

**EL CONTROL DE LA ACTIVIDAD DE LOS
REPARTIDORES DE TELEPIZZA**

Sentencia de la Audiencia Nacional de 6 de febrero de 2019

MARÍA JOSÉ ASQUERINO LAMPARERO*

SUPUESTO DE HECHO: El conflicto colectivo se suscita a raíz de la implantación de una directriz empresarial por la que se implanta un sistema de geolocalización obligatoria para los nuevos repartidores que accedan a la empresa, siendo potestativa para los que ya formaran parte de la plantilla. Una decisión idéntica a la adoptada por otras empresas del sector y con la que se pretende conocer tanto el tiempo real que se emplea en los repartos, como permitir al cliente seguir el estado de su pedido.

El sistema GPS se introduce a través de los terminales telefónicos de los repartidores que fueran contratados. El control efectivo obliga a que el trabajador porte un teléfono de su propiedad; de esta manera, constituye requisito sine qua non para entablar la relación laboral no solo que el futuro trabajador tenga el precitado medio de comunicación, sino que además acceda a la aplicación indicada por el empleador que asegura su localización, así como que mantenga conectado su aparato durante toda la jornada laboral. Otras obligaciones a las que se comprometen estos trabajadores son las de mantener operativa la línea telefónica y el acceso a internet, de ahí que se regule también en el contrato la consecuencia de su incumplimiento. En ese caso pasará a una situación de suspensión contractual por un período máximo de dos meses, tras ese lapso –se entiende, aunque no se expresa, sin que se haya resuelto– se procederá a la extinción de conformidad con el art.49.1.b) del Estatuto de los Trabajadores. Igual suerte resolutoria cabe señalar para los supuestos de “negativa reiterada” o “imposibilidad sobrevenida de aportación de esta herramienta”. La empresa, a modo de compensación por el desgaste de la herramienta, entrega al trabajador una cantidad económica que fija en atención al número de horas pactadas.

RESUMEN: La Audiencia Nacional acoge los argumentos esgrimidos por la representación sindical, entendiéndolo que la medida concreta de geolocalización im-

* Profesora sustituta interina de Derecho del Trabajo y de la Seguridad Social.

ECLI: ES:AN:2019:136.

puesta por la empresa atenta a los derechos de información de los representantes de los trabajadores y de los propios trabajadores afectados, lesionando de igual modo el derecho a la protección de datos de carácter personal de estos últimos. Conclusión que refuerzan los artículos 11 y 90 de la Ley Orgánica de protección de datos y garantía de los derechos digitales (Ley Orgánica 3/2018, de 5 de diciembre)¹.

ÍNDICE

1. INTRODUCCIÓN: LA FACULTAD DE VIGILANCIA Y CONTROL Y LOS DERECHOS DE LOS TRABAJADORES
2. LA UTILIZACIÓN OBLIGATORIA DEL GPS PARA LOS REPARTIDORES DE TELEPIZZA: SENTENCIA DE LA AUDIENCIA NACIONAL DE 6 DE FEBRERO DE 2019 (SENTENCIA NÚMERO 13/2019)
 - 2.1. El sistema de control empresarial: el GPS
 - 2.2. Sobre la presunta infracción de los artículos 64.5 y .6 del estatuto de los trabajadores
 - 2.3. Sobre la posible vulneración del derecho de protección de datos de carácter personal y del derecho de información de los trabajadores afectados
 - 2.4. Sobre la aportación por el trabajador de su teléfono móvil con conexión a internet
3. VALORACIONES
4. CONCLUSIONES

1. INTRODUCCIÓN: LA FACULTAD DE VIGILANCIA Y CONTROL Y LOS DERECHOS DE LOS TRABAJADORES

No es ni mucho menos innovador el discurso acerca de los límites y extensión del poder de dirección empresarial. Hasta dónde llega la facultad natural que define al empleador ha venido tradicionalmente preocupando a los juristas, siendo no pocos los pronunciamientos judiciales vertidos sobre la materia.

La “novedad” suscitada proviene de los medios que puede emplear el empresario para desplegar esas potestades del art.20 del Estatuto de los Trabajadores, sobre todo cuando las “nuevas” tecnologías han dispensado un mundo de posibilidades desconocidas treinta años atrás. Estas nos han abierto a un mundo impensable de oportunidades –laborales y personales– pero, como suele ocurrir, no están exentas de posibles consecuencias no deseadas. Así, simplificando, de un lado el acceso a

¹ A nuestro juicio, han quedado cuestiones sin resolver que hubiera sido recomendable que el Tribunal las hubiera abordado aun cuando fuera obiter dicta, tales y como la imprecisión empresarial en la expresión de “negativa reiterada”, por cuanto la vaguedad con la que se expresa el empleador denota la situación de indefensión en la que quedaría el trabajador de aceptarse esta causa como resolutoria y que, en definitiva, abunda en el dato final considerando que la cláusula resolutoria es nula por abuso de Derecho.

internet nos ha traído indudablemente ventajas a la hora, por ejemplo, de ofrecer mayor visibilidad a nuestros perfiles (y ahora únicamente estamos pensando en la dimensión profesional del sujeto), pero hemos tenido que pagar el peaje de deshacernos de una parte de nuestra privacidad². Si deseamos conseguir cierta proyección a través de las posibilidades que nos brinda internet, tendremos que renunciar a parte de nuestra intimidad. Baste recordar cómo la mayor parte de las aplicaciones o redes sociales exigen la transmisión de datos propios y, a cambio de los mismos, logramos acceder a este nuevo mercado.

Aquí está por tanto la diferencia que, si la trasladamos al ámbito laboral y concretamente a la dimensión empresarial, supone que el empleador va a disponer de una serie de instrumentos informáticos mucho más precisos y potentes que los medios que tenía en el pasado que le van a resultar de suma utilidad para poder desplegar todas sus capacidades organizativas, decisorias y de ejecución, así como –y aquí nos encontramos con el problema que queremos abordar– de control y vigilancia sobre el quehacer de sus trabajadores, lo que finalmente también le supondrá poder ejercer sus facultades disciplinarias con mayor índice de fiabilidad y acierto.

Sin negar este resultado, y centrándonos en las facultades de vigilancia y control que indiscutidamente posee el empleador, en la medida en la que los instrumentos tendentes a supervisar al trabajador son portados –y soportados– por este son susceptibles de provocar injerencias no deseadas en aspectos que pertenecen a la más estricta privacidad del ser humano, lesionando derechos fundamentales y haciendo real el riesgo psico-social al que puede someterse a este empleado.

De todas las medidas o instrumentos de control que puede emplear el empresario, fijaremos nuestra atención en un dispositivo: el GPS, que permite sin género de dudas, localizar e identificar al trabajador durante el tiempo que esté activado y que surgió “como una forma evolucionada de videovigilancia para aquellos casos en los que la actividad del trabajador es móvil”³.

En estos supuestos, la controversia se plantea entre la legítima postura empresarial de conocimiento del cumplimiento de la actividad contratada y la posible lesión concreta que los medios empleados suponen a derechos fundamentales e irrenunciables del trabajador y que, normalmente, suelen ser el relativo a la intimidad (art.18.1 CE) y el de protección de datos (art.18.4 CE).

En lo que hace al primero (derecho a la intimidad) consideramos necesario dispensar, al menos, un esbozo de su contenido esencial. Enraizando con el derecho a

² Goñi Sein, J.L. (2017) “Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016”, en *Revista de Derecho Social*, nº78: “La nueva era comunicativa que inauguran las TIC es del todo punto diversa al mundo cerrado y sustraído a la publicidad, que preconiza el derecho a la intimidad en su vertiente negativa, por lo que su reivindicación y defensa en el mundo digital ha perdido gran parte de su sentido”.

