LAS FACULTADES DE CONTROL A DISTANCIA DEL TRABAJADOR: GEOLOCALIZADORES Y TACÓGRAFOS

SANTIAGO GONZÁLEZ ORTEGA
Catedrático de Derecho del Trabajo y de la Seguridad Social
Universidad Pablo de Olavide de Sevilla

EXTRACTO **Palabras Clave:** Geolocalización, privacidad, juicio de ponderación, derechos de información

El artículo versa sobre la implantación empresarial de dispositivos de geolocalización del trabajador tanto a la luz de las resoluciones judiciales como del contenido de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Partiendo de la consideración indiscutible de los datos de localización como datos personales, el análisis se centra en las exigencias referidas a la licitud de la obtención y tratamiento de esos datos así como en la necesaria ponderación entre los intereses empresariales y los derechos fundamentales del trabajador, sea a la intimidad (art. 18.1 de la Constitución) sea a la particular libertad informática (art. 18.4 de la Constitución). Se consideran, en consecuencia, las diferentes hipótesis de confrontación entre la función de control de los dispositivos mencionados y la privacidad del trabajador, estableciendo en qué casos y bajo qué condiciones dicho control es legalmente posible; con una atención particular a los derechos de información fuertemente revalorizados por la normativa de protección de datos.

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

The article deals with the business implementation of geolocation devices of the worker both in the light of judicial decisions and the content of Ley Orgánica 3/2018, of December 5, de Protección de Datos y Garantía de los Derechos Digitales. Starting from the unquestionable consideration of location data as personal data, the analysis focuses on the requirements related to the legality of obtaining and processing such data as well as the necessary balancing between business interests and the fundamental rights of the worker, either to privacy (art. 18.1 CE) or to particular computer freedom (art. 18.4 CE). Consequently, the different hypotheses of confrontation between the control function of the mentioned devices and the worker's privacy are considered, establishing in what cases and under what conditions such control is legally possible; with a particular attention to the information rights strongly revalued by the data protection regulations.

 Recepción de original: 16.11.2019. Aceptación: 26.11.2019

ÍNDICE

1. DISPOSITIVOS DE GEOLOCALIZACIÓN Y TACÓGRAFOS: SU USO EMPRESARIAL

Según el apartado 9 del Anexo II (Definiciones) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, los datos de localización son: *"Cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público"*[1]. La información básica, pues, de un geolocalizador es de tipo geográfico ya que permite establecer en cada momento la posición del dispositivo electrónico de que se trate. Algo que puede obtenerse, bien incorporando el concreto sistema de geolocalización (un navegador o un GPS) a un elemento móvil (un vehículo o medio de transporte, por regla general), bien porque la aplicación geolocalizadora forma parte de un dispositivo electrónico móvil como un smartphone, una tablet o un ordenador portátil, bien, en fin, porque se trate de los llamados *wearable de-*

[1] La misma definición se encuentra en el art. 2 de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), a la que se refiere el art. 95 del 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 datos personales y a la libre circulación de estos datos (norma a la que se hará referencia en lo sucesivo como RGPD). También en el art. 64, b) del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

vice (WD), es decir, dispositivos de geolocalización diseñados para ser llevados o vestidos tales como pulseras, relojes, prendas de vestir o de trabajo[2]. En todo caso, hay que subrayar que los datos suministrados por los geolocalizadores pueden ser muy variados y completos ya que no solo realizan la función básica de indicar la posición en cada momento del dispositivo (geolocalización estática),sino también sus movimientos, el trayecto realizado, el tiempo invertido en cada recorrido yel de espera (geolocalización dinámica); o, incluso, el tipo de conducción o el consumo de combustible, si se trata del uso de vehículos, o datos de lugar y de actividad en el caso de los teléfonos y de determinados WD[3].

Por su parte, el tacógrafo es también un dispositivo electrónico que registra continuamente ciertos datos correspondientes al movimiento de un vehículo de transporte terrestre o ferroviario y que, pudiendo ser analógico, ha sido sustituido de forma generalizada por el tacógrafo digital el cual envía señales o datos que pueden ser recopilados y tratados informáticamente[4]. Mediante el tacógrafo se registran datos e incidencias producidas durante la conducción del vehículo tales como, entre otros, la distancia recorrida, el tiempo invertido, la velocidad promedio

[2] Sobre estos últimos dispositivos y su posible función geolocalizadora, entre otras, Mercader Uguina, J. *Protección de datos en las relaciones* laborales, Francis Lefevre, 2018, pp. 137-138. Para la función de geolocalización también pueden servir las redes wifi en la medida en que transmitan la posición de los dispositivos; los archivos electrónicos que se envían y que den datos de la ubicación del dispositivo; las estaciones base de telefonía que recogen constantemente la ubicación espacial de los teléfonos móviles; o, incluso, las propias direcciones IP de los ordenadores, debido a que la asignación de un número de IP se hace mediante criterios geográficos (Cabello Gil, L. "Geolocalización a través de direcciones IP", *Revista de Derecho UNED*, 20/2017, p. 284). No obstante, estos sistemas de localización sirven esencialmente a otras finalidades tales como la seguridad pública y, en consecuencia, no se tendrán en cuenta en el presente trabajo. Un dispositivo peculiar, aunque también con función geolocalizadora se menciona en la Sentencia del Tribunal Superior de Justicia (STSJ, en adelante) de Cataluña, de 23 de mayo de 2013 (AS 2013/2445) en relación con un denominado acelerómetro instalado en los teléfonos móviles de los trabajadores de la sección de mantenimiento, consistente en un aparato electromecánico que permite convertir fenómenos físicos en señales, es decir, es un aparato que se encarga de captar el movimiento o la ausencia del mismo y que, en el caso, se complementaba con un GPS integrado en el teléfono.

[3] Así se evidencia en el caso juzgado por la STSJ 3058/2017, de Asturias, de 27 de diciembre (AS/2018/296), en cuyos hechos probados se establece que el dispositivo instalado por la empresa en los vehículos de la misma destinados al uso productivo (en el supuesto, tareas móviles de instalación y mantenimiento de sistemas de telecomunicación) tenía como funciones las siguientes: localización en tiempo real, visualización de trayectos con posición segundo a segundo, visualización de tramos conducidos con exceso de velocidad, detección del vehículo más cercano a un punto o calle, cuentakilómetros basado en un GPS y creación de alertas (hora de arranque y aparcamiento del vehículo, paradas no autorizadas, duración excesiva de las paradas y puntos de paso); todo lo cual permitía elaborar informes de distancia o por periodos, ralentí, itinerarios y su reconstrucción con duración y kilometraje así como recorridos efectuados fuera de horario, exceso de velocidad, número de paradas, duración y retrasos. Esto es, una información mucho más completa y precisa que la simple de ubicación física; aunque es obvio que las potencialidades de la aplicación pueden modularse y limitarse, lo que es esencial a la hora de establecer el equilibrio entre los intereses empresariales y los derechos fundamentales de los trabajadores.

[4] El uso de tacógrafos digitales es obligatorio para vehículos de transporte de más de 3.5 toneladas o que puedan transportar más de 9 personas y que se hayan matriculado a partir del1 de enero de 2006, según lo establece el art. 3 del Reglamento (CEE) nº 3821/85 del Consejo, de 20 de diciembre de 1985, relativo al aparato de control en el sector de los transportes por carretera.

y máxima, las aceleraciones y frenadas bruscas o frenadas de pánico, las revoluciones por minuto, el tiempo al ralentí durante el cual el vehículo está detenido y con el motor encendido, o las interrupciones en la conducción. Como se ha indicado, su ámbito de actuación es más restringido ya que se limita a los vehículos terrestres tales como los automóviles, los vehículos de carga y de pasajeros, así como a los ferroviarios.

Sin duda que el recurso empresarial a este tipo de dispositivos puede tener una justificación organizativa, técnica o productiva en términos de eficiencia, de control y de seguridad. Es así respecto de prestaciones de servicios que se desarrollan fuera de los centros de trabajo para las que la utilización de geolocalizadores sirve para una mejor y más eficiente prestación laboral al permitir, por ejemplo, asignar tareas en razón de la situación concreta del trabajador por tratarse de destinatarios de servicios ubicados en su entorno (el supuesto de trabajadores dedicados a reparto, mantenimiento, reparación, instalación, entrega de productos o cualquier tipo de servicio técnico a prestar en el domicilio del cliente o en el lugar donde éste se encuentre)[5]. El conocimiento de la concreta ubicación del trabajador es igualmente útil en todas las actividades de transporte de mercancías o de pasajeros en la medida en que permite planificar la ruta a seguir, conocer las incidencias que puedan surgir en el trayecto y rediseñarlo en función de ellas, establecer su duración y ponerla en conocimiento del destinatario o cliente. Por otra parte, también puede ser útil y productivamente necesario conocer la ubicación de determinados trabajadores en relación con actividades que, no siendo estáticas en la medida en que carecen de un concreto lugar de trabajo, se desarrollan dentro de la empresa pero en centros muy grandes o con varias instalaciones separadas entre sí pero concentradas en un espacio geográfico; sirva el ejemplo de empresas con dependencias de gran dimensión como almacenes o depósitos, el trabajo en grandes obras de construcción o de infraestructura, o cuando el lugar exacto donde se presta el trabajo o el servicio puede variar constantemente como sucede con los trabajos de seguridad o de vigilancia.

