

La protección de los derechos fundamentales de la persona trabajadora ante la utilización de GPS: ¿reformulación o continuidad?

The protection of the fundamental rights of the worker against the use of GPS: reformulation or continuity?

María Elisa Cuadros Garrido¹

¹ Universidad de Murcia, España; <https://orcid.org/0000-0003-0297-5330>

Resumen:

Los datos de tiempo-localización, son una de las fuentes del Big Data más sensibles a la privacidad de los usuarios; por ello tienen una gran aplicación práctica, además de la oportunidad del uso de grandes volúmenes de datos, traen consigo enormes riesgos para la privacidad y son una fuente creciente de información que genera problemas de almacenamiento. Desde la óptica de la regularidad de la obtención de las informaciones del GPS, con el objeto de que puedan servir de prueba en un posible proceso judicial, hay que entender que nos encontramos, en muchos casos, ante datos sensibles de la vida privada, por lo que en España se ha optado por una regulación expresa de la materia. La normativa actual vigente, establece un deber de información previo a la fiscalización del GPS, de manera que obliga que se detalle por parte de la empresa de manera previa, expresa, clara e inequívoca. Ello obedece a una tendencia continuista por parte del legislador que recoge la anterior doctrina judicial. Pero, aún a pesar de tal línea no rupturista, el terreno no es llano porque los derechos fundamentales en conflicto y su interrelación parece que ha quedado como un asunto sin resolver para el legislador de la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales.

Palabras clave: GPS, derecho a la protección de datos, derecho a la intimidad, control empresarial, derechos fundamentales

Abstract:

Time-location data is one of the sources of Big Data most sensitive to user privacy; This is why they have a huge practical application, in addition to the opportunity to use large volumes of data, they carry enormous risks for privacy and are a huge growing source of information. From the perspective of the regularity of obtaining the GPS information, in order that they can serve as evidence in a possible judicial process, it is necessary to understand that we are, in many cases, faced with sensitive data of private life, by what in Spain has opted for an express regulation of the matter. Current regulations, establish

Correspondencia a:

María Elisa Cuadros Garrido, Facultad de Derecho, Departamento de Derecho del Trabajo, Campus de la Merced, Calle Santo Cristo 1, 30001 Murcia, España.

Email: mariaelisa.cuadros@um.es

Recibido: 13-9-2019; aceptado: 23-12-2019.

ISSN 1575-7048 - eISSN 2444-5819 / © 2019 UPV/EHU



2019 CC BY Autor/a o Autores/as y UPV/EHU Press

a duty of prior information to the GPS inspection, so that it requires that the company be detailed in a prior, express, clear and unambiguous way, this is due to a continuous trend by the legislator that collect the previous judicial doctrine. But even in spite of such a non-disruptive line, the terrain is not flat because the fundamental rights in conflict and their interrelation seem to have remained an unresolved issue to the legislator of the LO 3/2018.

Keywords: GPS, right to data protection, right to privacy, business control, fundamental rights.

1. Presentación

Hace ya tiempo, que viene destacándose la importancia de concordar los parámetros trabajadores tecnológicos y empresas digitales, dado que la implantación en el ámbito laboral de las denominadas tecnologías de la información y las comunicaciones (en adelante TIC's) genera una serie de conflictos que a veces acceden al terreno jurídico.

La referencia a las innovaciones, en el ámbito de la inteligencia artificial, origina inevitables terremotos conceptuales. El debate sobre los límites humanos, éticos o científicos carece de fronteras. La pretensión de una absoluta libertad de investigación científica y la reivindicación del uso incondicionado de todas las oportunidades, que la innovación científica pone a disposición de las personas, es un discurso que aparece y reaparece.

Esta explosión tecnológica, paralela a la crisis de valores en nuestro entorno, se relaciona con el fenómeno de la globalización; entre otras muchas razones derivadas, aparece una de ellas caracterizada por una especie de imperialismo cultural, de corte anglosajón, que supone un detrimento para la identidad cultural propia de cada país. Es evidente que tales realidades, minoran el poder clásico, el de las instituciones públicas, los Estados, las sociedades organizadas y los agentes sociales.

Como consecuencia de la rápida evolución de la economía mundial ha surgido un *Derecho líquido o blando*, donde se invierte el tradicional sistema de fuentes del Derecho a través de reglas jurídicas comunes en el ámbito de ordenamientos jurídicos diferentes. Las diversas manifestaciones del *soft law* no son sino una expresión de este proceso. La transformación en responsabilidad social corporativa de lo que son auténticos deberes no anda lejos de ese enfoque, inaceptable para el mundo jurídico.

La cuestión objeto de debate se enmarca en la fenomenología que gira alrededor del *Big Data*¹, el Internet de los ciudadanos 2.0² o el *Internet de las Cosas 3.0*(Sicre García,

¹ El concepto de *big data* significa gran volumen de datos, que se obtiene de fuentes diversas, de alta velocidad y que requieren herramientas específicas que posibiliten tanto un tratamiento y análisis adecuado y nos lleva a hablar de tecnología, de muy diversa índole, que permite capturar un gran volumen de datos. Constituye una nueva forma de acceder al uso de la información, un término o categoría relacionado con el crecimiento de la información automatizada, de ahí que no se aprecie como una tecnología en sí misma. Aunque ello es cuestionado.

² La expansión de Internet a nivel global ha dado lugar a profundos cambios en la naturaleza intrínseca de la práctica mayoría de las ciudades del mundo, que han tenido que adaptar sus infraestructuras para dar cobertura analógica a los servicios de la sociedad red. Pero, sobre todo, las transformaciones más profundas de la antigua metrópolis se han producido como consecuencia del desarrollo de los entornos virtuales 2.0 y de las nuevas tecnologías de la comunicación a ellas inherentes que han dado lugar a un nuevo concepto de ciudadanía.

2016)³ y otros muchos epifenómenos actuales o de inminente aparición (Cobas Cobiella, 2019). Si la información es poder, su tratamiento y control lo es en grado sumo. Los propios actores políticos confían crecientemente en algoritmos para adoptar estrategias o ganar elecciones; desde luego, las empresas los utilizan para procesos de asignación de tareas e incluso de selección de personal (Pérez Álvarez, 2014).

Toda esta revolución en actividades tan distintas tiene su correspondiente impacto en el mercado de trabajo, donde aparecen nuevas profesiones y surgen nuevos modelos de negocio como las plataformas *Uber*, *Glovo*, *Deliveroo* y análogas. Que el ordenamiento laboral se perciba frecuentemente como un estorbo para la implantación de todo ello es tan lógico como repudiable, al menos por parte de quienes sigan creyendo en los valores consagrados por nuestra Constitución y los Tratados Internacionales con los que concuerda.

La incidencia de todo ello en el volumen de empleo (el “mercado” de trabajo) o en su calidad (los trabajadores “pobres”) también es un debate inevitable, en el que todo extremismo parece condenado al fracaso. A título de ejemplo, recordemos la polémica sobre si los robots deben cotizar a la Seguridad Social, por expresarlo en términos coloquiales.

El jurista Stefano Rodotà, insistía en la necesidad de que el Derecho pusiera freno al auge de la ciencia dado el evidente abuso del ser humano por parte de las máquinas. Preconizó, por ello, que lo jurídico tenga un papel destacado, en particular el constitucionalismo y los derechos a la igualdad y a la dignidad de la persona, pues no todo lo tecnológicamente posible es al mismo tiempo éticamente admisible, socialmente aceptable y jurídicamente legítimo.