³ Pérez del Prado, D. (2009) “Instrumentos GPS y poder de control del empresario”, *Revista de contratación electrónica*, n. 107, disponible Vlex 74451572.

la dignidad como “valor espiritual y moral inherente a la persona”⁴, la intimidad es una manifestación de la libertad del individuo que se plasma en un doble sentido. Por un lado, desde el prisma positivo, se caracteriza como un derecho de acción, de exigencia de que exista un ámbito que se reconozca como propio de autodeterminación. De igual modo, el citado derecho tiene una faceta que podríamos calificar de negativa, por cuanto se abre la posibilidad de reaccionar frente a determinados comportamientos de terceros invasivos a esta dimensión personal.

De esta forma, el derecho a la intimidad se concreta, a decir por la doctrina especializada –Herrán Ortiz⁵– como “un derecho de la persona a decidir por sí mismo (sic) en qué medida desea compartir con otros sus pensamientos, sus sentimientos y su vida personal”; “de todo ello se concluye que el derecho a la intimidad constituye una respuesta jurídica a las aspiraciones de cada persona por alcanzar un ámbito de desarrollo interior, ajeno a la intromisión de terceros”.

En cuanto a la protección de datos, observamos cómo este derecho fue abordado tempranamente por la Sentencia de 15 de diciembre de 1983 del Tribunal Constitucional alemán, identificándolo con la “autodeterminación informativa” que también enlaza con la dignidad humana, siendo este una manifestación de “la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo, cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida”⁶.

Este derecho, el de protección de datos⁷, acaso tradicionalmente no gozara de relevancia pero, en la actualidad, los efectos fatídicos que pueden entrañar los nuevos sistemas de información, en lo que hace a la recogida y tratamiento de datos personales, hace fácilmente imaginable su importancia. Lo verdaderamente peligroso –como nos ha hecho ver la doctrina especializada y pronunciamientos como el apuntado *ut supra*– no solo es que la informática pueda recopilar esos datos con velocidad vertiginosa, sino que puede almacenarlos sin límite temporal alguno

⁴ STC 53/1985, de 11 de abril, BOE de 18 de mayo de 1985

⁵ Herrán Ortiz, A.I (2003) El derecho a la protección de datos personales en la sociedad de la información, Cuadernos Deusto de Derechos Humanos, núm. 26, Instituto de Derechos Humanos, Universidad de Deusto, pág.11.

⁶ Continúa diciendo el aserto antes mencionado que “la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos de protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona”; a nuestro juicio resulta especialmente ilustrativo el ejemplo que incluye, pues da cuenta de la importancia de esta protección que acaso en abstracto es difícilmente imaginable. Así el Alto Tribunal alemán manifiesta “Quien sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales”.

⁷ En la actualidad, “y principalmente después de la STC 202/00, se muestra seguro [el Tribunal Constitucional] en sus afirmaciones ya que primero, institucionaliza definitivamente el término derecho a la protección de datos, antes se había referido a la libertad informática; y segundo, define y delimita el concepto, la naturaleza jurídica y el contenido del derecho a la protección de datos”, Hernán Ortiz, A.I (2003) *El derecho a la protección de datos personales en la sociedad de la información*, op.cit., pág.19.

ni constricción espacial y –quizás lo más perverso– que esos datos son susceptibles de ser cedidos a terceros, permaneciendo el sujeto afectado (el titular) en la más absoluta y total ignorancia.

Descendiendo a los argumentos de nuestros tribunales y refiriéndonos concretamente a nuestro Tribunal Constitucional, se deja constancia (así, STC de 30 de noviembre de 2000, STC 292/2000 -RTC 2000/292) cómo el contenido del derecho a la protección de datos está conformado por varias facetas; de un lado, la decisión particular del individuo a disponer de los datos y de otro el control sobre los mismos, lo que en definitiva supone que es el único legitimado para “decidir cuáles de estos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar y que permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso”. En definitiva, el derecho ahora analizado permite a cada persona disponer –ceder– y controlar –saber– quién posee sus datos y para qué los tiene, pudiendo de igual forma “oponerse a esa posesión y usos”.

Aislada e individualmente es fácil analizar el contenido y extensión de los derechos, pero ¿qué ocurre cuando los derechos –y en particular el de la intimidad así como el de protección de datos– del trabajador se encuentran ante el poder de dirección de su empresario ya sea para organizar o para vigilar e incluso sancionar?

La convivencia pacífica entre las pretensiones empresariales y las que defiende el trabajador va a hacer necesario rescatar el tradicional juicio de proporcionalidad que señalaba nuestro Alto Tribunal y a través del cual, de forma casuística –dado que carecíamos de respuesta legal expresa–⁸, se tenía que valorar la idoneidad de la medida empresarial, la necesidad de esta y su proporcionalidad, lo que a su vez nos reconduce a otra idea asentada de que los derechos no son absolutos y pueden, por tanto, ceder “ante intereses constitucionalmente relevantes”.

Este juicio –el de proporcionalidad– será el que se emplee precisamente por nuestros tribunales (y, como más adelante veremos, también en el aserto que comentamos) para dirimir si concretos sistemas de control (particularmente los relativos a la videovigilancia) son invasivos al derecho de intimidad de los trabajadores.

En este sentido, se viene entendiendo que no constituye lesión alguna al derecho antes referido cuando existen sospechas fundadas y razonables acerca de la comisión previa de un ilícito laboral, cuya constatación se revela como necesaria, siendo un instrumento tremendamente hábil a los fines pretendidos la implantación de cámaras de videovigilancia que certificarán las irregularidades

⁸ Calvo Gallego, F.J.: “Este insuficiente, y por tanto, problemático marco legal, unido a su escaso tratamiento en la negociación colectiva española, ha obligado a una construcción básicamente jurisprudencial de los posibles límites a este poder, en especial en todo lo relacionado con las nuevas tecnologías” (op.cit., pág. 24). Por su parte, Goñi Sein (2017) “Nuevas tecnologías digitales...”, op.cit, indica que “A falta de unos principios específicos en el ordenamiento jurídico laboral, el debate sobre la identificación de los límites del poder de control empresariales a través de las nuevas tecnologías, se sustancia en una doble instancia –por una parte, en sede jurisdiccional y por otra, ante la autoridad de control del derecho a la protección de datos”.

detectadas, aun cuando el trabajador no haya sido avisado específicamente de su implantación.⁹

De esta manera, y centrando el discurso en este momento en los sistemas de videovigilancia por cuanto son los primeros que han suscitado controversias judiciales, se observa cómo la finalidad de la implantación de los sistemas en principio agresivos al trabajador, puede salvar al empresario del reproche jurídico en su actuación. Por descender al terreno concreto, se observa cómo no merece la misma respuesta jurídica la implantación de las cámaras en un casino que captaban el audio y recogían imágenes en unas zonas concretas –que por supuesto no estaban destinadas al recreo del trabajador– susceptibles por sí misma de sustracciones o malas praxis de terceros (así, en la ruleta francesa y en la caja) cuando no ha existido una razón objetiva y previa que avale esta fórmula de control (no hay robos ni conductas presumiblemente ilícitas) que cuando los mecanismos tradicionales de control resultan insuficientes para tutelar el patrimonio empresarial.¹⁰

El criterio de nuestro alto Tribunal es continuista en la Sentencia del Tribunal Constitucional de 11 de febrero de 2013 (sentencia número 29/2013¹¹); tras exponer que el poder de dirección no es omnímodo, se fundamenta la lesión al art.18.4 CE, por cuanto el empleado carecía de la información que debería haber precisado “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”.

Mas, la STC de 3 de marzo de 2016 (Sentencia número 39/2016)¹² sienta

⁹ STS de 2 de febrero de 2017, Sentencia número 96/2017, RJ 2017/1628.