A estas razones empresariales, vinculadas a la organización más eficiente del trabajo, se unen otras conectadas con un mejor control de la realización de la prestación laboral por parte del trabajador afectado. Una facultad que encuentra su fundamento no sólo en la libertad de empresa y en la defensa de la productividad (art. 38 de la Constitución Española, CE) sino, más concretamente, en el art. 20.3 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el

[5] A este respecto cabe resaltar la absoluta trascendencia que el conocimiento de la concreta ubicación del trabajador tiene en relación con la prestación de servicios a través de las plataformas digitales las cuales asignan los trabajos en razón de la posición del trabajador y su mayor o menor cercanía respecto del cliente ya se trate de servicios de transporte, en sus varias modalidades, o de entrega de productos de diverso tipo. Lo mismo sucede con los servicios de urgencia o de emergencia en los que la rapidez de la atención depende de la cercanía geográfica del trabajador al solicitante del servicio; el ejemplo de la asistencia en carretera de los titulares de un seguro que comprenda esta prestación, sea de reparación o de traslado mediante grúas al taller más cercano, es tópico.

Texto Refundido de la Ley del Estatuto de los Trabajadores (ET, en lo sucesivo) al que se remite el art. 90 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LO 3/2018, en lo sucesivo), justamente dedicado al tema de la geolocalización en el ámbito laboral. En consecuencia, la geolocalización, sobre todo cuando más que la mera ubicación proporciona informaciones adicionales en relación con el trayecto, el tiempo invertido, los tiempos de inactividad, parada o de espera, el consumo e incluso tipo de conducción si se trata de vehículos, constituye una forma de control a distancia de la prestación laboral en los numerosos casos en los que la supervisión personal directa es inviable, muy dificultosa o productivamente menos eficiente o más costosa. Un control similar al que los tacógrafos permiten.

Finalmente, los sistemas de geolocalización sirven igualmente para funciones de seguridad, tanto del vehículo y sus pasajeros como del dispositivo móvil de que se trate, frente a accidentes, pérdidas, robos u otras incidencias similares. Efectivamente, la identificación precisa de trayecto y lugar concreto hace más eficaz y pronta la prestación de servicios de asistencia o de reparación de cualquier tipo, así como de seguimiento y recuperación del vehículo o del dispositivo. Razones de seguridad relacionadas con el tráfico son igualmente las que justifican la implantación del tacógrafo; de aquí su obligatoriedad por la existencia de intereses generales a los que ese control satisface y respecto de los que la empresa es codefensora forzosa en relación con el comportamiento de sus trabajadores. Por último, el reclamo a la seguridad también puede hacerse respecto de trabajadores particularmente expuestos como es el caso de los que prestan servicios de seguridad o en condiciones de trabajo especialmente arriesgadas o singulares, en relación con los cuales conocer su ubicación concreta y su recorrido puede ser un factor adicional de seguridad.

2. LOS DATOS DE UBICACIÓN Y DE MOVIMIENTO COMO DATOS PERSONALES PERTENECIENTES A LA ESFERA DE PRIVACIDAD DEL TRABAJADOR: SUS CONSECUENCIAS

Que el recurso a los dispositivos de geolocalización y a los tacógrafos tenga una evidente utilidad empresarial, e incluso un fundamento constitucional y legal, no significa, obviamente, que su uso sea libre y que, en el caso de la empresa, puedan instalarse sin ningún tipo de motivación adicional, requisito o cortapisa. Dejando al margen los supuestos en los que esa instalación es obligatoria (el tacógrafo en ciertas circunstancias, como se ha dicho[6]), lo cierto es que la implantación y uso de tales herramientas empresariales tiene límites derivados de su condición

[6] En cuyo caso los requisitos de uso y sus limitaciones vendrán reguladas por las normas que establecen su obligatoriedad; de manera que el equilibrio entre los intereses públicos (a los que pueden

de datos vinculados con la persona del trabajador y que pueden calificarse como informaciones cuya obtención y uso empresarial digitalizado pueden invadir su esfera personal de reserva, de privacidad o de intimidad tutelada por el art. 18 de la Constitución Española.

A esta conclusión se llega esencialmente como consecuencia de la aplicación de la normativa de protección de datos que ha contribuido de forma directa a ampliar y mejorar la protección de los derechos reconocidos por el art. 18 CE sobre la base de la mayor potencialidad lesiva para la privacidad del trabajador del acceso a los datos referidos a su persona cuando, siendo la aportación esencial de las tecnologías de la información, esos datos se acumulan y combinan permitiendo obtener de forma instantánea un perfil del trabajador compuesto por una serie de informaciones respecto de comportamientos, actividades, hábitos, actitudes, relaciones y contextos que es indiscutible que, en cuanto caracterizadoras de su personalidad, pertenecen al espacio de su vida privada. Para lo que dicha normativa especializada ha introducido un referente determinador de su campo de aplicación que no es otro que el muy amplio concepto de "dato personal"[7].

2.1. Los datos de geolocalización como datos personales a los efectos del RGPD y de la LO 3/2018

Aunque podría sostenerse que los datos proporcionados por los dispositivos de geolocalización y por los tacógrafos no son, en principio y de forma directa, datos personales ya que se refieren a la ubicación y al movimiento del propio dispositivo, sin embargo, la amplia definición de dato personal permite concluir lo contrario. Así lo justifica la mención expresa a los datos de localización contenida en el art. 4 RGPD, en la medida en que se trata de datos que permiten la identificación de una persona concreta, vinculando a ella la información de ubicación, movimiento y actividades que tales datos reflejan. Y lo da por descontado, sin mayores precisiones y respecto de los trabajadores asalariados, el ya citado art. 90 LO 3/2018, el cual somete a las reglas de la norma, que tiene como objetivo el tratamiento de los datos personales, los datos de los trabajadores obtenidos mediante sistemas de geolocalización.

La calificación como dato personal de los logrados a través de mecanismos

asociarse los de tipo empresarial) y los derechos fundamentales del trabajador se establece, en principio, por la propia norma legal.

[7] En concreto, el art. 4.1 del RGPD establece que serán datos personales*: "toda información sobre una persona física identificada o identificable («el interesado»)"*; añadiendo 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"*.

de geolocalización (y también mediante los tacógrafos que cumplen, como se ha visto, una función similar) se fundamenta, según se ha dicho, en el hecho de la vinculación del dispositivo con una persona concreta. Lo que, en principio, puede hacerse a través de los títulos de propiedad o de uso del vehículo en el que va incorporado el dispositivo o del dispositivo mismo, títulos que harán relativamente fácil identificar al usuario. Algo que, específicamente en el terreno laboral, queda además facilitado en la medida en que el vehículo es una herramienta de trabajo, bien asignada al trabajador por la empresa o bien destinada, si es del propio trabajador, a tareas laborales por acuerdo de las partes, lo que permite identificar al trabajador concreto responsable de ese uso. También cuando el dispositivo móvil con sistemas de geolocalización es proporcionado al trabajador por la empresa, o, siendo privado, es utilizado a efectos laborales, basándose el proceso de identificación en el hecho de que tales dispositivos suelen acompañar y estar permanentemente a disposición de sus usuarios, no siendo habitual, por razones de defensa de la privacidad, que se presten a otros. En todo caso, la identificación personal es directa porque existe una orden empresarial de uso laboral de tales dispositivos, circunstancia que hace inmediata esa identificación. En consecuencia, todos los datos proporcionados por un geolocalizador o un tacógrafo deben ser considerados datos personales[8], mucho más cuando se trata de trabajadores en el desempeño de sus tareas.

La aceptación de que los datos de localización son datos personales[9] y que, en principio, pertenecen a la esfera privada del trabajador les garantiza la tutela que le ofrecen tanto el RGPD como la LO 3/2018. Se trata de normas que giran en torno a la idea de tratamiento que viene definido por el art. 4.2 del RGPD como: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".*

Las garantías establecidas en las normas citadas rigen ciertamente en relación

[8] Batuecas Caletrio, A. "Intimidad personal, protección de datos personales y geolocalización", *Derecho Privado y Constitución*, 29/2015, pp. 48-54; en igual sentido, Mercader Uguina, cit. p. 127 y Baz Rodríguez, J. "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático". *Trabajo y Derecho,* 54/2019, p. 21, citando en el mismo sentido al Dictamen del Grupo 29 (GT29), creado por la Directiva 95/46/CE, del Parlamento y del Consejo, de 24 de octubre de 1995 sobre la base del art. 29, 5/2005, de 25 de noviembre de 2005, sobre usos de los datos de geolocalización con vistas a prestar servicios con valor añadido. Un Grupo que ha dejado de ser activo desde mayo de 2018.