Exigencias de justicia y equidad comportan la aplicación de un principio de proporcionalidad a la hora de determinar una correcta ponderación de los intereses en pugna, aplicando los tres subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto. Esa tripleta constituye ahora mismo la brújula con la que debe recorrerse el camino hacia la solución de los casos surgidos en caso de conflicto por control de la prestación a través de TIC's (Sempere Navarro, 2007). Así ha sucedido, por ejemplo, con las importantes STEDH en el asunto *Barbulescu II*⁴ y su doctrina para alcanzar un justo

³ La evolución hacia la web 3.0, implica que Internet se entiende como una plataforma inteligente que filtra para nosotros no sólo los mejores contenidos y productos, sino que también permite al analizar el *feedback* que recibe la plataforma digital de sus clientes y seguidores en la web. Así, analizando sus comentarios, dudas, sugerencias, consultas, etc. Se puede extraer información muy preciada que puede llevar a redireccionar esfuerzos y abandonar otros menos productivos.

⁴ Caso *Barbulescu* contra Rumania. SETDH de 5 septiembre 2017 (TEDH 2017, 61). El TEDH reflexiona sobre varios aspectos para resolver sobre si se ha vulnerado o no el referido artículo 8 CEDH, con las siguientes preguntas:— *¿Se ha informado al empleado de la posibilidad de que el empleador tome medidas para controlar su correspondencia y otras comunicaciones, así como de la aplicación de esas medidas?* La información debe en principio ser clara en cuanto a la naturaleza de la vigilancia y anterior a su puesta en práctica y en supuesto enjuiciado no lo ha sido.— *¿Cuál fue el alcance de la vigilancia llevada a cabo por el empleador y el grado de intromisión en la vida privada del trabajador?* No se detalla, si el empresario hubiera podido valerse de medios menos intrusivos de fiscalización de la cuenta del trabajador, pues se afirma que existen varios tipos de control, unos muy intrusivos sobre el contenido de las comunicaciones electrónicas y otros menos invasores que analizan el tráfico generado sobre el número de las comunicaciones. No se justifica por qué se opta por la vigilancia más intrusiva y no se explica si al mismo resultado de hubiera podido llegar con otros métodos menos invasivos. No se especifica tampoco durante cuánto tiempo se ha llevado a cabo la vigilancia y cuántas personas han podido acceder al contenido de tales informaciones. — *¿Han existido motivos legítimos, debidamente acreditados por el empleador, para justificar la vigilancia y el acceso a los contenidos de las comunicaciones?* Se afirma que no se justifica

equilibrio entre el derecho de la persona trabajadora al respeto de su vida privada y de sus comunicaciones privadas, y los intereses de la empresa empleadora (Cuadros Garrido, 2017). O con la reciente STEDH de 17 de octubre de 2019 conocida como *López Ribalda II*⁵ que, valida la videovigilancia oculta arbitrada por la empleadora, al considerar que la medida interpuesta por la empresa estaba justificada por la necesidad al haberse producido irregularidades en la actuación profesional de las demandantes. Al efecto, y en función de la doctrina actual de Estrasburgo, son decisivos como factores a tener en cuenta los siguientes:

- a) El grado de intromisión del empresario.
- b) La concurrencia de legítima razón empresarial justificativa de la monitorización.
- c) La inexistencia o existencia de medios menos intrusivos para la consecución del mismo objetivo.
- d) El destino dado por la empresa al resultado del control.
- e) La previsión de garantías para la persona trabajadora.

Como se puede observar, tales consideraciones del Tribunal Europeo de Derechos Humanos no hacen sino corroborar la doctrina tradicional de nuestro Tribunal

cuáles son las razones concretas que determinan la fiscalización y monitorización de la cuenta del trabajador, por otro lado, tampoco y, en fin, si el acceso al contenido de las comunicaciones hubiera sido posible sin su conocimiento. Se concluye por el TEDH que los tribunales nacionales rumanos no verificaron si el trabajador había sido advertido con anterioridad de la vigilancia que iba a llevarse a cabo de sus comunicaciones electrónicas efectuadas desde la cuenta profesional, ni tampoco hasta qué punto se ha producido una intromisión en la vida privada del trabajador en el ámbito de la relación de trabajo que hubiera podido alcanzarse por vías menos invasivas. En definitiva, resuelve el TEDH que no se ha protegido de manera adecuada el derecho del trabajador al respeto de su vida privada, y desde ese momento, no han realizado una ponderación justa de los intereses en juego y han vulnerado el 8 CEDH.

⁵STEDH de 17 de octubre de 2019 (JUR 2019, 289974). El caso *López Ribalda* y otras contra el Reino de España, resuelve sobre una pretendida vulneración del art. 8 CEDH por lesionar la prueba videográfica el derecho a la privacidad de las cinco demandantes, antiguas empleadas de MERCADONA, en su día despedidas, por haber cometido diversos hurtos. Los hechos transcurren del siguiente modo: en un supermercado de la cadena antes mencionada, se realizó una auditoría de los últimos meses de facturación que desprendió un importante descuadre contable. Para detectar el origen de las anomalías, se decidió instalar varias cámaras de vigilancia oculta en la línea de caja, para fiscalizar la actividad de los empleados, que junto que a las cámaras permanentes en el área de entrada y de cuya existencia conocían los trabajadores, fiscalizaron la totalidad de la actividad de la plantilla. En el Juzgado de lo Social y en la Sala del TSJ Cataluña se consideraron los despidos como procedentes y la prueba videográfica que no era nula. El TS inadmitió los recursos unificación doctrina e igual respuesta dio el TC a través de auto de inadmisión. Agotada la vía judicial en España, las demandantes acudieron al TEDH, basaron su postulación en una infracción del art. 6 por no haberse garantizado el derecho a un juicio justo y 8 CEDH por vulneración del derecho a la privacidad. Una primera STEDH 9 de enero de 2018 *López Ribalda I* (TEDH 2018, 1) estimó lesionado el derecho a la privacidad de las demandantes por incumplimiento de la normativa nacional, puesto el derecho al respeto a la vida privada y familiar, implica un conocimiento previo de la fiscalización de la actividad de las trabajadoras a través de la videovigilancia, y respecto de las cámaras instaladas *ad hoc*, no existía pues no se había facilitado información previa. La segunda sentencia dictada en Gran Sala, estima el recurso del abogado del Estado en nombre de España y considera que no se ha vulnerado el derecho a la privacidad de las demandantes, la medida estaba justificada por un objetivo legítimo que no podía lograrse con otras medidas, dado que se parte de unas sospechas de irregularidades fundadas en unas importantes pérdidas que llevan a la empresa a arbitrar cámaras ocultas en los puestos de caja lugares en los que se insiste que eran de acceso público y a mayor abundamiento, únicamente se grabó durante diez días, en consecuencia, la intrusión muy está limitada en el tiempo.

Constitucional⁶ o del propio Tribunal Supremo⁷, con independencia de que la ponderación de cada caso en particular sea o no compartida.

Otro canon de enjuiciamiento esencial, en esta materia es el de *delimitación previa*, que no excluye una posterior ponderación, aunque sí delimita su campo de actuación. No existirá ponderación, cuando el método delimitador revele la ausencia de conflicto de derechos fundamentales ente los del empleado y los del empresario a través de la expectativa razonable de intimidad. Este criterio fue importado del derecho estadounidense y posteriormente incorporado al Derecho europeo a través de los casos *Halford*⁸ (constituyó la primera sentencia europea en el que se llevó a cabo una utilización explícita de la doctrina americana de la expectativa de privacidad: un ciudadano no puede ser sometido a una injerencia sobre su privacidad con la que no pudiera contar en términos razonables) y *Copland*⁹ y donde se declaraba vulnerado el art 8¹⁰ del Convenio Europeo para la protección de los Derechos Humanos y Libertades Fundamentales.

