Utilización de sistemas de geolocalización en el ámbito laboral*

Worker surveillance through geolocation devices

IVÁN ANTONIO RODRÍGUEZ CARDO**

1. INTRODUCCIÓN

El derecho a la protección de datos es un derecho de nuevo cuño, de «tercera generación»[1] si se quiere, que nació para hacer frente a riesgos a los que se exponía el ciudadano como cliente, usuario o consumidor de productos y servicios. Evidentemente, la protección de los datos personales no es un problema exclusivo de nuestros días, pero en los últimos tiempos ha cobrado nuevas dimensiones, por muy diversas razones. Ante todo, por la intensificación de las relaciones económicas y sociales, especialmente a escala global o internacional, indisolublemente unida al imparable avance de los medios tecnológicos.

En principio, la relación laboral no parecía el entorno más propicio para el desarrollo de este derecho, al menos respecto de su núcleo duro, esto es, los derechos y obligaciones más característicos de la persona a la que se refieren los datos. Sin lugar a dudas, el empleador no está legitimado para difundir información personal del trabajador cuando la haya conocido a consecuencia de la relación laboral, pero ni el legislador, ni los tribunales, ni tampoco el grueso de la doctrina científica consideraron inicialmente que el poder de dirección y organización empresarial pudiera verse condicionado por las exigencias que derivan de la normativa de protección de datos personales.

Esa percepción ha cambiado radicalmente en los últimos años fruto de la decidida labor de organismos o instancias de carácter supranacional (OIT, UE, TEDH), que ha contado con cierta acogida por parte de los tribunales españoles, en particular el TC. El derecho a la protección de datos personales se ha convertido en un límite para determinadas decisiones empresariales, y, en concreto, para aquellas que tienen por objeto el control del cumplimiento de las obligaciones laborales. Como se sabe, la videovigilancia ha sido la medida de control más controvertida, o cuando menos la que ha contado con mayor presencia ante los tribunales, pero cada vez son más frecuentes –o pueden anticiparse– conflictos análogos respecto de otras medidas de control. La potencialidad invasiva de las nuevas tecnologías ha provocado una reacción tuitiva que, en ausencia de otras garantías que se consideren más pertinentes, ha situado al derecho a la protección de datos en una posición nuclear y de vanguardia, como la primera y principal línea de defensa de los derechos de los trabajadores.

La geolocalización es un ejemplo de esta línea de tendencia, pues la tecnología permite determinar la ubicación en el espacio –en

* Estudio realizado en el marco del proyecto de investigación DER2016-80327-P del Ministerio de Economía y Competitividad.

** Profesor Titular de Derecho del Trabajo y Seguridad Social. Universidad de Oviedo. Experto Nacional en la *European Labour Law Network.*

[1] Cfr. A.E. PÉREZ LUÑO, *La tercera generación de Derechos Humanos*, Aranzadi, Pamplona, 2006, p. 28.

cualquier lugar del mundo– de una persona o un objeto en un sistema de coordenadas geográficas con un margen de error no superior a 50 metros[2], y además registrar todos sus desplazamientos. Gracias a ello se pueden elaborar perfiles y patrones de comportamiento[3] y desde luego es información que puede resultar de suma utilidad en el contexto de la relación laboral. La geolocalización del trabajador –a través de todas las tecnologías disponibles, no sólo GPS, Wifi o bluetooth, sino también otras como radiofrecuencia (RFID)[4]– es una medida con una complejidad particular, y no siempre se justifica, pues una monitorización permanente no parece compatible con el principio de proporcionalidad[5].

Por todo ello, el legislador ha considerado adecuado introducir un precepto legal específico para atender a este novedoso medio de control. En este sentido, el artículo 90 LOPD lleva por título «derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral» y habilita a los empleadores para «tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control», siempre que se respeten dos condiciones. En primer lugar, que «estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». Y en segundo lugar, que se informe de esa medida con carácter previo a los trabajadores, y eventualmente a sus representantes.

Es una regla sin precedentes en el ordenamiento español y que se formula al amparo, y como contenido, del derecho fundamental a la protección de datos. No es, por tanto, únicamente un derecho digital, sino un ingrediente más del derecho a la protección de datos, lo que genera una serie de consecuencias, como por ejemplo la supervisión constante de la AEPD para evitar extralimitaciones del empresario. Ahora bien, esos rasgos, principalmente la novedad y con ello la necesidad de configurar adecuadamente el alcance y el contenido de esta restricción a los poderes del empleador, justifican el análisis detenido, por un lado, de cuándo y cómo el empresario puede servirse de esta tecnología, y, por otro, de cuáles son los límites que el derecho a la protección de datos y el derecho a la intimidad imponen al uso de sistemas de geolocalización. Se prescindirá, sin embargo, de aspectos más accesorios o incidentales, que también pueden contar con relevancia práctica y presencia en la doctrina judicial, pero que no encajan en el marco del art. 90 LOPD, como por ejemplo la calificación de la geolocalización como indicio de laboralidad, al mostrar la dependencia del trabajador[6].

2. GEOLOCALIZACIÓN Y RELACIÓN LABORAL

La geolocalización puede convertirse en una herramienta valiosa desde una perspectiva de eficiencia empresarial y su implementación desde luego está amparada por las prerrogativas que derivan de la libertad de empresa consagrada en el art. 38 CE, que explícitamente alude a la «defensa de la productividad». Los potenciales riesgos de las nuevas tecnologías no pueden dar lugar a prohibiciones o limitaciones irreflexivas de las facultades empresariales que deriven en una desventaja competitiva en el mercado, pues en un mundo globalizado ello acabaría conduciendo, a buen seguro, a la propia desaparición de la empresa, pues no todos los Estados introducirán cautelas o limitaciones similares.

[2] *Vid.* D. Barinas Ubiñas, *El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada,* Revista Electrónica de Ciencia Penal y Criminología, nº 15, 2013 (http://criminet.ugr.es/recpc/15/recpc15.html).

[3] *Vid.* A. Batuecas Caletrío, *Intimidad personal, protección de datos personales y geolocalización,* Derecho Privado y Constitución, nº 29, 2015, p. 50.

[4] *Vid.* C. Gala Durán y A. Roig Batalla, *El uso de las etiquetas de identificación por radiofrecuencia en las empresas: ¿un nuevo riesgo para los derechos de los trabajadores?*, AL, nº 8, 2010.

[5] Dictamen 13/2011 del Grupo de Trabajo del art. 29.

[6] *Vid.* SSTSJ de Cataluña de 22-6-2018 (recurso 1638/2018) y de Andalucía/Málaga de 31-5-2017 (recurso 322/2017).

En este sentido, la geolocalización puede contribuir a una mejor optimización de los recursos en determinadas actividades, pues, a modo de ejemplo, permite programar mejores rutas o asignar tareas a los trabajadores en función de su mayor o menor cercanía al lugar al que deben desplazarse. Las actividades de transporte, reparto o resolución de averías o incidencias, entre muchas otras, pueden organizarse de manera mucho más eficiente si el empleador conoce la ubicación concreta de los trabajadores y puede tomar decisiones inmediatas para satisfacer de mejor forma las necesidades de los clientes, y además también permite proporcionar a esos clientes información sobre dónde se encuentra su producto o pedido, mejorando la satisfacción de estos con el servicio prestado. La geolocalización no implicaría más que una tecnificación de las facultades ordinarias del empresario, que pueden ser ejercitadas más fácilmente en entornos reducidos donde los trabajadores se encuentran en todo momento a la vista del empleador, pero que requieren de mayor asistencia técnica/tecnológica cuando el trabajo se desarrolla en ámbitos más extensos, sin esa proximidad que hace posible la interlocución directa. La tecnología permite sortear esas barreras y el derecho no habría de ser un obstáculo para que las más modernas formas de información y comunicación mejoren la eficiencia de las empresas.

Por supuesto, la geolocalización cuenta con muchos más usos, tanto en general[7], como desde la perspectiva de una empresa y, por ejemplo, puede jugar un relevante papel en el marco de la seguridad de las personas y los bienes. Qué duda cabe que un empresario puede valerse de dispositivos de localización para proteger herramientas o útiles de trabajo de su propiedad. Esa clase de medidas no deben interpretarse necesariamente como una muestra de desconfianza hacia los trabajadores, como un cuestionamiento de su probidad, sino como una legítima opción para la protección de bienes o herramientas frente a cualquiera –trabajadores o no– que, incluso, puede redundar en beneficio de los clientes o de los propios trabajadores. Los ejemplos son múltiples, pero piénsese en los dispositivos de geolocalización que llevan las aeronaves, que cumplen una función evidente de seguridad, pues el conocimiento exacto del lugar en el que se encuentran facilita la gestión del tráfico aéreo y, eventualmente, los rescates en caso de accidentes.

Esta clase de dispositivos también tienen otras finalidades dependiendo del contexto, y eventualmente pueden afectar a trabajadores aunque no sea el empleador quien haya decidido su uso ni quien gestione directamente la información que proporcionan. En este sentido, los chips de geolocalización son prácticamente imprescindibles en determinadas competiciones deportivas, no sólo del motor, sino también en ciclismo, atletismo y deportes acuáticos, como una forma de medir el tiempo empleado de manera precisa, de comprobar, en su caso, si el deportista ha respetado el recorrido establecido e incluso de proceder a su búsqueda y rescate en caso de que se haya producido alguna incidencia.

Sin embargo, las referencias a la geolocalización en las normas laborales o en la doctrina judicial y científica se vinculan, casi exclusivamente, con el uso de la información que proporcionan esos dispositivos como medio de control de la actividad del trabajador y, en último término, con la validez de dicha información como prueba a efectos de la imposición de una sanción. Es un enfoque limitado, porque pone el acento exclusivamente en los riesgos de esa tecnología y puede conducir a restricciones injustificadas en el uso de esos dispositivos que, como se ha dicho, deben enmarcarse en el legítimo ejercicio del poder de dirección y, a la postre, en la libertad de empresa. No obstante, es la perspectiva que procede en este momento, toda vez que ese es el propósito del art. 90 LOPD. En efecto, el «derecho digital» concedido al trabajador trata de protegerlo frente al uso de «sistemas de geolocalización

[7] *Vid.* R. MILLÁN GARCÍA, Geolocalización: legislación y consecuencias de su uso, Actualidad Administrativa, nº 4, 2019.

para el ejercicio de las funciones de control de los trabajadores». No se cuestiona, por tanto, la tecnología en sí misma, ni su implementación en el contexto de una actividad productiva, sino su uso como medida de vigilancia de la actividad de los trabajadores.

Por supuesto, en su vertiente de instrumento de control la geolocalización debe estar sujeta a límites, al igual que cualesquiera otros medios de vigilancia a disposición del empleador, máxime aquellos con un potencial invasivo más intenso, pues permiten conocer actividades y comportamientos que se enmarcan plenamente en la vida privada del trabajador, y que por tanto escapan a los poderes de control empresarial. En apariencia, los criterios tradicionales para conciliar las facultades empresariales y los derechos del trabajador pueden extenderse a este contexto de la geolocalización, aunque deben tenerse en cuenta algunas particularidades, que por lo demás tampoco son exclusivas de este mecanismo de control, que ni siquiera se presenta como el más invasivo para el trabajador de todos aquellos que la tecnología permite en la actualidad.

Una de esas peculiaridades, como se desarrollará en un epígrafe posterior, es la entrada en juego expresamente del derecho a la protección de datos. Los límites a la geolocalización parece que habrían de derivar del derecho a la intimidad, y desde luego ese es un derecho directamente involucrado cuando el empresario recurre a dispositivos de localización. Sin embargo, el legislador ha advertido explícitamente que el derecho a la protección de datos debe ser respetado, y ello exige una reflexión sobre cuál es el ámbito de actuación y el impacto de cada uno de esos derechos cuando el empresario quiere valerse de esta tecnología para controlar a sus trabajadores.

Otra peculiaridad, como se deduce de lo anterior, es que la geolocalización puede responder a varias finalidades distintas, no sólo al control del trabajador, lo que condiciona el análisis sobre la pertinencia de su implementación y sobre el uso de la información que proporciona, pues los límites serán distintos según cuál sea el propósito. Se trata, en cualquier caso, de peculiaridades no exclusivas de la geolocalización, sino que también están presentes en otros medios de control, como la videovigilancia.

Ahora bien, algún otro rasgo de la geolocalización le concede una identidad propia, como el hecho de que el dispositivo de geolocalización no siempre sea propiedad del empresario, sino que en ocasiones pertenezca al propio trabajador. A la postre, cualquier teléfono inteligente dispone de esa tecnología y el empresario puede verse tentado a beneficiarse de ello, sirviéndose de esas herramientas para alcanzar el objetivo pretendido, con el ahorro de coste que supone. Surgen entonces, inevitablemente, cuestiones relativas a la necesidad de consentimiento del trabajador y, también, de interferencia con otros derechos digitales, y en particular el reconocido en el art. 87 LOPD, en cuya virtud el derecho a la intimidad debe ser respetado en relación con el «uso de dispositivos digitales en el ámbito laboral», aunque el precepto constriñe su radio de acción a los dispositivos puestos a disposición del trabajador por su empleador. Obviamente, el derecho a la «desconexión digital» reconocido en el art. 88 LOPD también puede verse afectado.

Es, en cualquier caso, una problemática rica en matices, que afecta además a un derecho novedoso, pues con anterioridad a la LOPD de 2018 ni los «derechos digitales» estaban formalmente consagrados como tales en nuestro ordenamiento, ni la geolocalización contaba con una regulación expresa, aunque desde luego las reglas generales sobre control empresarial y la abundante jurisprudencia sobre otros medios de control ya permitían afrontar con buenas perspectivas y sólidas herramientas interpretativas el análisis de la problemática práctica que plantea la geolocalización en el ámbito laboral. El nuevo marco normativo proporciona reglas explícitas, aunque no ha despejado completamente todas las incertidumbres, especialmente las que se re-

fieren al impacto que deriva de la aplicación de la legislación de protección de datos.

3. LA PREOCUPACIÓN POR LA GEOLOCALIZACIÓN EN EL CONTEXTO INTERNACIONAL

Los textos internacionales en materia de protección de datos, al menos los más recientes, no se limitan a afirmar que ese derecho es de plena aplicación en la relación laboral, sino que descienden a un mayor detalle, identificando las parcelas donde actúa y valorando el impacto de su correcta implementación, que en último término debe conducir a una cierta evolución de la cultura organizativa empresarial y a limitaciones en el poder de dirección. En este escenario, las medidas de control y vigilancia, y entre ellas la geolocalización, son objeto de atención prioritaria en esos textos.

En el ámbito europeo, la primera intervención normativa de carácter supranacional con vistas a la protección de los datos personales surgió del Consejo de Europa, que con fecha de 28 de enero de 1981 aprobó a tales fines un Convenio específico (el Convenio 108). Esta pionera norma internacional concebía la protección de datos personales como un ingrediente del derecho fundamental a la vida privada[8], y se limitaba, seguramente por su contexto temporal, al tratamiento automatizado de los mismos, con especial atención a los datos especialmente sensibles. No se refería expresamente al ámbito laboral, pero el Consejo de Europa se ocupó más tarde de manera específica de ese terreno, a través de diversos instrumentos complementarios de aquella regulación básica, como es el caso de la Recomendación CM/Rec(2015)5 de su Comité de Ministros, que proporciona pautas relativas al ejercicio de los poderes empresariales de vigilancia y control en relación con la actividad del trabajador o el uso por el mismo de ciertos medios de trabajo. Esta Recomendación CM/Rec(2015)5, sobre tratamiento de datos personales en el contexto del empleo[9], fue aprobada a modo de revisión y actualización de una Recomendación de 1989[10].

En relación con la geolocalización, el apartado 16 de esa Recomendación parte de la premisa de que el empleador únicamente está legitimado para utilizar dispositivos que permitan conocer la ubicación de los trabajadores cuando resulten necesarios para alcanzar un propósito legítimo, si bien no resulta admisible una vigilancia constante del trabajador. Es más, se advierte que el control de la actividad no debería ser la principal función de esos dispositivos, sino un efecto colateral del objetivo primario, que habrá de ser la protección de la propiedad empresarial, la prevención de riesgos o, en general, la eficiencia de la organización productiva. En último término, se alerta sobre la necesidad de respetar la proporcionalidad en su implementación y de introducir mecanismos de protección frente a los riesgos para la intimidad, inclusive la pertinente información al trabajador sobre el tratamiento de sus datos.

Por supuesto, la UE también ha alertado sobre estos riesgos, como demuestra la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones de 4 de noviembre de 2011, titulada "Un enfoque glo-

[8] *Vid.* A.E. Pérez Luño, "La incorporación del Convenio Europeo sobre Protección de Datos Personales al ordenamiento jurídico español", en M.G. Losano, A.E. Pérez Luño y M.F. Guerero Mateus, *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 22 y ss; M.B. Cardona Rubert, *Tratamiento automatizado de datos personales del trabajador*, RTSS, nº 16, 1994, pp. 87 y ss, y J.L. Piñar Mañas, "Protección de datos: Origen, situación actual y retos de futuro", en P.L. Murillo de la Cueva y J.L. Piñar Mañas, El derecho a la autodeterminación informativa, Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 81 y ss.; J.L. Goñi Sein, *Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016*, RDS, nº 78, 2017, pp. 33 y ss.

[9] https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a.

[10] Recomendación R (89), https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf.

bal de la protección de los datos personales en la Unión Europea"[11], en la que se ponía de manifiesto como los «instrumentos de geolocalización facilitan la determinación de la ubicación de un individuo por el mero uso por su parte de un dispositivo móvil». Y del "Repertorio de recomendaciones prácticas sobre protección de los datos personales de los trabajadores" de la OIT puede extraerse una conclusión similar, pese a que no se mencione específicamente la geolocalización, a buen seguro por la fecha de elaboración de ese documento (1997)[12].