[9] Incluso cuando los datos solo reflejen información obtenida en tiempo de trabajo y sobre circunstancias relacionadas con la actividad laboral (en contra, STSJ de Cataluña 1706/2012, de 5 de marzo) ya que las normas de protección de datos no diferencian, a efectos del tratamiento, qué origen tienen esos datos, qué naturaleza ostentan y respecto de qué funciones se han obtenido, siendo en todo caso datos personales.

con lo que podría llamarse tratamiento en sentido estricto, comprensivo de todas las operaciones descritas por el art. 4.2 y que se conectan con medidas como, entre otras, las relacionadas con la transparencia y la información, los derechos de acceso, revocación, rectificación o supresión, con los elementos mínimos de seguridad de los sistemas, con la identificación de responsables, encargados y delegados así como el reparto de responsabilidades entre ellos, con la intervención de tutela de organismos públicos nacionales y comunitarios y con el conjunto de infracciones y sanciones en el caso de violación de esos derechos.

Pero también afectan al momento inicial del tratamiento como es el de la recogida u obtención de los datos que queda sujeto a lo establecido en el art. 5.1, b) RGPD (Principios relativos al tratamiento) donde se establece que los datos personales deberán ser recogidos *"... con fines determinados, explícitos y legítimos..."*; no pudiendo ser *"... tratados ulteriormente de manera incompatible con dichos fines..."*. De manera que los datos personales que el geolocalizador proporciona pueden ser obtenidos siempre que se someta la medida al criterio de que su recogida esté basada en fines determinados (es decir, concretos y precisos) que, además de ser explícitos (explicación que está a cargo del sujeto interesado en obtenerlos, aquí el empresario), deben ser legítimos (esto es, estar suficientemente justificada su obtención en razón de los intereses empresariales, no lesionando, o haciéndolo solo parcialmente y en la menor medida posible, otros derechos o intereses que se confronten con ellos y de los que sea titular el trabajador). Es decir que, previamente al tratamiento en sí de los datos personales, ha de dilucidarse cuáles y en qué circunstancias pueden ser legítimamente obtenidos. Y, de poder serlo, será un tratamiento, lícito en el momento de la recogida, cuya licitud se proyecta sobre el tratamiento digitalizado; licitud inicial que, de no existir, haría siempre en cambio ilegítimo dicho tratamiento.

A lo anterior contribuye el art. 6 RGPD referido, precisamente, a la licitud del tratamiento y a las causas o circunstancias que lo avalan, cuando menciona, entre otras[10], el que el tratamiento sea necesario *"... para la ejecución de un contrato en el que el interesado es parte..."* (letra b). Se trata de una referencia que ha de matizarse en relación con lo que se entienda necesario para la ejecución de un contrato, cuestión que no ha de resolverse exclusivamente en la lógica de la utilidad empresarial; de manera que no todos los datos que puedan ser necesarios en cuanto útiles y convenientes para el desarrollo y la ejecución del contrato de trabajo pueden ser, por esta exclusiva razón, obtenidos y, posteriormente, tratados. Por el contrario, la necesidad, para ser legítima, ha de hacerse compatible con otros intereses y derechos como así lo pone en evidencia el mismo art. 6 (letra f) cuando

[10] Necesidad del tratamiento para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (letra c), con la finalidad de proteger intereses vitales del interesado u otra persona física (letra d), o para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos atribuidos al responsable del tratamiento (letra e). Justificaciones presentes, por ejemplo, en el caso del tacógrafo obligatorio.

señala que la necesidad del tratamiento (y su licitud) respecto de la satisfacción *"... de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero...*", podrá existir salvo que *"...sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales...*".

Es decir que la licitud del tratamiento (entendido éste en sentido amplio comprendiendo también la recogida de la información) de los datos de geolocalización solo existirá tras una confrontación entre las necesidades derivadas de la ejecución del contrato de trabajo, de la satisfacción de los intereses legítimos perseguidos por el responsable empresarial y de la existencia de obligaciones legales a su cargo (el caso del tacógrafo), de una parte, y los intereses, derechos y libertades fundamentales del trabajador, de otra, que puedan quedar afectados desde el momento en que se trata de datos personales.

Esta es una de las consecuencias positivas, desde el punto de vista de la defensa de los derechos fundamentales del trabajador, de la vigencia del bloque de normas dedicadas a la protección de datos ya que, orientadas particularmente a la protección del dato en cuanto al tratamiento en sentido estricto, han establecido un criterio de selección muy amplio del objeto como es el concepto de dato personal del que solo se exige que sirva para identificar a una persona. Pero, al ser un dato personal y cualquiera sea su naturaleza, queda sujeto por esta razón a las exigencias del RGPD y de la LO 3/2018 en cuanto a la recogida u obtención del dato. De manera que, desde el punto de vista del RGPD y de la LO 3/2018, no hay diferencia en cuanto a la protección dedicada al conjunto de datos personales. Y será solamente cuando se dilucide la licitud del tratamiento y se haga un juicio de ponderación entre intereses empresariales y derechos del trabajador cuando pueda atenderse, si acaso, a las distintas clases de datos personales o, más específicamente, a su relación más o menos directa con la intimidad tutelada por el art. 18.1 CE[11].

2.2. De la intimidad a la privacidad

A la conclusión anterior también se llega en virtud de una ampliación del concepto mismo de intimidad o, cuando menos, de la expansión de los instrumentos de tutela de la misma hacia otros datos constitutivos de la vida privada del trabajador; expansión en la que ha jugado un papel determinante precisamente la normativa de protección de datos.

Es indudable que, cuando se habla de datos personales, se está haciendo referencia también a los que pueden calificarse como datos íntimos. Se trata de un

[11] Acerca de este impacto positivo de las normas de protección de datos, Molina Navarrete, C. "Saber es poder: conectividad empresarial, geolocalización (GPS) y autodeterminación digital del trabajador", *Revista de Trabajo y Seguridad Social* (CEF), 419/2018, pp. 140-141.

concepto limitativo, dentro del más amplio de datos personales, que se encuentra, por ejemplo, en la Sentencia del Tribunal Constitucional (STC, en adelante) 292/2000, de 30 de noviembre. Según esta Sentencia, los datos íntimos se refieren a informaciones relacionadas con las dimensiones más reservadas de la vida personal y familiar y que, siendo la expresión más clara y directa de la personalidad del sujeto, éste quiere y tiene derecho, con base en el art. 18.1 CE, a *"...excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad..."* (en el mismo sentido, la STC 144/1999, de 22 de julio). Lo que, según el TC (citando, entre otras, a las STC 134/1999, de 15 de julio, 144/1999, de 22 de julio y 115/2000, de 10 de mayo) el art. 18.1 CE confiere al sujeto es el *"...poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido*...". Un tipo de datos que pueden identificarse con los que el art. 9, tanto del RGPD como de la LO 3/2018, califican como "*categorías especiales de datos personales",* consistentes en los que ". …. *revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física..."*[12]. Una categoría especial de datos, por cierto, aunque nada puede excluirse, a los que es difícil adscribir los derivados de los sistemas de geolocalización salvo cuando, abarcando momentos externos a la jornada de trabajo, revelan dimensiones o aspectos de la vida íntima del trabajador

Sin embargo, existen otros datos, dentro de los datos personales, que, formando parte del halo de la personalidad del individuo, tienen una relación menos directa con la intimidad pero cuya adquisición y tratamiento permiten ofrecer una imagen o perfil del sujeto. Son informaciones que se integran en el espacio inter-

[12] Datos que, en principio, no pueden ser tratados y, en consecuencia, tampoco obtenidos, salvo las numerosas excepciones que se contienen en el propio art. 9 RGPD entre las que cabe destacar, además de cuando existe consentimiento del trabajador (algo que la LO 3/2018, en su art. 9 y merced a la autorización establecida en el RGPD al respecto, ha hecho irrelevante al impedir que el solo consentimiento del afectado sea suficiente para levantar la prohibición de tratamiento, art. 9), cuando el tratamiento *"es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado"*; cuando es preciso para proteger intereses vitales del interesado o de otra persona física; cuando se refiere a datos personales de este tipo a los que el interesado ha dado publicidad manifiesta; cuando es necesario para el ejercicio de acciones de reclamación o de tutela judicial; cuando el tratamiento es necesario por razones de un interés público esencial; cuando es *necesario "para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social"*; o, en fin, cuando el tratamiento es necesario por razones de interés público relacionados con la salud pública. Tratamiento que, una vez más, el RGPD recuerda que *"... debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado*".

medio entre vida íntima y vida pública y que viene ocupado por la vida privada del sujeto, constituyendo toda una constelación de informaciones que, aislada o combinadamente, hacen posible acceder a dimensiones, actividades o aspectos personales que constituyen el ámbito de privacidad del sujeto. Algo que, justamente las innovaciones tecnológicas en el ámbito digital, entre ellas los datos de geolocalización, propician de una forma cada vez más invasiva.