2. GPS: concepto y funcionamiento

El GPS, antaño empleado como sofisticado dispositivo para espías durante la Guerra Fría, se utiliza en la actualidad contra las manifestaciones grupales de delincuencia y contra la violencia de género¹¹. Pero el uso va más allá de las fuerzas y cuerpos de seguridad del Estado, pues se ha extendido a la población civil a través navegadores en carretera, diferentes modalidades de drones¹² e incluso productos comerciales

⁶ SSTC 241/2012, de 7 de octubre (RTC 2012, 241), 170/2013, de 7 de octubre (RTC 2013, 170) y 39/2016, de 3 marzo (RTC 2016, 39).

⁷ SSTC 26 de septiembre de 2007 (RJ 2007, 7514), 8 de marzo de 2011 (RJ 2007, 7514) y 6 octubre de 2011 (RJ 2011, 7699).

⁸ STDH de 25 de junio de 1997 (TEDH 1997, 37).

⁹ STDH de 3 de abril de 2007 (TEDH 2007, 23). El TEDH estima que el almacenamiento de la información personal sobre el teléfono de la demandante, sra. *Copland*, su correo electrónico y el uso que hace de Internet sin su consentimiento suponía una interferencia con su derecho a la vida privada del art. 8 de la CEDH.

¹⁰ Artículo 8 sobre el derecho al respeto a la vida privada y familiar, cuya literalidad es la siguiente:

1. Toda persona tiene derecho al respeto a su vida privada y familiar, de su domicilio y de su correspondencia; 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida, que en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y libertades de los demás.

¹¹ El GPS se implanta en una pulsera al agresor, con un sistema de aviso, si se entra en un radio de seguridad en torno a la víctima. Los tratamientos de datos por las fuerzas y cuerpos de seguridad para la investigación y prevención de delitos se rigen por la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

¹² Se ha generalizado el uso de drones en el ámbito civil y el crecimiento exponencial que está experimentando la utilización de estas aeronaves no tripuladas. Estos equipos son susceptibles de incorporar no sólo GPS y cámaras de vídeo sino también escáner 3D o sistemas de detección de dispositivos móviles, y su empleo puede suponer un impacto en el derecho a la protección de datos de las personas y, por extensión, una lesión de sus derechos y libertades. El artículo 26 del Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, establece la obligación de adoptar las medidas necesarias para garantizar el cumplimiento de lo dispuesto en materia de protección de datos personales y protección de la intimidad (AEPD, 2019). La Guía Drones y Protección de Datos, publicada por la AEPD proporciona orientaciones a los operadores de drones que registren o

cuestionados¹³. Asimismo, se han convertido también en posibles métodos de control del empresario a sus trabajadores¹⁴ lo que es objeto de análisis en nuestro estudio.

Los sistemas de localización pueden colisionar con el derecho a la intimidad del art. 18.1 CE¹⁵, que se concibe como el derecho que todo individuo tiene a una vida propia, sin interferencias ni invasiones por parte de los poderes públicos o de los particulares (Cuadros Garrido, 2018, 118-120). La intimidad es un término en desorden (*a concept in disarray*) que abarca la libertad individual, el control sobre el propio cuerpo, la potestad de información personal, en definitiva, la libertad ante los sistemas de control y vigilancia, y la protección al honor y a la reputación (Lucena Cid, 2014, 22). Así el art. 7.2 de la LO de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen¹⁶ considera como intromisiones ilegítimas la utilización de aparatos de escucha, dispositivos ópticos o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas, así como la grabación, registro o reproducción, siempre que el titular del derecho no haya otorgado el consentimiento expreso a tal efecto.

Además, el control empresarial por la vía del GPS también deberá respetar el derecho a la autodeterminación informativa¹⁷, ya que los datos obtenidos a través de este constituyen información de carácter personal y por ello, susceptible de tratamiento (Cuadros Garrido, 2018, 133-152). En este sentido el art. 2 de la Directiva Europea 2000/58/CE, de 12 de julio de 2002¹⁸, sobre el tratamiento de datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas, define los sistemas de geolocalización como “cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público”.

procesen imágenes, vídeos, sonido, datos biométricos, de geolocalización o de telecomunicaciones, entre otros, relacionados con personas identificadas o identificables para cumplir con lo establecido en el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018.

¹³ Una empresa brasileña ha comercializado un anillo con la aplicación de Google play *GPS phone tracker*, la aplicación solo se puede descargar después de comprar los anillos. Como la afectación a la privacidad es evidente, la marca brasileña alega en su defensa que sólo vende el producto si ambas partes están de acuerdo (elperiodico.com, 2019).

¹⁴ Se podrá geolocalizar a los trabajadores siempre y cuando empleados y representantes estén debidamente informados “acerca de la existencia y características de estos dispositivos”.

¹⁵ El derecho a la intimidad personal, en cuanto derivación de la libertad y dignidad de la persona, art. 10.1 CE, implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario según las pautas de nuestra cultura, para mantener una mínima calidad de vida humana. A fin de resguardar ese espacio reservado, este derecho confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido.

¹⁶ BOE, núm. 115, de 14 de mayo de 1982, páginas 12546 a 12548.

¹⁷ La autodeterminación informativa es un derecho de perfil muy formalista que garantiza a la persona el control activo de las informaciones que le afectan, y el derecho a no ser instrumentalizado a través del conocimiento adquirido de aspectos de su personalidad, en la medida en que supone ser informado de quien posee sus datos personales, a qué uso se están sometiendo y el derecho a oponerse, en su caso, a una posesión ilegítima o uso ilícito; es la potestad de control sobre el uso de los datos propios. Las vulneraciones a la autodeterminación informativa por parte de los particulares tienen relevancia constitucional y por consiguiente también se consideran violaciones del artículo 18.4 CE.

¹⁸ DOCE, núm. 201, de 31 de julio de 2002, páginas 37 a 47.

El Reglamento General sobre Protección de Datos de la UE (en adelante RGPD) ¹⁹ establece una normativa única, válida en toda la UE y aplicable al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

El RGPD da la posibilidad a los Estados miembros de establecer normas más específicas, a través de disposiciones legislativas o de convenios colectivos, 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.

Las normas que establezcan los Estados deben incluir medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

La Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales²⁰ (en adelante LO 3/2018) fue cuestionada en su tramitación parlamentaria con enmiendas a la totalidad, pues se entendía que el legislador español se había desmarcado de la senda establecida por el RGPD. Este aspecto ha sido incluso resaltado por la doctrina judicial, en la STJS núm. 3 de Pamplona de 18 de febrero de 2019²¹ no solo se resuelve un supuesto de videovigilancia encubierta, sino que se realiza un repaso de la doctrina general en materia de TIC's y control laboral. La mencionada sentencia afirma que el deber informativo es imprescindible para la validez de las grabaciones audiovisuales y de los otros medios tecnológicos de control empresarial de acuerdo con lo establecido en el RGPD, esa exhaustiva información exigida a nivel europeo no es la obligación que recoge la LO 3/2018 que pues dista mucho de ser amplia, en algunos supuestos como el del art. 89.1 último párrafo de su cuerpo legal, respecto a videovigilancia oculta cuyo requisito es la existencia de un cartel informativo en el lugar de trabajo. El magistrado considera que la normativa española choca con el Reglamento europeo que ha de primar ya que se debe respetar el deber informativo previo que permita tener cabal conocimiento a la persona trabajadora de quién posee los datos personales y para qué se utilizan.

¹⁹ 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 datos.

²⁰ LO 3/2018, de 5 de diciembre. BOE núm. 294, de 6 de diciembre de 2018, páginas 119788 a 119857. La aprobación del texto orgánico, supone una novedad respecto a la anterior normativa ya que extiende su ámbito material a las relaciones de trabajo. De la propia literalidad del nombre de la Ley y de su Exposición de Motivos, se desvela que son objeto de protección *el derecho a la autodeterminación informativa* (art. 18.4 CE) y los *derechos digitales* que podemos definirlos como derechos y libertades reconocidos a todos los ciudadanos predicables al entorno de Internet.