¹⁰ STC 98/2000, de 10 de abril, RTC 2000/98. En este caso, se entiende que la conducta de la empresa a través de la implantación de los medios antes comentados no superaba el juicio de proporcionalidad, pues no quedaba acreditada la insuficiencia de los anteriores medios que salvaguardaban el patrimonio empresarial.

¹¹ En esta ocasión el Órgano se enfrentaba a la suspensión de empleo y sueldo de un trabajador por haber sido sorprendido –filmado por las cámaras– llegando tarde y ausentándose antes de finalizar su jornada; el empleado afectado no conocía específicamente de esta forma de control laboral, pues tan solo existían genéricos distintivos anunciando a los diferentes transeúntes (el centro de trabajo era una Universidad) que podían ser grabados.

¹² RTC 2016/39. En este caso el Alto Tribunal desestima las pretensiones de una trabajadora despedida con base a las grabaciones obtenidas por el empresario, por medio de las cuales se constata cómo la misma distrajo una cantidad cierta de dinero de la caja registradora. La trabajadora –los empleados– no conocía de la ubicación exacta de la cámara que vigilaba sus movimientos, aun cuando es cierto que en el escaparate de la tienda donde prestaba sus servicios esta empleada sí constaba una advertencia: un distintivo informativo adherido en el escaparate del negocio.

Los representantes de los trabajadores no sabían de la preexistencia ni subsistencia de la específica cámara de seguridad y el empresario demandado y recurrido en amparo acreditada, durante el desarrollo de la litis a la que se dio origen, que la implantación de la mencionada cámara había sido la respuesta empresarial a la previa constancia de “múltiples irregularidades, de lo que podría desprenderse una apropiación dineraria por parte de alguno de los trabajadores que trabajaban en dicha caja”.

La sentencia aludida presenta un profundo voto particular formulado por D. Fernando Valdés que de forma sutil recuerda que “confunde la legitimidad del fin (en este caso, la verificación del cumplimiento de las obligaciones laborales a través del tratamiento de datos, art.20.3 LET en relación

un nuevo criterio¹³, considerando que la implantación de cámaras ocultas por el empresario está legitimada si existen sospechas fundadas de incumplimientos laborales anteriores.

No hay que dejar de señalar, no obstante, que en el momento en que se pronuncia el Tribunal Constitucional existía un silencio legal en lo que hacía al específico tratamiento de los datos concernientes a los trabajadores. Esa ausencia de expresión normativa, posibilitaba entender que el consentimiento sobre los datos propios se entendía implícito con la vinculación laboral; así, el concierto del contrato de trabajo posibilitaba al empresario recabar los datos personales de los trabajadores y, de esta forma, no era preciso el consentimiento expreso de los empleados.

De esta forma, la Sentencia distinguió entre el consentimiento y la información que, en todo caso, sí consideró necesaria pero que se ve salvada por la mera advertencia genérica de captación de la imagen. La valoración conjunta de los hechos probados hacen concluir al Tribunal que, de nuevo aplicando el juicio de proporcionalidad, la medida de la empresa fue ajustada a Derecho¹⁴.

Salvando las distancias –por cuanto no gozaban de un escenario normativo que expresamente contemplara “las condiciones en las que un empleador podía recurrir a la videovigilancia de un empleado para investigar un delito penal”– el Tribunal Europeo de Derechos Humanos interpreta (Sentencia Köpke contra Alemania, de 5 de octubre de 2010) que un sistema de videovigilancia oculto al conocimiento de los trabajadores, es respetuoso con el art.8 del Convenio Europeo¹⁵ por cuanto se

con el art.6.2 LOPD) con la constitucionalidad del acto (que exige previamente la información necesaria, art.5 LOPD)”.

¹³ Sin ánimo exhaustivo, algo similar ocurrirá con la STS 96/2017, en recurso de casación para la unificación de doctrina número 554/2016 (RJ 2017/1628) que desestima los argumentos de vulneración al derecho a la intimidad, por cuanto el trabajador aun cuando no conociera expresamente el destino de las imágenes captadas por los sistemas de videovigilancia sí sabía de su existencia y “Existía constancia de las conductas irregulares”.

En la STS de 1 de febrero de 2017 (Sentencia número 86/2017, RJ 2017/1105) –de nuevo aplicando el juicio de proporcionalidad– se aprecia la inexistencia de lesión al derecho a la intimidad y al de protección de datos, siendo causa justificativa del proceder empresarial la concurrencia de razones de mantenimiento de la seguridad en su negocio.

¹⁴ Los argumentos básicamente pasan por considerar que la medida empresarial era “justificada (ya que existían razonables sospechas de que alguno de los trabajadores que prestaban servicios en dicha caja se estaban apropiando de dinero); idónea para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja)” y, por ende, no existe lesión al derecho a la intimidad personal.

¹⁵ Art.8 Convenio Europeo para la Protección de Derechos Humanos y de las Libertades Fundamentales: “1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

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

limitó a la captación de imágenes que afecta a dos trabajadoras y además durante un lapso temporal definido en cuanto a su duración (dos semanas). Al no concurrir estas circunstancias en los hechos que dilucidará la Sentencia de este Tribunal en caso de López Ribalda y otros contra España (sentencia de 9 de enero de 2018) desestimará los alegatos empresariales¹⁶.

Pero los sistemas de vigilancia y control no se escapan a otras posibles consecuencias no deseadas, aun cuando estas se encuentren en otro plano diferente al de la eventual colisión con los derechos fundamentales. Así, es tradicional también –y de nuevo lo veremos aquí con la Sentencia de la Audiencia Nacional– discutir sobre la participación previa de los representantes de los trabajadores cuando el empresario pretende acometer una concreta medida de vigilancia y control¹⁷.

Acaso este último problema pueda entenderse resuelto en lo que hace a los sistemas de geolocalización por mor del art.90 de la nueva LOPD¹⁸, que literalmente dispone que:

¹⁶ Recuérdese que el asunto finaliza en el TEDH tras haber sido inadmitidos los recursos de casación ante el TS y de amparo ante el TC.

Nos parece importante señalar que la sentencia del Juzgado de primera instancia resolvió a favor del empresario con base, fundamentalmente, en la STC 186/2000. En esta última –a diferencia de lo que ocurrió cuando dicta la Sentencia el Juzgado de lo Social de Granollers número 1 de 16 de marzo de 2011– sí tenemos un marco normativo específico que abordaba el derecho a la protección de datos, la Ley Orgánica 15/1999, de 13 de diciembre, a la que debemos aunar –por ser este un argumento hondamente fundamentado por la parte primero actora y más adelante recurrente– la Instrucción 1/06 de 8 de noviembre de la AEPD.

Centrándonos en el pronunciamiento del TEDH, vemos cómo se resuelve la extralimitación de los poderes empresariales por vulnerarse con su actuación el derecho a la vida privada consignado en el art.8 del citado Convenio. Para fundamentar la conclusión, se parte de unos hechos que básicamente consisten en la instalación de unas videocámaras en unas zonas concretas cuales son los puestos de trabajo de las cajas vigiladas, sin conocimiento previo de estas ni de sus representantes. El contenido de estas grabaciones fue visionado posteriormente por otros trabajadores (concretamente el representante de la empresa y el representante sindical)

De esta forma, la premisa viene dada por la consideración de que cualquier captación de la imagen del trabajador –si es encubierta– ha de ser considerada como “una importante intromisión en su vida privada” y esta será la pauta para interpretar cómo esta concreta medida de vigilancia que “no estaba motivada por una sospecha previa contra las demandantes” y que tenía, por tanto, como destinatario a cualquier trabajador que prestara sus servicios en las cajas registradoras, “durante semanas, sin límite de tiempo y durante todo el horario laboral”, no cumple con los requisitos legales específicos que se señalaban en nuestro ordenamiento jurídico y, en definitiva, cercena el principio de proporcionalidad al que debe acomodarse la actuación empresarial.

