función de control. El artículo 90 de la LOPD/2018 no da respuesta a esta situación. ¿Basta con que el trabajador haya sido informado de la instalación y características del correspondiente dispositivo? Esta es la única obligación que el precepto impone al empresario, sin que en ningún momento exija que los empresarios informen a los trabajadores de que este sistema podrá ser utilizado para su control. El casuismo se impone de nuevo en estos casos. A mi juicio, resulta significativa la diferente redacción del artículo 89, en relación con los dispositivos de videovigilancia y grabación, y el artículo 90, en relación con los sistemas de geolocalización. Así, el artículo 89, tras señalar que los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras

para el ejercicio de las funciones de control de los trabajadores, afirma que estos habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores «acerca de esta medida». Es decir, habrán de informarles de que las cámaras o videocámaras podrán controlar su trabajo. Por el contrario, el artículo 90, tras señalar igualmente en el apartado 1 que los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de funciones de control, en el apartado 2 no dice que los empresarios deberán informar de forma expresa, clara e inequívoca a los trabajadores sobre esta medida, sino que habrán de informar «acerca de la existencia y características de estos dispositivos». No parece, por tanto, que deban informarles sobre la posibilidad de control laboral por los correspondientes sistemas de geolocalización. Si el legislador así lo hubiera querido podría haber utilizado la misma expresión que para los sistemas de videovigilancia, sin embargo no lo ha hecho.

La utilización de los sistemas de geolocalización en vehículos o dispositivos móviles puestos a disposición de los trabajadores por la empresa viene planteando también problemas cuando los mismos siguen siendo utilizados fuera de la jornada de trabajo. En estos casos, el problema surge si el trabajador no está informado de que el sistema de geolocalización puede ser utilizado para controlar su actividad fuera de la jornada laboral. La AEPD ha señalado en su Informe 90/2009 que el tratamiento de los datos de localización fuera del tiempo de la prestación laboral resulta excesivo en relación con la finalidad perseguida, por lo que vulnera el principio de proporcionalidad y resulta contrario a la LOPD. En este mismo sentido, el Dictamen 5/2005 del Grupo de Trabajo del artículo 29, al que anteriormente hemos hecho referencia, señala que:

> […] en cualquier caso, el requisito relativo a la finalidad implica que un empresario no debería recoger datos de localización en relación con un empleado fuera de su tiempo de trabajo. Por consiguiente, el Grupo recomienda que se dote a los equipos puestos a disposición de los empleados, y especialmente a los vehículos que también puedan ser utilizados con fines privados, de un sistema que les permita desactivar la función de localización.

Uno de los pilares fundamentales para la licitud del control de los desplazamientos por medio de dispositivos GPS y del tratamiento de los datos personales obtenidos por su medio es que la existencia de relación laboral faculta a la empresa para, en el ejercicio de sus facultades directivas y supervisoras, establecer algunos límites a derechos fundamentales de los trabajadores. Ahora bien, cuando finaliza la jornada laboral o acaba el tiempo de trabajo, la doctrina judicial considera que dichas facultades empresariales desaparecen y el contrato de trabajo deja de constituir el vínculo entre las partes que ampara el poder de la empresa para imponer medidas de captación y tratamiento de datos. A partir de ese momento, es imprescindible el consentimiento de los trabajadores para mantener en funcionamiento los dispositivos GPS y para el análisis automatizado de los datos personales conseguidos por ese medio.

Es indiferente, como ha señalado la doctrina judicial, que «al finalizar la jornada laboral, los trabajadores se hagan cargo de los vehículos que utilizan». Finalizada la jornada:

> […] el contrato de trabajo ya no ampara la restricción en los derechos fundamentales que supone la aplicación de la medida y por tanto no hay razón suficiente para prescindir del necesario consentimiento de los afectados. La protección por la empresa de sus bienes y el control del uso que de ellos se haga una vez terminada la jornada de trabajo no constituye una excepción a la vigencia de la indicada regla general (STSJ de Asturias de 27 de diciembre de 2017, rec. 2241/2017)[14].

Por ello, salvo que los trabajadores den su consentimiento, la empresa está obligada a contar con un procedimiento que le permita desactivar el sistema de posicionamiento global instalado, de forma que no capte datos a partir del momento en el que finalice la jornada laboral.