²¹ STJS núm. 3 de Pamplona de 18 de febrero de 2019 (AS 2019, 1014).

La regulación de las facultades de control empresarial se encuentra, con carácter general, en el art. 20. 3 ET²², que establece los principios generales a los que se sujeta este poder empresarial. La LO 3/2018 añade un nuevo art.20 *bis* ET²³ en el que se reconoce a los trabajadores y empleados públicos el derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

3. Admisibilidad del GPS en el ámbito de las relaciones laborales

3.1. Marco jurídico de referencia

La geolocalización, los sistemas de proximidad y los controles biométricos poseen en común la creación de registro de actividades de tratamiento que empleen a más de 250 personas, o que trabajen con datos, especialmente sensibles o aquellas que realicen tratamientos de datos personales de forma no ocasional ²⁴ en el que se identifique los siguiente:

- Los datos de contacto del sujeto responsable del registro y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
- Los fines del tratamiento.
- Una descripción de las categorías de interesados y de las categorías de datos personales y las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales.

La Ley 3/2018 de, recoge de manera expresa que existe un derecho a la intimidad ante la utilización de sistemas de geolocalización, en el ámbito laboral de la siguiente manera:

²² Art 20.3 ET importado del derecho italiano que autoriza al empresario a adoptar:

Las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad de los trabajadores disminuidos.

Ya en la propia dicción de la norma, se apunta la íntima relación existente entre las genéricas facultades empresariales de dirección y de organización que permiten adoptar medidas de supervisión o vigilancia de la actividad laboral al empresario, y la atribución de tales facultades sobre el trabajador; lo que se justifica en las potestades derivadas del contrato de trabajo, cuyo fundamento se encuentra en la libertad de empresa, reconocida en el art 38 CE.

²³ Las DD.FF. 13.^a y 14.^a de la LO introducen este nuevo artículo.

²⁴ El RGPD regula en su artículo 30. 1 el denominado *registro de actividades de tratamiento* que sustituye la inscripción de ficheros y establece que cada responsable y, en su caso, el encargado del tratamiento, llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. El nuevo Reglamento General de Protección de datos elimina la obligación de notificar los ficheros ante la Agencia Española de Protección de Datos del derogado art. 26.1. LOPD.

a) Los empresarios habrán de informar de forma expresa y previa, clara e inequívoca²⁵, a las personas trabajadoras o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos²⁶.

b) Asimismo, deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión de datos obtenidos²⁷.

Cabe señalar que la redacción del precepto no es del todo afortunada, pues el legislador se refiere de manera expresa al derecho a la intimidad y entendemos que, de manera implícita al derecho a la protección de los datos personales. Lo que podemos afirmar sin lugar a duda, es que “se abre la caja de Pandora” a posibles interpretaciones judiciales contradictorias sobre el bien jurídico constitucionalmente tutelado, no se delimita claramente si trata de derechos fundamentales autónomos, o bien estamos ante un derecho fundamental independiente (art. 18.1 CE) y otro fundamental pero instrumental (art. 18.4 CE). En este punto, una parte importante de la doctrina advierte que el Tribunal Constitucional se afana en deslindar la libertad informática respecto del derecho a la intimidad, pero tácitamente, reconoce que la escisión no puede ser absoluta, porque el derecho a la protección de datos comprende el derecho a la intimidad, aunque lo exceda (Sempere Navarro, San Martín Mazzuconi 2015, 120-122).

Asimismo, cabe precisar que, desde la perspectiva de la informática, el derecho a la intimidad cobra una nueva dimensión, pues resulta insuficiente concebir la intimidad como un derecho garantista. Existe un *status* negativo de defensa frente a cualquier intromisión de la esfera privada, sin contemplarla, al propio tiempo, como un derecho activo de control y un status positivo sobre el flujo de informaciones que conciernen a cada sujeto. Identifican así un nuevo derecho, configurándolo como aquel que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones que le conciernen archivadas en bancos de datos (*habeas data*); controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su transmisión. En definitiva, la autodeterminación informativa, consiste en la facultad de disponer sobre la revelación y el uso de los datos

²⁵ Si acaso, anotemos como precedente importante de estos adjetivos la doctrina de la STC 29/2013, de 11 febrero, (RTC 2013, 29) caso del empleado de la Universidad de Sevilla marca el cénit de la protección constitucional, negando la posibilidad de que el empleador utilice imágenes grabadas por las cámaras de seguridad existentes en sus instalaciones cuando previamente no lo ha advertido. Se afirma que el poder de control sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin: por ello se precisa una “información previa y expresa, precisa, clara e inequívoca” de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida.

²⁶ Art. 90.1. LO 3/2018, recoge lo siguiente:

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.

²⁷ Art. 90.2. LO 3/2018 dice lo siguiente:

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.

personales, en todas las fases de elaboración y utilización de estos datos, es decir, su acumulación, su transmisión, su modificación y cancelación (García Ninet y Vicente Pachés, 2015, 137-192).

3.1. Presupuestos necesarios para su admisibilidad

3.1.1. Proporcionalidad, idoneidad y necesidad

El principio de proporcionalidad es un criterio metodológico que cumple la función de estructurar el procedimiento interpretativo para la determinación del contenido de los derechos fundamentales. Sirve para controlar cualesquiera actos que inciden sobre los intereses de los particulares y no está expresamente previsto en nuestra Constitución, con toda la jurisprudencia, viene haciendo un uso cada vez más frecuente del mismo. Desde el punto de vista del Derecho del Trabajo, la proporcionalidad es una técnica tendente a que los intereses del empresario no se logren a costa de los derechos e intereses del trabajador, sino que se busque un punto de equilibrio entre ambos. No se trata pues de enjuiciar la corrección de la conducta del empresario, sino de realizar un juicio ponderativo (Rodríguez Escanciano, 2015, 49-50).

El juicio de proporcionalidad resuelve el conflicto entre el sacrificio que se le impone a la persona trabajadora con sus derechos fundamentales restringidos y sus límites, argumentando la idoneidad de la medida, su necesidad y el debido equilibrio entre el sacrificio sufrido por el derecho fundamental limitado y la ventaja que se obtendrá del mismo, que suele ser el control de la prestación en contratos de trabajo que implican desplazamientos continuos. Se debe examinar si la persona trabajadora, ha sido informada previamente de la posibilidad de que el empresario aplique medidas de control del GPS, exigiendo que se tenga información, expresa, previa, clara e inequívoca sobre los sistemas de vigilancia –principio de transparencia–, además de exigir un control intenso de proporcionalidad en el caso del acceso al contenido de los mensajes.

Las primeras sentencias de TSJ²⁸ que versan sobre vehículos de empresa fiscalizados por GPS y sanciones disciplinarias, datan de 2002, pero no es hasta años más tarde, cuando de una manera clara se plantea la colisión con los derechos fundamentales del trabajador con la potestad de control de la prestación del empresario a través de los dispositivos GPS utilizando como canon de enjuiciamiento el principio de proporcionalidad. La primera sentencia que localizamos a este respecto es la STSJ del País Vasco de 22 de marzo de 2011²⁹ que incluso plantea la cuestión de oficio, admitiendo que tal extremo no ha sido objeto de impugnación ni comentado en la sentencia de la instancia, pero se considera que ha de ser traído a colación ya que la ponderación es la técnica más recomendable para resolver la cuestión. En consecuencia, los actos del empresario de fiscalización a través de dispositivos GPS, solo podrán reputarse proporcionados, y por tanto válidos, cuando respeten cumulativamente tres requisitos:

-Idoneidad como medida susceptible de conseguir el objetivo propuesto. Toda intervención en los derechos fundamentales debe ser adecuada para contribuir a la obtención de un fin constitucionalmente legítimo. Y aplicándolo al control empresarial, si la medida del empleador es susceptible de conseguir el objetivo

²⁸ STSJ de Castilla la Mancha de 11 de marzo de 2002 (AS 2003, 62) y STSJ de Madrid de 3 de abril de 2002 (JUR 2002, 163818).