En general, esos documentos advierten que las nuevas tecnologías permiten el control de los trabajadores no sólo en el lugar y tiempo de trabajo, sino en cualquier otro entorno gracias a las funciones que incorporan los teléfonos móviles, las tabletas, los vehículos o los denominados *wereables*, aparatos tecnológicos diseñados como prendas de vestir y que pueden captar y registrar datos personales, inclusive la localización. Esas instancias internacionales solicitan la implementación de límites al control y vigilancia del empleador, así como transparencia para evitar que el interés empresarial anule los derechos fundamentales de los trabajadores[13].

Por su parte, el Grupo de Trabajo del art. 29, en su Dictamen 2/2017[14], aconsejaba una previa evaluación de impacto y clarificar la finalidad específica de la geolocalización (*v.gr*., control del trabajador, control horario, seguridad de las herramientas empresariales), para poder valorar adecuadamente la condición de licitud y el respeto a la proporcionalidad y al principio de minimización. También dedica una atención especial al control indirecto del trabajador que puede tener lugar cuando la geolocalización afecta a los vehículos de la empresa que son utilizados por los trabajadores. En tales casos no sólo está en juego que el empleador conozca la ubicación del trabajador, sino que algunos de esos dispositivos permiten obtener datos relativos a la conducción, e incluso posibilitan un control total del trabajador[15].

El Dictamen reconoce que el empleador puede contar con un interés legítimo en la implementación de estas medidas, como la protección de la propiedad empresarial o reforzar la seguridad de los conductores, pero exige la introducción de las pertinentes cautelas, como por ejemplo habilitar al trabajador para que desactive el dispositivo fuera de la jornada laboral o cuando concurran «circunstancias especiales», entre las que se menciona la «visita a un médico». El Grupo de Trabajo del art. 29 insistía en que «los dispositivos de seguimiento de vehículos no son dispositivos para la localización de trabajadores, ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo». El derecho a la información ocupa también un lugar relevante entre las preocupaciones del Dictamen, pues se exige al empresario que informe claramente a los trabajadores de que se ha instalado un dispositivo de seguimiento y que sus movimientos están siendo registrados mientras utilizan el vehículo de empresa.

En fin, el Dictamen pone de manifiesto que la configuración concreta del instrumento (*v.gr*., posibilidad de desactivación fuera

[11] https://eur-lex.europa.eu/legal-content/es/TXT/?uri=-CELEX%3A52010DC0609.

[12] http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf.

[13] *Vid.* M. Recio Gayo, "Nuevo dictamen del GT29 sobre tratamiento de datos en el trabajo: el interés legítimo", en AA. VV., *Especial protección de datos. Guía para afrontar la nueva regulación*, Wolters Kluwer, Madrid, 2018 (www.smarteca.es).

[14] https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1308. También, Dictamen 5/2005 del Grupo de Trabajo del art. 29.

[15] *Vid.* J. Baz Rodríguez, *La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático*, Trabajo y Derecho, nº 54, 2019, pp. 49 y ss.

de horas de trabajo, los datos a los que pueda acceder el empleador y el carácter continuado o no de la monitorización) es un aspecto relevante en el análisis de licitud, aunque el derecho afectado no siempre es la protección de datos, sino más bien la intimidad. Por ello, sistemas como los registradores de datos de incidencias, capaces de proporcionar muy variada información, no sólo la ubicación, sino indicadores sobre la forma de conducción e incluso grabaciones de audio y video, pueden resultar especialmente invasivos. Y, por supuesto, el propósito de la medida debe ser convenientemente valorado, porque más razonable parece un dispositivo de esta índole instalado con la finalidad de registrar el tiempo de trabajo, o incluso con la intención de comprobar que el trabajador preste servicios dentro de una zona previamente asignada, que la geolocalización dirigida a averiguar los movimientos del trabajador durante un proceso de incapacidad temporal, contexto donde será más fácil considerar que esa es una medida desproporcionada.

4. GEOLOCALIZACIÓN CON FINALIDAD DE CONTROL DEL TRABAJADOR: ¿DERECHO A LA INTIMIDAD O DERECHO A LA PROTECCIÓN DE DATOS?

La Directiva 95/46/CE no se ocupó directamente de la geolocalización en el contexto de la relación laboral, como tampoco lo hace el RGPD. Es una omisión razonable en normas que no están diseñadas ni concebidas específicamente para el ámbito del contrato de trabajo. En cualquier caso, el art. 4 del RGPD deja claro que los «datos de localización» deben ser considerados como datos personales, y el art. 88 permite a los Estados miembros, «a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral». Por consiguiente, el RGPD habilita explícitamente a los legisladores estatales para incorporar reglas expresas en este campo, y entre ellas las relativas a geolocalización.

Con ese aval, el art. 90 LOPD se ocupa de esa forma de control empresarial en el marco del Título dedicado a los «derechos digitales». El precepto lleva por rúbrica «derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral», lo que podría conducir a la errónea conclusión de que este es un derecho digital independiente de la protección de datos, como sucede con algún otro (*v.gr.,* desconexión digital o uso de dispositivos digitales). Sin embargo, el apartado 1 de ese art. 90 demuestra que esa conclusión es apresurada, pues el objeto de ese derecho consiste en establecer límites al control empresarial que pueda derivarse del tratamiento de datos obtenidos a través de sistemas de geolocalización.

En cualquier caso, la rúbrica y el texto de los apartados de ese precepto no resultan completamente consistentes, pues mientras la rúbrica únicamente menciona el derecho a la intimidad, el cuerpo del artículo se refiere al derecho a la protección de datos, sin alusión alguna a la intimidad. Por su parte, el art. 20. bis ET reconoce que los «trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales», lo que parece situar el debate en el marco del derecho a la intimidad y no de la protección de datos.

El legislador, así pues, muestra ciertas dudas sobre cuál es el derecho principalmente concernido, aunque en último término parece decantarse por la protección de datos, como se desprende del apartado 1 de ese art. 90 LOPD, que faculta a los empleadores para «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». Ese art. 20.3 ET, por cierto, permite al empresario «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 y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad», sin aludir ni al derecho a la intimidad ni a la protección de datos personales.

No obstante, el art. 90.2 LOPD vuelve a incidir en el cumplimiento de los derechos y obligaciones básicos aparejados al derecho a la protección de datos, pues exige a los empleadores que, con carácter previo a la implantación de la medida, informen «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» de geolocalización, así como «acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión». Este es un contexto, por tanto, con similitudes con la videovigilancia (art. 89 LOPD), porque en ambos casos se procede a una captación y conservación de información en un fichero que, efectivamente, hace entrar en juego las garantías de la legislación de protección de datos[16].

A la vista de esta regulación, seguramente cabría afirmar que los eventuales límites a la implantación de dispositivos de geolocalización que permitan conocer la ubicación de los trabajadores deberán analizarse a partir del derecho a la protección de datos, pues el art. 90, a pesar de su rúbrica, no parece dejar mucho espacio al derecho a la intimidad. Sin embargo, y como se desarrollará posteriormente, el derecho a la protección de datos no ha sido concebido para actuar como freno a los poderes empresariales de control y vigilancia. Es un derecho con un bien jurídico protegido diferente y que se mueve en otro plano. Un análisis más sosegado seguramente permite concluir que la valoración sobre la licitud de la implantación de una medida de ese tipo debería efectuarse a partir del derecho a la intimidad, mientras el derecho a la protección de datos entraría en juego para garantizar que la información que ha obtenido el empleador no se utilice con fines distintos a los que motivaron su recogida.

5. REQUISITOS Y GARANTÍAS PARA LA IMPLEMENTACIÓN DE DISPOSITIVOS DE GEOLOCALIZACIÓN A PARTIR DEL NUEVO MARCO LEGAL

Es claro que ni los arts. 20 y 20 bis ET ni el art. 90 LOPD prohíben que el empleador ejerza su legítimo poder de control y vigilancia de la actividad del trabajador a través de dispositivos de geolocalización. Más bien al contrario, esos preceptos le facultan para utilizar esa tecnología. Ahora bien, todas las medidas de control, y esta no constituye ninguna excepción, han de someterse a límites para respetar los derechos del trabajador, principalmente la intimidad, la dignidad, el secreto de las comunicaciones y la protección de datos personales. En apariencia, así pues, la instalación y utilización de estos dispositivos sigue pautas muy similares a las de otros mecanismos de control, como la videovigilancia.

En este sentido, los puntos de conexión son múltiples, porque tanto geolocalización como videovigilancia exigen de medios técnicos, más o menos sofisticados, tienen una alta potencialidad invasiva y, además, son medidas polifacéticas, pues su finalidad no es siempre el control del trabajador, sino que pueden ser-

[16] *Vid.* M. Miñarro Yanini, *La "Carta de los derechos digitales" para los trabajadores del Grupo Socialista en el Congreso un análisis crítico ante su renovado interés,* RTSS (CEF), nº 424, 2018, pp. 91 y ss.; A. Fernández García, *Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial*, Revista Aranzadi Doctrinal, nº 17, 2010 (BIB 2009\1901).

vir bien como instrumento de protección o tutela de intereses o útiles empresariales, bien a modo de medidas de prevención o disuasión frente a daños o robos, bien como ayuda en la persecución de los eventuales infractores, que en modo alguno han de ser los trabajadores. Claro está, son también medidas que, aun sin haber sido implementadas con la finalidad de controlar al trabajador, pueden utilizarse eventualmente con ese fin, y ello suscita asimismo preguntas en relación con los derechos del trabajador, con la utilización desviada del poder de dirección empresarial y, en último término, con la buena fe. De ahí que no sorprenda que los tribunales hayan aplicado miméticamente a la geolocalización las reglas diseñadas por la jurisprudencia constitucional sobre videovigilancia[17].

En cualquier caso, no conviene olvidar que la geolocalización cuenta asimismo con peculiaridades que la alejan de otras medidas de control, pues los dispositivos de seguimiento permiten conocer la ubicación del trabajador en todo momento, incluso fuera de horas de trabajo, y con ello son susceptibles de proporcionar al empleador información superflua o impertinente a los fines del contrato de trabajo. No es, conviene recordarlo, un efecto exclusivo de la geolocalización, pues consecuencias similares se producen cuando el empleador recurre a la contratación de detectives privados para constatar si el trabajador cumple sus obligaciones.

La problemática con los dispositivos de geolocalización puede ser más rica, pues tales dispositivos son a menudo instalados en herramientas o bienes propiedad de la empresa, pero ya es habitual que el empleador pretenda utilizar para tal fin aparatos propiedad del trabajador, como un teléfono móvil. Y no es descartable que en un futuro cercano se prefieran tecnologías modernas y notablemente más invasivas, como por ejemplo chips subcutáneos[18], aunque las cautelas y garantías deben ser máximas en ese escenario y, estando en juego la integridad física, no parece haber resquicio alguno que permita un medio de control de esta índole sin consentimiento del trabajador, todo ello sin perjuicio de una justificación –examinada con elevado rigor– sobre la necesidad y proporcionalidad de esa medida, pues su carácter invasivo es muy superior a otros medios de control como la videovigilancia o incluso los controles biométricos.

En ese contexto, el art. 90.1 LOPD se limita a afirmar que el control a través de dispositivos de geolocalización debe tener lugar dentro del «marco legal» de las funciones o poderes de vigilancia y control del empleador y «con los límites inherentes al mismo», mientras que los arts. 20.3 y 20.bis ET exigen el respeto a la dignidad y a la intimidad del trabajador. Se trata, como cabe apreciar, de afirmaciones muy genéricas que requieren de ulterior precisión, porque ni siquiera se alude al principio de proporcionalidad. La doctrina judicial está llamada a convertirse en un apoyo imprescindible, principalmente la jurisprudencia constitucional, sin perder de vista la jurisprudencia del TS y, en su caso, la doctrina del TEDH.

En principio, y entrando en juego derechos fundamentales como la intimidad, debería extrapolarse a este ámbito, al menos como premisa de partida, la jurisprudencia elaborada para situaciones análogas. En este sentido, las medidas de control empresarial más conflictivas en los últimos tiempos, como la comprobación del ordenador utilizado por el trabajador, incluyendo el correo electrónico, la eventual apertura por el empresario de la correspondencia de los empleados recibida en

[17] *Vid.* SSTSJ de Andalucía/Sevilla de 19-7-2017 (recurso 2776/2016) y de Castilla-La Mancha de 31-3-2015 (recurso 19/2015).

[18] *Vid.* J.M. Quílez Moreno, *La garantía de Derechos Digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores,* REDT, nº 217, 2019 (BIB 2019\1558); F.J. Fernández Orrico, *Protección de la intimidad del trabajador frente a dispositivos digitales*, REDT, nº 222, 2019 (BIB 2019\7744); M. Arrúe Mendizábal, *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*, RGDTSS (iustel), nº 54, 2019.

las dependencias de la empresa[19] o incluso el uso del polígrafo para determinar la veracidad de las respuestas del trabajador[20], deben valorarse desde la perspectiva de la razonabilidad y adecuación del ejercicio de los poderes empresariales para garantizar que no invaden desproporcionadamente la intimidad, el secreto de las comunicaciones o la propia imagen del trabajador, en relación con la dignidad[21].

En esa línea, la implantación de dispositivos de geolocalización debe venir precedida de una valoración sobre la idoneidad, necesidad y proporcionalidad de la medida, en un juicio clásico de proporcionalidad, y seguramente en esa valoración pueda jugar un papel la negociación colectiva, instrumento especialmente apto para configurar reglas que proporcionen un equilibrio entre los intereses del trabajador y los del empresario[22]. Bajo esas premisas, es claro que no puede valorarse igual la implantación de medidas de geolocalización que tengan como propósito la seguridad de los bienes empresariales (*v.gr.,* vehículos de empresa), que la utilización de esos dispositivos con exclusiva finalidad de control del trabajador. En el contexto del control del trabajador, el lugar y el tiempo son aspectos muy relevantes, pues no puede merecer igual valoración, en primer lugar, que el empleador quiera conocer dónde se encuentran los trabajadores durante el tiempo y lugar de trabajo; en segundo lugar, que el empleador desee comprobar la ubicación de un trabajador durante la jornada laboral cuando la prestación de servicios no se desarrolla en un centro de trabajo al uso (*v.gr.,* operadores mercantiles, repartidores, etc.); y, en tercer lugar, que la información a disposición del empleador comprenda también actividades privadas desarrolladas fuera del tiempo y lugar de trabajo.

La práctica dará lugar a situaciones de muy distinta naturaleza, que obligarán a los tribunales a sopesar cuál es el objetivo del empleador, pues contará con menos restricciones una medida dirigida a mejorar la organización de la actividad y la productividad que una con propósito exclusivo de control. Es probable que en muchos casos ambas finalidades confluyan, pues, por ejemplo, la geolocalización de vehículos permite conocer la actividad del trabajador, pero también optimizar la organización empresarial mejorando rutas o proporcionando asistencia más rápida en caso de incidencias, como por ejemplo averías o accidentes[23]. Por supuesto, también será necesario valorar si es una medida que afecta a todos los trabajadores o sólo a un grupo, si el dispositivo puede ser desactivado por los propios trabajadores, si permite conocer la actividad extralaboral[24], si, en caso de geolocalización de un bien empresarial que utilice el trabajador, ese bien puede ser utilizado parcialmente con finalidad privada o si sólo procede un uso como herramienta de trabajo, si el trabajador debe aportar instrumentos propios o proporcionar datos adicionales para implementar la geolocalización[25] y si, en definitiva, no había medios menos invasivos para alcanzar la finalidad perseguida.

---

[19] *Vid.* Informe AEPD 0147/2009, http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/ambito_aplicacion/common/pdfs/2009-0147_Apertura-de-correspondencia-del-empleado-por-el-empresario.pdf.

[20] *Vid.* OIT, *Repertorio de recomendaciones prácticas de la OIT. Protección de los datos personales de los trabajadores*, OIT, 1997, pp. 7 y 38; http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf.

[21] *Vid.* D. Martínez Fons, "La doctrina del Tribunal Constitucional Sobre el uso y el control del correo electrónico en la relación de trabajo", en E. Borrajo Dacruz (Dir.), *Controversias vivas del nuevo Derecho del Trabajo,* La Ley, Madrid, 2015, p. 348; F. Ferrando García, *Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías*, RTSS (CEF), nº 399, 2006, pp. 37 y ss.

[22] *Vid.* A. Baylos Grau, *Los derechos digitales y la negociación colectiva,* Diario La Ley, nº 9331, Sección Tribuna, 7 de Enero de 2019.

[23] *Vid.* STSJ de Asturias de 27-12-2017 (recurso 2241/2017).

[24] *Vid.* STSJ de Madrid de 12-7-2019 (recurso 197/2019).

[25] *Vid.* SAN de 6-2-2019 (conflicto colectivo 318/2018). Un comentario a la misma en J. Martínez Moya, *El derecho a la protección de datos personales y sistema de geolocalización impuesto por la empresa a los trabajadores-repartidores*, Revista de Jurisprudencia Laboral, nº 1, 2019 (https://www.boe.es/publicaciones/anuarios_derecho/articulo.php?id=ANU-L-2019-00000000333).

A este respecto, conviene traer a colación la STEDH *Uzun vs. Alemania*[26], pues, aunque elaborada en el contexto del Derecho Penal, y por tanto en relación con la investigación de delitos, puede ofrecer pautas valiosas en el ámbito laboral, especialmente en relación con la imposición de sanciones. En dicha sentencia el Tribunal de Estrasburgo consideró admisible la información obtenida a partir de la vigilancia por GPS de un investigado por terrorismo porque previamente existía una sospecha, se utilizaron otros métodos para el seguimiento que no se demostraron completamente eficaces y la geolocalización se limitó en el tiempo (tres meses) y no afectó a todas las actividades del presunto infractor, sino únicamente a aquellas que se presumían más vinculadas con la actividad delictiva que se investigaba. El Tribunal, por consiguiente, no parece admitir la vigilancia cuando es «total y exhaustiva», por considerarla especialmente invasiva. Seguramente por ello, la existencia de una sospecha previa justifica más fácilmente una medida de vigilancia de esta índole que un control más rutinario y generalizado.