¹⁷ En la STSJ de la Comunidad Valenciana de 21 de marzo de 2017 (AS 2017/723) se consideró que se vulneraba el derecho a la intimidad de los trabajadores, con la consiguiente declaración de nulidad de la prueba obtenida por el medio de supervisión implantado unilateralmente por el empleador, la instalación de cámaras sin que se hubiera posibilitado previamente la intervención de los representantes de los trabajadores y sin haber informado previamente a los trabajadores ni tan siquiera a través de un genérico aviso.

¹⁸ Ley Orgánica de Protección de Datos (Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales).

Adviértase que la mayor parte de los pronunciamientos judiciales nacionales que han versado sobre sistemas de geolocalización se han ceñido a examinar el derecho del trabajador desde la perspectiva de la intimidad, entendiendo a esta como ausencia o presencia de una expectativa y minimizando el interés por observar los problemas suscitados desde el prisma de la calidad en el tratamiento de datos.

“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.”

2. LA UTILIZACIÓN OBLIGATORIA DEL GPS PARA LOS REPARTIDORES DE TELEPIZZA: SENTENCIA DE LA AUDIENCIA NACIONAL DE 6 DE FEBRERO DE 2019 (SENTENCIA NÚMERO 13/2019)

2.1. El sistema de control empresarial: el GPS

Partimos de los hechos desglosados en el comienzo del presente y que provocan la reacción sindical tanto de UGT como CCOO –que habían sido informados de la fórmula controladora, una vez la medida fue hecha pública a través de una normativa interna–.

Los sindicatos manifiestan su oposición frontal a la indicación empresarial¹⁹, entendiéndola:

De un lado, CCOO estima que es insostenible la pretensión empresarial de exigir que sea el propio trabajador no solo el que aporte el móvil sino que asuma el gasto de su conservación, siendo de otro lado desproporcionada la sanción prevista para el supuesto de la falta de operatividad posterior del instrumento telefónico, propugnando su ilegalidad.

De igual forma, este sindicato entiende que se ha vulnerado el derecho a la información por cuanto no se manifiesta empresarialmente al trabajador afectado el tratamiento y los fines de los datos recopilados. En suma, la cláusula contractual sería nula por abusiva.

¹⁹ Recuérdese, en este punto, que la empresa había redactado una cláusula por medio de la cual obligaba a los repartidores de nuevo ingreso a que portaran su dispositivo telefónico, asegurando en todo momento de la duración de la relación laboral la óptima conexión a las redes, so pena de declarar la suspensión contractual e incluso –si la situación se demoraba en el tiempo– la extinción de la relación laboral.

UGT, por su parte, manifiesta su desconfianza de que el móvil pueda ser una herramienta de trabajo²⁰, cuestionando las posibilidades sancionadoras que unilateralmente ha previsto el empresario.

A estas críticas, se le suma Inspección de Trabajo por considerar, básicamente, que la medida empresarial atenta varios preceptos de la norma básica laboral. De un lado, porque el clausulado introduce una condición menos beneficiosa que la que está asumida legal y convencionalmente, produciéndose una quiebra de esta manera del art.3.1.c) del Estatuto de los Trabajadores.

Además, esta actuación empresarial lesiona abiertamente los postulados de la por aquel entonces vigente Ley Orgánica de Protección de Datos, pues no se prevé en ningún momento la obligación empresarial de proporcionar información exacta y puntual al trabajador afecto acerca de cómo se van a tratar sus datos.

En tercer lugar, Inspección advierte una conculcación en el art. 64.5 del Estatuto de los Trabajadores, al no haberle otorgado a los representantes de los trabajadores la posibilidad de participar y ser consultados en esta materia.

Por último –aunque no menos importante– este organismo expresa que la previsión explícita del empresario sobre las consecuencias jurídicas que entrañaría la actuación del trabajador que incumple esta nueva directriz empresarial de mantener operativo el móvil durante la jornada laboral, supone una perversión de las instituciones jurídicas de suspensión y extinción por causas válidamente consignadas en el contrato.

2.2. Sobre la presunta infracción de los artículos 64.5 y .6 del Estatuto de los Trabajadores

La empresa entendía que la medida alcanzada podía ser decidida unilateralmente por ella con base a su poder de dirección, a diferencia de lo apreciado por las demandantes que sostienen la necesidad de ser informadas previamente de manera adecuada para poder emitir su dictamen en el plazo que legalmente tienen para ello.

Entienden en este sentido que la información suministrada por la empresa limitándose a informar de la medida que pretendía implantar es a todas luces insuficiente.

La Audiencia Nacional estima la pretensión sindical pues los representantes de los trabajadores tenían derecho a conocer previa y exactamente el funcionamiento y alcance de la aplicación, los datos que iba a recoger, qué compromisos concretos se exigían a los trabajadores y cuál era el destino de la información que se proporcionaba a través de la aplicación, todo con base a los preceptos anteriormente reseñados y reforzando su argumentación con el actual art.90.2 de la LOPD.

²⁰ Aunque podamos intuirlos, no aparecen reflejados los motivos barajados por este sindicato para esa “desconfianza”.

2.3. Sobre la posible vulneración del derecho de protección de datos de carácter personal y del derecho de información de los trabajadores afectados

Partiendo de la incontrovertida naturaleza jurídica de que los datos de localización de una persona constituyen datos de carácter personal²¹, examina la doctrina contenida en nuestras Salas de los Tribunales Superiores de Justicia, que, a su vez, recogen asertos constitucionales para, y conforme a la aplicación del juicio de proporcionalidad, dejar constancia de que la medida no supera este canon aun cuando sí responda a fines constitucionalmente legítimos, proponiendo al efecto otros sistemas alternativos menos agresivos para el trabajador, cuales pueden ser la implantación de sistemas de geolocalización en las motos²² de las que se valen para sus encargos o pulseras que “no implican para el empleado la necesidad de aportar medios propios y lo que es más importante, ni datos de carácter personal como son el número de teléfono o la dirección de correo electrónico”.

En lo que respecta al derecho de información de los repartidores, la Audiencia Nacional entiende lesionado este derecho tanto al amparo de la normativa vigente durante el inicio del conflicto como a la luz del actual art. 11 y 90 de la LOPD.

2.4. Sobre la responsabilidad del trabajador a la aportación por el trabajador de su teléfono móvil con conexión a internet

Situados ahora en el plano de la más estricta legalidad ordinaria, se examina la exigencia empresarial de que el trabajador aporte su propio teléfono móvil para desarrollar la actividad laboral.

La Audiencia manifiesta que si se admite esta pretensión del empresario se estaría haciendo caso omiso a uno de los requisitos que definen la relación laboral, cual es la ajenidad en los medios, sin que sea factible realizar la analogía con lo que ocurre con los falsos autónomos.

De otro lado, y derivada de la exigencia anterior, de admitirse la pretensión empresarial se estaría desplazando la obligación que recae en esa parte –empleador– de dar ocupación efectiva (art.4.2.a) y art.30 ET) por cuanto cualquier problema que sufriera el trabajador al no poder activar el sistema de geolocalización le acarrearía una suspensión con los efectos que tal declaración entraña para la relación laboral.

²¹ Calvo Gallego, F.J. : “ Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral”, 2019, pág. 2: “...cuando estos objetos, singularmente etiquetas, vehículos o dispositivos electrónicos, pueden relacionarse aun de forma mediata o indirecta con una persona física determinada, los datos que proporcionen no serían ya genéricos o simplemente informaciones geográficas, sino auténticos datos personales –art.4.1 RGPD–, sometidos a las garantías que se derivan tanto de la normativa europea como española”.

²² La misma consideración –el GPS en el vehículo es menos invasivo que si se instala en el teléfono móvil– para la STSJ Asturias de 27 de diciembre de 2017 (AS 2018/296).