²⁹ STSJ del País Vasco de 22 de marzo de 2011 (JUR 2011, 303171).

propuesto supera la idoneidad. De modo que se convierte, de inicio, en legítimo cualquier interés empresarial que pueda ser satisfecho por la medida de control; lo único que se precisa es adecuación. La idoneidad es que la medida no sea manifiestamente irracional, arbitraria ni caprichosa (Valdés Dal-Ré, 2003, 100-101).

-Necesidad en el sentido de que no exista otra medida más moderada para conseguir el propósito con igual eficacia, implica la comparación entre la medida adoptada por la empresa y otros medios alternativos que se pudieran haber escogido. En esta comparación se examina si alguno de los medios opcionales logra cumplir dos exigencias: en primer lugar, si reviste el grado de idoneidad para contribuir a alcanzar el objetivo inmediato de esta última; y en segundo lugar, si afecta al derecho fundamental en un grado menor. Es decir, que no exista otra medida más moderada para la consecución del propósito perseguido por la empresa con igual eficacia (Bernal Pulido, 2007, 55-58).

-Y finalmente, un juicio de proporcionalidad en sentido estricto, que existan más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. En definitiva, constituye un juicio de adecuación, una optimización relativa a las posibilidades jurídicas (Bernal Pulido, 2007, 60-66).

Tras la regla del triple test, cierto sector de la doctrina, afirma que adicionalmente se exige también que la restricción o medida sea necesaria; ha de revelarse como indispensable para el correcto y ordenado desenvolvimiento de la actividad productiva, lo cual significa que responda a motivaciones objetivas, distintas del mero interés empresarial (Sempere Navarro y San Martín Mazzuconi, 2002, 46-48) , como recoge la doctrina de la STC núm. 98/2000, de 10 de abril³⁰ con la siguiente alusión: “la mera utilidad o conveniencia no legitima sin más”.

La Sala vasca concluyó que podría admitir la monitorización por GPS o localización vigilante, por técnicas telemáticas y de nuevas tecnologías, en tanto en cuanto se presentan con las garantías y preservan la dignidad e intimidad del trabajador. Pero una cuestión distinta es que la buena fe reciproca exige la necesidad de avisar de su instalación y presentación al objeto de contrastar la dinámica propia de una actividad laboral, sin perjuicio de situaciones excepcionales que permiten atender a esos juicios de proporcionalidad o necesidad. No había conocimiento previo por parte del trabajador por lo que la medida arbitrada no supera el canon de enjuiciamiento bajo el test de proporcionalidad, pues no cabe predicar idoneidad de la medida.

En igual sentido, unos meses después se vuelve a pronunciar la misma sala con la STSJ País Vasco 10 de mayo de 2011³¹, que declara nulo el despido de un trabajador al que se le fiscalizó el vehículo particular de la persona trabajadora por GPS a través de un detective privado a los efectos de comprobar que no defraudaba a la empresa con su baja médica. Se considera que la fiscalización por detective es admisible pero no por GPS, pues existen otros métodos de vigilancia directos, que son menos intrusivos. El empleo del mecanismo GPS, no respeta el principio de proporcionalidad, pues resulta totalmente innecesario atendiendo al objetivo perseguido de comprobar las actividades realizadas por el demandante en los espacios públicos y privados de acceso libre, respondiendo a la mera conveniencia del investigador, lo que no justifica el uso de un medio tan invasor de

³⁰ STC 98/2000, de 10 de abril (RTC 2000, 98).

³¹ STSJ País Vasco 10 de mayo de 2011 (AS 2012, 2277).

la vida privada. La sala alude a doctrina constitucional, que considera aplicable y entre otras la STC núm. 292/2000, de enero ³² que sabemos consagra el art. 18. 4 CE como derecho autónomo y lo excluye del debate, ya que admite que aun cuando los datos obtenidos a través del localizador son datos de carácter personal susceptibles de tratamiento, sujetos a las disposiciones de la LOPD vigente en aquel momento, la Sala no considera adecuado pronunciarse de oficio sobre la eventual vulneración del derecho fundamental a la protección de datos de carácter personal consagrado en el artículo 18.4 de la Constitución, que no ha sido invocado en el proceso, y tampoco en este trámite. Esta sentencia fue ratificada por el Alto Tribunal en la STS de 21 de junio de 2012³³.

3.2.2. Conocimiento previo

La doctrina constitucional, ha reconocido reiteradamente que la garantía del derecho a la intimidad personal y a la protección de datos impone, como regla general un deber de información que protege frente a intromisiones ilegítimas. Este deber de información es más relevante si cabe en el derecho a la protección de la autodeterminación informativa, al formar parte de su núcleo esencial el derecho del afectado a ser informado de quien posee los datos personales y con qué fin. Al amparo de esta doctrina se ha dicho que dado que los dispositivos GPS sirven para captar datos personales la empresa debe facilitar a las personas trabajadoras información, previa y expresa de la instalación de los GPS y demás aparatos de control remoto, así como la finalidad del control a la que va dirigida.

Además, ahora tal conocimiento previo lo prevé de manera expresa el art. 90. 1 LO 3/2018, recogiendo así el legislador la doctrina judicial anterior que aunque de GPS no existe doctrina constitucional se aplicaba por analogía lo considerado respecto a videovigilancia, sirvan como botón de muestra las siguientes sentencias: STSJ Castilla-La Mancha de 17 de septiembre de 2015 ³⁴ que rechaza la prueba del GPS por falta de información previa a la persona del trabajador afectado, la STSJ de Madrid de 29 de septiembre de 2014³⁵ que exige información e incluso consentimiento y exige

³² STC núm. 292/2000 (RTC 2000, 292)

³³ STS de 21 de junio de 2012 (RJ 2012, 7627).

³⁴ STSJ Castilla-La Mancha de 17 de septiembre de 2015 (JUR 2015, 137206). La demanda es desestimada en la instancia, pero posteriormente, la Sala estima el recurso de suplicación del trabajador, pues, aunque el empleado conocía la existencia del GPS, no había sido informado de manera suficiente de la finalidad disciplinaria del control del mencionado dispositivo:

En el presente caso no existe esa constancia clara y expresa de que se hubiera informado al trabajador, no ya de la instalación del GPS, que cabe deducir que pudiera tener un conocimiento general de ello, sino de la eventualidad de poder ser dicho dispositivo utilizado por la empresa para tener un conocimiento y control de su ubicación, a todos los efectos laborales, incluido sancionadores en su caso. (...) más especialmente, sobre la posibilidad de utilizar los datos que de dicho dispositivo se pudieran obtener, como medio de prueba de alcance disciplinario en contra del trabajador, debe considerarse que la utilización de tal medio probatorio, y los datos obtenidos de ello, lo fueron ilícitamente. Y que, por lo tanto, en cuanto fueron obtenidos de modo ilícito, no eran datos que pudieran ser aportados como medio de prueba, al quedar contaminados por ese origen (FJ 4.º).