En verdad, tampoco es necesario recurrir a asuntos criminales, pues el test de proporcionalidad deriva inequívocamente de la doctrina sentada en la STEDH *Barbulescu II*[27], que puede ser aplicada sin dificultad a otras medidas distintas al control del ordenador, como ha reconocido la STEDH López Ribalda II en relación con la videovigilancia[28]. Por tanto, es menester valorar los siguientes aspectos: 1– Si el trabajador ha sido informado de la adopción de esas medidas de vigilancia. 2– Cuál ha sido el alcance de la vigilancia realizada por el empresario y el grado de intrusión en la vida privada del trabajador 3– Las razones alegadas por el empleador. 4– La existencia de medidas menos invasivas. 5– Las consecuencias para el trabajador. 6– Las garantías para minimizar el impacto sobre los derechos fundamentales[29].

Esta riqueza en la doctrina judicial contrasta con la parquedad del art. 90 LOPD que, al menos en su apartado 1, no ofrece mayor novedad que la referencia expresa a la geolocalización, resultando sorprendente que ni siquiera aluda al principio de proporcionalidad. También es curioso, por la norma en la que se ubica y el encabezamiento de ese mismo art. 90, que no ponga el acento en la protección del trabajador, sino más bien en la habilitación al empleador para utilizar estas tecnologías. Sea como fuere, ya se ha visto que el ordenamiento proporcionaba herramientas suficientes para tutelar adecuadamente al trabajador, por lo que si bien es cierto que el art. 90 LOPD no implica un salto cualitativo, tampoco supone un retroceso. Dicho de otro modo, la LOPD no ha introducido nuevos elementos al debate ni va a cambiar sustancialmente la perspectiva de aproximación de los tribunales cuando se enfrenten a conflictos de esta índole.

En efecto, la proporcionalidad como elemento clave para dilucidar la licitud del uso de estas tecnologías como instrumento de control del trabajador es una exigencia de la Constitución, así como de los compromisos internacionales suscritos con España, por elementales razones de respeto a los derechos fundamentales. En cualquier caso, es menester tener claros los distintos planos de análisis en atención al asunto que pretenda abordarse, y, en concreto, debe distinguirse nítidamente entre la implantación del dispositivo de geolocalización y la posterior utilización de los datos que proporciona. En efecto, el test de proporcionalidad que se exige para la instalación de estos dispositivos debe respetarse, por imperativo del derecho fundamental afectado, pero ello no justifica el uso de toda información obtenida a través de ese medio ni con cualquier finalidad,

[26] De 2-9-2010 (recurso 35623/2005).
[27] De 5-9-2017 (recurso 61496/08).
[28] De 17-10-2019 (recursos 1874/13 y 8567/13).
[29] *Vid.* STSJ de Canarias/Las Palmas de 26-1-2018 (recurso 1409/2017).

porque el test de proporcionalidad requiere conocer el objetivo que persigue la medida. Por tanto, si ese objetivo nunca fue el control del trabajador, la información obtenida no podrá utilizarse para probar un incumplimiento[30], pero no porque ello sea contrario al derecho a la protección de datos, sino porque es un ejercicio desviado del poder de dirección empresarial.

El análisis no estaría completo sin una referencia al apartado 2 del art. 90 LOPD, a cuyo tenor la implementación de este tipo de dispositivos como medidas de control del trabajador requiere que «con carácter previo», el empleador informe «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». Asimismo, también deberá «informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión».

Como se observa, el precepto exige una información «inequívoca», a diferencia del art. 89 en materia de videovigilancia, en el que tal información ha de ser «concisa». Quizá ese carácter inequívoco de la información se convierta en un punto de apoyo decisivo para delimitar el contenido de esa información, que según el precepto sólo debe alcanzar a la «existencia y características de estos dispositivos», y con ello no se requeriría explícitamente informar sobre la finalidad. Desde esta perspectiva, una interpretación literal no exigiría informar al trabajador de que la geolocalización puede ser utilizada con fines de control laboral, pero el carácter «inequívoco» de la información seguramente conduzca a otro resultado[31].

Es una problemática que incide de lleno en la valoración sobre la licitud o ilicitud del medio de control, y en la eventual utilización de la información obtenida como prueba de incumplimiento, pero que entronca con una cuestión más de fondo, de la configuración misma del poder de dirección empresarial y sus límites, cual es el impacto del derecho a la protección de datos sobre las facultades de control y vigilancia. En efecto, ese derecho a la información previa nace de la legislación de protección de datos y los tribunales lo extendieron en un primer momento a la videovigilancia, con el fin, sustancialmente, de proteger al trabajador que, sin su conocimiento, había sido captado por cámaras de vigilancia incumpliendo sus obligaciones laborales. El legislador no sólo ha recogido esa exigencia para la videovigilancia, sino también para otras medidas de control, en particular la geolocalización, aunque en este campo no se dulcifica la exigencia de información previa ante la captación de actos delictivos. Recuérdese que el art. 89.1 LOPD concluye afirmando que «en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica». Ese es un distintivo que no está presente en caso de geolocalización, lo que conduce a preguntarse si puede utilizarse en juicio la información obtenida por geolocalización cuando «se haya captado la comisión flagrante de un acto ilícito» pero los trabajadores no hubieran sido informados previamente de la implantación de un dispositivo de geolocalización. Esa diferencia quizás conduzca a interpretaciones más estrictas en la geolocalización que en la videovigilancia.

No se trata, en cualquier caso, de problemas totalmente novedosos, pues esa obligación de información ya se había deducido de la legislación de protección de datos y los tribunales venían comprobando su cumplimiento con anterioridad a la LOPD/2018, utilizando

[30] *Vid.* STSJ de Andalucía/Granada de 19-10-2017 (recurso 1149/2017).

[31] *Vid.* R. Serrano Olivares, *Los derechos digitales en el ámbito laboral, IUSLabor*, nº 3, 2018 (https://www.raco.cat/index.php/IUSLabor/article/view/10.31009-IUSLabor.2018.i03.06); C. Molina Navarrete, ¿Saber es poder?: conectividad empresarial, geolocalización (GPS) y autodeterminación digital del trabajador, RTSS (CEF), nº 419, 2018.

a menudo como parámetro interpretativo los criterios elaborados por la AEPD[32], aunque muchas veces no se exigía una información exhaustiva en el sentido de la legislación de protección de datos, sino solamente que el trabajador conociera la existencia del dispositivo[33]. Cierto es que un sector de la doctrina judicial declaraba nula la prueba de incumplimiento laboral proporcionada por un dispositivo de geolocalización ante la ausencia de información previa a los trabajadores[34], aunque se requería la expresa impugnación de la validez de la prueba[35]. No obstante, la exigencia de información previa y las consecuencias de su omisión merecen una valoración más sosegada, que tendrá lugar en los siguientes epígrafes.

Finalmente, no es claro el papel de los representantes de los trabajadores, que el art. 90.2 LOPD menciona al atribuirles un deber de información sobre la existencia y características de los sistemas de geolocalización, pero solamente «en su caso», lo que plantea serias dudas sobre el contenido y alcance de ese derecho-deber y, en particular, sobre su carácter obligatorio o, simplemente, subsidiario[36]. El art. 64 ET podría convertirse en un marco de referencia a estos efectos, máxime cuando el apartado 7 atribuye a la representación de los trabajadores funciones «de vigilancia en el cumplimiento de las normas vigentes en materia laboral», si bien el art. 90.2 LOPD es una norma más específica. Desde luego, parece deseable, o al menos conveniente, que la representación de los trabajadores sea informada de la implantación de medidas de control con potencialidad invasiva elevada, pero en todo caso dicha información no es un requisito de licitud o validez de la medida, o cuando menos esa conclusión no puede deducirse fácilmente de la redacción del precepto legal, que sitúa a la representación de los trabajadores en un segundo plano, a buen seguro porque desde la perspectiva del derecho a la protección de datos el «interesado» es el trabajador, y no los representantes, que, salvo excepciones vinculadas al cumplimiento de obligaciones legales, no tienen legitimación para conocer datos personales del trabajador sin consentimiento de este. En el ámbito de la protección de datos las garantías no provienen de los representantes de los trabajadores, sino de otras instancias como la AEPD o los tribunales. Por consiguiente, las consecuencias del incumplimiento de esa obligación, si es que existe como tal, repercutirían en el estricto ámbito de la relación entre el empleador y los representantes de los trabajadores, pero en ningún caso afectarían a la validez de la medida, porque se trata más bien de una vulneración del derecho a la libertad sindical, y no del derecho a la protección de datos.

6. GEOLOCALIZACIÓN Y PODER DISCIPLINARIO: LA DOCTRINA JUDICIAL SOBRE LA VALIDEZ DE LA PRUEBA Y SOBRE LA LICITUD DE LA DECISIÓN EMPRESARIAL

El poder disciplinario del empleador puede ejercerse frente a incumplimientos laborales de los trabajadores, incumplimientos que en el contexto de la geolocalización pueden manifestarse o actuar en dos planos diferentes. En primer lugar, esa tecnología puede haber sido utilizada para obtener la información que sirva de prueba de la infracción que ha cometido el trabajador. Y en segundo lugar, la infracción puede afectar directamente al dispositivo o herramienta de geolocalización, pues su des-

[32] *Vid.* STSJ de Asturias de 27-12-2017 (recurso 2241/2017).

[33] *Vid.* STSJ de la Comunidad Valenciana de 2-5-2017 (recurso 3689/2016).

[34] *Vid.* SSTSJ de Madrid de 21-3-2014 (recurso 1952/2013) y de 29-9-2014 (recurso 1993/2013) y de Castilla-La Mancha de 28-4-2015 (recurso 134/2015).

[35] *Vid.* SSTSJ de Asturias de 3-10-2017 (recurso 1908/2017) y de Castilla y León/Valladolid de 8-5-2013 (recurso 453/2013).

[36] *Vid.* C. Molina Navarrete, *Poder de geolocalización, intimidad y autodeterminación digital en las relaciones de trabajo: ¿un nuevo orden eficaz de garantías y límites?*, Diario La Ley, nº 9319, sección Tribuna, 17 de Diciembre de 2018; J.P. Landa Zapirain, *La repercusión del régimen de protección de datos personales en el ejercicio de los derechos informativos de los representantes legales y sindicales de los funcionarios públicos*, RGDTSS (iustel), nº 54, 2019.

activación, inutilización o destrucción constituye un incumplimiento de las obligaciones laborales con entidad propia, diferente al que, en su caso, se hubiera tratado de encubrir con ese acto[37].

Este segundo plano resulta menos problemático desde la perspectiva de los poderes empresariales, y verdaderamente no suscita dificultades específicas en materia de geolocalización, sino que merece el mismo tratamiento que cualquier otro comportamiento del trabajador que implique desactivar instrumentos de control y/o dañar bienes propiedad de la empresa. Habrá que estar, obviamente, al catálogo de infracciones y sanciones para determinar la gravedad de los hechos, pero elementales exigencias de proporcionalidad obligan a diferenciar en atención a las circunstancias del caso, pues no podrá ser valorada de igual forma la desactivación de la geolocalización cuando el empresario controla la ubicación del trabajador a través de una aplicación instalada en el propio móvil del empleado que la destrucción de un dispositivo de localización instalado en un vehículo de la empresa que utiliza el trabajador. Entre esas dos conductas existen diferencias sustanciales que justificarían una sanción distinta, obviamente, como también pueden apreciarse esas diferencias en atención al momento de desactivación, pues no habría de merecer igual reproche esa conducta fuera de horas de trabajo que durante la jornada laboral, aunque las circunstancias concretas obligan a una valoración casuística.

Sea como fuere, la mera desactivación del dispositivo de geolocalización constituye una infracción, salvo que previamente la empresa hubiera sido sancionada por su instalación vulnerando derechos fundamentales. Si ello no es así, el trabajador no está legitimado para desactivar el dispositivo, y mucho menos para dañarlo o destruirlo. No lo está en ningún caso cuando la finalidad de ese dispositivo no es la de control laboral, o no es esa exclusivamente, porque en tal caso se podría estar poniendo en peligro a personas o bienes de la empresa, o perjudicando la eficiencia empresarial. Y tampoco lo está cuando el dispositivo se utilice como medida de control en tanto no se dicte sentencia o resolución de un órgano competente deslegitimando la decisión empresarial. Es probable que los tribunales no aceptasen una sanción al trabajador en tales casos si finalmente se prueba la extralimitación del empleador, de modo que se considere vulnerado el derecho a la intimidad o a la protección de datos, pero el riesgo que asumiría el trabajador es considerablemente elevado, porque la orden empresarial no siempre podrá ser calificada como manifiestamente irregular o injusta, y por tanto no ampararía la rebeldía (*v.gr.,* actuación conforme a una doctrina judicial previa modificada por la sentencia condenatoria). Todo ello sin perjuicio, por supuesto, de que también debe valorarse la vía por la que el empleador ha conocido que el trabajador ha desactivado, inutilizado o dañado el dispositivo[38]. En cualquier caso, la desactivación del sistema de geolocalización no es prueba, en absoluto, de que efectivamente el trabajador incumpliera otras obligaciones.

No obstante, desde la perspectiva de los «derechos digitales» las eventuales sanciones vendrán motivadas por incumplimientos diversos de las obligaciones laborales donde la geolocalización actuará como medio de prueba. La ubicación del trabajador permite al empleador conocer con precisión dónde se encuentra el trabajador en cada momento y, gracias ello, comprobar si durante el tiempo de trabajo está en el lugar pertinente para desarrollar la actividad. Ahora bien, ya se advirtió que la geolocalización, como cualesquiera otros medios de control, únicamente puede actuar como medio de prueba si respeta el «marco legal» y «los límites inherentes» al poder de dirección empresarial (art. 90.1 LOPD).

[37] *Vid.* C. Sánchez-Rodas Navarro, *Poderes directivos y nuevas tecnologías,* TL, nº 138, 2017, pp. 163 y ss.

[38] *Vid.* SSTSJ de Andalucía/Granada de 18-9-2017 (recurso 770/2017) y de 25-1-2012 (recurso 2924/2011).

La doctrina judicial se ha pronunciado sobre la validez de la prueba de geolocalización en muchas ocasiones, pero sin consolidar un criterio claro. El análisis casuístico resulta inevitable, como también la remisión a la doctrina sobre videovigilancia, mucho más aquilatada, ya que, a diferencia de la geolocalización, cuenta con criterios elaborados por el TEDH, el TC y el TS. Como premisa de partida, conviene advertir que la monitorización del trabajador a través de esta clase de dispositivos no está prohibida, y por tanto no cabe rechazar de plano una eventual prueba. Sin embargo, este es un medio con potencialidad invasiva elevada, por lo que no se justifica su utilización porque resulte más cómodo, o porque simplemente sea eficaz, debido a que un seguimiento constante del trabajador es desproporcionadamente intrusivo[39]. En general, y siempre en aplicación del test de proporcionalidad, los tribunales vienen admitiendo el uso de esa tecnología cuando la actividad se realiza fuera de las dependencias empresariales, sin horario ni jornada, y por tanto el empleador carece de medios menos invasivos[40]. Por supuesto, y como también ha sucedido en relación con el control de ordenador o la videovigilancia, las sospechas previas de incumplimiento pueden convertirse en un elemento clave para justificar el uso de la geolocalización[41], pero siempre salvaguardando los derechos de los trabajadores.

No obstante, las dificultades surgen en estas situaciones porque la finalidad del dispositivo no siempre es la de control laboral, sino que a menudo el propósito principal consiste en proteger los bienes de la empresa (*v.gr.,* vehículos), por lo que no es el trabajador el que porta el dispositivo, sino ese bien o herramienta, pero a través de la geolocalización puede comprobarse indirectamente la actividad del trabajador. Lógicamente, si se considera que en tal caso tiene lugar una vulneración del derecho a la intimidad esa información no podría servir como válida prueba de incumplimientos laborales.

Los tribunales se muestran divididos, aunque tradicionalmente venían admitiendo la validez de la prueba obtenida mediante geolocalización, por el interés legítimo en comprobar dónde están los vehículos, y considerar indisociable el conocimiento de la ubicación del trabajador cuando este debe encontrarse en el vehículo en cumplimiento de sus obligaciones laborales. En tal escenario, si el vehículo no se halla donde debería, tampoco el trabajador, y si esas comprobaciones se circunscriben al tiempo y lugar de trabajo no se acierta a ver una actuación desproporcionadamente invasiva del empresario, que cuenta con escasos medios de control en algunas actividades[42].

Lógicamente, esa es una conclusión que exige modulación en determinadas circunstancias, porque no cabe admitir sin más una sanción cuando el trabajador está autorizado a realizar un uso privado del bien, o cuando no se ha especificado concretamente qué obligaciones han de cumplir los trabajadores fuera del tiempo y el lugar de trabajo, pues si las obligaciones carecen del suficiente grado de precisión el propio objetivo del control es difuso y no se justificaría el ejercicio del poder disciplinario. Ahora bien, en un contexto como el antes descrito, donde el dispositivo de geolocalización no proporciona información sobre actividades privadas del trabajador, sino que permite constatar el cumplimiento estricto de las obligaciones laborales, por ejemplo registrando cuándo el vehículo para, se pone en movimiento y dónde se encuentra, la prueba debe considerarse válida como regla general, pues esas facultades de control son inherentes al poder de dirección empresarial. Cierto es que la geolocalización se valora como una prueba más, no necesariamente cualificada, y que debe tenerse en cuenta que su fiabilidad técnica en ocasiones resulta dudosa[43].

[39] *Vid.* STSJ del País Vasco de 10-5-2011 (recurso 644/2011).

[40] *Vid.* STSJ de Galicia de 14-2-2013 (recurso 5195/2012).

[41] *Vid.* STSJ de Cataluña de 5-3-2012 (recurso 5194/2011).

[42] *Vid.* STSJ de Galicia de 6-6-2014 (recurso 903/2014).

[43] *Vid.* STSJ de Cantabria de 22-1-2016 (recurso 991/2015).