Puede decirse, por tanto, que los datos personales comprenden tanto el círculo más cerrado de protección, como es el relativo a los datos íntimos que configuran la identidad más privada del sujeto, como también otras dimensiones de la persona como son sus ocupaciones, actividades, aficiones, relaciones sociales, hábitos y pautas de comportamiento que los datos de geolocalización, junto a otros obtenidos por ejemplo mediante sistemas de grabación de imágenes o de sonidos y conversaciones, pueden poner de manifiesto. Lo anterior provoca que, en alguna medida, el derecho a la intimidad se transmute en un derecho fundamental a la privacidad en la medida en que los datos derivados de la vida privada del sujeto se consideren vinculados, solos o de forma conjunta, con la intimidad misma, aunque no formen parte del núcleo irreductible de la misma.

La proyección de la tutela de la intimidad sobre los datos personales, incluidos los de geolocalización, en el sentido de requerir una justificación suficiente para recabarlos y tratarlos, está favorecida por el art. 8 de la Convención Europea para la protección de los derechos humanos y las libertades públicas (CEDH), de 14 de noviembre de 1950, al establecer como derecho fundamental el de toda persona al respeto a su vida privada y que la Sentencia del Tribunal Europeo de Derechos Humanos (STEDH), de 2 de septiembre de 2010 (Caso Uzun contra Alemania)[13] considera *"...una noción amplia, que no se presta a una definición exhaustiva"*, ya que, *"...El artículo 8 protege principalmente el derecho a la identidad y al desarrollo personal, así como el derecho de todo individuo de empezar y desarrollar relaciones con sus semejantes y el mundo exterior. Existe pues una zona de interacción entre el individuo y terceros, que aun en un contexto público, puede competer a la vida privada…"*.

Por esta razón, el concepto de la intimidad tutelada por el art. 18.1 CE se ha ido ampliando hacia datos que integran, más que la estricta intimidad, otras dimensiones de la vida privada del sujeto. O, cuando menos, se ha proyectado la tutela de la intimidad, y con iguales garantías instrumentales en cuanto al momento de su recogida, sobre dimensiones de la vida del trabajador que pertenecen a su ámbito de privacidad[14]. Algo que confirma el TC (Sentencia 202/1999, de 8 de noviembre, entre otras muchas), al sostener que *"...si bien hemos afirmado en alguna ocasión*

[13] JUR\2010\301139, en un caso de instalación de geolocalizadores por la policía con la finalidad de investigar un delito.

[14] Superando las limitaciones del derecho a la intimidad cuando se confronta con el derecho fundamental (autónomo según la misma STC 292/2000) a la protección de datos, como así lo señala

que los hechos referidos a las relaciones sociales y profesionales en que el trabajador desempeña su actividad no se integran, en principio, en la esfera privada de la persona (...) no es menos cierto que también hemos matizado esa afirmación inicial señalando que no cabe ignorar que, mediante un análisis detallado y conjunto de esos hechos, es factible en ocasiones acceder a informaciones atinentes a la vida íntima y familiar del trabajador que pueden resultar lesivas del derecho a la intimidad personal protegido por el art. 18.1 CE…"[15].

Y a lo que han contribuido sin duda las normas relativas a la protección de datos, hoy condensadas en el RGPD y en la LO 3/2018, las cuales, merced a la amplitud del concepto de dato personal como objeto de tratamiento, exigen que cualquier dato personal, en la medida en que, con carácter general, puede afectar a la intimidad personal (lo que puede incluir sin duda a los datos de geolocalización), solo pueda ser obtenido, y tratado, cuando existan razones empresariales atendibles, adecuadas y proporcionales que justifiquen la invasión empresarial en la privacidad del trabajador.

Por este motivo destaca la STC 292/2000 "*…la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos*

la STC 292/2000, al indicar que*: "...Sin necesidad de exponer con detalle las amplias posibilidades que la informática ofrece tanto para recoger como para comunicar datos personales ni los indudables riesgos que ello puede entrañar, dado que una persona puede ignorar no sólo cuáles son los datos que le conciernen que se hallan recogidos en un fichero sino también si han sido trasladados a otro y con qué finalidad, es suficiente indicar ambos extremos para comprender que el derecho fundamental a la intimidad (art. 18.1 CE) no aporte por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico.."*. O que *"...el reconocimiento* (en el art. 18 CE) *de los derechos a la intimidad y al honor en el apartado inicial* (…) *no ofrecían garantías suficientes frente a las amenazas que el uso de la informática podía entrañar para la protección de la vida privada*…". De manera que *"...el constituyente quiso garantizar mediante el actual art. 18.4 CE no sólo un ámbito de protección específico sino también más idóneo que el que podían ofrecer, por sí mismos, los derechos fundamentales mencionados en el apartado 1 del precepto*…". Un plus de garantía que se materializa en la facultad de control asociada al derecho fundamental autónomo de libertad informática, o de autogestión informativa, establecido en el art. 18.4 CE. Sobre estas limitaciones del apartado 1 del art. 18 CE, Molina Navarrete, cit. pp. 140-141.

[15] Añadiendo que el derecho fundamental a la intimidad incluye, *"...tendiendo en especial al elemento teleológico que la proclamación de este derecho fundamental incorpora, la protección de la vida privada como protección de la libertad y de las posibilidades de autorrealización del individuo…"* Lo que alcanza *"...tanto a la intimidad personal stricto sensu, integrada, entre otros componentes, por la intimidad corporal (SSTC 37/1989, fundamento jurídico 7º; 137/1990, fundamento jurídico 10º; 207/1996, fundamento jurídico 3º) y la vida sexual (STC 89/1987, fundamento jurídico 2º), como a determinados aspectos de la vida de terceras personas que, por las relaciones existentes, inciden en la propia esfera de desenvolvimiento del individuo (SSTC 231/1988, fundamento jurídico 4º y 197/1991, fundamento jurídico 3º). Por lo que se refiere a los hechos referidos a las relaciones sociales y profesionales en que el trabajador desarrolla su actividad, si bien no se integran en principio en la esfera privada de la persona (STC 142/1993, fundamento jurídico 7º y ATC 30/1998, fundamento jurídico 2º), sin embargo no cabe ignorar que, mediante un análisis detallado y conjunto de los mismos, es factible en ocasiones acceder a informaciones atinentes a la vida íntima personal y familiar (STC 142/1993, fundamento jurídico 8º), en cuyo ámbito se encuentran, sin duda, las referencias a la salud..."*. En la misma línea y en relación con la videovigilancia, la Sentencia del Tribunal Europeo de Derechos Humanos (Gran sala), de 17 octubre 2019, en el asunto López Ribalda y otros contra España (Jur\2019\289974).

extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal…(…). Añadiendo que *"…El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado…".*

La protección de los datos personales, establecida en el art. 18.4 CE, refuerza por tanto la dispensada desde el art. 18.1 CE en relación con el derecho fundamental a la intimidad. Si no equiparándola, al menos extendiendo hacia el conjunto de los datos personales, catalogándolos como pertenecientes a la vida privada del individuo y, en consecuencia, integrantes de su privacidad, las formas de tutela prevista para los datos más íntimos. Si bien variando su intensidad en función de la relación más o menos directa existente entre el dato y el núcleo de la intimidad del trabajador. Algo que afecta, sin duda, a los datos de geolocalización. Así debe ser entendida la identificación hecha por el art. 90 LO 3/2018, específicamente dedicado a la geolocalización, del derecho fundamental a preservar como el de intimidad[16], ya que igualmente indica que la obtención de este tipo de datos, debiendo ser siempre funcionales al ejercicio de las potestades de control de la empresa (de aquí la cita expresa del art. 20.3 ET),será legítima "*siempre que estas funciones* (de

[16] Art. 90 LO 3/2018: *"Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. 1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización 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. 2. 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".* La referencia a la intimidad como el derecho fundamental a tutelar se encuentra en todos los artículos de la LO 3/2018 relativos a la protección de datos y el uso de dispositivos electrónicos por parte de los trabajadores en cuanto herramientas de trabajo y también como por parte del empresario para finalidades de control. Así sucede con el art. 87, referido al uso de dispositivos digitales en el ámbito laboral que menciona repetidamente el derecho a la intimidad como el derecho fundamental a proteger. Sin embargo, el art. 89, en cuanto al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, que también se encabeza con la mención al derecho a la intimidad, se recoge lo establecido en el art. 90 en lo que hace al hecho de que las funciones de control deben ejercitarse dentro del marco legal y con los límites inherentes a las mismas; lo que remite a un juicio de ponderación que afecte a los datos personales. Más clara es la privacidad, tal y como se identifica en el texto, en el art. 88, referido a la desconexión digital y que, en puridad, no tiene una relación directa con la problemática del tratamiento de datos ya que con ella lo que se pretende es proteger la intimidad personal y familiar así como el derecho al descanso y a la conciliación de la vida personal, familiar y laboral de la persona trabajadora que pueden quedar afectadas, de una forma particularmente agresiva, mediante el uso empresarial de herramientas digitales de comunicación; de aquí seguramente su inclusión en el texto de la LO 3/2018, aunque, en realidad, podría igualmente haber quedado incluida en el propio ET.

control instrumentada a través de la obtención del dato y su posterior tratamiento) *se ejerzan dentro de su marco legal y con los límites inherentes al mismo"*[17].