³⁵ STSJ de Madrid de 29 de septiembre de 2014 (JUR 2014, 2981). La posibilidad de conocer en todo momento, mediante un sistema de geolocalización, que permite un continuo y permanente seguimiento del vehículo cedido al trabajador, durante su uso, no solo posicionamiento de este por razones de seguridad, sino también muestra el lugar exacto en donde se halla y, a su vez, el posterior tratamiento de los datos obtenidos con una finalidad completamente distinta de la anunciada y sin conocimiento del conductor. Las conclusiones extraídas, a merced de este dispositivo tecnológico y su aportación como medio de prueba en sede judicial para demostrar un pretendido incumplimiento contractual, constituyeron un procedimiento que lesiona los derechos fundamentales del trabajador, en concreto la trabajadora no ha cedido de manera

conocimiento previo pues sino no se puede considerar superado el juicio de proporcionalidad STSJ de Madrid de 21 de marzo de 2014³⁶.

3.2.3. Derecho a la portabilidad

El RGPD en su art. 20 y en el 17 LO 3/2018, permite a los trabajadores fiscalizados por GPS obtener los datos que han facilitado al responsable de un tratamiento en un formato estructurado, de uso común y de lectura mecánica y transmitirlos a otro responsable cuando: a) se haya prestado el consentimiento expreso por el interesado o se base en un contrato, y b) el tratamiento se efectuó por medios automatizados. Si es técnicamente posible la portabilidad podrá hacerse directamente de un responsable a otro. El derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. Apuntes jurisprudenciales sobre GPS

Previamente a realizar una clasificación actual, cabe recordar que las sentencias de los distintos TSJ, tradicionalmente, han optado por aplicar a la fiscalización de la prestación laboral por GPS la doctrina general sobre videovigilancia, por analogía, probablemente porque de aquella existe doctrina constitucional al respecto y no así de GPS, sirva como ejemplo STSJ Galicia 17 de enero de 2014³⁷ que aplica la doctrina de las SSTC núm. 98/2000, de 10 de abril³⁸ y núm. 186/2000, de 10 de julio³⁹. Resolviendo,

expresa su consentimiento para la cesión de sus datos personales, lo cual vulnera su derecho a la autoprotección informativa del art. 18.4 CE.

³⁶ STSJ de Madrid de 21 de marzo de 2014 (AS 2013, 906). Se resalta el rasgo claramente intrusivo del dispositivo GPS en la esfera personal del trabajador:

Otro tanto cabe decir en el caso de autos en cuanto a los cánones constitucionales de enjuiciamiento del dispositivo de localización utilizado, que en modo alguno supera los juicios de necesidad, idoneidad y proporcionalidad, por cuanto que si lo que quería demostrar la empresa era que algunos días el trabajador no agotó la duración de su jornada laboral, o utilizó en una ocasión para uso propio el vehículo que le había facilitado, o no tenía que haber pasado gastos de comida otros días en que después de comer regresó sin más a su domicilio, se trata de hechos que pudieron ser probados sin ninguna dificultad por otros medios mucho menos aflictivos e intrusivos en la esfera de su intimidad personal y vida privada (FJ 21.º 6.º).

Por tanto, la intrusión es clara ante la ausencia de información previa acerca del uso del GPS, el trabajador no era conocedor de la dimensión de los actos por los que podía ser sancionado; lo que vulneraba su derecho a la autodeterminación informativa.

³⁷ STSJ Galicia 17 de enero de 2014 (AS 2014, 637).

³⁸ STC 98/2000, de 10 de abril (RTC 2000, 98).

³⁹ STC 186/2000, de 10 de julio (RTC 2000, 186).

respectivamente, los casos del *Casino de La Toja*⁴⁰ y del *Economato de Ensidesa*⁴¹, que supusieron la declaración en el orden constitucional de que en el centro de trabajo pueden producirse actuaciones lesivas a la intimidad del trabajador; lo que provocó el posterior cambio en la doctrina social. Estas sentencias, constituyen doctrina constitucional de referencia en lo que respecta a la extensión de los poderes de control de las nuevas tecnologías por el empresario.

Ambas sentencias definen toda una pauta de resolución de conflictos en el ámbito laboral, habiéndose convertido en el canon prevalentemente utilizado en la práctica constitucional y judicial para valorar la legitimidad de cualquier medida restrictiva de derechos fundamentales; pues hasta ese momento existían distintos pronunciamientos de los tribunales laborales, que no siempre eran coincidentes. Suponen un cambio de método, o de enfoque, a la hora de enjuiciar el problema, puesto que parten de que la instalación de los medios es *a priori*, una medida restrictiva de los derechos del trabajador; y por tanto, se ha de considerar también de modo restrictivo la posibilidad de recurrir a tal medida.

4.1. Desobediencia y despido por no fiscalizar por GPS el vehículo de empresa

Si para el desempeño de la actividad profesional, fuera preciso el uso de estos dispositivos y existe una negativa reiterada por parte del trabajador a activar el dispositivo GPS de seguimiento y control de rutas, la desobediencia es constitutiva de un despido disciplinario procedente⁴².

4.2. Rutas falsas

La acreditación mediante seguimiento del trabajador a través del sistema GPS instalado en su vehículo, con su conocimiento, no lesiona del derecho a la intimidad, al resultar una medida proporcionada para el fin perseguido. La sentencia hace un repaso de la doctrina general sobre videovigilancia (STC 186/2000, STC 29/2013 y STC 39/2016)

⁴⁰ Este hito jurisprudencial resuelve el recurso de amparo interpuesto contra la sentencia de la Sala de lo Social del TSJ de Galicia, que revocaba otra anterior de instancia y declaraba que la decisión de una empresa sobre la instalación de micrófonos en un casino en La Toja, con la finalidad de controlar las conversaciones entre los empleados y los clientes, concretamente en la zona de ruleta y de la caja, que se realizaron con información previa a los trabajadores en determinadas dependencias del centro de trabajo, no vulneraba derecho fundamental alguno de aquellos. Disconforme con este fallo, se pidió el amparo ante el Tribunal Constitucional el cual lo otorgó al entender que se había producido una intromisión ilegítima en el derecho a la intimidad. La Sentencia comienza rechazando la premisa de la que partía la anterior sentencia recurrida, de acuerdo con la cual el centro de trabajo no es un lugar por definición en el que se ejerza el derecho a la intimidad por parte de los trabajadores. Como novedad, respecto a la anterior doctrina constitucional, el TC rechaza su idea originaria de que el alcance del derecho a la intimidad de los trabajadores quede limitado *a las zonas del centro de trabajo donde no se desempeñen los cometidos propios de la actividad profesional* y acepta que *pueda producirse lesión del referido derecho fundamental en el ámbito del desempeño de las tareas profesionales*.

⁴¹ El pronunciamiento, que resuelve sobre la instalación de un circuito cerrado de televisión de manera clandestina, enfocado a dos puestos de trabajo, en concreto, a la caja registradora y al mostrador de paso de un economato, ante las sospechas de la empresa de un comportamiento irregular, se reafirma, una vez más, en el principio de proporcionalidad como criterio base para determinar la legitimidad de cualquier medida restrictiva de derechos fundamentales.

⁴² STSJ Andalucía 18 de septiembre de 2017 (AS 2017, 2124).

que considera plenamente aplicable al supuesto a través de someter la medida de fiscalización del GPS al principio de proporcionalidad.

Lo determinante para la Sala y para ponderar los intereses en conflicto, es el conocimiento previo por parte del trabajador de la instalación del dispositivo GPS en su vehículo al objeto de la exclusiva finalidad de analizar recorridos y mejorar la actuación comercial, con utilización de los datos única y exclusivamente generados en la jornada de trabajo. El dispositivo GPS, en el caso enjuiciado, permite la comprobación del cumplimiento de los deberes laborales, en una finalidad lícita de verificación y control empresarial, que no puede ser objeto de consideración ilícita o irregular, en tanto en cuanto se justifica su conocimiento y finalidad.