Sea como fuere, el análisis casuístico conduce a rechazar las interpretaciones que limitan el control, y por consiguiente las sanciones, a la actividad del trabajador durante el tiempo de trabajo[44]. Dicho de otro modo, en función de las circunstancias el empleador está facultado para comprobar los datos de geolocalización aun cuando se correspondan a un momento en el que el trabajador formalmente no está prestando servicios. Por supuesto, esas facultades son muy limitadas cuando el dispositivo de geolocalización tiene como finalidad exclusiva el control del trabajador, pues difícilmente el empleador podrá proporcionar una razón que justifique esa vigilancia en momentos que teóricamente son privados. Únicamente en situaciones donde se trate de verificar una sospecha previa de incumplimiento y ese sea el único medio, o el menos invasivo, cabría teóricamente validar esa actuación, pero se trataría de supuestos claramente excepcionales.

Ahora bien, cuando la finalidad del dispositivo de geolocalización no es exclusivamente el control del trabajador, sino también la seguridad y protección de bienes empresariales, como por ejemplo un vehículo, el empleador cuenta con mayores facultades para comprobar si ese bien se encuentra donde debería fuera de horas de trabajo, máxime cuando no se admita un uso privado del mismo. Obviamente, habrá que introducir las pertinentes cautelas para evitar que el empleador aproveche el contexto para efectuar una indebida vigilancia al trabajador, por lo que no será posible una monitorización continua, pero sí desde luego comprobaciones periódicas y puntuales, acotadas en el tiempo, que permitan constatar el buen uso de las herramientas empresariales, especialmente aquellas de valor económico significativo. En suma, se trata, como se dijo, de respetar los límites consustanciales a los medios de control y vigilancia, que son similares a los que los tribunales vienen imponiendo respecto del control del ordenador, la videovigilancia o el seguimiento a través de detectives[45].

Por supuesto, en caso de extralimitación la prueba es nula, lo que conduce a cuestionarse cuál debe ser la calificación de la sanción, y principalmente del despido, esto es, si resulta de aplicación la doctrina del árbol envenenado (o de la fruta podrida), de modo que ante una decisión empresarial basada exclusivamente en una prueba obtenida en vulneración de un derecho fundamental se extrae como consecuencia la nulidad de la decisión[46].

Los tribunales laborales se muestran divididos, y parecen partidarios de la teoría del árbol envenenado, decantándose a menudo por la nulidad[47], con apoyo en la STC 196/2004, de 15 de noviembre, siempre que no existan otros medios de prueba obtenidos lícitamente[48]. Cierto es que en tiempos recientes se encuentran sentencias de suplicación que entienden que la vulneración de un derecho fundamental en la obtención de la prueba sólo conlleva «la supresión de los hechos probados redactados valorando la misma y que no sean tenidos en consideración a los efectos de resolver jurídicamente la pretensión de declaración de nulidad o improcedencia del despido planteada»[49], doctrina que también se ha aplicado al control mediante geolocalización[50]. La LOPD no apuesta decididamente por ninguna de las opciones, aunque parece descartar la teoría del árbol envenenado en supuestos de video-

[44] *Vid.* M.A. Purcalla Bonilla, *Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados*, REDT, nº 218, 2019 (BIB 2019\2891).

[45] *Vid.* I.A. Rodríguez Cardo, *Pruebas obtenidas a través de detectives privados y derecho a la intimidad del trabajador*, AL, nº 12, 2014, pp. 1397-1410.

[46] *Vid.* M.A. Falguera Baró, *Nuevas tecnologías y trabajo (III): perspectiva procesal*, Trabajo y derecho nº 22, 2016.

[47] *Vid.* SSTSJ del País Vasco de 12-9-2006 (recurso 1270/2006) y de Galicia de 3-3-2008 (recurso 6219/2007).

[48] *Vid.* SSTSJ de Canarias/Las Palmas de 30-4-2002 (recurso 1220/2001) y 26-2-2016 (recurso 1296/2015) y del País Vasco de 10-5-2011 (recurso 644/2011).

[49] Cfr. STSJ de Galicia de 26-6-2015 (recurso 406/2015). También, SSTSJ de Cataluña de 14-10-2013 (recurso 3413/2013) y de Galicia de 30-12-2015 (recurso 3596/2014).

[50] *Vid.* STSJ de Castilla-La Mancha de 10-6-2014 (recurso 1162/2013).

vigilancia cuando se constate la comisión flagrante de un acto ilícito.

En cualquier caso, no conviene olvidar que el empleador tiene derecho a efectuar indagaciones o comprobaciones vinculadas al rendimiento y a la ejecución del trabajo. La nulidad de la decisión empresarial supone una extensión quizá desmesurada de la protección del trabajador, que realmente puede haber cometido los hechos que se le imputan. La nulidad de la prueba no debería presuponer necesariamente la nulidad de la decisión, pues si bien es razonable que en ausencia de otras pruebas el despido –o la sanción– no sea procedente, consecuencia coherente con el principio *pro operario*, la calificación de nulidad debería asentarse en la motivación empresarial para tomar la decisión, y no en el modo de obtener la prueba. Si la motivación empresarial no vulnera un derecho fundamental la nulidad resulta excesiva, porque, en último término, el art. 11.1 LOPJ y el 90.2 LRJS únicamente indican que «no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales». La nulidad de la prueba, y por tanto la ausencia misma de prueba, conducen a la calificación del despido como improcedente, no pudiendo extrapolarse sin más al ámbito laboral la doctrina sentada en el orden penal, donde rige el principio de presunción de inocencia[51]. Es más, incluso en la jurisdicción penal la nulidad de una prueba por vulneración de derechos fundamentales no conduce necesariamente a la absolución del imputado cuando los hechos se acreditan por otros medios probatorios lícitos[52].

El derecho a la protección de datos no es un punto de apoyo sólido para alcanzar una conclusión diferente, pues la normativa que lo regula no contempla como consecuencia propia o automática la nulidad de los actos que vulneran ese derecho, a diferencia de otros derechos fundamentales, sino que los remedios se mueven principalmente en el terreno de las responsabilidades económicas. En los supuestos más graves los incumplimientos pueden dar lugar a sanciones penales, que el CP ubica en los delitos «contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio». En concreto, el art. 197 del CP, dentro del Capítulo referido al «descubrimiento y revelación de secretos», prevé una pena de prisión de tres a cinco años para quienes realicen conductas de esa índole en condición de «personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros», o bien a través de la «utilización no autorizada de datos personales de la víctima»[53].

Sin embargo, en la generalidad de los casos las normas que regulan el derecho a la protección de datos apuestan por otro tipo de responsabilidades. En efecto, el responsable del tratamiento, y el encargado respecto de las obligaciones que le correspondan específicamente o cuando no haya respetado las instrucciones del responsable, incurrirá en responsabilidad civil (solidaria si hubiera varios infractores), y deberá por tanto hacer frente a la indemnización por los daños y perjuicios causados por el tratamiento ilícito, o por la vulneración de las facultades y garantías que derivan de ese derecho aun cuando el tratamiento sea lícito.

Además, el RGPD contempla específicamente sanciones administrativas, que deben resultar «efectivas, proporcionadas y disuasorias» (art. 83.1 RGPD). La multa para las infracciones administrativas podría alcanzar los veinte millones de euros, o incluso superar esa cantidad, pues la sanción puede ascender, en

[51] *Vid.* A.V. Sempere Navarro y C. San Martín Mazzucconi, *Nuevas tecnologías y relaciones laborales*, Aranzadi, Pamplona, 2002, p. 57; J. Gil Plana, *El uso particular por los trabajadores de las nuevas tecnologías empresariales en los códigos de conducta*, REDT, nº 155, 2012 (BIB 2012\2800); I. Baviera Puig, *Sobre la calificación del despido basado en pruebas ilícitas,* Aranzadi Social, nº 12, 2008 (BIB 2008\2159); J.F. Lousada Arochena, *La prueba ilícita en el proceso laboral*, Aranzadi Social, nº 11, 2006 (BIB 2006\1250).

[52] *Vid.* STS (Penal) de 23-10-2018 (recurso 1674/2017).

[53] *Vid.* STS (Penal) de 17-6-2014 (recurso 136/2014).

caso de empresas, a «una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior» (art. 83.5 RGPD). No obstante, se admite que determinadas autoridades y organismos públicos podrían no ser objeto de multa administrativa, pero que sí cabe la adopción de otra serie de medidas correctoras (art. 83.7), que la LOPD concreta en apercibimientos e incluso proposición de medidas disciplinarias para los responsables (art. 77 LOPD), a cargo de la autoridad de control (AEPD o agencia autonómica en Cataluña y País Vasco).

Esta opción legislativa, que contempla la reparación económica pero no la nulidad de posibles decisiones, parece razonable, pues el bien jurídico protegido por el derecho a la protección de datos no es la intimidad, la libertad religiosa, la libertad ideológica o cualquier otro derecho sustantivo, sino la capacidad de decisión de la propia persona sobre la información personal que desea difundir. Desde esta perspectiva, la vulneración del derecho a la protección de datos podría no repercutir directamente en ninguno de esos derechos, ni provocar mayor perjuicio al interesado que la concreta difusión de esa información personal, no necesariamente íntima.

La eventual calificación como nulo de un despido por el indebido tratamiento de datos personales carece de encaje legal o constitucional, porque esa declaración de nulidad será consecuencia, realmente, de que la decisión conduzca a una diferencia de trato prohibida y, a la postre, a una discriminación, o bien a una intromisión ilegítima en los derechos a la intimidad, honor, propia imagen o cualquier otro de carácter o contenido ideológico y, por tanto, con una faceta o vertiente sustantiva. Por supuesto, la vulneración del derecho a la protección de datos dará derecho a indemnización para el afectado, y a una eventual sanción administrativa para el infractor, pero no debería provocar otras consecuencias sobre la dinámica de la relación laboral. En verdad, resulta paradójico que la ausencia de información previa adecuada pueda derivar en una consecuencia tan aparentemente gruesa como la nulidad de la medida adoptada por vulneración de un derecho fundamental, cuando el remedio legalmente previsto y en el que desembocan muchos procedimientos es una sanción administrativa, a menudo por infracción meramente leve[54].

En este sentido, conviene recordar que la STEDH López Ribalda II[55] distingue explícitamente entre los distintos remedios o consecuencias que el ordenamiento puede contemplar frente a una vulneración de la privacidad, y considera que no es incompatible calificar como proporcional una medida de control (en ese caso la videovigilancia) y al mismo tiempo iniciar los procedimientos civiles o administrativos de reparación o sanción frente a la empresa por el incumplimiento del deber de información previa en materia de protección de datos, lo que demuestra, en esencia, que la nulidad de la medida por vulneración de un derecho fundamental y las responsabilidades económicas son garantías que actúan en planos distintos, y que la ausencia de información no ha de conducir *per se* a una declaración de nulidad por vulneración de un derecho fundamental.

7. EL IMPACTO DEL DERECHO A LA PROTECCIÓN DE DATOS SOBRE LA GEOLOCALIZACIÓN COMO MEDIDA DE CONTROL DE LOS TRABAJADORES

En el contexto actual no cabe duda que la geolocalización supone un tratamiento de datos personales, en la medida en que se considera dato personal «toda información sobre una persona física identificada o identifica-

[54] *V.gr.,* Resolución R/00956/2013 de la AEPD, en relación con la instalación de dispositivos GPS en los vehículos de la policía municipal sin respetar la obligación de información previa; http://www.agpd.es/portalwebAGPD/resoluciones/admon_publicas/ap_2013/common/pdfs/AAPP-00040-2012_Resolucion-de-fecha-06-06-2013_Art-ii-culo-5.1-LOPD.pdf.

[55] De 17-10-2019 (recursos 1874/13 y 8567/13).

ble», y es una «persona física identificable» todo aquel sujeto «cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona» (art. 4 RGPD).

El art. 90.1 LOPD faculta al empleador para «tratar los datos obtenidos a través de sistemas de geolocalización», estableciendo una clara conexión entre la geolocalización y la protección de datos y abriendo con ello una vía para que el ejercicio de las facultades empresariales de control y vigilancia de los trabajadores se vea constreñido por ese derecho a la protección de datos. En este sentido, el art. 90 LOPD consagra el derecho de información previa, que deriva de la protección de datos, y que exige que el trabajador conozca, por un lado, «la existencia y características de estos dispositivos» y, por otro, las condiciones «del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión».

Como premisa de partida, conviene tener presente que el ejercicio de las facultades empresariales de control y vigilancia no exige el consentimiento del trabajador. Es cierto que el derecho a la protección de datos es, en cierta forma, un derecho de autodeterminación informativa, que otorga a su titular amplios poderes de disposición, como pusieron de manifiesto las SSTC 290 y 292/2000, de 30 de noviembre[56]. Sin embargo, no es razonable que la implementación de medidas de control y vigilancia se supedite al consentimiento previo del trabajador, o al menos esta exigencia no puede derivarse del derecho a la protección de datos, porque el consentimiento no es la única base legal para el tratamiento. En este sentido, el art. 6.1 RGPD admite el tratamiento de datos personales sin el consentimiento del interesado en otras circunstancias, y en particular cuando sea necesario «para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales», «para el cumplimiento de una obligación legal aplicable al responsable del tratamiento», o «para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento», entre otras circunstancias. En la misma línea, el art. 6.3 de la LOPD considera innecesario el consentimiento cuando el tratamiento sea necesario para «el mantenimiento, desarrollo o control de la relación contractual»[57].

El empleador, por consiguiente, no requiere el consentimiento de los trabajadores para implementar controles basados en la geolocalización, pero el derecho a la protección de datos exige que se proporcione información «de forma expresa, clara e inequívoca acerca de la existencia y características de estos dispositivos». Desde luego, el precepto podría haber sido más explícito, pues insta al empleador a que proporcione información, pero no necesariamente a que comunique al trabajador la finalidad de la geolocalización. Literalmente, el art. 90.2 LOPD limita el contenido de la información a la «existencia» y a las «características» del dispositivo, y en esta última expresión

[56] *Vid.* L.A. Fernández Villazón, "La Ley de Protección de datos de carácter personal y su impacto en el ámbito laboral: Sentencia 292/2000, de 30 de noviembre", en J. García Murcia (Dir.), *El control de constitucionalidad de las normas laborales y de seguridad social*, Aranzadi, Pamplona, 2015, pp. 495 y ss.; M. Recio Gayo, *El consentimiento en el RGPD: comentarios al borrador de Directrices del Grupo de trabajo del artículo 29*, Diario La Ley, nº 13, 10 de enero de 2018.

[57] *Vid.* J.M. Goerlich Peset, "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas", en AA.VV., *El derecho a la privacidad en un nuevo entorno tecnológico*, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pp. 130-131; J.L. Goñi Sein, Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016, RDS, nº 78, 2017, pp. 33 y ss;); S. Rodríguez Escanciano, El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679, RTSS (CEF), nº 423, 2018, pp. 35 y ss.; M.B. Cardona Rubert, Informática y contrato de trabajo, Tirant lo Blanch, Valencia, 1999, pp. 20 y ss.

no ha de incluirse necesariamente una referencia a la finalidad, sino que formalmente el empleador podría cumplir con la exigencia proporcionando las especificaciones técnicas del aparato (*v.gr.,* modo de funcionamiento, alcance, grado de precisión, etc.).

Sin embargo, todo tratamiento de datos debe respetar los «principios relativos al tratamiento» (art. 5 RGPD), y entre ellos los principios de minimización y limitación de la finalidad. En su virtud, los datos deben ser «recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines» (limitación de la finalidad) y habrán de ser «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos)». Por consiguiente, si la finalidad de la geolocalización fuera la de registro horario los datos no podrían ser utilizados para verificar la ubicación del trabajador en cada momento, sino las horas de inicio y fin de la actividad, que es lo que permite la base legal del registro horario (art. 34.9 ET).

Además, la información que debe proporcionarse al interesado (arts. 13 y 14 RGPD) debe incluir «los fines del tratamiento a que se destinan los datos personales», de modo que la legislación de protección de datos exige informar al trabajador de que el dispositivo de geolocalización será utilizado con finalidad de control laboral, sin que se contemplen excepciones, por ejemplo la existencia de sospechas previas de incumplimiento, ni matices cuando se haya captado la comisión de un acto ilícito, como sucede en caso de videovigilancia (art. 89.1 LOPD).

En este contexto, no resulta cuestionable que la geolocalización supone un tratamiento de datos que exige el respeto a las reglas y límites que impone ese derecho fundamental, aunque debe tenerse presente que «un dato o conjunto de datos no sometidos a tratamiento o no susceptibles del mismo, o que no estén destinados a ser incluidos en un fichero, quedan fuera del ámbito de aplicación, y por tanto de protección, de la legislación de protección de datos»[58]. De ahí la trascendencia del concepto de «tratamiento», que el RGPD define como «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción» (art. 4.2 RGPD).

Desde esa perspectiva, no tendría lugar un tratamiento de datos en sentido estricto, al no generarse fichero, ni información susceptible de conservación o difusión, en caso de utilización de tecnologías para la vigilancia en tiempo real, sin grabación de esos datos para usos ulteriores. El derecho a la protección de datos no puede actuar, pues no se ha generado un fichero, ni los datos son susceptibles de acceso, rectificación o cancelación. Es cierto que la AEPD considera que se produce un tratamiento de datos en caso de cámaras que reproduzcan imágenes en tiempo real[59] –sólo excluye la aplicación de la legislación de protección de datos ante cámaras falsas o simuladas[60], que podrían vulnerar el derecho a la intimidad porque la incertidumbre sobre el hecho mismo de estar siendo grabado puede perturbar el normal desenvolvimiento de la vida personal y familiar[61]–, pero esa es una interpretación desmesurada, pues carece de lógica extender la legislación de protección de datos personales a actividades como la reproducción de imágenes o geolocalización en

[58] Cfr. J.L. PIÑAR MAÑAS, "Comentario al art. 3", en A. TRONCOSO REIGADA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010, p. 187.

[59] En este sentido, *vid.* SAN (Cont-Adm) de 27-5-2010 (recurso 621/2009).

[60] *Vid.* AEPD, *Guía sobre el uso de videocámaras para seguridad y otras finalidades*, p. 49 (https://www.aepd.es/media/guias/guia-videovigilancia.pdf).