En este sentido se ha declarado nulo el despido de una trabajadora, en situación de incapacidad temporal, que fue despedida por utilizar el vehículo de la empresa durante dicha situación, a pesar de la prohibición de uso para fines ajenos a la actividad laboral. La empresa aportó como prueba el sistema de geoposicionamiento (GTA) con el que estaba dotado el vehículo. La Sala de lo Social del TSJ de Andalucía considera que:

> […] se han utilizado dichos datos, no con la finalidad de control durante su jornada laboral, sino en relación a tramos horarios ajenos a la jornada laboral, como era los periodos de baja por incapacidad temporal, para lo que no se encontraba autorizado, todo lo cual comporta […] la consiguiente declaración de nulidad del despido acontecido, al quedar constancia de que la actora no era conocedora de la instalación del GPS, en el vehículo que conducía, para supuesto ajeno al control de su jornada de trabajo (Sentencia de 19 de octubre de 2017, rec. 1149/2017).

[14] En el mismo sentido, STSJ de Castilla-La Mancha de 10 de junio de 2014 (rec. 1162/2013), según la cual el trabajador «no puede ser objeto de seguimiento durante todos los días de su vida laboral, y tanto durante la jornada como fuera de ella (al no tener prohibida la utilización del teléfono móvil fuera del tiempo de actividad laboral)».

Referencias bibliográficas

Adsuara Varela, B. (2016). El consentimiento. En J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Reus.

Córdoba Castroverde, D. y Díez-Picazo Giménez, I. (2016). Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico. En Asociación de Letrados del Tribunal Constitucional (Coord.), *El derecho a la privacidad en un nuevo entorno tecnológico. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional* (pp. 99-122). Madrid: Centro de Estudios Políticos y Constitucionales.

Charcategui Jávega, C. (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 Derecho Social*, *83*, 119-132.

Desdentado Bonete, A. y Muñoz Ruiz, A. B. (2012). *Control informático*, *videovigilancia y protección de datos en el trabajo.* Valladolid: Lex Nova.

Fernández García, A. (2010). Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial. *Aranzadi Social. Revista Doctrinal*, *17*(2), 91-105.

García Murcia, J. y Rodríguez Cardo, I. A. (2019). La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo. *Nueva Revista Española de Derecho del Trabajo*, *216*, 19-64.

García-Perrote Escartín, I. y Mercader Uguina, J. R. (2017). La protección de datos se come a la intimidad: la doctrina de la Sentencia del TEDH de 5 de septiembre de 2017 (caso Bărbulescu v. Rumania; n.º 61496/08; Gran Sala). *Revista de Información Laboral*, *10*.

Goerlich Peset, J. M. (2016). Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas. En Asociación de Letrados del Tribunal Constitucional (Coord.), *El derecho a la privacidad en un nuevo entorno tecnológico. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional* (pp. 123-150). Madrid: Centro de Estudios Políticos y Constitucionales.

Goñi Sein, J. L. (2009). Controles empresariales: geolocalización, correo electrónico, internet, videovigilancia y controles biométricos. *Justicia Laboral*. *Revista de Derecho del Trabajo y de la Seguridad Social*, *39*, 11-58.

Gude Fernández, A. (2014). La videovigilancia laboral y el derecho a la protección de datos de carácter personal. *Revista de Derecho Político (UNED)*, *91*, 43-90.

Navarro Nieto, F. (2019). La videovigilancia laboral. Un comentario a la STEDH de 17 de octubre de 2019. Asunto López Ribalda, *Diario La Ley*, *9519*.

Orellana Cano, A. M. (2019). *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores.* Pamplona: Aranzadi.

Rodríguez Escanciano, S. (2019). Videovigilancia empresarial: límites a la luz de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. *Diario La Ley*, *9328*.

Rojo Torreccilla, E. (2018). Derecho del empleador a la privacidad en la empresa y límites a su control por cámaras de videovigilancia. Estudio del caso López Ribalda y otros contra España (a propósito de la STEDH de 9 de enero de 2018). *Derecho de las Relaciones Laborales*, *2*, 135-152.

Thibault Aranda, J. (2009). La vigilancia del uso de internet en la empresa y la protección de datos personales. *Relaciones Laborales. Revista Crítica de Teoría y Práctica*, *1*, 215-226.

Troncoso Reigada, A. (Dir.). (2010). *Comentario a la Ley orgánica de protección de datos de carácter personal*. Madrid: Civitas.

Vizcaíno Calderón, M. (2001). *Comentarios a la Ley orgánica de protección de datos de carácter personal*. Madrid: Civitas.