Lo anterior reclama unos referentes de juicio y de valoración que no se encuentran esencialmente ni en el RGPD ni en la LO 3/2018 sino en los intereses y derechos que puedan quedar afectados en el proceso de obtención del dato. Que, por lo dicho, no es solo el derecho a la intimidad personal y familiar y a la propia imagen sino, más ampliamente, a la reserva de todo dato mediante el cual se pongan de manifiesto hábitos, comportamientos, actitudes personales, relaciones y actividades; es decir, circunstancias que pertenecen al espacio de privacidad que debe ser tutelado frente a invasiones no consentidas. Mucho más cuando el hecho de que tales datos personales puedan ser tratados digitalmente incrementa la agresividad de la obtención del dato en la medida en que ese tratamiento puede contribuir de forma decisiva, merced a su capacidad de acumulación y de combinación de la información, a ofrecer una imagen, extremadamente detallada de la persona de que se trate. Imagen que, así obtenida, invade sin duda los espacios protegidos por el derecho a la intimidad, o si quiere, de la vida privada. Todo ello como una manifestación de respeto al más genérico valor de la dignidad humana, constitucionalmente reconocido en el art. 10 CE como soporte y condensación de todos los derechos fundamentales, al que precisamente se refiere el art. 20.3 ET como aparentemente el único límite a la facultad de control por parte del empresario.

La ponderación anterior es necesaria, por tanto, siempre que lo que se recaben sean datos personales, incluidos los datos de localización. Así lo reclama la STC 202/1999, antes citada, sosteniendo que *"...para comprobar si una medida restrictiva de derechos fundamentales supera el juicio de proporcionalidad, 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*...".

[17] De esta forma debe ser también entendida la referencia a la intimidad del art. 20 bis ET (añadido precisamente por la LO 3/2018) señalando el derecho de los trabajadores a la misma en relación con el entorno digital.

3. LOS DATOS DE GEOLOCALIZACIÓN DESDE LA PERSPECTIVA DEL DERECHO A LA INTIMIDAD Y AL RESPETO A LA VIDA PRIVADA DEL TRABAJADOR

El primer momento de tutela de los datos de geolocalización, directamente relacionado con la obtención misma del dato, es la exigencia de una justificación empresarial suficiente del conjunto de formas de control que la empresa pretende establecer; para valorar en qué medida esa intromisión en la privacidad del trabajador está suficientemente motivada. Lo cual, y respecto de los datos de geolocalización, significa que habrá de procederse a un juicio de razonabilidad atendiendo a los criterios ya consolidados por el TC de la necesidad, la adecuación, la subsidiariedad y la proporcionalidad en sentido estricto de la medida empresarial[18]. Y solo tras esa valoración, que debe hacerse atendiendo a las características concretas y específicas de la medida de control, de su alcance, de su duración y de su justificación laboral, de su naturaleza más o menos invasiva, y de la posibilidad de que existan otros medios menos lesivos para la privacidad de lograr los objetivos productivos o de control, podrá aceptarse o rechazarse su práctica.

En definitiva, los datos recopilados deben limitarse a lo necesario para lograr la finalidad empresarial y la captación de información debe adecuar su contenido y forma con el concreto objetivo perseguido; en el entendido de que el recurso a modos de control de los trabajadores, como la geolocalización, no puede ser un objetivo en sí mismo, sino exclusivamente una consecuencia indirecta de una medida necesaria e imprescindible para garantizar el funcionamiento eficiente de la empresa y para proteger la producción, la salud y la seguridad.

No obstante, y aunque los datos de ubicación física y de movimiento del trabajador son datos personales, el grado de agresividad de los sistemas de geolocalización respecto de la vida privada del trabajador depende directamente de qué se considere que son los datos obtenidos y, sobre todo, de su vinculación, más o menos lejana o directa, con la intimidad personal.

3.1. La tesis de la escasa conexión de los datos de geolocalización con la intimidad del trabajador

Es lo que refleja una determinada orientación jurisprudencial que tiende a considerar plenamente legítimo, recurriendo para ello a los habituales apoyos constitucionales y legales (arts. 38 CE y 20.3 ET), el interés empresarial, ya sea debido a razones organizativas o de control de los trabajadores, de recabar datos de ubicación y de actividad a través de los dispositivos de geolocalización, siempre que esos datos

[18] Mercader Uguina, cit. p.127; Baz Rodríguez, cit. p. 22

se limiten a informaciones de carácter laboral o vinculadas de forma directa con la prestación del trabajo. Tras esta posición late sin duda la convicción de una escasa potencialidad lesiva para la privacidad del trabajador de los datos de geolocalización en la medida en que se limitan a señalar la posición y el recorrido del vehículo o de la persona o reflejan de forma indirecta las actividades laborales desempeñadas o no hechas, por lo que su captación no supone ninguna invasión desmesurada de la intimidad del trabajador que requiera una particular justificación. De aquí que se acepten razones muy someras para considerar legítima su obtención y tratamiento

De este modo la fundamentación empresarial se hace casi prescindible puesto que basta con argumentar mínimamente la conveniencia empresarial del dato para que su obtención se dé por legítima[19]. Sin que se descienda a valorar en profundidad el alcance de la medida de control, el tipo de dato, la información que se obtiene y las consecuencias de su tratamiento poniéndolo en conexión con el concreto y específico interés empresarial a tutelar y valorando si, por su naturaleza y alcance, la pretensión empresarial debe tener pese a todo, y en qué medida, forma y duración, preferencia sobre el derecho del trabajador a la tutela de su privacidad.

Es el caso, por ejemplo, de la STSJ de Galicia 668/2014, de 17 enero (AS/2014/637), para la cual el control empresarial mediante GPS es respetuoso con la dignidad y la intimidad del trabajador en la medida en que "…*en ningún momento el GPS instalado en el coche de la empresa tiene por objeto captar imágenes íntimas de los trabajadores sino facilitar el control, incluso en beneficio de la propia seguridad de los trabajadores…*". De lo que se deduce que los datos de geolocalización se consideran fuera del ámbito de la intimidad y, al ser banalizados solo como datos personales pero no íntimos, se minusvalora la intrusión que los mismos suponen respecto de la intimidad personal, no siendo en la práctica ningún obstáculo real que oponer frente a la justificación empresarial de la medida de organización y de control. De esta forma la ponderación entre el interés empresarial y el derecho fundamental del trabajador se decanta fácilmente hacia el lado empresarial cuya pretensión solo encuentra como límite unos datos cuya relevancia para la intimidad, aun siendo datos personales, la Sentencia devalúa haciéndolos más fácilmente obtenibles.

En un sentido similar se pronuncia la STSJ de Cataluña, 1706/2012, de 5 marzo (AS\2012\996) para la que *"...La instalación por parte de la empresa de*

[19] STSJ de Galicia, 2348/2017, de 26 abril (JUR\2017\125997) y STSJ de Valencia, 1165/2017 de 2 mayo (JUR\2017\221347) la cual justifica la instalación de geolocalizadores considerando que *"…no se vulneró el derecho a la intimidad del trabajador, puesto que la instalación del dispositivo de localización y control del vehículo es una medida proporcional para que la empresa pudiese controlar el destino de sus vehículos y el modo de prestación del servicio por unos comerciales que pasaban buena parte de su jornada fuera de su centro de trabajo. De este modo, el uso de medios de geolocalización debe estar relacionado con la actividad de la empresa y el trabajador (en este caso, como comercial), y tener una finalidad específica, en el caso de autos, como elemento de valoración, ante las quejas de clientes de la empresa sobre la falta de atención o retrasos por parte del trabajador como encargado de atenderlos…*".

un dispositivo GPS en un vehículo propio que pone a disposición del trabajador para realizar su trabajo con la finalidad de comprobar donde se encuentra el vehículo durante el tiempo en que el trabajador lo utiliza dentro de su jornada laboral, no es propiamente una recogida de datos de carácter personal que pueda afectar a la intimidad del trabajador, sino un medio de vigilancia y control para comprobar que el mismo cumple sus obligaciones laborales…". Es decir, una especie de legitimación por sí mismos de los instrumentos de control empresarial por el hecho de serlo toda vez que, en puridad, los datos que se obtienen y tratan tienen una connotación personal limitada y, en consecuencia, una relación con la intimidad muy debilitada.