[61] *Vid.* STS (Civil) de 7-11-2019 (recurso 5187/2017).

tiempo real[62]. El derecho a la protección de datos, entendido como haz de facultades de autodeterminación informativa, no puede ser aplicable en ese contexto, donde no cabe rectificación, supresión o acceso, puesto que los datos no se almacenan, ni se pueden cruzar con otros ni son susceptibles de tratamiento en sentido estricto. Desde luego, ese derecho no nació para limitar el seguimiento en tiempo real, y probablemente tenga poco sentido extenderlo hasta esos confines. Si se entiende que la geolocalización debe restringirse por resultar especialmente invasiva, parece más pertinente que sean otros los derechos que deban actuar como contrapeso a las facultades empresariales.

Sea como fuere, la cuestión nuclear, desde la perspectiva del poder de dirección, consiste en dilucidar si el derecho a la protección de datos, y más concretamente la obligación de información previa, condiciona la utilización de dispositivos de geolocalización con propósito de controlar al trabajador y/o impide utilizar como prueba la información obtenida a través de ellos. La extrapolación de la jurisprudencia sobre videovigilancia, y más tras la STEDH López Ribalda I[63], parecía conducir a una respuesta afirmativa antes incluso de la LOPD. Una vez en vigor esta norma, el art. 90.2 LOPD, aun cuando pudieran ponerse reparos a su tenor literal, aboca a la misma conclusión, pues si no se ha informado sobre la «existencia y características de estos dispositivos» en apariencia el empleador no está legitimado para utilizarlos. Esa es una consecuencia excesiva y que concede al derecho a la protección de datos una relevancia que no habría de tener en el contexto del ejercicio de poderes empresariales, como se desarrollará a continuación.

En fin, estas reglas parecen sustancialmente aplicables al ámbito público, pues el art. 14.j.bis) del EBEP, introducido por la LOPD, reconoce a los empleados públicos el derecho «a la intimidad en el uso de 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». Es cierto que en el orden contencioso administrativo el interés público ha contado con gran peso en la valoración de la licitud de las medidas de control, aunque también lo es que en los últimos años la doctrina de la expectativa de privacidad ya se integra plenamente como criterio interpretativo en la jurisdicción contenciosa, toda vez que la doctrina del TEDH no distingue entre el ámbito público y el privado, y que si bien es cierto que el interés público debe tomarse en consideración en el análisis de la proporcionalidad, en modo alguno puede conducir a la completa anulación de los derechos fundamentales individuales[64].

8. DESMONTANDO UN MITO: LA INEXISTENCIA DE UNA OBLIGACIÓN DE INFORMACIÓN PREVIA SOBRE LA IMPLANTACIÓN DE MEDIDAS DE CONTROL EMPRESARIAL HASTA LA LOPD DE 2018

Las dificultades de integración de la legislación de protección datos en el ámbito de la relación laboral vienen dadas por la falta de adecuación de esa normativa a este específico contexto, y quizá también por una extensión precipitada, o poco aquilatada, de las pertinentes garantías. Así sucede con la obligación

[62] Un sector doctrinal distingue entre «información» y «fuente de información» para concluir que la mera grabación de imágenes no puede considerarse como dato personal, sino como mera fuente de información, puesto que no ha sido «extractada» ni sometida a un «proceso» o tratamiento, como podrían ser el reconocimiento de rostros o la lectura automática (*v.gr.*, matrículas de vehículos); *vid.* J. APARICIO SALOM, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal,* Aranzadi, Pamplona, Tercera Edición, 2009, pp. 59-60.

[63] De 9-1-2018 (recursos 1874/13 y 8567/13).

[64] *Vid.* A. BOTO ÁLVAREZ, *Control a través de las TIC en el sector público y expectativa razonable de privacidad: la visión del contencioso-administrativo*, RGDTSS (iustel), nº 54, 2019.

de proporcionar información previa a la adopción de medidas de control empresarial cuya potencialidad invasiva genera graves riesgos para la privacidad del trabajador. Es un remedio ante la peculiaridad del ámbito laboral, donde el tratamiento de datos no requiere de ordinario el consentimiento del trabajador. La información previa actuaría a modo de garantía, sustituyendo el consentimiento por el conocimiento.

Esta exigencia de información previa deriva de la legislación de protección de datos y de una doctrina judicial que la ha interpretado de forma un tanto desenfocada en su aterrizaje en el contexto laboral, ligando la información previa a la doctrina de la expectativa de privacidad que proviene de la doctrina del TEDH. En efecto, las SSTEDH Halford[65], en un asunto relativo al control de las llamadas telefónicas en el trabajo, Copland[66] y Barbulescu I[67], sobre el control del ordenador, introdujeron el concepto de «expectativa de privacidad», que el trabajador podía invocar cuando el empleador no había establecido reglas expresas sobre la utilización de las herramientas empresariales con fines personales, doctrina que acogerían las SSTC 241/2012, de 17 diciembre, y 170/2013, de 7 octubre. Por su parte, las SSTC 29/2013, de 11 de febrero, y 39/2016, de 3 marzo, convirtieron la información en un requisito para la implantación de la videovigilancia, al igual que la STEDH López Ribalda I[68].

Al margen de que el TEDH fundase su doctrina en el derecho a la vida privada y el TC haya recurrido al derecho a la protección de datos, y de que esa diferencia técnicamente podría conducir a resultados distintos, lo cierto es que la información previa al trabajador no puede servir como parámetro de valoración de la licitud de la medida, que ha de descansar en el test de proporcionalidad. Así parece derivarse de la doctrina más reciente, por ejemplo las SSTEDH Barbulescu II[69], Libert v. Francia[70] y López Ribalda II[71], en las que el Tribunal de Estrasburgo matiza que la política empresarial previa no permite eliminar la expectativa de privacidad o, en mejor expresión, no concede al empleador facultades de control ilimitadas, sino que es exigible en todo caso una valoración de la proporcionalidad de la medida implementada o que pretende implementarse.

No obstante, la doctrina de los tribunales en materia de geolocalización, apoyándose en los criterios sentados para la videovigilancia, ha venido condicionando la licitud de la medida a la previa información, esto es, a que el trabajador conociera que estaba siendo controlado y a través de qué medio. En concreto, los tribunales deducían que el derecho a la protección de datos se oponía a controles sorpresivos en el ámbito laboral, concusión que habría requerido un punto de apoyo sólido que las normas no proporcionaban, al menos hasta la LOPD de 2018. De hecho, ni la Directiva ni la legislación interna avalaban esa conclusión.

En efecto, el art. 5.1 LOPD/1999 se limitaba a exigir, con carácter general, no específicamente en el contexto del contrato de trabajo, que el responsable del tratamiento proporcionase información previa «de modo expreso, preciso e inequívoco» a los interesados «a los que se soliciten datos personales». Sin duda, esa obligación de informar previamente estaba presente en la norma, pero no alcanzaba a todo tratamiento de datos, sino específicamente a aquellas situaciones en las que los datos fueran solicitados a los interesados. Como es sabido, «solicitar» implica «pedir algo de manera respetuosa, o rellenando una solicitud o instancia», en atención al Diccionario de la RAE.

De este modo, el art. 5.1 LOPD/1999 estaba pensando, al igual que el art. 13.1 del RGPD,

[65] *Vid.* STEDH *Halford vs. Reino Unido* (de 25-6-1997, recurso 20605/92), apartado 45.

[66] *Vid.* STEDH *Copland vs. Reino Unido* (de 3-4-2007, recurso 62617/00), apartado 42.

[67] De 12-1-2016 (recurso 61496/08).

[68] De 9-1-2018 (recursos 1874/13 y 8567/13).

[69] De 5-9-2017 (recurso 61496/08).

[70] De 22-2-2018 (recurso 588/13).

[71] De 17-10-2019 (recursos 1874/13 y 8567/13).

cuando se refiere a datos personales que «se obtengan del interesado», en el usuario o consumidor que rellena una instancia, una encuesta o realiza una solicitud donde constan datos personales. En tal caso, la empresa que recaba esos datos no sólo debe pedir el pertinente consentimiento para el tratamiento, sino que además debe informar sobre el destino y uso de los datos. Ese el radio de acción natural del derecho a la información previa. En verdad, requiere un importante esfuerzo interpretativo entender que la información obtenida por un dispositivo de geolocalización o las imágenes captadas por una cámara implican una «solicitud» de datos personales al interesado, pues esas herramientas no «solicitan» a los trabajadores dato alguno.

Sin lugar a dudas, la geolocalización y la videovigilancia cuentan con un mejor encaje en el actual art. 14 RGPD (o en el ya derogado art. 5.4 LOPD/1999). Ese precepto se refiere a los datos personales que «no hayan sido recabados del interesado», y respecto de esos datos la obligación de informar tiene otro régimen distinto, toda vez que el derecho a la información no queda anulado, pero sí sufre una rebaja en sus condiciones, o en su intensidad, porque en este caso la obligación de informar no nace con carácter previo o simultáneo a la recogida de datos o a su tratamiento, sino que se admite el cumplimiento posterior. Es decir, esa normativa no exige información previa respecto de los datos que no proporcione directamente el interesado, sino que concede al responsable del tratamiento un plazo para cumplir la obligación de información, plazo que tradicionalmente se extendía hasta «los tres meses siguientes al momento del registro de los datos» (art. 5.4 LOPD/1999)[72], pero que tras la entrada en vigor del RGPD se limita a un «plazo razonable», como máximo de un mes (art. 14.3). Por consiguiente, cuando los datos no se solicitan directamente al interesado «el deber previo de información se sustituye por un deber de información posterior con la principal finalidad de que el titular de los datos pueda ejercitar, si lo desea, los derechos de acceso, rectificación, cancelación u oposición»[73].

La traslación de estas reglas al ámbito laboral implicaría, a partir de una interpretación literal, que la instalación de mecanismos de control no exigiría información previa al trabajador, siendo coherente con la finalidad misma de la medida, cuya efectividad podría quedar frustrada en otro caso. No es obstáculo a esa conclusión la Instrucción 1/2006, de 8 de noviembre, de la AEPD, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, cuyo art. 3 contemplaba la necesidad de información, pero no necesariamente previa, ni desde luego obligaba a advertir al trabajador en caso de sospecha previa. Esa Instrucción admitía como información la colocación de «al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados», sin mayores precisiones.

Sea como fuere, lo cierto es que el radio de acción de esa Instrucción únicamente alcanzaba la videovigilancia, y no otras formas de control, como la geolocalización. Con ello, resulta difícil sostener que la ausencia de información previa relativa a la instalación de dispositivos de geolocalización conllevara necesariamente la nulidad de la medida. Es esta una cuestión que entronca con los espacios naturales que debe ocupar el derecho a la protección de datos, pues no deben confundirse el modo de obtención de los datos, las condiciones de almacenamiento/conservación o su eventual uso.

La información previa ni siquiera es un requisito para la licitud del tratamiento de datos en el RGPD (no se incluye en el art. 6), y por ello no puede erigirse en un límite natural

[72] *Vid.* R. Tascón López, *Tecnovigilancia empresarial y derechos de los trabajadores (intento de construcción de una regla conceptual en el Derecho del Trabajo español)*, RTSS (CEF), nº 415, 2017, pp. 90-91.

[73] *Vid.* A. Canales Gil, "Comentario al art. 5", en A. Troncoso Reigada, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010, pp. 398 y ss.

para una medida de control empresarial. El salto lógico e interpretativo es demasiado difícil de salvar, pues no cabe extrapolar sin más un requisito o garantía instrumental (información) diseñado para garantizar que el interesado pueda ejercitar otros derechos, como los de supresión o rectificación, por ejemplo, a un entorno tan distinto como el control empresarial, cuyos parámetros de enjuiciamiento son, o habrían de ser, notablemente diferentes. Ese papel tan relevante que pretende concederse al derecho a la información previa resulta artificial, pues ese derecho debería estar vinculado naturalmente al consentimiento, como explícitamente indica el art. 6.1 de la LOPD[74], y la ausencia de información previa cuando el consentimiento resulta innecesario no provoca realmente un menoscabo al trabajador, que siempre puede invocar el derecho de acceso.

En cierto modo, la aplicación del derecho a la protección de datos a los mecanismos de control y vigilancia empresarial se ha valido de una técnica de "espigueo", porque se recurre al derecho a la información sin una adecuada contextualización. El derecho a la protección de datos no debería condicionar que la información obtenida e incorporada a un fichero pudiera servir para demostrar un incumplimiento del trabajador, porque la normativa aplicable no aludía, en realidad, a «finalidad distinta», sino a finalidad «incompatible» (art. 4.2 LOPD/1999)[75]. Es más, el art. 6.3 de la LOPD/2018 utiliza la expresión «finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual», y el art. 6.4 RGPD no prohíbe esa finalidad distinta, aunque exige efectuar una valoración que tome en consideración la relación entre el motivo inicial que justificó la captación de los datos y el fin distinto del ulterior tratamiento, la relación entre el interesado y el responsable del tratamiento, la naturaleza de los datos personales, las posibles consecuencias para el interesado y las medidas de seguridad adoptadas. Por consiguiente, lo determinante es, o habría de ser, si el empleador ha hecho un uso desviado de su poder de dirección implementando controles desproporcionados, no razonables o innecesarios, que no superan por tanto el juicio de ponderación.

Obviamente, podría argüirse que la STEDH López Ribalda I no permitía esas interpretaciones, porque exigía la información previa sobre la videovigilancia para poder utilizar las imágenes. Sin embargo, la aproximación a esa sentencia debía efectuarse con suma cautela –como demostró su rectificación en Gran Sala–, máxime cuando partía de la premisa de que la legislación española exigía la información previa antes de la instalación de las cámaras de video, lo que no se deducía del art. 5 LOPD/1999. La argumentación de la sentencia se construye, no se olvide, a partir de la expectativa razonable de privacidad que genera en los trabajadores la obligación legal impuesta al empleador de informar previamente a la instalación de las cámaras. De ahí que esa conclusión no pueda alcanzarse cuando la expectativa de privacidad desaparece, o ni siquiera llega a nacer, al no exigir la ley la información previa antes de la implementación de la medida de control. Esa información previa no se requería verdaderamente con la LOPD/1999, aunque sí tras la LOPD/2018, en virtud de su art. 89, si bien el precepto indica que «en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo», de modo que el distintivo eliminaría esa expectativa de privacidad. Cuestión distinta es que la falta de la pertinente información pueda afectar al núcleo esencial del derecho fundamental cuando la condición de licitud es el consentimiento,

[74] «De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que éste acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen».

[75] *Vid.* R. Tascón López, *El tratamiento por la empresa de los datos personales de los trabajadores ¿un problema resuelto o caído en el olvido?*, Aranzadi Social, nº 16, 2005 (BIB 2005\2432).

pues ese consentimiento, si no es informado, carece de validez[76].

Las conclusiones precedentes podrían extrapolarse a la geolocalización con anterioridad a la LOPD/2018, pero tras su entrada en vigor el art. 90.2 deja poco margen a la interpretación, de modo que la ausencia de información previa provocará, a buen seguro, dificultades interpretativas de entidad y conducirá a la nulidad de determinadas pruebas de incumplimiento obtenidas a través de estos dispositivos. El legislador español, por consiguiente, ha optado por configurar una garantía adicional que no está en el RGPD y ha conferido a la información previa un papel que no tiene en otros contextos donde entra en juego el derecho a la protección de datos, y lo ha hecho manteniendo por inercia interpretaciones de los tribunales muy cuestionables, pues, por ejemplo, el TEDH se basaba en un derecho distinto (vida privada) y se ha replanteado esa doctrina concediendo un mayor peso a la proporcionalidad (v.gr., STEDH *Barbulescu II* y López Ribalda II).

9. LA TRASLACIÓN A LA RELACIÓN LABORAL DEL CONCEPTO DE DATO PERSONAL: ¿LA UBICACIÓN DEL TRABAJADOR ES UN DATO PERSONAL O UN DATO PROFESIONAL?

Los datos de localización, o de ubicación, se califican como datos personales, y por ello entran en el radio de acción del derecho fundamental a la protección de datos. Se consideran datos de localización, en atención al art. 2.c) de la Directiva 2002/58/CE y al art. 64.b) del RD 424/2005, de 15 de abril, «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». Ahora bien, la escasa precisión sobre el concepto de «dato personal» suscita dudas razonables sobre el ámbito concreto de aplicación de la legislación sobre protección de datos con carácter general, y también explica que su traslación al contexto laboral no resulte particularmente sencilla. Muestra de ello es que el art. 88 del Reglamento (UE) 2016/679 contempla la aprobación de normas «más específicas» mediante las que se adapte ese derecho a las peculiaridades de la relación de trabajo. Sin embargo, el legislador –nacional o supranacional– no ha procedido todavía a elaborar esas normas, dando lugar a una serie de dificultades, como el propio concepto de dato personal, que no puede significar lo mismo en un contexto general que en el marco de un contrato de trabajo.

En efecto, la definición de dato personal no se acomoda bien a todos los ámbitos a los que en principio debería llegar, porque se concibe al afectado como un cliente o usuario[77]. Los esfuerzos, valiosos sin duda, por acotar el concepto de dato personal parten de una perspectiva de aproximación muy genérica[78], no trasladable a la relación de trabajo, porque no cabe asumir, sin más, que datos como el nombre, la edad, la imagen o la ubicación del trabajador merezcan la consideración de personales, con todo lo que conlleva, en el contexto de la relación entre el empleador y el trabajador. Por supuesto, esa es una información personal que puede ser susceptible de autodeterminación en la relación que une a un cliente o consumidor con una empresa que pretende ofertarle o publicitar bienes, productos o servicios. Sin embargo, el contrato de trabajo conduce a un escenario muy distinto, con un juego recíproco

[76] *Vid.* M.A. Castro Argüelles, "Protección de datos de carácter personal en el ámbito laboral", en J. García Murcia (Coord.), *Nuevas tecnologías y protección de datos personales en las relaciones de trabajo,* ASG 2003, Lugones, 2019, pp. 35-37; F.J. Díaz Revorio, "Comentario al art. 5", en A. Troncoso Reigada, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010, pp. 447-448.