4.3. GPS *más allá* de la jornada laboral

El control exhaustivo de la localización del vehículo de empresa, las 24 horas del día, todos los días del año, indudablemente, es una invasión de la vida privada del trabajador para la que no está facultado el empresario, esta es la doctrina de las dos sentencias reseñadas en este epígrafe. A sensu contrario, se nos dice que no hay lesión del derecho a la intimidad por parte del empresario, al adoptar medidas de vigilancia y control, colocación de dispositivos de localización GPS en los vehículos puestos a disposición de los trabajadores para su uso profesional si es una circunstancia conocida por los operarios y autorizada por la Agencia de Protección de Datos.

En cierto modo, podríamos afirmar las resoluciones judiciales son “visionarias” de lo que luego fue el futuro legislativo, ya que guardan una relación muy estrecha con el actual art.88 LO 3/2018 que regula el derecho digital a la desconexión⁴³, consiste este derecho a en el ámbito laboral, en evitar que el trabajador o empleado público se vea sometido a la presión o estrés que puede conllevar que la empresa le siga dando instrucciones o incluso nuevas órdenes fuera de su jornada laboral (Barrios Baudor, 2019). De esta manera, el empleado se siente intimidado a responder satisfacer los requerimientos empresariales por temor a algún tipo de represalia (Fernández Orrico, 2019). En los siguientes supuestos, se declara que existe, vulneración de dicho derecho fundamental del 18.4 CE:

- a) Por continuar activado el GPS del coche tras la finalización de la jornada laboral, sin el imprescindible consentimiento de los trabajadores⁴⁴.
- b) Por fiscalizar controlar el GPS, la prestación de IT de la trabajadora, ya que no es la finalidad de cumplimiento del trabajo debido como comercial puesto que el contrato se encuentra suspendido⁴⁵.

Por lo tanto, una vez finalizada la jornada laboral, por parte de la empresa, se deben arbitrar los mecanismos para desactivar el localizador GPS de una manera imperiosa.

⁴³ En nuestro país, carecíamos de un tratamiento normativo específico del derecho a la desconexión digital en el ámbito de las relaciones laborales: Ahora bien, pese a ser ello así, normativa venía contemplando previsiones normativas que avalarían más que sobradamente el derecho de los trabajadores a desconectar laboralmente fuera de su horario de trabajo dentro del sector de los convenios colectivos.

⁴⁴ STSJ Asturias 27 de diciembre de 2017 (AS 2018, 296).

⁴⁵ STSJ Andalucía 19 de octubre de 2017(JUR 2017, 12280).

4.4. Dispositivo GPS sin conocimiento previo y a un delegado sindical

La STSJ de Madrid de 12 de julio de 2019⁴⁶, desestima el recurso de suplicación interpuesto por la empresa de seguridad SECURITAS recurrente, y en consecuencia, valida el fallo de la instancia que declaró vulnerado el derecho fundamental a la protección de los datos de carácter personal del demandante por haber sido fiscalizado el vehículo sin información previa, lo que la Sala califica como *el alma del fraude es la ocultación*.

Se enfatiza que la ocultación de la fiscalización por GPS es causa de la conducta fraudulenta por parte del empresario, que vulnera el art. 18.4 CE, dentro de este derecho se matiza que la lesión es en concreto a la intimidad personal del recurrido por uso inadecuado de la informática, por lo que observamos que el derecho a la autodeterminación informativa se concibe para la Sala como un derecho instrumental del derecho a la intimidad CE. A ello se añade que el demandante es delegado sindical de UGT en la empresa, por lo que sus circunstancias personales privadas se extienden a su condición sindical. De lo que se deriva que la irregular conducta del empresario no sólo violaría el derecho fundamental básico del actor a su intimidad sino también su derecho a la libertad sindical. Por lo que el recurrido ha sido doblemente lesionado en sus derechos fundamentales. Lo novedoso del supuesto es que en el proceso de tutela de derechos fundamentales que se declaran vulnerados, se ordena la retirada del GPS del vehículo de empresa, y asimismo se condena al pago del daño moral en la suma de 12.000 euros (no se especifica el desglose del *quantum* porque se recoge que se reproduce el Fundamento Jurídico de la sentencia de instancia por economía procesal). La cantidad impuesta en la instancia y ratificada por el TSJ madrileño, condena a la empresa al pago en concepto de indemnización por el impacto o sufrimiento psíquico o espiritual que en la persona del representante sindical se ha podido producir por una actuación especialmente intrusiva y dañina sobre la persona de la persona trabajadora.

4.5. Proyecto Tracker de Telepizza

La SAN de 6 de febrero de 2019⁴⁷, en el contexto de un conflicto colectivo, originado por la implantación de un sistema informático de localización a través del GMS del teléfono personal del repartidor la Sala manifiesta lo siguiente:

- a) La implantación del sistema de geolocalización previsto por la empresa es nula, pues se considera que no respeta el derecho constitucional a la privacidad de los datos personales vía art. 18.4 CE de los trabajadores de Telepizza por cuanto que no supera el juicio de proporcionalidad, supone abuso de derecho por el empresario. La aplicación informática requiere proporcionar datos de carácter personal, como son el número de teléfono o el correo electrónico, sin informar, con carácter previo al trabajador, sobre dicho sistema y sus implicaciones y siendo, además, una medida

⁴⁶ STSJ de Madrid de 12 de julio de 2019 (AS 2019, 1866). La Sala matiza que se ha afectado al derecho de autodeterminación informativa y también al derecho fundamental a la libertad sindical, del recurrido, por ser representante de UGT. Condena asimismo a que de modo inmediato proceda a retirar el dispositivo GPS del vehículo que el actor tiene asignado, a que el fallo de esta sentencia se comunique a todos los trabajadores de la demandada y a indemnizar al demandante por los daños morales causados con la suma de 12.000 euros.

⁴⁷ SAN de 6 de febrero de 2019 (AS 2019, 905).

en la que no se ha respetado la proporcionalidad debida. Se cita, en apoyo de la argumentación el art. 90 LO 3/2018, a modo ilustrativo, pues no estaba vigente en el momento del enjuiciamiento de los hechos.

- b) Determina la nulidad de la cláusula resolutoria incluida en los contratos, por la que la empresa, ante la negativa reiterada o imposibilidad sobrevenida de aportación del teléfono móvil por parte del trabajador, o de la aplicación informática de geolocalización, impone medidas disciplinarias prescindiendo del régimen establecido en el convenio colectivo de aplicación y en el ET.
- c) La medida incumple, además, la legalidad ordinaria respecto a los deberes de información y consulta respecto de los representantes de los trabajadores art 64. 5 apto f) ET, ya que no se recabó informe previo a los representantes de los trabajadores, sino que únicamente se les informó de que la empresa pretendía implantar un sistema de geolocalización de pedidos lo que conllevaría que los empleados aportasen una terminal de telefonía móvil en la que descargarse una *App* confeccionada al efecto a instancias de la empresa, que se efectuaría una compensación y que la negativa reiterada o imposibilidad sobrevenida de aportación de esta herramienta por parte del trabajador, o de la aplicación informática antes mencionada, será causa suficiente para la extinción del contrato de trabajo al amparo de lo previsto en el 49 ET .

5. Conclusiones

La instalación de los dispositivos GPS en los vehículos como medida de vigilancia es ajustada a derecho, por lo tanto, no hay de lesión de derechos fundamentales por parte del empresario, si la circunstancia es conocida por los empleados previamente. Sin embargo, se estima vulneración de derechos fundamentales, por estar activado el GPS también a partir de la finalización de la jornada laboral.

La negociación colectiva, en cualquier caso, constituye el cauce idóneo para que se asuman soluciones equilibradas en un aspecto tan ligado a la intimidad, privacidad y autodeterminación informativa como son los dispositivos GPS. Aunque no demasiados, los casos de éxito en la negociación colectiva muestran interesantes resultados acerca del fiscalizador del GPS mientras se trabaja y la posibilidad de desconectarlo cuando el vehículo de la empresa está en funciones de uso particular.