No obstante, también existen ejemplos en los que los tribunales proceden a realizar el juicio de ponderación con todas sus consecuencias reclamando de la empresa una justificación pormenorizada del tipo de control, de sus características y de su finalidad respecto de necesidades organizativas, productivas o de vigilancia de la prestación laboral. Así lo hace, por ejemplo, la STSJ 53/2018, de 26 de enero, de las Islas Canarias (AS/2019/822), la cual, en el caso de un conductor-limpiador que es despedido a consecuencia de la información generada por un GPS instalado en el smartphone entregado por la empresa que detecta incumplimientos laborales repetidos, aplica el llamado "test Barbulescu"[20] según el cual, al margen de la cuestión del derecho de información que se afrontará en el epígrafe siguiente, se pregunta sobre el alcance y consecuencias del control, sobre el grado de intrusión en la vida privada del trabajador, sobre la justificación empresarial de dicho control y sobre su carácter imprescindible o necesario. En una línea semejante se pronuncia la Sentencia de la Audiencia Nacional (SAN) 13/2019, de 6 de febrero (AS/2019/905).

3.2. La tesis de la jornada de trabajo y la prestación laboral como límites a la obtención de datos de geolocalización

La lasitud en cuanto al tratamiento de los datos de geolocalización encuentra, sin embargo, un límite como es el establecido por la invasión mediante dicha información en los tiempos y actividades privadas del trabajador; algo que dichos sistemas pueden hacer si la información que proporcionan se refieren a movimientos y actividades fuera de la jornada o del lugar de la prestación laboral. En estos casos se entiende que esa invasión conecta de forma directa los datos de geolocalización con la intimidad del trabajador que se vería afectada por ese control externo al trabajo, debiendo ser defendida en cuanto revela datos que son, o deben ser, irrelevantes respecto de la prestación laboral.

[20] Establecido por la STEDH de 5 de septiembre de 2017, en el caso Barbulescu contra Rumanía respecto de un sistema de control del uso de internet por parte del trabajador.

Así lo entiende la STSJ de Asturias (3058/2017, de 27 de diciembre, AS/2018/296), la cual, aceptando la existencia de facultades empresariales que implican introducir límites a los derechos fundamentales, indica que *"...Cuando finaliza la jornada laboral o acaba el tiempo de trabajo, dichas facultades empresariales desaparecen y el contrato de trabajo deja de constituir el vínculo entre las partes que ampara el poder de la demandada para imponer las medidas implantadas de captación y tratamiento de datos..."*. Pero, y lo que es más relevante, se considera que el tratamiento del dato es igualmente ilegítimo incluso cuando los trabajadores, como parte del contrato, se hacen cargo de los vehículos puesto que *"...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..."*. Aunque en este punto la Sentencia abra la problemática, al pronunciarse en sentido positivo, de si el consentimiento prestado por el trabajador a ese control fuera del tiempo de trabajo basta para legitimar la recogida del dato; o, si por el contrario, la evidente desigual posición frente a la empresa hace que ese consentimiento deba ser irrelevante[21].

En este sentido se pronuncia la STSJ de Cataluña, de 23 de mayo de 2017, para la que la instalación de un dispositivo de geolocalización en el teléfono móvil de los trabajadores constituye una invasión de la intimidad personal en cuanto que debían llevarlo no solo en tiempo de trabajo sino también a su domicilio considerando *que "...la intromisión en lo que es la esfera de la vida privada y familiar de los trabajadores que se produce cuando finaliza la jornada laboral y continúan (los trabajadores) con esa obligación de tener ambos dispositivos con la batería cargada para que puedan cumplir su finalidad en la jornada laboral, que no es sino un control y fiscalización del trabajo a través de los citados dispositivos..."*. Una invasión de la intimidad, en consecuencia, no suficientemente justificada por el hecho de la suscripción del contrato (y del consentimiento que con ello se presta a las condiciones de trabajo establecidas) frente a la cual han de articularse mecanismos de desconexión durante los tiempos privados que aparecen como la alternativa a un control que carece de legitimidad[22].

[21] A ello contribuye, como se ha dicho, el art. 9 del RGPD (y el mismo art. de la LO 3/2018) al rechazar el valor del consentimiento a la hora de permitir a un tercero la obtención y el tratamiento de los datos íntimos, categoría que adquieren los datos de geolocalización cuando se toman fuera de las coordenadas de lugar y, sobre todo, tiempo de trabajo.

[22] Con un resultado similar pero con motivaciones diferentes, basándose ahora en la desproporción del control (al entender que existían medidas alternativas menos invasoras de la intimidad) pero también en el hecho de que la empresa no proporcionaba la herramienta de control al trabajador sino que éste tenía que aportar un teléfono móvil de su propiedad, con conexión a internet, debiendo proporcionar a la empresa datos de carácter personal como el número de teléfono o el correo electrónico, se pronuncia la ya citada SAN 13/2019, de 6 de febrero, comentada por Martínez Moya, J. "El derecho a la protección de datos personales y sistema de geolocalización impuesto por la empresa a los trabajadores-repartidores", *Revista de Jurisprudencia Laboral*, 1/2019. Sin que tampoco el exclusivo fundamento de la seguridad de los bienes sea tan relevante como para justificar la obtención del dato de geolocalización en tiempo privado ya que, finalmente, la encomienda al trabajador de una herramienta empresarial cuya custodia tiene que asumir fuera de las horas de trabajo no es sino una alternativa

Lo anterior trae a colación el tema de si la legitimidad del control se refuerza por el hecho de que el instrumento de que se trate, dotado de esa función geolocalizadora, haya sido proporcionado por la empresa y a su costa; lo que, por otra parte, es lógico dados los intereses a los que sirve. En estos casos, lo habitual es que la empresa, en cuanto titular del dispositivo, exija que se haga un uso laboral de la herramienta de trabajo, imponiendo al trabajador reglas rígidas como es la prohibición absoluta de un uso privado o particular, tanto dentro como fuera de la jornada de trabajo[23]. La cuestión es si, justamente para controlar el uso exclusivamente laboral del dispositivo, el control empresarial puede invadir espacios de privacidad del trabajador de forma que su intimidad desaparezca tanto en la obtención de datos por el geolocalizador durante el tiempo de trabajo como, en virtud de la prohibición, fuera de él.

Puede discutirse, no obstante, que la prohibición absoluta de un uso privado permita el control de su utilización en todas las circunstancias por parte de la empresa, entendiendo que, advertidos los trabajadores de la existencia del dispositivo e informados de la prohibición de un uso privado, el propio control eficaz del respeto de la prohibición legitima una invasión permanente de la privacidad del trabajador funcionando no solo durante la jornada de trabajo sino también fuera de ella. La función de control del uso del dispositivo no requiere necesariamente la invasión en la parte privada de la vida del trabajador, particularmente siempre que existan otros métodos menos lesivos para garantizar ese uso exclusivamente productivo y formas, igualmente menos invasivas, para controlar que la prohibición se respeta[24].

Un rechazo que es mucho más contundente si se permite un uso privado, incluso en el tiempo de trabajo, debiendo quedar a voluntad del trabajador producir la desconexión del geolocalizador en esos tiempos en los que tiene primacía la vida privada a la que puede ser funcional el uso del dispositivo que lleva acoplado el

empresarial cuyo coste, sea económico u organizativo, en cuanto decisión de la empresa, ésta debe asumir y no descargarlo sobre los trabajadores a costa de su vida privada.

[23] Como sucede con los vehículos o los teléfonos. Cuando, por el contrario, la empresa acepta el uso privado es evidente que las informaciones obtenidas durante ese uso pertenecen, por definición, a la esfera de la privacidad del trabajador más directamente relacionada con la intimidad por lo que ninguna invasión empresarial es tolerable debiendo desactivarse de forma automática o por decisión del trabajador cuando se vaya a proceder a ese uso privado. Una información, por cierto, que ya releva comportamientos del trabajador pero que es inevitable precisamente para garantizar su intimidad.