[77] *Vid.* M.R. Llácer Matacás, *La autorización al tratamiento de información personal en la contratación de bienes y servicios*, Dykinson, Madrid, 2012, pp. 19 y ss.

[78] *Vid.* Dictamen 4/2007, del Grupo de Trabajo del Artículo 29, sobre el concepto de datos personales; http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358.

de derechos y obligaciones derivados tanto del contrato como de la ley que repercuten decisivamente en el catálogo o categoría de datos personales que el empleador tiene derecho a conocer.

La jurisprudencia, a partir de la STS (Cont-Adv.) de 31-10-2000[79], distinguió varios tipos de datos personales: los «datos personales *stricto sensu*», entre los que se incluirían no sólo el nombre, el estado civil o el documento personal de identidad, sino también los «datos referentes a la actividad profesional»; la «información sobre las condiciones materiales»; y las «evaluaciones y apreciaciones que puedan figurar en el fichero y que hagan referencia al afectado». A partir de esa clasificación parece claro que las condiciones de empleo y trabajo formarían parte del núcleo duro del derecho a la protección de datos, pues son datos personales en su sentido más estricto. Ahora bien, no conviene olvidar que esa sentencia pretendía resolver el acceso de un tercero a la información que obraba en posesión de la administración pública, que ese tercero no era el interesado y que no concurría una condición de licitud que justificase la aceptación de esa concreta pretensión.

Esa no es una situación parangonable a la que une a un empresario con un trabajador, porque el empleador conoce y/o debe conocer determinada información de carácter personal de sus trabajadores para el correcto devenir de la relación laboral, y porque, además, el contrato de trabajo es condición de licitud para el tratamiento de datos personales. Dicho de otro modo, el trabajador no puede ejercitar un derecho de autodeterminación informativa frente al empleador, y por tanto no cabe invocar que es un dato personal susceptible de protección plena «toda información sobre una persona física identificada o identificable», porque se llegaría al absurdo de que el empleador no pueda comprobar si el trabajador ha acudido al trabajo, ya que en tal caso se identificaría a la persona y se conocería su ubicación. Esa es una regla que tiene sentido para compañías que pretenden ofertar bienes y servicios, pero no entre dos partes que mantienen un vínculo contractual que conlleva una prestación laboral y que además han de hacer frente a determinadas obligaciones y exigencias legales.

Desde esta perspectiva, la relación de trabajo exige una adaptación del concepto de dato personal que se ajuste a las características singulares de este sector, y, con esta finalidad, cabría distinguir tres tipos de datos, dando lugar a una clasificación que habrá de generar las pertinentes consecuencias en la aplicación de la legislación de protección de datos. En primer lugar, los datos de naturaleza personal pero imprescindibles para el normal desarrollo de la relación laboral, bien para hacer frente a aspectos instrumentales, bien por convertirse en requisitos o condiciones esenciales para la celebración del contrato y/o la ejecución del trabajo (nombre, sexo, edad, discapacidad, datos bancarios si el salario se abona mediante transferencia, formación académica, competencias lingüísticas, etc.). En segundo lugar, datos de naturaleza personal no imprescindibles para la ejecución de la relación de trabajo (aficiones, estado civil, ideología, número de teléfono móvil, dirección de correo electrónico particular, nombre de usuario en una red social, etc.). Y en tercer lugar, datos que en el contexto de la relación laboral tienen naturaleza netamente profesional (horas de entrada y salida del trabajo, actividades desarrolladas, ubicación del trabajador durante el tiempo y lugar de trabajo, uso de medios o herramientas propiedad de la empresa, etc). Obviamente, los datos que encajan en cada una de esas categorías, en particular en las dos primeras, pueden variar en atención al concreto escenario laboral, como ha puesto de manifiesto la OIT[80], pues el elenco de datos que el emplea-

[79] Recurso 6188/1996.

[80] «Tanto el volumen como el tipo de información que cabe legítimamente recabar varían según el tipo de trabajo, la posición del trabajador o el contexto de una decisión que pueda afectar, por ejemplo, a los cambios estructurales en la empresa», cfr. OIT, *Repertorio de recomendaciones prácticas*

dor necesite conocer dependerá del interés legítimo que pueda acreditar en atención a la concreta actividad.

Esa clasificación viene referida estrictamente al contexto de la relación laboral, es decir, a la interacción entre empresario y trabajador. En consecuencia, esa es una clasificación con efectos meramente internos a la empresa, porque todos esos datos merecen la calificación de personales respecto de quienes que no acrediten el pertinente interés legítimo. De ahí que la normativa de protección de datos haya de ser aplicada, en toda su intensidad, con el fin de articular las garantías vinculadas a la protección y seguridad de los ficheros, pues aun cuando los datos pudieran calificarse como «profesionales» dicha calificación sólo puede operar con efectos *ad intra* del contrato de trabajo, pero no *ad extra*, donde seguirán contando con toda la tutela que el ordenamiento ofrece a los datos personales. Dicho de otro modo, o con expresiones más clásicas del ámbito laboral, algunos datos personales pueden desplegar efectos *erga omnes*, esto es, el trabajador puede hacer valer su derecho de autodeterminación informativa también frente al empleador, que sólo excepcionalmente podrá acreditar un interés legítimo para el conocimiento y posterior tratamiento, mientras que otros datos personales cuentan con eficacia limitada, de modo que las garantías del derecho a la protección de datos no se activan *inter partes*.

En este sentido, los datos personales imprescindibles para el normal desarrollo o ejecución de la relación de trabajo son datos personales de eficacia limitada, esto es, únicamente reciben la tutela máxima del ordenamiento frente a terceros ajenos a la relación laboral. El empleador, sin embargo, no necesita el consentimiento del trabajador para su tratamiento, ni realmente debería estar sometido a estrictas obligaciones de información sobre la finalidad para la que se recaban y tratan esos datos, pues la buena fe inherente al contrato exige del empresario un comportamiento acorde a dicho principio, que desde luego se resentiría si se utilizan los datos –que adquieren naturaleza profesional– con una finalidad ajena al contrato de trabajo. La licitud de la indagación sobre tales datos habrá de valorarse conforme a la buena fe, la intimidad, la libertad ideológica, el secreto de las comunicaciones, etc., pero la incorporación a un fichero no condicionaría en modo alguno su utilización dentro del estricto marco de la relación laboral, por más que se incumplan las obligaciones de información, porque ello podría llevar al absurdo de considerar que el pago mediante transferencia bancaria es nulo cuando el empleador no ha informado al trabajador de la concreta finalidad que motivó la solicitud del número de cuenta.

Por supuesto, el art. 5.1.b) RGPD advierte que los datos personales deben ser «recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines», pero esa previsión no puede introducir limitaciones artificiales en el poder de dirección. En este sentido, difícilmente cabe calificar como incompatible el uso de tales datos para decisiones o actuaciones de diversa naturaleza, pero todas ellas directamente vinculadas con la relación laboral, siempre en ausencia de transgresión de la buena fe o de uso desviado del poder de dirección. A la postre, y a tenor del diccionario RAE, «incompatible» se refiere a aquella persona o cosa que no «puede estar, funcionar o coexistir sin impedimento con otra». Y en un contexto como el de la relación laboral, donde el consentimiento del afectado no es condición de licitud para el tratamiento de datos, precisamente porque nacen una serie de derechos y deberes para ambas partes tanto del contrato como de la ley, no procede crear barreras adicionales –y artificiales– que dificulten el normal desenvolvimiento de esa relación.

Sin duda, deben descartarse las interpretaciones rigoristas y reduccionistas mediante las cuales se produzca una parcelación de los

de la OIT. Protección de los datos personales de los trabajadores, OIT, 1997, pp. 26-27; http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf.

conceptos de «ejecución» o «cumplimiento» de la relación laboral que obligue a especificar de manera muy concreta el propósito del tratamiento y califique como «finalidad incompatible» –que no meramente distinta[81]– cualquier otro uso de los datos que no coincida estrictamente con el que motivó su recogida aunque se enmarque en el normal desenvolvimiento de la relación laboral. En verdad, si el tratamiento se circunscribe a la ejecución y cumplimiento de la relación laboral, no debería ser necesario que el empresario ofrezca un mayor detalle sobre la utilización de los datos para calificar como lícito el tratamiento.

Bien mirado, el concepto de dato profesional ha estado presente de alguna manera en nuestra legislación durante años, por ejemplo en el art. 2.2 RD 1720/2007, que declara inaplicable el derecho a la protección de datos a los «ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales»[82].

La naturaleza personal de determinados datos se difumina en el ámbito de la relación laboral, pues en la medida en que se requieran adaptaciones o ajustes en la organización o en la dinámica del trabajo se convertirán en «datos profesionales» y, por tanto, el trabajador no podrá invocar las reglas sobre protección de datos para limitar el poder de dirección empresarial. Los datos profesionales, a la postre, disfrutan de una naturaleza mixta o dual: profesionales *ad intra*, pero personales *ad extra*. Y, por ello, en el contexto de la relación laboral el empleador podrá servirse de tales datos –y entre ellos la ubicación del trabajador durante el tiempo y lugar de trabajo– para toda finalidad lícita conforme al alcance de su poder de dirección y el interés legítimo que pueda acreditar.

10. PRIVACIDAD, INTIMIDAD Y PROTECCIÓN DE DATOS: LA NECESARIA DELIMITACIÓN DEL OBJETO Y EL CONTENIDO DEL DERECHO A LA PROTECCIÓN DE DATOS

Los avances tecnológicos de las últimas décadas proporcionan al empleador instrumentos de control y vigilancia con un potencial invasivo mucho más intenso que los tradicionales, y de ahí que resulte razonable implementar los pertinentes contrapesos para equilibrar los riesgos que genera una «empresa panóptica»[83]. Esa es, seguramente, la razón principal del notable desarrollo del derecho a la protección de datos en los últimos tiempos, cuya evolución muestra una progresiva e irrefrenable expansión, hasta el punto de que se ha llegado a afirmar que ese derecho «se ha comido a la intimidad»[84], pero también a otros derechos próximos, como el derecho a la propia imagen o al secreto de las comunicaciones. Por supuesto, la preocupación por la protección de datos se ha intensificado a consecuencia de la generalización de las TIC, pero constituye un error de concepto, y de apreciación, vincular la protección de datos exclusivamente a las nuevas tecnologías. Dicho de otro modo, ni el derecho a la protección de datos

[81] *Vid.* A. Desdentado Bonete y A.B. Muñoz Ruiz, *Protección de datos y contrato de trabajo,* Justicia Laboral, nº 46, 2011 (BIB 2013\51914).

[82] *Vid.* A. Puente Escobar, "Ámbito objetivo de aplicación", en J. Zabía de la Mata, *Protección de datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008, pp. 61 y ss.; J.R. Mercader Uguina, *Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679*, Trabajo y Derecho, nº 41, 2018.

[83] Cfr. J.R. Mercader Uguina, *Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?*, RL, Tomo I, 2001, pp. 665 y ss.

[84] Cfr. J.L. Goñi Seín, "Intimidad del trabajador y poderes de vigilancia y control empresarial", en J. García Murcia (Coord.), *Jornadas sobre derechos fundamentales y contrato de trabajo,* Consejería de Empleo, Industria y Turismo del Principado de Asturias, Oviedo, 2017, p. 33. También, I. García-Perrote Escartín y J.R. Mercader Uguina, *La protección de datos se come a la intimidad: la doctrina de la sentencia del TEDH de 5 de septiembre de 2017 (caso Barbulescu v. Rumanía)*, Revista de Información Laboral, nº 10, 2017, p. 12.

se agota en las TIC, ni los derechos potencialmente afectados por las nuevas tecnologías se circunscriben a la protección de datos.

No obstante, la labor de los grupos de trabajo a nivel supranacional y las decisiones judiciales han provocado en los últimos años un cierto solapamiento del radio de acción de varios derechos fundamentales que deberían contar con un espacio propio, y principalmente el derecho a la intimidad y el derecho a la protección de datos. Es probable, en este punto, que el concepto de *privacy*[85] esté conduciendo a una confusión de planos, y más en el ordenamiento español, donde los respectivos ámbitos de influencia de la intimidad y la protección de datos deberían encontrarse más claramente delimitados.

Como es sabido, durante largo tiempo en España se ha traducido *privacy* por intimidad. Sin embargo, es una asimilación arriesgada, porque ni la *privacy* ni la intimidad se encuentran completamente perfiladas en la actualidad. De este modo, un sector doctrinal considera que la intimidad es un derecho «abierto y dinámico», que incluye desde luego una faceta negativa «de defensa frente a cualquier intromisión de la esfera privada», pero también una faceta activa que permite controlar «el flujo de informaciones que conciernen a cada sujeto»[86]. Desde esta perspectiva, la *privacy* se convertiría en la faceta negativa del derecho a la intimidad, mientras que la protección de datos sería un ingrediente más, de carácter activo, integrado en ese derecho. Es una concepción opuesta a la del legislador español, que ya en la Exposición de Motivos de la LORTAD consideraba que la privacidad era más amplia que el derecho a la intimidad, de modo que es la intimidad la que forma parte de la privacidad, y no a la inversa[87].

El entorno geográfico también influye en el perímetro o radio de acción de la *privacy*, mucho más amplio en Europa que en otros lugares, principalmente Estados Unidos[88]. El concepto de *privacy* tiene su germen en EEUU, en la década de los 80 del siglo pasado, a resultas de la publicación en la prensa de noticias sobre las relaciones sentimentales de la hija de un senador, lo que derivó en la creación y desarrollo de instrumentos de tutela jurídica para bienes inmateriales, como la intimidad, la vida privada o inclusive la reputación[89]. De este modo, el concepto de *privacy* nace vinculado a la difusión de información en los medios de comunicación, pero progresivamente fue evolucionando, principalmente a escala europea, hasta el punto de exceder de los contornos del derecho a la intimidad, como demuestra la Directiva 95/46, que, a diferencia del RGPD, vinculaba explícitamente el derecho a la protección de datos a la *privacy*, y mencionaba ese término en numerosas ocasiones en su versión en inglés, inclusive en su art. 1.1 al definir el objeto de la Directiva: «*in accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*».

El contenido de la *privacy*, por consiguiente, se encuentra en expansión, y no se agota en el derecho a la intimidad, que es uno más de sus ingredientes, muy relevante, pero no el único. En la actualidad, ese derecho a la privacidad del trabajador englobaría los derechos a la intimidad, al secreto de las comunicaciones, a la protección de datos y la vertiente negati-

[85] *Vid.* C. Conde Ortiz, *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Universidad de Cádiz, 2005, pp. 24-26.

[86] Cfr. A.E. Pérez Luño, *Los derechos humanos en la sociedad tecnológica*, Universitas, Madrid, 2012, pp. 92-94.

[87] *Vid.* M. Álvarez Caro, *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital,* Reus, Madrid, 2015, pp. 53 y ss.

[88] *Vid.* M. Martínez López-Sáez, *La vigilancia electrónica en el contexto laboral europeo y estadounidense: perfilando el derecho a la protección de datos en el trabajo,* RGDTSS (iustel), nº 47, 2017; C. Conde Ortiz, *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Universidad de Cádiz, 2005, pp. 24-26.

[89] *Vid.* M.G. Losano, "Los orígenes del «Data Protection Act» inglesa de 1984", en M.G. Losano, A.E. Pérez Luño y M.F. Guerero Mateus, *Libertad informática y leyes de protección de datos personales,* Centro de Estudios Constitucionales, Madrid, 1989, pp. 15-16.

va de los derechos vinculados a la ideología o a las creencias, como la libertad religiosa, la libertad ideológica o la libertad sindical. Se explica así sin dificultad, ya en el plano de la relación laboral, que muchos desarrollos supranacionales relativos al control empresarial aludan a la privacidad o a la vida privada, y no estrictamente a la intimidad[90].

Sin embargo, la doctrina judicial en los últimos años ha venido a equiparar *privacy* con derecho a la protección de datos, pues sólo así se explica que ese derecho haya irrumpido en el debate jurídico sobre la licitud de las medidas de control empresarial. El derecho a la protección de datos ha conseguido un protagonismo que nunca tuvo, máxime cuando ha sido relegado durante años a una posición casi irrelevante en el ámbito de la relación laboral. Ello es debido a la ausencia de una construcción dogmática sólida sobre el objeto y el contenido del derecho, aspectos que no han sido convenientemente precisados en la normativa que lo regula, porque los derechos de acceso y rectificación, u otros análogos, y las restricciones impuestas al tratamiento no son equivalentes a una delimitación precisa de los rasgos esenciales de ese derecho fundamental.

La labor de construcción dogmática y teórica, como se sabe, ha correspondido a la doctrina científica y, especialmente, a los tribunales, con protagonismo principal para el TC. La premisa de partida es la aceptación del derecho a la protección de datos como derecho autónomo, pero también como ingrediente o componente accesorio o instrumental del derecho a la intimidad[91]. Desde esta perspectiva, las SSTC 290 y 292/2000, de 30 de noviembre, afirmaron que el derecho a la protección de datos «garantiza a la persona un poder de control y disposición sobre sus datos personales», ya que «confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos». En orden a conseguir su efectividad, el titular tiene «derecho a ser informado de quién posee sus datos personales y con qué finalidad», así como también el «derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos». Por consiguiente, «el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos», de modo que «es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes».

La Exposición de Motivos de la LOPD, inspirándose en la STC 292/2000, advierte que el derecho a la protección de datos atribuye «un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso». Desde esta perspectiva, «la funcionalidad del derecho a la intimidad es defensiva frente a la activa o de disposición relativa a la protección de datos»[92], lo que supone que el derecho a la protección de datos se convertiría en un derecho de disposición plena sobre los datos personales, que el "tenedor" o "depositario" de los mismos únicamente podría utilizar en los términos y con la extensión

[90] *Vid.* A. Plá Rodríguez, *The Protection of Workers' Privacy: The Situation in the Americas*, *International Labour Review*, Vol. 134, 1995, nº 3, pp. 298 y ss.

[91] *Vid.* S. del Rey Guanter, *Tratamiento automatizado de datos de carácter personal y contrato de trabajo (Una aproximación a la "intimidad informática" del trabajador)*, RL, nº 15, 1993, p. 13.