Se estima, igualmente, que la cantidad económica otorgada por el empresario para compensar el gasto por desgaste-conservación del terminal telefónico es, a todas luces, insuficiente, tras haber hecho –y así consta en la sentencia– los cálculos sobre los gastos que reportaría un móvil de gama baja.

En línea con lo anterior, la previsión de la cláusula de resolución no prevista por convenio es en realidad una forma de despido disciplinario que, además, no encuentra cobertura legal, pues su aplicación no exige la concurrencia de las notas de culpabilidad y gravedad ni observar los requisitos formales preceptivos que se regulan en el art.55 del Estatuto de los Trabajadores.

3. VALORACIONES

Echamos en falta un análisis más exhaustivo y fundamentado de cada uno de los puntos que se sometían a su consideración, debiendo –pues la ocasión lo merecía, aunque no sea una exigencia legal– haber anudado a cada uno de los hechos probados su correspondiente conclusión jurídica.

Así, a título de ejemplo se observa que como hecho probado en la Sentencia también se recoge el funcionamiento de la aplicación, y esta circunstancia –desde nuestra visión– no ha sido valorada. En la actualidad la posibilidad de acceder a la cámara no se ha activado, por lo que únicamente los datos almacenados son los relativos al trayecto del trabajador, concretamente la representación en un mapa de la ruta que sigue el repartidor, al que de otro lado, se identifica con un código numérico que tiene una validez de 8 horas o, en su defecto, coincidiendo con la finalización de su jornada laboral, no asociando de forma estable un número a un concreto trabajador.

Si el trabajador-repartidor no tiene ningún encargo pendiente, no se produce el envío de ningún dato. Los datos (relativos únicamente al número de identificación del repartidor) se almacenan en una base desde la que se interpretan para representarlos en el mapa correspondiente al lugar desde donde se hayan realizado los pedidos. Los datos son automáticamente borrados al día siguiente.

No es posible acceder a la información por parte de terceros. Para la instalación de la aplicación basta con proporcionar un correo electrónico o número de teléfono móvil.

Asentados los considerandos anteriores, y siempre desde nuestro punto de vista, hay que diferenciar entre los dos planos examinados por la Sentencia, pues cada uno de ellos merece un tratamiento diferente. Así pues, encontramos de un lado el examen del posible derecho fundamental lesionado y de otro el análisis del terreno puramente legal que nos conduce a dilucidar si concurren los requisitos legales relativos a la información al trabajador afectado y la previa consulta a quienes son sus legítimos representantes.

En cuanto al primer análisis nuestra modesta opinión es no hay lesión de ningún tipo. La sentencia es realmente parca cuando analiza la posible contravención constitucional (le dedica a ello un escaso fundamento jurídico –el Sexto–); había que acudir al criterio de la proporcionalidad, ciertamente, pero –y prueba de ello son los pronunciamientos antes aludidos– descendiendo sobre el terreno concreto. Esto es, si bien es cierto que el parámetro para medir la conducta empresarial estriba en la aplicación del principio de proporcionalidad, para comprobar si este se cumple es preciso descender casuísticamente, analizando los hechos que concurren en cada supuesto para anudar sus correspondientes consecuencias jurídicas.

A nuestro juicio esto no ha ocurrido en el pronunciamiento judicial que hoy se analiza. Se reseñan los criterios ya conocidos para realizar el juicio de proporcionalidad, remitiéndose para ello a otros supuestos de hecho en vez de desgajar los hechos probados para constatar si la medida empresarial era adecuada e idónea.

De un lado se echa en falta –a nuestro juicio siempre– un examen más pormenorizado y que sin restar importancia a los pronunciamientos judiciales de duplicación nos conduzcan a Altos Tribunales, pues son la fuente a la que hemos de acudir cuando se trata de fundamentar cuestiones jurídicas²³.

¿No tiene ninguna trascendencia para el fallo el cómo funciona la aplicación en la práctica? Entendemos que esta circunstancia sí es relevante a los efectos finales. Partimos de la consideración de que si la prueba sobre la misma se consideró pertinente, se debería haber valorado conforme a los datos que se extraían de la misma. No podemos dejar de preguntarnos qué hubiera ocurrido si la información vertida por la pericial hubiera sido otra diferente y, concretamente, se hubiesen arrojado datos de los que inferir nítidamente que sí se producía una huida de datos a terceros, entonces, en ese caso, ¿se habrían tenido en cuenta?

Continuemos con las afirmaciones de la Audiencia Nacional; salvando esta fórmula de invocación a pronunciamientos destacados pero que no constituyen jurisprudencia, observamos cómo no se aprecia la proporcionalidad de la medida empresarial por cuanto existen otras fórmulas menos agresivas al derecho controvertido, cuales puedan ser colocar el GPS en el medio de transporte del trabajador o que este porte una pulsera que indique dónde se encuentra.

Entendemos que efectivamente el GPS instalado en la motocicleta o ciclomotor es menos invasivo²⁴ que la aplicación móvil que se exige, básicamente porque es un objeto el que lo tiene adherido y no acompaña en todo momento al sujeto, por lo que este no está permanentemente ubicado, pero no acertamos a entender cómo la pulsera que llevaría en su propio cuerpo el trabajador afectado puede ser

²³ Obsérvese, además, como en el exiguo Fundamento de Derecho está reflejado literalmente el precepto –art.90 LOPD– y la literalidad de la sentencia del TSJ de la Comunidad Valenciana, que son los que prácticamente se emplean para deducir la lesión al derecho fundamental.

²⁴ Recuérdese que el Dictamen 2/2017 emitido por el Grupo de Trabajo el 8 de junio de 2017 señalaba como deber empresarial la selección de dispositivos de seguimiento que consigan garantizar el respeto a la privacidad del trabajador.

menos incisiva a sus derechos fundamentales (intimidad y nos atrevemos a decir dignidad) que la aplicación móvil que se cuestiona.

Echamos en falta que se explique precisamente cómo estas opciones que ofrece el Tribunal (que, de otro lado, no le corresponde valorar al órgano jurisdiccional, por cuanto es una potestad empresarial el fijar los medios de vigilancia y control, quedando reservado para el órgano el control ex post) son menos lesivas y alcanzan el fin pretendido y constitucionalmente también digno de protección del empresario.

Así, consideramos que el GPS en la motocicleta no cumple con la finalidad a la que iba destinada la aplicación y ello porque el recorrido que realiza el trabajador para culminar con éxito la labor de pedido no se lleva a cabo únicamente en este medio de transporte. El trabajador tendrá que, a golpe de borceguí, consumir la entrega del pedido y acaso esto también es lo que quiere ser objeto de control por parte del empresario y por parte del cliente. A lo mejor, los retrasos en la entrega se producen no por el camino que con el vehículo se recorre, sino en la demora –imputable o no al trabajador, es esta una cuestión que en este momento no se ha de analizar– del camino que se ha de realizar andando.

Si la preocupación que subyace en la mente del enjuiciador es el temor a que el trabajador pudiera estar permanentemente controlado porque, por descuido –por ejemplo– el trabajador no desconectara la aplicación cuando finaliza la actividad laboral (circunstancia esta que entra en el mundo de lo hipotético y de la que, en todo caso, el empresario no sería responsable), el mismo recelo podría presentar la pulsera que indica podría portar el trabajador, pues resulta también posible que este no se despoje de este elemento justo en el momento en que finaliza la jornada.

Continuando con este argumento –el relativo a la falta de idoneidad de la pulsera sugerida– es posible precisamente (dadas las desproporcionadas consecuencias con las que el empresario anudaría la omisión de este mecanismo de control) que el trabajador antes del inicio de su jornada ya lleve esa insignia de control para evitar olvidos de última hora, con lo cual entendemos que la vigilancia a través de este medio puede ser más exhaustiva que el de implantarla en un móvil, al ser este un instrumento cotidiano.