[24] Hay que subrayar que, en este caso, no se trata de controlar la actividad laboral del trabajador sino solo que no hace uso de las herramientas de trabajo fuera de la jornada y al margen del cumplimiento de obligaciones laborales. Para lo que, en el caso de vehículos, referencias como los kilómetros recorridos (sin indicación de lugares de partida o destino) o el consumo de carburante, pueden servir; o la inserción de dispositivos de desconexión automática vinculados a la jornada de trabajo o puestos a disposición del trabajador que deberá activarlos al finalizar su actividad laboral. Cuestión distinta es si se permite esa invasión en el caso de que existan sospechas fundadas de que el trabajador está haciendo un uso inadecuado de las herramientas de trabajo; lo que, de aceptarse, solo es posible a partir del cumplimiento de las preceptivas obligaciones de información por parte del empresario aun en estos casos y siempre que la captación de esa información tenga determinados límites que se abordarán en el siguiente epígrafe.

geolocalizador. En todo caso, los confines de los tiempos privados de uso deben establecerse muy detalladamente ya que constituye la frontera en la que el control mediante geolocalizador pasa de ser un instrumento legítimo en manos de la empresa, aun a costa de un recorte de la privacidad del trabajador, para convertirse en una lesión del derecho a la privacidad y a la intimidad del sujeto.

En definitiva, si incluso cuando la prohibición es absoluta es rechazable que el geolocalizador esté conectado de forma permanente, tanto durante la jornada como fuera de ella, cuando se permita un uso privado, dentro o fuera de la jornada, ese control no puede implantarse ya que se trata de tiempos en los que el geolocalizador deberá estar inactivo. Entendiéndose, en caso contrario, una invasión de la intimidad desproporcionada que no se justifica solamente por razones de seguridad.

3.3. La tesis de la existencia de intimidad en el tiempo de trabajo que puede ser afectada por la obtención de datos de geolocalización

Por lo que se acaba de decir, solo si los instrumentos de geolocalización tienen una connotación laboral (lo que incluye que sean proporcionados por la empresa) y no invaden de manera alguna los espacios de privacidad o de intimidad del trabajador, puede estar justificado su uso y, en consecuencia, pueden instalarse, recoger datos y tratarlos de forma legítima sin que el trabajador pueda oponerse a ello ni a las consecuencias que de la obtención y tratamiento de esos datos se derivan. Naturalmente siempre que el juicio previo de ponderación haya sido favorable a los intereses de la empresa y se cumplan las exigencias informativas de que se hablará ahora[25].

Con lo anterior se traza así una división rigurosa entre tiempos privados y tiempos laborales, no tolerándose el uso de geolocalizadores para invadir los primeros. Ciertamente, las resoluciones anteriores significan un avance en la medida en que son rigurosas a la hora de tutelar los espacios de intimidad y privacidad del trabajador, excluyéndolos del control mediante geolocalizadores. Pero también tienen una consecuencia no tan positiva. Y es que, si tales instrumentos se han proporcionado por el empresario y se deben usar exclusivamente para una finalidad productiva y en conexión directa con el lugar y el tiempo de trabajo, se tiende a pensar que todo tipo de control en ese tiempo está justificado. Esto es, que tratándose de datos con una clara y directa connotación laboral, por funcionalidad y momento de la obtención, no hay motivo para rechazar la legitimidad de su tratamiento. De nuevo opera aquí un concepto reductivo de la intimidad, que se asocia a actividades fuera del tiempo y lugar de trabajo, concluyéndose en consecuencia que en el tiempo de trabajo no existe ningún espacio para la intimidad o para la privacidad.

[25] Sobre estos temas, Baz Rodríguez, cit. pp. 24-25.

No obstante, un pequeño paso en sentido contrario de objetar la legitimidad absoluta del control en el tiempo de trabajo lo dan algunas resoluciones judiciales que aceptan que la intimidad también puede quedar afectada por datos obtenidos durante el trabajo, particularmente cuando se refieren a situaciones en las que la imbricación entre vida privada y trabajo es fuerte. Como sucede con la STSJ de Madrid 260/2014,de 21 de marzo (AS/2014/823), la cual, en un caso de un vehículo cedido al trabajador para uso exclusivamente profesional, entendió que, si el vehículo solo podía ser utilizado por el trabajador *"... y, además, debía permanecer siempre bajo su custodia, mantenimiento y cuidado, cuantos datos se conecten a su manejo y, por ende, a su localización y desplazamientos fuera del centro de trabajo (...),*todo ello hace posible obtener una información que refleja "*…la forma de proceder del usuario, que no es otro que el conductor, permitiendo de este modo conocer en todo momento durante su uso 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…".* Es decir, posible lesión de la intimidad en la medida en que el control laboral afecta a comportamientos privados pero que son relevantes para la prestación laboral.

Una tesis que también asume la STSJ de Madrid 739/2014, de 29 septiembre (AS\2014\2981), en la que, en un supuesto de una trabajadora a la que se pone a disposición un vehículo para su uso exclusivamente profesional dotado de un sistema de geolocalización, considera que *"...aunque la recurrente cedió a la trabajadora para uso exclusivamente profesional el vehículo de referencia que, además debía permanecer siempre bajo su custodia, mantenimiento y cuidado, todos los datos que se refieren a su utilización, localización y desplazamientos fuera del centro de trabajo (...) planean sobre la forma de actuar de la trabajadora (...) permitiendo acceder de este modo en todo momento durante su uso determinadas parcelas de la vida de la misma por muy relacionadas que estén en el desarrollo de la relación laboral y que inciden en la esfera de su derecho a la intimidad personal...*".

Se trata, sin embargo, de una posición minoritaria frente a la generalizada convicción de que, tratándose de informaciones con una adecuada justificación empresarial, la captación y el tratamiento de los datos son perfectamente legítimos y superan las exigencias del juicio de ponderación en cuanto a la necesidad y proporcionalidad de la medida. En gran parte porque funciona la idea preconcebida de que los datos así obtenidos no inciden sino mínimamente en el espacio de la intimidad o de la privacidad del trabajador. Sólo de forma excepcional, como sucede con controles exorbitantes, excesivos o desproporcionados, la medida de control, aunque de carácter exclusivamente laboral, supone una intromisión en la intimidad del trabajador. Lo contrario llevaría a analizar si, incluso cuando se trata de una herramienta de aplicación exclusiva en el ámbito laboral, también deben ser tenidas en cuenta las circunstancias en que ese control tiene lugar tutelando, cuando sea

necesario, las parcelas de privacidad que también existen en los lugares y tiempos de trabajo. Pero es un enfoque que no tiene una particular acogida en las resoluciones judiciales referidas al control mediante herramientas de geolocalización.

4. EL DEBER DE INFORMACIÓN COMO REQUISITO NECESARIO DE LA LICITUD TANTO DE LA OBTENCIÓN DEL DATO COMO DE SU TRATAMIENTO

Sin duda alguna una de las consecuencias de la aplicación de las normas de protección de datos ha sido la de revalorizar y reforzar el derecho a la información que ostentan los titulares de los datos y que, al tener que producirse en el momento previo a la obtención de los mismos, lo convierten en un requisito necesario para la licitud de la recogida y del tratamiento del dato. Según estas normas, ningún dato personal, lo que incluye a los datos de geolocalización, puede ser lícitamente recogido si esa recogida no está precedida de la observancia correcta del deber de información que pesa sobre el empresario. Así lo prevé el art. 90.2 de la LO 3/2018 exigiendo que la empresa informe, *"...de forma expresa, clara e inequívoca..."* a los trabajadores, no solo acerca de la existencia y características de los dispositivos sino también de los derechos de acceso, de rectificación, de limitación del tratamiento y de supresión de los datos. Una información que el art. 90 establece que debe darse también a los representantes de los trabajadores, aunque, no haciéndolo un derecho pleno, indique que la misma solo se dará a esos representantes, *"...en su caso..."*. Lo que, sin duda, remite a los derechos de información establecidos en el art. 64 ET, particularmente en el apdo. 5, f) cuando se refiere a la obligación empresarial de informar sobre la implantación de sistemas de organización y control del trabajo[26].

Ya en el contexto de normas anteriores sobre protección de datos, numerosas resoluciones judiciales han venido articulando y consolidando ese derecho a la información, considerando nulos los dispositivos de control establecidos por la empresa basándose esencialmente en el hecho de que el empresario no ha proporcionado a los trabajadores afectados información suficiente acerca de la existencia del control y de sus características. Es el caso de la STSJ de Andalucía 2307/2017, de 19 de julio (AS/2017/1847), para la que el derecho a la información en una especie de compensación por la posibilidad empresarial de introducir sistemas de control geográfico en cuanto ejecución del contrato suscrito sin necesidad de requerir el consentimiento del trabajador, que afirma: *"...En el ámbito laboral el*

[26] Un derecho que el art. 10.3 de la Ley Orgánica 11/1985, de 2 de agosto, de libertad sindical extiende a los delegados sindicales y que la propia negociación colectiva puede establecer precisando contenido, caracteres, momento, periodicidad y formas de esa información así como los destinatarios de la misma.