[92] Cfr. O. García Coca, *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, Laborum, Murcia, 2016, p. 37.

que le permitiera el titular. Por consiguiente, el derecho a la protección de datos atribuye al titular facultades de disposición sobre sus datos personales, es decir, convierte al derecho a la protección de datos en un derecho de «autodeterminación informativa»[93], en un derecho que permite que el afectado «sepa, consienta y pueda disponer en todo momento sobre la publicidad de sus datos y el alcance que ella tenga»[94]. Es, en definitiva, y en expresión anglosajona, un «derecho a estar solo» y libre de injerencias no deseadas (*right to be let alone*).

En esta línea, la STC 96/2012, de 7 mayo, precisó que el derecho a la protección de datos se distingue del derecho a la intimidad por su contenido, pues, «a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido», el «derecho a la protección de datos atribuye a su titular […] un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos».

Obviamente, el derecho a la protección de datos únicamente se despliega en toda su intensidad cuando el tratamiento de datos personales requiere el consentimiento del interesado. En cambio, cuando la condición de licitud no es el consentimiento el derecho a la autodeterminación informativa no nace como tal, lo que obliga a plantearse cuál es el objeto y contenido del derecho. A tal fin, conviene distinguir las dos facetas principales de ese derecho a la protección de datos, que desde la perspectiva del interesado podrían calificarse como activa y pasiva. La faceta activa es la que se corresponde propiamente con la autodeterminación informativa, con ese poder de disposición sobre la información personal en poder de otros que desean proceder a su tratamiento. En el ámbito de la relación laboral, aunque las mismas premisas serían extrapolables a otras situaciones donde la condición de licitud no fuera el consentimiento, esa faceta activa únicamente se desarrolla plenamente respecto de los datos no necesarios para el cumplimiento o ejecución de la prestación de trabajo. Esa información adicional, superflua o directamente impertinente para la ejecución del contrato sólo podrá ser objeto de tratamiento cuando medie el consentimiento del trabajador y, por la posición de desequilibrio de las partes, el empleador debería demostrar un interés legítimo.

En este sentido, la ley prohíbe utilizar los datos incorporados a un fichero con una finalidad incompatible a aquella para la que se recogieron, lo que implicaría, en el ámbito de la relación laboral, que no cabe utilizar esos datos proporcionados por el trabajador para una finalidad distinta del cumplimiento y ejecución del contrato (*v.gr.,* publicidad de productos y/o servicios). En puridad, cuando el empleador efectúa un tratamiento de datos personales con fines distintos a los propios del poder de dirección y organización (dar órdenes e instrucciones al trabajador, cumplir sus obligaciones o controlar la correcta ejecución del trabajo) no está ejercitando esos poderes, sino tratando de conseguir otros fines que, aunque económicamente pudieran resultar le-

[93] *Vid.* P. LUCAS MURILLO DE LA CUEVA, "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en P. LUCAS MURILLO DE LA CUEVA y J.L. PIÑAR MAÑAS, *El derecho a la autodeterminación informativa,* Fundación Coloquio Jurídico Europeo, Madrid, 2009, pp. 13 y ss.

[94] Cfr. I. VILLAVERDE MENÉNDEZ, "La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos personales", en A. FARRIOLS I SOLÁ (Dir.), *La protección de datos de carácter personal en los centros de trabajo,* Cinca, Madrid, 2006, p. 63.

gítimos, colisionan con el derecho a la protección de tales datos, porque ya no tiene lugar una exención del consentimiento a efectos del tratamiento. Y, en ese momento, el trabajador podría hacer valer su autodeterminación informativa.

Por el contrario, donde no se requiere el consentimiento el derecho a la protección de datos debe reubicarse o reacomodarse para desplegar los efectos que le son propios. El empleador no requiere el consentimiento del trabajador para el tratamiento de los datos personales imprescindibles para el correcto cumplimiento del contrato, y por ello el trabajador carece de facultades de autodeterminación respecto de esa información que el empleador puede legítimamente conocer y tratar. Sin embargo, el derecho a la protección de datos entraría en juego para imponer determinadas obligaciones al responsable del tratamiento, que debe implementar las garantías técnicas pertinentes vinculadas a la seguridad del fichero –seudonimización, cifrados, cortafuegos, etc.– que impidan el acceso y la difusión de esa información fuera del radio de acción donde el tratamiento es legítimo. El trabajador no puede oponerse válidamente el tratamiento de datos personales admitido por la ley, pero sí puede exigir garantías de que esos datos personales no se utilizarán y difundirán sobrepasando los límites que la ley ha establecido[95].

Por consiguiente, el derecho a la protección de datos personales no actúa, ni debe hacerlo, con la misma intensidad en todos los ámbitos. De ahí que el tratamiento de datos personales no siempre conduce a que entren en juego todas las facultades y atribuciones que derivan ordinariamente de ese derecho. Por supuesto, la faceta pasiva no admite excepciones, pues el responsable del tratamiento debe implementar las soluciones técnicas precisas para evitar accesos no autorizados al fichero, y para lograr, en definitiva, que los datos personales permanezcan en todo momento seguros y bajo control. Sin embargo, la faceta activa, de autodeterminación, dependerá en esencia de cuál sea la condición de licitud, pues las facultades del titular del derecho están más limitadas cuando el tratamiento no tenga su base en el consentimiento. Es decir, el interesado no podrá oponerse al tratamiento, aunque sí podrá ejercitar algunos derechos, como los de acceso, para comprobar qué datos personales están siendo tratados, o el de rectificación, cuando sean inexactos.

De ahí que tanto el objeto como el contenido del derecho a la protección de datos pueden adoptar una fisonomía distinta en atención al ámbito donde ese derecho debe operar, como demuestra la STJUE Nowak[96]. En particular, la condición de licitud que justifica el tratamiento de datos será determinante en la identificación de las facultades que asisten al interesado, aunque en todo caso ese derecho requerirá la adopción de medidas de seguridad relativas al modo de conservación, registro o almacenamiento de datos. La mayor visibilidad del derecho a la protección de datos, y su elevación a derecho autónomo, no debe hacer olvidar que se trata de una garantía instrumental al servicio de otros derechos, a modo de «condición preventiva para poder ejercer de modo efectivo otros derechos y libertades fundamentales»[97]. El derecho a la protección de datos únicamente despliega efectos por su relación con derechos como la intimidad, el honor, la dignidad o la prohibición de discriminación, de modo que su aparente autonomía no puede derivar en la sobredimensión.

[95] *Vid.* R. Miralles López, "Comentario al art. 9", en A. Troncoso Reigada, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010, pp. 762 y ss.; A. Desdentado Bonete y A.B. Muñoz Ruiz, *Control informático, videovigilancia y protección de datos en el trabajo,* Lex Nova, Valladolid, 2012, pp. 116 y ss.; A. Ortega Giménez, *Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de datos de la UE*, REDT, nº 216, 2019 (BIB 2019\1435).

[96] De 20-12-2017, asunto C-434/16.

[97] Cfr. S. Rodotà, *Democracia y protección de datos*, Cuadernos de Derecho Público, nº 19-20, 2003, p. 21.

Por ejemplo, no cabe defender que todo incumplimiento de la legislación de protección de datos impide que los datos recopilados puedan tomarse como base para adoptar una decisión o imposibilita que generen efecto alguno, positivo o negativo. Las garantías formales han de ser respetadas, pero las vinculadas al derecho a la protección de datos no pueden desplegar efectos exorbitantes. La legislación registral, por ejemplo, se basa en principios similares, como los de publicidad o exactitud (arts. 15 y 16 Ley 20/2011, de 21 de julio, del Registro Civil), pero, más allá de supuestos de eficacia constitutiva, la incorporación o no de un determinado hecho al registro no es obstáculo para que se produzcan los efectos oportunos, sin perjuicio de aspectos relacionados con la prueba. Un ejemplo gráfico: la no inscripción de la defunción de un trabajador, o las eventuales irregularidades en el registro, no pueden suponer que el contrato de trabajo no se extinga por tal circunstancia. El aspecto formal no puede prevalecer sobre la realidad material. Y argumentos análogos podrían elaborarse en relación con el depósito (arts. 1758 y ss. CC y arts. 303 y ss. del Código de Comercio), pues de alguna manera quien recaba datos personales se convierte en depositario de los mismos, y las normas sobre protección de tales datos establecen las oportunas cautelas en cuanto a su conservación, utilización y destino, pero no implican que la información sólo existe dentro de ese fichero, registro o almacén.

En efecto, esos datos tienen vida propia al margen de donde se encuentren almacenados y pueden ser conocidos por múltiples vías, ya que algunos datos, en particular de personas con trascendencia social, son públicos y accesibles sin dificultad[98]. Volviendo al símil con el registro o el depósito, el interesado tiene derecho a conocer los bienes que se han incluido o se conservan en ese registro o depósito, a oponerse a que el depositario o el titular del registro o depósito los utilice o los mueva, o a retirarlos cuando desee. La ausencia de la pertinente información sobre el lugar de depósito de los bienes embargados o la negativa injustificada al acceso a las instalaciones correspondientes para comprobar su estado pueden suponer un incumplimiento de la normativa, pero en modo alguno condicionaría la valoración sobre el motivo de un embargo, que ha de enjuiciarse conforme a otros parámetros. El derecho a la protección de datos debería operar con una lógica similar, máxime cuando ni siquiera cuenta con un reconocimiento expreso en sede constitucional, por más que pueda derivarse del art. 18.4 CE, y por ello no debería invadir y adueñarse de espacios que son propios de otros derechos.

11. A MODO DE CONCLUSIÓN: LOS ESPACIOS NATURALES DEL DERECHO A LA PROTECCIÓN DE DATOS EN LA RELACIÓN LABORAL

El deslumbramiento que en tiempos recientes ha provocado el derecho a la protección de datos ha llevado incluso a afirmar que el derecho a la intimidad «cada vez se entiende menos» si no se relaciona el derecho a la protección de datos[99]. Sin embargo, desde una perspectiva estrictamente técnica, y ubicando cada derecho en el espacio que le es propio, la protección de datos únicamente despliega toda su intensidad tuitiva en la relación laboral respecto de los datos que no sean necesarios para el cumplimiento o ejecución de la prestación de trabajo, pues en tal caso el tratamiento requiere el consentimiento del trabajador. En cambio, la condición de licitud para el tratamiento de datos necesarios en orden al cumplimiento de las obligaciones y el ejercicio de los derechos que nacen de la rela-

[98] *Vid.* M.N. DE LA SERNA BILBAO, "Comentario al art. 3", en A. TRONCOSO REIGADA, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2010, pp. 260 y ss.

[99] Cfr. L. EZQUERRA ESCUDERO, *Nuevas tecnologías en el control de la actividad del trabajador y sus límites. Especial referencia al derecho a la intimidad del trabajador* (http://www.iuslabor.org/jornades-i-seminaris/ponencies/any-2018/).

ción de trabajo no es el consentimiento, sino el propio contrato, lo que obliga a plantearse cuál es el espacio que ha de ocupar el derecho a la protección de datos cuando el consentimiento, y en buena medida la información, pierden esa posición nuclear.

Por supuesto, estas singularidades que introduce la relación laboral no implican que el derecho a la protección de datos quede postergado o excluido completamente, sino que debe reubicarse para desplegar los efectos pertinentes, y más en aquellos sectores donde la penetración de las TIC es intensa. A tal fin, conviene recordar que el derecho a la protección de datos cuenta con dos facetas netamente diferenciadas, que desde la perspectiva del trabajador podrían calificarse como activa y pasiva. La faceta activa es la que atribuye al titular facultades de plena disposición sobre sus datos personales, es decir, la que convierte al derecho a la protección de datos en un derecho de «autodeterminación informativa», en un derecho que permite que el afectado «sepa, consienta y pueda disponer en todo momento sobre la publicidad de sus datos y el alcance que ella tenga»[100]. Esa es la razón que explica, por cierto, el difícil encaje del principio de proporcionalidad con el derecho a la protección de datos, pues la proporcionalidad presupone la colisión entre dos derechos legítimos que exigen sacrificios recíprocos –y proporcionales, de ahí la expresión– para que uno no anule el otro. En el derecho a la protección de datos no existe esa colisión entre derechos en posición de igualdad, sino que uno de los derechos en juego prevalece. A la postre, la persona a la que se refiere la información dispone de esas facultades que se imponen a la intención de otra de utilizarlos, normalmente en beneficio propio. De ahí que el análisis desde la perspectiva de la proporcionalidad deba implicar a derechos como la intimidad, por ejemplo.

Sin embargo, esa faceta activa, de autodeterminación informativa, no siempre puede activarse, porque en ocasiones la ley legitima a un sujeto para efectuar el tratamiento de datos personales modulando sustancialmente esas facultades de autodeterminación, como sucede en el ámbito de la relación laboral. El empleador no requiere el consentimiento del trabajador para el tratamiento de los datos personales imprescindibles para el correcto cumplimiento del contrato, y por ello el trabajador carece de facultades de autodeterminación respecto de esa información que el empleador puede legítimamente conocer y tratar. Dicho de otro modo, en el ámbito de la relación laboral el interés legítimo del empleador es manifiesto, al menos en lo tocante a los datos necesarios para el cumplimiento de determinadas obligaciones legales y el correcto y ordinario devenir de la prestación de servicios. El derecho a la protección de datos pierde en tal caso algunos de sus rasgos identificativos, pues muchos datos que en otro escenario podrían considerarse como personales mutan y se convierten en datos profesionales respecto del empleador, aun cuando pudieran mantener ese carácter de datos personales *ad extra*, fuera del marco de la relación de trabajo, lo que obliga a cumplir las exigencias del derecho a la protección de datos vinculadas con la conservación y protección del fichero, pero obviamente las facultades del titular de los datos no se aproximan a las que le corresponderían si pudiera ejercitar un verdadero derecho de autodeterminación informativa. Es decir, el derecho a la protección de datos no siempre permite al interesado ejercer un derecho de autodeterminación informativa, sino que en ocasiones se traduce en obligaciones para el responsable del tratamiento, que debe implementar las garantías técnicas pertinentes vinculadas a la seguridad del fichero –cifrados, cortafuegos, etc.– que impidan el acceso y la difusión de esa información fuera del radio de acción donde el tratamiento es legítimo.

Claro está, la ley prohíbe utilizar la información incorporada a un fichero con una finalidad incompatible a aquella para la que

[100] Cfr. I. VILLAVERDE MENÉNDEZ, "La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos personales", en A. FARRIOLS I SOLÁ (Dir.), *La protección de datos de carácter personal en los centros de trabajo*, Cinca, Madrid, 2006, p. 63.

se recogió, lo que implicaría, en el ámbito de la relación laboral, que no cabe utilizar esos datos si no resultan necesarios para el cumplimiento y ejecución del contrato. En puridad, cuando el empleador utiliza el fichero con fines distintos a los propios del poder de dirección y organización (dar órdenes e instrucciones al trabajador, cumplir sus obligaciones o controlar la correcta ejecución del trabajo) no está ejercitando esos poderes, sino tratando de conseguir otros fines que, aunque económicamente pudieran resultar legítimos, sí colisionan con el derecho a la protección de tales datos, porque ya no tiene lugar una exención del consentimiento a efectos del tratamiento. Y, en ese momento, el trabajador podría hacer valer su autodeterminación informativa[101].

Lógicamente, debe evitarse, en la medida de lo posible, que la legislación de protección de datos de carácter personal provoque desajustes en la dinámica de funcionamiento normal de la relación laboral. Así podría suceder, por ejemplo, con la eventual declaración de nulidad de las decisiones empresariales que vulneren ese derecho. El ordenamiento debe proporcionar la pertinente defensa de la privacidad del trabajador ante «ataques intrusivos y desproporcionados en su esfera privada»[102], y ha de rechazarse una «vigilancia impersonal e inhumana»[103], pero es deseable que los errores individuales no se corrijan a través de la extensión artificial de derechos diseñados para otros contextos, y que las personas se responsabilicen de sus actos. El derecho a la protección de datos personales no es una herramienta idónea, eficaz y ni siquiera pertinente para proteger al trabajador que ha incumplido gravemente sus obligaciones laborales, y que pretende ocultar ese incumplimiento amparándose en construcciones dogmáticas de los derechos fundamentales de escasa solidez.

Por supuesto, es posible defender que nuestro ordenamiento debe abandonar su configuración tradicional, que distingue entre el derecho a la intimidad, el secreto de las comunicaciones y el derecho a la protección de datos, y ha de apostar por atribuir a los individuos un «derecho a la privacidad», que engloba todos esos derechos y que, en definitiva, permite al trabajador construir una esfera personal inaccesible al resto. Desde esa perspectiva, el derecho a la privacidad podría ser protegido a través de todos los instrumentos y herramientas que proporcionan esos tres derechos mencionados (y algún otro, como el derecho a la libertad sindical, el derecho de asociación, el derecho a la libertad ideológica, etc.). Pero en tanto el ordenamiento español se decante por diferenciar esos derechos, la protección de datos personales cuenta con su propio espacio y no debe invadir el radio de acción del derecho a la intimidad.

A modo de ejemplo, y en el contexto de la geolocalización, la declarada pretensión de algunas empresas, y en particular Amazon, de conocer mediante un dispositivo que debe portar el trabajador, en concreto una pulsera, dónde se encuentran sus empleados durante el tiempo y el lugar de trabajo dentro de las instalaciones empresariales[104] no contraviene el derecho a la protección de datos, aun cuando pudiera resultar una medida invasiva por desproporcionada, y por consiguiente una lesión del derecho a la intimidad. La utilización de nuevas tecnologías con un propósito rutinario y ordinario de control exhaustivo y permanente de la actividad laboral excede de los límites y facultades concedidos por el poder de dirección, y se convierte en un uso desviado de las facultades empresariales cuando ese medio de control no ha superado los filtros propios del

[101] *Vid.* C.H. Preciado Domènech, *El derecho a la protección de datos en el contrato de trabajo,* Aranzadi, Pamplona, 2017, pp. 161 y ss.

[102] Cfr. M.B. Cardona Rubert, *La utilización de las redes sociales en el ámbito de la empresa,* RDS, nº 52, 2010, p. 77.