Se siguen obviando determinados hechos probados –constan como tales en la sentencia comentada– a través de la prueba pericial. No se puede olvidar, a nuestro juicio es un dato que tiene una entidad en absoluto desdeñable, que al trabajador se le concede la alternativa de elegir cómo acceder a la aplicación, a través del número de su teléfono móvil o facilitando un correo de contacto²⁵.

En este punto enlazamos con nuestra introducción, ¿cuál es la condición que en el tráfico ordinario se impone al sujeto a poder descargar una aplicación?

²⁵ En el Fundamento de Derecho Sexto letra g, se indica que “los trabajadores para descargar la aplicación en su teléfono móvil han de proporcionar un número de teléfono o una dirección de correo electrónico en la que reciben el código de descarga”.

La identificación de su beneficiario ya sea a través de un correo electrónico y/o de la aportación del teléfono móvil. Así pues, la petición de los datos que realiza la empresa a fin de poder instalar la aplicación no es extraña al tráfico normal.

Pero es que, además, hay un dato que nos parece de especial importancia y al que ni siquiera se alude cuando se resuelve esta posible lesión al derecho fundamental. El trabajador era libre de o bien facilitar su teléfono móvil para instalar la aplicación o bien hacerlo a través de la aportación de una cuenta de correo electrónico. Así, si lo que se pretende es garantizar el derecho a la intimidad y protección de datos, el trabajador que pueda sentir un lógico temor a ser invadido, puede acceder a través de una cuenta de correo electrónico creada y mantenida solo a los efectos de que se proceda a la instalación de la aplicación, sin facilitar por tanto información personal –si no lo desea– alguna.

La realidad como criterio hermenéutico ha de ser contemplada también para resolver las situaciones jurídicas conflictivas. Es frecuente la imputación a nuestra norma –específicamente la laboral– de que no resuelve cuestiones reales y problemas que en la práctica se producen, entendiéndose (una muestra, a nuestro juicio, es el art.18 del Estatuto de los Trabajadores) que en muchos casos la norma está obsoleta. Pues bien, esa realidad no puede ser desconocida por los tribunales, como tampoco puede dejar de valorarse una prueba que se ha considerado acreditada (la opción del trabajador a facilitar la cuenta de correo o el móvil que destina al trabajo).

Los hechos se prueban, se acreditan y aparecen como tales reseñados en un aserto para derivar conclusiones jurídicas de los mismos. No es factible a nuestro juicio dejar constancia de los hechos probados y omitir la consecuencia jurídica que se derivan de los mismos.

Abundando en esta idea, también se omite la elucubración sobre otro de los hechos probados que a nuestro juicio es totalmente pertinente para la solución final de la controversia: la circunstancia de que la subsistencia de los datos se hacía coincidir con la duración de la jornada diaria, sin que hubiera un registro de aquellos²⁶. De igual modo, tal y como consta probado por la pericial, esta información en ningún momento pasaba a terceros.

El juicio de proporcionalidad no estaba –a nuestro juicio– por tanto cerrado, por cuanto los datos anteriores eran necesarios para estimar si se producía o no una lesión al derecho a la privacidad. Nuestra aseveración no quiere conducir al

²⁶ En este sentido, recuérdese como la STJ de 2 de octubre de 2018, Ministerio Fiscal, asunto C-207/16 entendió que la protección al derecho de intimidad y al de protección de datos no es uniforme, sino que depende de cuánto tiempo se almacenen los datos y la exactitud de los mismos. Aquí, en el aserto comentado, se afirma que cada día los trabajadores-repartidores tienen un número aleatorio diferente, lo que supone que el trabajador no sea identificado a través de un único código, lo que en definitiva implica que se asocian los datos diariamente. Nadie sabe –salvo si se realizan otro tipo de actuaciones que sí podrían ser lesivas al derecho de intimidad o protección de datos– más allá de la jornada diaria el tiempo que tarda un concreto repartidor en hacer el pedido. No se pueden extraer conclusiones más allá de la indicada jornada laboral diaria.

lector a un terreno de negación de que esos datos sean “peligrosos” en el sentido que recoge Calvo Gallego²⁷, por supuesto que lo son pero esta aseveración no nos debe conducir a la afirmación de que su tratamiento fuera de las previsiones legales conduce a la inexorable declaración de atentado contra los derechos fundamentales.²⁸ Lo que aquí consta no es un desconocimiento palmario del trabajador acerca de la cesión de datos, pues la conoce (aunque efectivamente no con la exhaustividad que merece, ni tampoco del destino de esos datos) por lo que no puede ser parangonado con otros asertos jurisprudenciales en lo que hace a la lesión del derecho fundamental.

Creemos que le bastaba al Órgano acudir a los textos más importantes que desde el ámbito europeo ofrecen las pautas precisas a fin de interpretar qué tipo de dispositivos de control son absolutamente inviables por lesionar derechos fundamentales de los trabajadores. Así, la Recomendación del Comité de Ministros de los Estados Miembros de 1 de abril de 2015²⁹ nos aporta esas máximas que, a continuación, pasamos a recordar.

De un lado nos encontramos con que:

1. No deben admitirse los instrumentos cuyo objetivo central es el control de la actividad y el comportamiento del trabajador.

Si aplicamos esta aseveración al supuesto que hoy nos ocupa, observamos cómo la medida empresarial de vigilancia está amparada jurídicamente, siendo el instrumento que se ha escogido como medio para llevar a cabo este control el GPS que tiene como objetivo directo el control de tiempos, esto es, no supervisa el comportamiento del trabajador –ni siquiera se tiene constancia a través de este sistema de cuál es el mismo– ni tampoco controla la actividad que se desarrolla.

Presente hemos de tener en todo momento que el sistema de control se aplica solo a unos trabajadores concretos: los repartidores.

2. La finalidad a la que deben atender esos medios de vigilancia son los relativos a la buena gobernanza de la actividad profesional o aquellos relacionados con la salud o seguridad.

El GPS que la empresa implanta obedece a una clara finalidad –no discutida– de optimizar los recursos humanos y conseguir que la productividad de

²⁷ Calvo Gallego, F.J. “Artículo 90...”, op.cit., pág. 3. Destaca que si bien es cierto que los datos de localización no se incluyen “expresamente en la categoría de datos “especiales” del art.9 RGPD, presentan sin duda una evidente singularidad o, si se nos permite, “peligrosidad” sobre todo cuando su tratamiento se hace de forma relativamente exacta y prolongada en el tiempo”.

²⁸ Una clara conculcación al derecho de intimidad o de libertad informática se provocaría ante determinadas acciones empresariales tendentes al control de la actividad laboral desde el propio móvil del trabajador: Cremades Chueca, O. (2018) “El enriquecimiento injusto en la utilización del dispositivo móvil personal con fines profesionales” (Bring Your Own Device) en *Trabajo y Derecho*, nº 47.

²⁹ Para un estudio más detallado, Calvo Gallego, F.J (2019): “Artículo 90...”, op.cit., pág. 9, sobre el que nos basamos para establecer cada uno de los puntos reflejados con números arábigos en el cuerpo del presente.

determinados trabajadores alcance los estándares empresariales en lo que hace a la optimización del tiempo.

Por supuesto, este sistema concreto de control supone una supervisión indirecta del trabajador, más hay que recordar que esta consecuencia está admitida³⁰ y se considera lícita también para la citada Recomendación, pues hemos de partir cómo el interés legítimo que ostenta el empresario es un fundamento sólido para sustentar una concreta medida de vigilancia y control³¹.