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..", añadiendo, *"... Ahora bien, aunque no sea necesario el consentimiento en los casos señalados, 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…".*

También la STSJ de Castilla-La Mancha, 715/2014, de 10 de junio (AS/2014/1619), la cual se remite a la STC 29/2013, de 11 de febrero, que indica que el interés privado del empresario no puede justificar que el tratamiento de datos sea empleado en contra del trabajador *"...sin una información previa sobre el control laboral puesto en práctica…*", ya que *"...No hay en el ámbito laboral, por expresarlo en otros términos, una razón que tolere la limitación del derecho de información que integra la cobertura ordinaria del derecho fundamental..*(…); por lo que será necesaria *"...una 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…*". Concluyendo la STSJ de Castilla-La Mancha que: *"...resulta claro que no existió la adecuada información, en los términos de claridad y suficiencia que son exigibles a los efectos de evitar actuaciones sorpresivas, y que en todo caso, no consta la existencia de la expresa autorización del trabajador, que no puede ser objeto de seguimiento durante todos los días de su vida laboral, y tanto durante la jornada como fuera de ella…".*

La exigencia de una información concreta y precisa acerca del dispositivo de geolocalización y de su funcionalidad productiva, organizativa y de control, y de sus consecuencias, ofrecida como compensación a la ausencia de consentimiento, no permite, sin embargo, considerar que toda captación de los datos de que se trata es lícita con la sola condición de que se haya informado previamente de ella. Porque no se trata de una condición, superada la cual, toda captación de datos es lícita, sino un requisito previo necesario para proceder, si cumplido, al juicio de ponderación que es preciso realizar en todo caso frente a la causa de justificación alegada por el empresario.

La afirmación del derecho de información no puede eludir el inevitable juicio, evidentemente muy casuístico, acerca del contenido de la información, si completa o parcial, si suficientemente expresiva de las funcionalidades del control, si clara en cuanto al alcance del control, sus utilidades y consecuencias y si razonablemente

relacionada con los intereses empresariales igualmente merecedores de tutela[27]. Con la consecuencia de que, si la información se considera defectuosa, no se entenderá cumplido el requisito y la obtención del dato y su tratamiento serán juzgados ilegítimos. Un déficit que está esencialmente relacionado con la instalación misma del dispositivo, o con funciones de control que se mantienen ocultas, o con el alcance y características de la medida y las razones empresariales que las justifican de forma directa y necesaria. En todo caso, lo que parece obvio es que la forma de proporcionar la información se requiere que sea individualizada, expresa, concisa, clara y accesible en relación con la finalidad del dispositivo; excluyendo, por tanto, informaciones implícitas, tácitas, fragmentadas, escasas, incompletas o de difícil acceso y comprensión[28].

A estos efectos y para precisar el contenido de la información que ha de proporcionarse puede servir lo establecido en el art 13 RGPD respecto de la información que ha de facilitarse al titular de los datos cuando se obtengan del interesado. Un precepto muy amplio en el que se señalan los datos que constituyen el contenido mínimo del derecho a la información de entre lo que puede destacarse, al margen de todos los referidos al tratamiento en sentido estricto, lo relativo a los fines del tratamiento. Es decir, concreta utilidad empresarial de las medidas de control y de su alcance y consecuencias.

Lo anterior no elude los casos, ya apuntados antes, en los que el control de los datos de geolocalización tiene la finalidad de verificar situaciones de incumplimiento contractual por parte del trabajador de las que existen sospechas. En estos supuestos se justifica a veces la ausencia de información en la finalidad del control del trabajador a partir de la existencia de indicios negativos acerca del correcto cumplimiento laboral, razonando que la comunicación de la existencia de un sistema de control haría inútil el propio sistema al estar advertidos los trabajadores de la existencia del mismo, basándose su eficacia indagatoria en el hecho de ser un procedimiento oculto. Y, aunque esa función controladora no informada se entiende que no queda justificada solamente por el interés empresarial en la eficacia de la medida, existen determinadas circunstancias en las que, si bien por lo que hace a los sistemas de videovigilancia y ante sospechas fundadas de incumplimiento, se admite un control puntual y limitado pese a que el trabajador no haya sido informado[29]. Algo semejante

[27] Una referencia acerca de las distintas posiciones de los tribunales de suplicación en torno a las características que debe reunir la información y la valoración de la proporcionada como suficiente se encuentra en Molina Navarrete, cit. pp.141-142, mencionando desde las que se apoyan en un supuesto conocimiento presunto del trabajador respecto del uso del dispositivo, hasta las que afirman la necesidad de una información directa, personal y específica, siendo estas últimas las que mejor respetan el espíritu y la letra del RGPD (arts. 13 y 14) y de la LO 3/2018 (art. 11).

[28] En este sentido, Rojas Rosco, R. y López Carballo, D. "El impacto del RGPD en el ámbito del control laboral y la era de la innovación", *Actualidad Civil,* 5/2018, número dedicado a la "Protección de datos: entre el RGPD y la nueva LOPD", p. 17

[29] STC 186/2000, de 10 de julio; o, con una información extraordinariamente sumaria (STC 36/2016, de 3 de marzo).

a lo que sostiene la STSJ de Galicia, 3031/2014, de 16 de junio que argumenta la suficiencia de la justificación empresarial afirmando que "…*Finalmente, tampoco parece razonable que la empresa, ante la comisión de faltas laborales, desvele las medidas de control y de seguridad tendentes a prevenir a disuadir o 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…*".

Se tolera así un control de naturaleza no general, de espacios concretos y con una duración limitada; respetuoso de la exigencia de proporcionalidad respecto del fin perseguido y el derecho constitucional lesionado; imprescindible en cuanto no existe otra alternativa de detección de las irregularidades; sobre la base de sospechas razonables en relación con hechos concretos constitutivos de una infracción grave; con independencia de que exista un doble sistema de control, uno conocido y otro oculto; pudiendo sustituir la información personalizada por otra dirigida a los representantes o mediante fórmulas menos exigentes mediante carteles informativos o sistemas semejantes[30].

Atendiendo no obstante a la regulación contenida en la LO 3/2018, nada se dice al respecto en el art. 90. Solo el art. 89 LO 3/2018, relativo al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, se refiere, aunque de forma indirecta, a esta hipótesis cuando establece que *"... En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica…*". Lo que, pudiendo aplicarse de forma analógica a los controles de geolocalización, no autoriza directamente, como excepción al deber de información, ni siquiera los casos en los que el control es puntual y dirigido a confirmar sospechas de incumplimiento laboral[31]; pero sí legitima la obtención del dato mediante una información indudablemente menos rigurosa y precisa que la que se exige normalmente.

En efecto, lo que el art. 22.4 de la LO 3/2018 dice es que, el deber de información establecido en el art 12. RGDP, queda cumplido "… *mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de*

[30] Rojas Rosco y López Carballo, cit. pp. 12-15, que se hacen eco de la STEDH, de 9 de febrero de 2018, en el Asunto López Ribalda que, en un caso de videovigilancia oculta ante sospechas de robo, ha sostenido, de conformidad con la legislación española, la necesidad, en todo caso, de una información previa de la existencia de tal sistema de control.

[31] Baz Rodríguez, cit., pp. 22-24.

conexión o dirección de internet a esta información". Es decir, unas obligaciones de información evidentemente elementales y que permiten acceder y tratar datos personales, en este caso imágenes y sonido pero también datos de geolocalización, tanto si los datos se obtienen de forma habitual o si se trata de controles de comprobación de incumplimientos laborales[32]. Otra cosa es qué tipo de información se considera suficiente, debiendo recordarse al efecto la muy discutible STC 39/2016, de 3 de marzo, que consideró suficiente información en un supuesto de los descritos la instalación de un distintivo en el escaparate de una tienda para legitimar el control de las trabajadoras de la misma por entenderse que se habían cumplido las obligaciones informativas.

32 Sin llegar a la conclusión de Rojas Rosco y López Carballo, en el sentido de que la previsión de la LO 3/2018 deja abierta la posibilidad de una videovigilancia sin necesidad de información previa. En este sentido, es importante tener en cuenta la Sentencia del Tribunal Europeo de Derechos Humanos (Gran sala), de 17 octubre 2019, en el asunto L**ópez** Ribalda y otros contra España (Jur\2019\289974), la cual remite a un juicio de ponderación de los tribunales nacionales el considerar si la ausencia de información constituye o no una lesión del derecho a la preservación de la vida privada, aceptando que pueda ser suficiente el que se haya informado de la existencia de sistemas de videovigilancia ya que con ello queda socavada la confianza de los trabajadores en la ausencia total de control, entendiendo, por tanto, que la información de la implantación de tales sistemas hace lícita la obtención de las informaciones, sea a través de cámaras visibles u ocultas.