[103] Cfr. S. Rodríguez Escanciano, "Vigilancia y control en la relación de trabajo: la incidencia de las nuevas tecnologías", en A. Farriols i Solá (Dir.), *La protección de datos de carácter personal en los centros de trabajo*, Cinca, Madrid, 2006, p. 99.

[104] https://www.economiadigital.es/directivos-y-empresas/amazon-patenta-un-brazalete-que-rastrea-a-sus-trabajadores_535550_102.html.

juicio de ponderación vinculado al derecho a la intimidad, y, por tanto, no se ha demostrado que sea un instrumento de control idóneo, necesario y proporcional, menos invasivo que otros. La previa información al trabajador en el marco de la ley de protección de datos en modo alguno puede eximir al empleador de este juicio de proporcionalidad, ni convalida esa práctica, pues son planos absolutamente distintos de valoración. De este modo, la información previa al trabajador no justifica cualesquiera medios de control por el mero hecho de que esté advertido, mientras que la falta de información no ha de invalidar por sí mismo el control.

Tampoco conviene olvidar que el derecho a la protección de datos deriva del art. 18.4 CE, a cuyo tenor la «ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». A partir de una exégesis literal, la geolocalización no encajaría en dicho precepto, porque la vulneración del «honor» o de la «intimidad personal y familiar» no sería consecuencia de la utilización de medios «informáticos». Es cierto que este argumento decae interpretando que «informática» es equivalente a «nuevas tecnologías», pero seguramente también cabe entender que la «libertad informática» es un derecho mucho más amplio que la protección de datos, de modo que el tratamiento automatizado es únicamente una de sus vertientes, y por ello resulta distorsionador extender las garantías diseñadas para un determinado derecho de carácter eminentemente instrumental y técnico a otros de contenido más sustantivo.

En suma, la licitud de que el empleador establezca mecanismos de control más o menos invasivos, como la geolocalización, no puede enjuiciarse tomando como parámetro el derecho a la protección de datos personales. Son otros los derechos en juego para dilucidar si el empleador está legitimado o no para conocer determinada información. Las garantías relativas a la obtención de la información derivan de unos derechos, y las garantías aplicadas al tratamiento derivan de otro, del derecho a la protección de datos personales, que no habría de prejuzgar si la información ha sido correcta o incorrectamente obtenida.

Es menester situar el derecho a la protección de datos en el espacio que le corresponde, de modo que el empleador habrá de respetar la confidencialidad (art. 5 de la LOPD), garantizar la correcta conservación de los datos y protegerlos de ataques externos (arts. 32 y ss. RGPD), normalmente a través del pertinente cifrado[105], asegurar su exactitud (art. 4 de la LOPD), así como permitir que el interesado ejercite los derechos pertinentes cuando proceda (acceso, rectificación, supresión, etc.), pero resulta absolutamente indispensable limitar las consecuencias de su vulneración a aquellas previstas específicamente por la ley. Como regla general, la legislación de protección de datos está diseñada para evitar que los datos personales de los trabajadores circulen libremente sin consentimiento y/o conocimiento del afectado, y las consecuencias de su incumplimiento se circunscriben al ámbito estrictamente económico, bien en forma de sanción administrativa, bien en forma de indemnización por daños y perjuicios, que más bien serían daños y perjuicios vinculados a la vulneración de los derechos a la intimidad o al honor (intromisión ilegítima en la esfera privada de la persona o difusión pública injustificada de hechos o circunstancias de naturaleza privada, especialmente cuando dañen la reputación).

En cambio, la normativa de protección de datos no contempla la exclusión como prueba de la información que pueda ser considerada como «dato personal» y que haya sido obtenida a través de un tratamiento no respetuoso con las normas. Las interpretaciones jurídicas exigen mesura y proporcionalidad, y desde luego no es el derecho a la protección de datos el

[105] *Vid.* ABANLEX, *Guía sobre el Reglamento General de Protección de datos* (https://gdpr.eset.es/pdf/ESET_Guia_sobre_el_reglamento_general_de_proteccion_de_datos_GDPR.pdf).

que debe determinar si resulta admisible la geolocalización como prueba para demostrar el incumplimiento del trabajador, y menos aún hacer pivotar la argumentación sobre el incumplimiento del deber de información, porque ello supone desfigurar ese derecho y distorsionar completamente el normal devenir de las relaciones laborales. El derecho a la información debe ligarse al consentimiento en este contexto de la protección de datos personales, y no cabe invocar artificialmente un derecho como este cuando el titular, el trabajador, carece de margen de actuación, ni posibilidad de autodeterminación, porque el empleador actúa en ejercicio legítimo de sus facultades de control y vigilancia, que en muchos casos podrían verse completamente desvirtuadas si se advierte al presunto incumplidor de que va a ser objeto de una medida de control para verificar una sospecha de incumplimiento. En ningún otro contexto social el presunto infractor disfruta de una ventaja de tal calibre que le permita eludir las responsabilidades por los hechos anteriores –que ya no son susceptibles de constatación– y evitar ser detectado en incumplimientos futuros, pues debe ser informado de cuáles son las medidas de control y cómo actúan.

Es curioso que el derecho a la protección de datos se esté utilizando para conceder un margen de impunidad frente a incumplimientos, incluso de naturaleza penal, consecuencia que en otros contextos, y en relación con otros delitos, resultaría socialmente inaceptable, porque no es concebible que la policía, por ejemplo, debiera advertir al sospechoso que está siendo objeto de vigilancia. Podría argüirse que en tales casos la intervención del juez –que parece necesaria para implementar la geolocalización en el ámbito penal[106]– exime de la necesidad de informar, pero es llamativo que no se contemple una excepción similar en la LOPD, pues el dispositivo de geolocalización, o cualquier otra medida de control, podría haber sido implementada por el empresario con la aquiescencia judicial (art. 76.4 LRJS). Sea como fuere, conviene tener presente que la investigación policial es, en principio, más invasiva que la investigación del empleador, pues en la primera el ciudadano afectado cuenta con una expectativa de privacidad casi absoluta, ya que el escrutinio alcanza facetas de su vida personal o privada, mientras que en el contexto laboral esa expectativa de privacidad suele desaparecer, máxime en tiempo y lugar de trabajo si el empleador ha prohibido determinados usos de los medios o instalaciones empresariales. Exigir además que exista información expresa sobre las medidas de control para validar su utilización es absolutamente desproporcionado y rompe cualquier equilibrio entre las partes, protegiendo injustificadamente al supuesto incumplidor. Otra cosa distinta es que deba informarse sobre cómo se tratarán esos datos y, en concreto, sobre cómo se difundirán, en su caso.

Esa expansión desmesurada, y artificial, del derecho a la protección de datos no ha tenido en cuenta que la información que exigía la norma reguladora, al menos hasta 2018, no era una información previa, sino posterior, porque los datos no los proporcionaba el propio interesado. La redacción actual de la LOPD, en relación con la videovigilancia y la geolocalización, deriva de una muy defectuosa integración del derecho a la protección de datos en el contexto de la relación de trabajo y da lugar a un resultado completamente insatisfactorio. La implementación de garantías para evitar la vulneración de los derechos del trabajador no puede conducir a que el empleador se vea privado de los más elementales mecanismos de control para detectar incumplimientos laborales, ni tampoco, como efecto perverso, a que la mera información faculte para adoptar cualquier medida de control por invasiva que resulte. La doctrina de las SSTEDH Barbulescu II[107], Libert v. Francia[108] y López Ribalda II[109], en la que se pone el acento sobre la pro-

[106] *Vid.* J.I. Reyes López, *Los dispositivos técnicos de geolocalización. Régimen jurídico a partir de la L.O.13/2015*, Aranzadi Doctrinal, nº 4, 2016 (BIB 2016\1098).

[107] De 5-9-2017 (recurso 61496/08).

[108] De 22-2-2018 (recurso 588/13).

[109] De 17-10-2019 (recursos 1874/13 y 8567/13).

porcionalidad de la medida empresarial y no sobre aspectos meramente formales –y tampoco entra en juego el derecho a la protección de datos–, es mucho más satisfactoria, por equilibrada, que la mera remisión a la expectativa de privacidad o a la información previa.

En definitiva, el control empresarial es inherente al contrato de trabajo y forma parte de los derechos y obligaciones inmanentes al poder de dirección, por lo que habrá de ponerse el acento en si esas facultades empresariales han sido utilizadas legítimamente, o si, por el contrario, se ha producido un uso desviado de ese poder de dirección, al no haber superado la medida de control el previo test de constitucionalidad dirigido a comprobar su idoneidad, necesidad y proporcionalidad. Tomando en consideración todos esos elementos, parece evidente que no deben valorarse de la misma forma un control empresarial individual y específico, dirigido a verificar una sospecha de incumplimiento, y un control general e indiscriminado. La sospecha previa de incumplimiento laboral obliga a ajustar ciertas interpretaciones, sea del derecho a la intimidad, sea del derecho a la protección de datos, como ya indicó en su momento la OIT[110], y ha confirmado la STEDH López Ribalda II[111], por lo que la validez del control no puede condicionarse a la información previa al investigado, pues ello privaría a la medida de toda eficacia.

[110] *Vid.* OIT, *Repertorio de recomendaciones prácticas de la OIT. Protección de los datos personales de los trabajadores*, OIT, 1997, p. 8. http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_span.pdf.

[111] De 17-10-2019 (recursos 1874/13 y 8567/13).

RESUMEN

El derecho a la protección de datos nació para hacer frente a riesgos a los que se exponía el ciudadano como cliente, usuario o consumidor de productos y servicios. Los datos proporcionados voluntariamente al vendedor o proveedor podían circular sin el debido control y encontrarse a disposición de un gran número de personas, físicas o jurídicas. Esa información es susceptible de utilización con fines muy diferentes, no sólo de mercadotecnia, sino que puede ser determinante, por ejemplo, para decidir si una persona es o no apta para adquirir un producto o contratar un servicio. Los evidentes riesgos para el derecho a la intimidad, y en general para la vida privada de las personas, exigían introducir las pertinentes garantías instrumentales, misión encomendada, precisamente, al derecho a la protección de datos. De ahí que el consentimiento del afectado y la obligación de proporcionar toda la información relevante sobre el destino y uso de los datos personales constituyan garantías esenciales para que este derecho resulte eficaz, y que el engranaje se asiente en la atribución al interesado de facultades de disposición sobre esos datos, de un derecho de autodeterminación informativa que puede implicar, en último término, la prohibición completa de la captación, tenencia o uso de los datos personales.

La relación laboral no parecía un entorno propicio para el desarrollo de este derecho, pues exige adaptaciones que no se han llevado a cabo completamente. La aplicación, sin esas adaptaciones, de la legislación de protección de datos a un contexto tan complejo y singular como la relación laboral da lugar a disfunciones que derivan en conflictos, máxime cuando la normativa no ha conseguido la suficiente difusión entre algunos de sus destinatarios principales, como las empresas, que no siempre conocen las obligaciones que impone respecto de la información que poseen de sus clientes, y que en muchas ocasiones ni siquiera son conscientes de que esa regulación también se aplica a la relación con sus trabajadores.

La legislación de protección de datos ha introducido escasas peculiaridades cuando se aplica a la relación laboral, aunque la más significativa es verdaderamente relevante, toda vez que el empleador no requiere el consentimiento del trabajador para el tratamiento de datos personales que sea necesario para la celebración y ejecución del contrato. El derecho a la protección de datos alcanza verdadera virtualidad gracias al consentimiento, esto es, a que el interesado pueda decidir quién, cómo y hasta cuándo podrá efectuar el tratamiento de sus datos personales. Si el consentimiento no forma parte de la ecuación el derecho a la protección de datos no puede ser considerado como un derecho de autodeterminación informativa, por lo que en cierto modo se desnaturaliza y sus efectos prácticos se reducen de manera considerable.

Sin embargo, la legislación de protección de datos ha sido utilizada como un límite para determinadas decisiones empresariales, y, en concreto, para aquellas que tienen por objeto el control y vigilancia del cumplimiento de las obligaciones laborales. La potencialidad invasiva de las nuevas tecnologías ha provocado una reacción tuitiva que, en ausencia de otras garantías que se consideren más pertinentes, ha convertido al derecho a la protección de datos en uno de los principales mecanismos de defensa de la privacidad del trabajador.

La geolocalización ilustra esa línea de tendencia, como demuestra que su primera regulación como instrumento de control laboral se haya introducido a través de la norma dedicada al derecho a la protección de datos. Esa ubicación normativa no es irrelevante, y el derecho a la protección de datos influye decisivamente en la configuración legal, introduciendo la exigencia de información previa a los trabajadores como requisito para la utilización de estas tecnologías.

El principio de proporcionalidad debe volver a ganar peso frente a interpretaciones netamente formalistas, porque el empleador no deberá recurrir a herramientas desproporcionadamente invasivas ni tomar decisiones con base en motivos jurídicamente inaceptables. En cambio, se aprecia en los últimos años una acusada tendencia a incrementar las garantías formales o instrumentales de los derechos en detrimento del análisis material y de la realidad misma. Por supuesto, las garantías formales e instrumentales son muy relevantes, pues su eliminación supondría que la finalidad perseguida justifica cualesquiera medios, lo que no es aceptable porque en último término el descubrimiento de una infracción validaría el más invasivo de los medios de control. Pero la información previa no puede sustituir al principio de proporcionalidad y la falta de esa información no siempre puede conducir a la nulidad de la medida empresarial. Es necesario encontrar un equilibrio entre los derechos de los trabajadores y los legítimos intereses del empresario.

De este modo, la implantación de medidas de geolocalización que tengan como propósito la seguridad de los bienes empresariales (v.gr., vehículos de empresa), no es equivalente a la utilización de esos dispositivos con exclusiva finalidad de control del trabajador. En el contexto del control del trabajador el lugar y el tiempo son aspectos muy relevantes, pues no puede merecer igual valoración, en primer lugar, que el empleador quiera conocer dónde se encuentran los trabajadores durante el tiempo y lugar de trabajo; en segundo lugar, que el empleador desee comprobar la ubicación de un trabajador durante la jornada laboral cuando la prestación de servicios no se desarrolla en un centro de trabajo al uso (v.gr., operadores mercantiles, repartidores, etc.); y, en tercer lugar, que la información a disposición del empresario comprenda también actividades privadas desarrolladas fuera del tiempo y lugar de trabajo.

El presente estudio tiene por objeto analizar esa nueva regulación legal, así como la doctrina judicial, pero también poner de manifiesto que la extensión de las garantías propias de la protección de datos al contexto de la relación laboral, y en concreto a modo de límites u obstáculos a la implementación de medidas de control empresarial, se ha llevado a cabo con excesiva premura y sin una valoración sosegada de las consecuencias que provoca, porque el derecho a la protección de datos no puede cercenar las legítimas facultades de control de un empleador y dar amparo a quien reiteradamente incumple obligaciones laborales básicas o incluso incurre en ilícitos penales.

Palabras clave: Geolocalización; intimidad; datos personales; derechos digitales; poderes empresariales.

ABSTRACT The right to data protection is primarily aimed at the user or consumer of products and services. The data voluntarily provided to a seller or to a service supplier could circulate without due control and be known by a large number of people. This information can be used for very different purposes, not only for marketing, but also, for example, to decide whether a person is able to acquire a product or hire a service. The risks to the privacy of people required protection measures, a mission entrusted to the right to data protection. Hence, the consent of the data subject and the obligation for the data controller to provide all relevant information about the destination and use of personal data constitute essential guarantees for the effectiveness of this right. In addition, data protection regulations grants the data subject a power to prohibit the collection, possession or use of personal data.

The employment relationship did not seem the best environment for this right, which requires adaptations that have not been fully implemented yet. The expansion, without these adaptations, of the data protection legislation to such a complex and unique context as the employment relationship leads to dysfunctions that result in conflicts, especially when this legal framework have not achieved sufficient dissemination among companies, which are not always aware that these regulations also applies to the relationship with their workers.

Data protection legislation has introduced few peculiarities when applied to the employment relationship, although the most significant one is of great importance, because the employer does not require the consent of the worker for the processing of personal data that is necessary for the performance of a contract. The right to data protection is truly effective thanks to consent, because the data subject can decide who, how and until when the processing of their personal data may be carried out. That is not possible in the case of the employment contract. However, data protection legislation has become a limit for employer´s decisions on the control and monitoring of the compliance with labour standards by workers.

Geolocation is an example and that is why its first regulation as a worker control tool has been introduced through data protection legislation. Thus, the right to data protection decisively influences the legal configuration, introducing the obligation of prior information to workers as a requirement for the use of geolocation devices.

Surely, the principle of proportionality must regain relevance. The employer cannot use disproportionately invasive tools or make decisions based on legally unacceptable grounds. However, there is a strong trend in recent years towards the increase of the formal guarantees of some rights to the detriment of an in-depth analysis. Of course, formal safeguards are very relevant, since their elimination leads to a situation where the end justifies any means, which is not acceptable. The verification of an infraction cannot validate the most invasive means of control. However, prior information to the worker cannot replace the principle of proportionality and the lack of such information may not always lead to the nullity of the corporate measures. A balance between the rights of workers and the legitimate interests of the employer must be found.

Many circumstances should be taken into account in the analysis of the validity of the use of geolocation devices. For example, the purpose of these measures may be to protect business assets (e.g., vehicles) and not exclusively the control of the worker. Place and time are very relevant aspects in the context of worker control, as the employer may want to know where the workers are during work time, or the location of a worker when the job takes place outside of the employer premises (e.g., delivery), or even activities carried out by the worker during his/her spare time. The impact on the right to privacy is not the same in all these situations.

The purpose of this paper is to analyze this new legal regulation, as well as case law, but also to show that the expansion of the safeguards of the right to data protection to the context of the employment relationship has been carried out too quickly and without a deep assessment of the consequences that it might provoke. The right to data protection cannot reduce the legitimate employer´s powers and cannot create an escape route for those who repeatedly breach basic labour obligations or even incur in criminal offences.

Keywords: Geolocation; right to privacy; personal data; digital rights; corporate powers.