En su defecto, ante la falta de norma convencional, resulta muy conveniente que las empresas, siempre que ello sea posible, posean unas reglas claras, comprensibles para sus destinatarios y comunicadas previamente acerca de todas las cuestiones relacionadas con las TIC's. Se trata de deslizar la actuación patronal hacia la admonición y clarificación, evitando que el poder disciplinario asuma el protagonismo de cara a conseguir los objetivos de eficiencia y productividad; de que la prevención de conductas abusivas prevalezca sobre la detección de infracciones.

Si nos preguntamos ¿qué ha supuesto la legislación sobre GPS con respecto a la doctrina judicial⁴⁸ una reformulación o una continuidad? El derecho a la protección de los derechos fundamentales del trabajador ante la utilización de GPS en la actual legislación de la LO 3/2018, sin duda, supone una continuidad respecto a la doctrina

⁴⁸ Recordemos, no muy abundante, y sin doctrina general de TC y TS, tan solo de TSJ.

judicial anterior a dicha normativa, tal y como hemos podido analizar en la tipología judicial.

Y para terminar, centrándonos en los derechos en colisión, podríamos afirmar, que el perfil del art. 18.4 CE no queda dibujado de una manera clara como independiente del derecho a la intimidad del art. 18.1 CE, lo que es predecible que pueda provocar fallos judiciales contradictorios en los TSJ hasta que se unifique la doctrina por parte del Tribunal Supremo, con arreglo a la actual normativa en protección de datos.

6. Bibliografía

- AEPD (2019) *Guía Drones y protección de datos*, <https://www.aepd.es/media/guias/guia-drones.pdf>.
- Arredondo Pacheco, Jorge (2012) “Ideas a tener en consideración ante la irrupción de un nuevo mecanismo de control empresarial: el GPS Estudios financieros”, *Revista de trabajo y seguridad social: Comentarios, casos prácticos : recursos humanos*, 351.
- Arrúe Mendizabal, Marta (2019) “Los derechos a la intimidad, a la propia imagen y a la protección de datos de los empleados públicos vs el control por parte de la Administración: un estudio a partir de la regulación del sector privado / similitudes y (pocas) diferencias en comparación con los trabajadores por cuenta ajena”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, 54.
- Asquerino Lampareno, María José (2019) “Régimen jurídico del contrato de trabajo. El control de la actividad de los repartidores de Telepizza”, *Temas laborales: Revista andaluza de trabajo y bienestar social*, 148.
- Barrios Baudor, Guillermo (2019) “El derecho a la desconexión digital en el ámbito laboral español: primeras aproximaciones” *Revista Aranzadi Doctrinal*, 1.
- Baz Rodríguez, Jesús (2019) “La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático”, *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, 54.
- Bernal Pulido, Carlos (2007) *El Principio de proporcionalidad y los derechos fundamentales*, Madrid: Centro de Estudios Políticos y Constitucionales.
- Castilleja Sánchez-Ostiz, Joaquín (2018) “Novedades en el ámbito laboral de la nueva Ley Orgánica de Protección de Datos”, *Actualidad Jurídica Aranzadi*, 947.
- Cobas Cobiella, María Elena (2019) “¿Como proteger las bases de datos y los productos derivados del Big Data?”, *Aranzadi doctrinal*, 1.
- Cuadros Garrido, María Elisa
- (2018) *Trabajadores tecnológicos y empresas digitales*. Pamplona: Aranzadi.
- (2017) “La mensajería instantánea y la STEDH de 5 de septiembre de 2017”, *Revista Aranzadi Doctrinal*, 11.
- ElPeriodico (2019) “Polémica por un anillo de compromiso con GPS para rastrear a tu pareja en tiempo real”, *El Periodico* <https://amp-elperiodico.com.cdn.ampproject.org/c/s/amp.elperiodico.com/es/tecnologia/20191127/crean-anillo-compromiso-gps-rastrear-novio-7752640> (última consulta 27 noviembre de 2019).

- Escudero Alonso, Luis José (2012) “Comentario de Jurisprudencia Social. Despido disciplinario y validez de la prueba (uso de un dispositivo GPS)”, *Consell obert: Recull informatiu del Consell General de Col·legis de Graduats Socials de Catalunya*, 277.
- Fernández García, Antonio (2010) “Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial”, *Aranzadi Social: Revista Doctrinal*, 17.
- Fernández Orrico, Francisco Javier (2019) “Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre”, *Revista Española de Derecho del Trabajo*, 222.
- García Ninet, José Ignacio y VICENTE PACHÉS, Fernando (2015) “El derecho valor a la dignidad humana y el derecho a la protección de datos personales en la Constitución Europea”, *Revista del Ministerio de Trabajo e Inmigración*, 57, 137-192.
- Goñi Sein, José Luis (2009) “Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos”, *Justicia laboral: revista de Derecho del Trabajo y de la Seguridad Social*, 39.
- Lucena Cid, Isabel Victoria (2014) “El nuevo concepto de la intimidad en los nuevos contextos tecnológicos” en AA. VV. GALÁN MUÑOZ, Alfonso (coord.) *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y de la comunicación*, Valencia: Tirant Lo Blanch.
- Martínez Moya, Juan (2019) “El derecho a la protección de datos personales y sistema de geolocalización impuesto por la empresa a los trabajadores-repartidores: SAN, Sala Social, de 6 de febrero de 2019 (procedimiento núm. 318/2018)”, *Revista de Jurisprudencia Laboral (RJL)*, 1.
- Molina Navarrete, Cristóbal (2018) “¿Saber es poder? conectividad empresarial, geolocalización (GPS) y autodeterminación digital del trabajador: comentario a sentencia del Tribunal Superior de Justicia de Andalucía”, *Revista derecho del trabajo*, 20.
- Pérez Alvarez, Salvador (2014) “La generación @ como paradigma de la ciudadanía digital”, *Actualidad Jurídica Aranzadi*, 877.
- Pérez Del Prado, Daniel (2009) “¿Puede el empresario controlar a sus trabajadores mediante dispositivos GPS?: algunas notas sobre el cómo, el dónde y el por qué”, *Información laboral. Jurisprudencia*, 10.
- Purcalla Bonilla, Miguel Ángel (2019) “Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: Notas a propósito de la Ley 3/2018, de 5 de diciembre”, *Revista Española de Derecho del Trabajo*, 218.
- Rodríguez Escanciano, Susana (2015) *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales de los trabajadores*. Madrid: Dykinson.
- Sepulveda Gómez, María (2019) “Negociación colectiva y derechos digitales en el empleo público”, *Revista General de Derecho del Trabajo y de la Seguridad Social*, 54.

Sempere Navarro, Antonio Vicente (2007) “Tras el pronunciamiento del Tribunal Supremo, ¿cabe controlar el ordenador de los trabajadores?”, *Actualidad Jurídica Aranzadi*, 741.

Sempere Navarro, Antonio Vicente y San Martín Mazzuconi, Carolina

— (2015): *Las TIC's en el ámbito laboral*. Madrid: Dykinson, 120-122.

— (2002) *Nuevas tecnologías y Relaciones Laborales*. Valencia: Tirant Lo Blanch, 46-48.

Valdés Dal-Ré, Fernando (2003) “Contrato de trabajo, derechos fundamentales de la persona del trabajador y poderes empresariales, una difícil convivencia”, *Relaciones Laborales: revista crítica de teoría y práctica*, 2.

Sicre García, Lucía (2016) “¿Cómo ser abogado 2.0?”, *Actualidad Jurídica Aranzadi*, 918.