A ello hemos de aunarle la circunstancia de que nos encontramos ante un servicio concreto que presta la mercantil: el reparto a domicilio, no siendo –aunque pueda resultar obvio– la única empresa que satisface esta necesidad del cliente. Creemos que es razonable pensar que la persona que solicita la comida desea que el reparto se haga con la mayor celeridad, e incluso opinamos que no es descartable que uno de los aspectos que valore el consumidor a la hora de dirigirse a una u otra cadena de comida, se haga en función de la rapidez con la que se tramita el pedido. Aquí tenemos, a nuestro juicio, la justificación más que razonable (y no exportable a otro tipo de empresas e incluso tampoco a otro tipo de trabajadores que prestan sus servicios para esta misma entidad) que tiene el empresario de implantar esta concreta medida de vigilancia.

Desde la perspectiva empresarial, razonable nos parece pensar que una de las expectativas legítimas que tiene el empleador sobre los repartidores es que estos realicen con diligencia la tramitación de pedidos. No es un control caprichoso.

3. Adopción de garantías para proteger los datos personales y respetar la intimidad de los afectados.

No nos cabe duda que estas se cumplen. Recuérdese que en los hechos probados, se garantiza esa confidencialidad. En el decimoquinto se señala que “ningún tercero puede acceder a los datos allí almacenados sin contar con las debidas autorizaciones y permisos de acceso”. De otro lado, concurren los requisitos de protección y privacidad –reflejo literal del mismo hecho– de datos establecidos en el Reglamento Europeo.

³⁰ Calvo Gallego, F.J., “Artículo 90...”, op.cit., señala en relación con las tecnologías de geolocalización que “solo debieran incorporarse si son necesarias para cumplir los objetivos legítimos perseguidos por los empleadores y si su uso no conduce a un control permanente de los asalariados. De ahí que, en definitiva, el control de los trabajadores mediante estos instrumentos no debería ser el objetivo principal, sino solo una consecuencia indirecta de una acción necesaria para proteger la producción, la salud, la seguridad o la gestión eficiente de una organización”. Esa eficiencia a la que alude el actor está aquí presente y es una realidad, tal y como se acredita de la razón que impulsa al empresario a implantar el GPS: su competidora ha llevado a cabo este sistema de control, logrando una mayor eficiencia. Esto es, la implantación del GPS obedece no a meras elucubraciones teóricas del empresario sino a datos reales que le hacen pensar que sus recursos serán mejor aprovechados con la aparición de esta aplicación que controla determinadas acciones laborales del trabajador.

³¹ De nuevo Calvo Gallego, F.J., “...”, op.cit., pág. 11 que trayendo a colación el Dictamen 13/2011 del Grupo –16 de mayo de 2011– señala “cómo los empresarios deberían analizar si este control constituía una necesidad demostrable con un fin legítimo y sopesar además dicha necesidad con los derechos y libertades fundamentales de los trabajadores. En tales casos, la base jurídica del tratamiento podría ser el interés legítimo”.

La aplicación –continuamos basándonos en la prueba pericial– no almacena ningún dato “relativo al empleado/repartidor, más allá del código numérico asignado por el “Monitor de reparto” (cuyo número –código– recordemos era diferente cada jornada) “mientras no se cierre la sesión en el dispositivo” (clausura que realiza el propio trabajador) “o el código haya expirado” (que tenía una validez máxima de 8 horas³²).

En lo que hace al resto de argumentaciones del Tribunal sobre aspectos que rozan ya el plano de la más estricta legalidad, no podemos dejar de manifestar nuestro más absoluta conformidad.

De un lado, porque la intervención necesaria a los representantes de los trabajadores no se produce³³. Efectivamente, no se les otorgó la posibilidad de conocimiento previo sobre el funcionamiento de la nueva medida y, por ende, se les negó su potestad legal de informar previamente sobre la misma³⁴.

Esa información tampoco es accesible para el trabajador concretamente afectado, a pesar de que este tiene derecho a conocerla, actualmente previsto en el art.90 LOPD pero que ya fue puesto de manifiesto en el ámbito de la Unión Europea por el Grupo de Trabajo en su Dictamen 2/2017³⁵ de 8 de junio y también en la Recomendación de la que hablábamos párrafos atrás (Comité de Ministros de los Estados Miembros de 1 de abril de 2015 –CM/Rec (2015)5–). A mayor abundamiento, no olvidemos que el Reglamento de Protección de Datos (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016) parte en su Considerando número de la capacidad normativa de los Estados y la convencional siempre sobre la “base del consentimiento del trabajador” acaso como manifestación del principio de transparencia (ex art.88. 2 del RPD).

De todas formas, y sin pretender restar importancia a la necesidad de facilitar esa información a su legítimo destinatario, esto es, el trabajador, entendemos que las consecuencias de esa falta de información no son las mismas que las que con antelación los Tribunales han tenido la oportunidad de analizar. Así, a nuestra memoria llegan los asertos que dilucidaban si la simple exposición de un cartel

³² El Grupo de Trabajo antes aludido, señalaba la necesidad de establecer un lapso para conservar los datos que no fuera superior a dos meses. Creemos que esta referencia nos aporta la idea de valoración de unos datos que se almacenan solo por ocho horas. Estos criterios temporales también nos permiten dilucidar acerca de la posible transgresión a un derecho fundamental del trabajador.

³³ Pérez del Prado, D. (2009) “Instrumentos GPS y poder de control del empresario”, op.cit., recuerda cómo el informe a recabar de la representación unitaria ex art.64.1.3.d) ET es “una cuestión de mera legalidad ordinaria”.

³⁴ Consciente de la importante labor desempeñada por los representantes de los trabajadores también en relación con esta fórmula de control, la CM/Rec (2015) 5, sugiere que sea el convenio colectivo el que contenga las pautas de estos sistemas de vigilancia.

³⁵ Es ese “deber de transparencia” aludido por Calvo Gallego, F.J. “Artículo 90...”, op.cit., pág.12. “... el Dictamen recuerda, por ejemplo, cómo en los casos de nuevas tecnologías, el deber de transparencia –y, por tanto, el deber de información– se hace más “evidente” para un tratamiento leal de los trabajadores”. Todo ello sin perjuicio de considerar –como así lo hace el autor y el Dictamen– que el consentimiento del trabajador no equivale per se a la viabilidad de la medida.

informativo a la vista de hipotéticos clientes y trabajadores era suficiente como para entender que determinados medios de control estaban justificados³⁶. El desconocimiento de estos trabajadores sobre esa vigilancia era superior –y a pesar de ello el Tribunal Constitucional entiende no violado el derecho– a la inopia a la que se enfrentan estos concretos trabajadores/repartidores, pues son conocedores –de hecho ellos son los que han de descargarse la aplicación y saben desde el principio, esto es desde que se inscriben a la oferta de trabajo– de estas reglas de vigilancia y control, aun cuando efectivamente no se les haya explicado pormenorizadamente en qué consisten.

El sistema que la empresa hoy implanta en absoluto es secreto.

Otro aspecto de legalidad que nos parece adquiere una gran relevancia es el que se plantea sobre la previsión de la empresa en torno a la declaración de la suspensión contractual automática en los supuestos en los que el trabajador no procede a la sustitución del móvil que se encuentra en estado defectuoso. Recordemos que esta situación –y no nos queda claro que el plazo de 10 días sea suficiente conforme a los estándares normales en el mercado para arreglar los desperfectos o saber si ante la carestía de su reparación, se impone la sustitución– supone la imposición al empleado de una sanción que no solamente no está recogida en el convenio de aplicación, sino que además incumple frontalmente con los requisitos previos que han de exigirse a todo incumplimiento laboral: la culpabilidad y la gravedad. La suspensión contractual la contemplamos aquí como sanción y efectivamente admitir la misma supone a la postre lo que la Audiencia reflejaba en torno al desplazamiento de la titularidad del deber a la ocupación efectiva.

Y si esto es así con relación a la suspensión del contrato, mucho más si aludimos a la sanción que finalmente podría imponer el empresario, el despido disciplinario –al ser la cláusula de extinción manifiestamente abusiva– al que parece que el trabajador se ve automáticamente abocado en los supuestos en los que –prescindiendo de la gravedad y culpabilidad de nuevo– no porta el sistema móvil indicado por la empresa en los plazos que esta señala.

A mayor abundamiento, habría que indicar que la conducta que unilateralmente señala el empresario como transgresora de los deberes contractuales laborales queda indefinida al emplearse el adjetivo “reiterada” cuando se refiere a la negativa del trabajador a aportar la herramienta de trabajo. En este punto, el lector se pregunta, ¿cuántas veces ha de negarse el trabajador a portar el útil? ¿Basta con dos días? En definitiva, la entrada de estas causas de suspensión y de extinción se han dejado al albur de una de las partes contratantes, el empresario, con el peligro que su valoración unilateral conlleva.

Por supuesto, y ya casi finalizando, la exigencia empresarial tanto de que el trabajador aporte el útil de trabajo como de la ínfima cantidad que se pretende

³⁶ Al respecto, véase la antes citada STS de 2 de febrero de 2017, Sentencia número 96/2017, RJ 2017/1628.

dispensar al empleado por el desgaste de tal herramienta, vuelve a darnos muestra del abuso empresarial, del enriquecimiento injusto del empleador³⁷ que se produce –de conformidad con el entendimiento más genuino de esta doctrina– al establecer esta obligación de aportación de dispositivo propio del trabajador “sin título jurídico ...o, existiendo dicho título, este último no es compensado adecuadamente y además se tiene la capacidad en abstracto de alternativas” provocándose “de facto una transferencia de utilidad”³⁸.

4. CONCLUSIONES

La sentencia hoy comentada ha sido valorada positivamente por nuestra doctrina laboral más especializada, apreciándose la vulneración del derecho a la protección de datos de carácter personal de los trabajadores, lo que en definitiva supone la imposibilidad de llevar a cabo el control de la actividad de los repartidores cuando el instrumento para controlar la misma es el GPS, entendiéndose que es invasivo y que existen otras medidas más proporcionadas para alcanzar el objetivo de supervisión de la actividad prestacional.

De igual modo –y en este sentido parece que los servicios jurídicos de la competidora de Telepizza acaso han sido más eficaces– la forma a través de la cual se ha implantado este sistema de control choca abiertamente con el panorama legal que existía cuando el proceso comenzó y, aún más pudiera decirse lesiona frontalmente la previsión expresa contenida en el art.90 LOPD, al no haberse garantizado ni la oportuna intervención previa de los representantes de los trabajadores ni la información a los concretos empleados afectados por tal medida.

Desde nuestro modesto punto de vista, las cuestiones que en torno a los sistemas de vigilancia y control se puedan plantear, han de resolverse –para concluir si son o no lesivos a los derechos fundamentales– preguntándonos sobre

³⁷ Cremades Chueca, O. (2018) “El enriquecimiento injusto en la utilización del dispositivo móvil personal con fines profesionales” (Bring Your Own Device) en *Trabajo y Derecho*, nº 47. Reseña este autor en su artículo cómo el ahorro anual medio del “uso por parte de los empleados de los dispositivos móviles (teléfonos móviles, ordenadores portátiles, tabletas, etc) personales para uso profesional” –BYOD– supone un ahorro anual de costes empresariales entre trescientos cincuenta y mil seiscientos cincuenta dólares por trabajador. Aparte de este nada despreciable dato económico, se señalan como ventajas para esa aportación del útil personal la “familiaridad-libertad que tiene el trabajador en utilizar su dispositivo y la mayor disponibilidad (locativa y temporal) para trabajar”. Continúa este autor proponiendo que ante la exigencia de aportación de dispositivo propio del trabajador como herramienta laboral, se debería retribuir específicamente, entendiendo que “este principio de retribución específica se incumple cuando no hay una cláusula contractual que ampare el BYOD (imposición empresarial del BYOD sin título jurídico) o bien, existiendo, sin retribución específica adecuada” y proponiendo una reforma del art.85 del ET, con el objeto de incluir en los convenios colectivos una serie de directrices para proteger los derechos de los trabajadores, haciendo hincapié en los métodos de control empresariales y esa retribución a la que se ha aludido.

³⁸ IBÍDEM.

las cuestiones puestas de manifiesto por Calvo Gallego, esto es: “legitimidad de los fines, la licitud del tratamiento, la proporcionalidad y minimización de los datos, la seguridad de los ficheros o la duración de la conservación de los mismos”³⁹.

Ninguno de estos –a nuestro juicio– ha sido examinado con profundidad por el aserto hoy comentado, pudiendo dar la sensación (siempre hablando en nuestra opinión) de que la omisión de las pautas legales que ciertamente existían en el supuesto que suscita el debate, han sido suficientes para también concluir con la existencia de la lesión del derecho.

En definitiva, parece cómo este pronunciamiento no sigue la estela marcada por los parámetros que anteriormente se han puesto de manifiesto (y atinentes a la finalidad empresarial, la necesidad de la medida, la limitación temporal, etc.) al entender que son otras las cuestiones que hay que examinar para entender lesionado un derecho fundamental. Así, a nuestro juicio, más que el argumento de la proporcionalidad, la Sentencia se ha fijado para apreciar el atentado al derecho, en la obligación legal de información que aquí se entiende obviada⁴⁰, junto al claro abuso empresarial al pretender desplazar el gasto que supone la adquisición y conservación de un útil de trabajo al empleado, así como las consecuencias sancionadoras a la pérdida de esta herramienta incluso superiores que las que podrían merecer otros incumplimientos laborales del trabajador que automáticamente no suponen ni la suspensión ni, por supuesto, la extinción contractual.

Insistimos en que el comportamiento del empresario al exigir la aportación de la herramienta imprescindible a su juicio para acometer la prestación de servicios es abusiva, sin que la exigua compensación económica sea suficiente como para cubrir los gastos que el mantenimiento y la conexión a internet suponen. Ese juicio en torno al manifiesto abuso de derecho del empleador se observa aún más claramente cuando se comprueban las consecuencias que entraña para el trabajador y que, en ocasiones, no está ni siquiera en su mano resolver.

Desde luego no se puede pretender válidamente disfrazar de cláusula resolutoria lo que en realidad sería una posibilidad extintiva que recae en la discrecionalidad unilateral del empresario, sin embargo estos comportamientos abusivos no nos pueden llevar a concluir que hay lesión de derechos fundamentales.

³⁹ Calvo Gallego, F.J (2019), “Artículo 90...” op.cit.

⁴⁰ *Ibidem*, pág. 25 ahonda en esta cuestión destacando cómo los parámetros utilizados por nuestra doctrina constitucional y por la propia doctrina judicial no valoran aspectos como “la existencia o no de un fin empresarial determinado, lícito y legítimo, su tratamiento posterior de manera compatible con los mismos, la necesidad o no de estas medidas y su rechazo ante la existencia de otros mecanismos menos invasivos para la esfera privada del trabajador, la limitación al máximo de los datos recabados en función del fin legítimo admitido, su adecuación y pertinencia, el rechazo a todo mecanismo de seguimiento constante –aún más cuando este no resulte necesario–, la existencia o no de medidas de seguridad en el acceso y tratamiento de estos datos, o la duración de la conservación de los mismos”.

No podemos descartar la idea de que primero ha sido la conclusión y después los argumentos jurídicos –débiles a nuestro juicio– para alcanzar la misma. Y esta aseveración la realizamos fundamentalmente tras constatar cómo esa prueba pericial a la que hemos hecho referencia a lo largo del presente, ha sido completamente obviada para obtener el resultado final.