ESTUDIO

NUEVAS TECNOLOGÍAS DIGITALES, PODERES EMPRESARIALES Y DERECHOS DE LOS TRABAJADORES: ANÁLISIS DESDE LA PERSPECTIVA DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS DE 2016[1]

José Luis Goñi Sein
Catedrático de Derecho del Trabajo. Universidad Pública de Navarra

1. LA TECNOLOGÍA DIGITAL: CAPACIDADES Y EFECTOS SOBRE LA PERSONA DEL TRABAJADOR

Las nuevas tecnologías digitales son el auténtico motor de transformación de la economía y de la vida social. Su imparable y rápido desarrollo, han supuesto una profunda revolución, cuya verdadera dimensión está aún por venir. La digitalización constituye una "nueva forma de vivir, de trabajar y de relacionarse" que ofrece enormes oportunidades de progreso, de mejoras económicas y de beneficios sociales[2].

Pero es también un entorno que suscita recelo y preocupación por la incorporación de datos de las personas físicas. En las nuevas tecnologías digitales, adquieren una dimensión esencial las manifestaciones de identidad subjetiva, esas huellas digitales que las personas dejan al contratar una tarjeta de crédito, dar de alta una wifi, navegar por Internet, realizar una compra, etc. Esa cesión constante de datos comporta un riesgo para la privacidad, y plantea la necesidad de una efectiva tutela de la persona frente al tratamiento de sus datos.

Como es sabido, las nuevas tecnologías digitales están dotadas de capacidades inéditas. Comportan, ante todo, una enorme posibilidad de recogida y obtención de datos personales. Los dispositivos móviles inteligentes, como *smartpho-*

1 El presente estudio reproduce la conferencia pronunciada por el autor en la Jornada sobre "Derecho a la intimidad y relaciones laborales" el día 27 de abril de 2017 en el Paraninfo "Ernesto Martínez" de Ciudad Real organizada por la Universidad de Castilla-La Mancha, y constituye una versión actualizada de algunos de sus trabajos previos.

2 La Sociedad digital es la gran apuesta de futuro. Véase, CEOE: "*Plan Digital 2020- La digitalización de la sociedad española*" (2016); se afirma que un incremento de la digitalización superior al 10%, supondría un aumento de más del 40% de la tasa de crecimiento del PIB.

nes y tabletas, el GPS, las aplicaciones informáticas, "internet de las cosas"[3], las tarjetas de crédito, redes sociales, etc., al estar íntimamente relacionados con un individuo específico, permiten a los proveedores de servicios o a los fabricantes de los dispositivos, recopilar, mediante aplicaciones, sensores inalámbricos, micrófonos o lectores de identificación instaladas en las mismas, una ingente cantidad de datos personales del titular.

Conllevan, asimismo, una capacidad ilimitada de acumulación de datos personales, permitiendo almacenar una cantidad enorme de información y datos personales en un espacio de reducidas dimensiones, lo que se conoce como Big data. Los sistemas de datos, que admiten grandes volúmenes de datos, tanto estructurados como desestructurados, solo tienen valor potencial.

No obstante, a ello añaden una inmensa capacidad de combinar los datos y de analizarlos de forma cruzada, extrayendo valor e información derivada de ellos. El Biga data permite obtener todo tipo de datos relativos a las preferencias ideológicas, políticas, sexuales, y demás aspectos sanitarios, afectivos o íntimos de la persona. En este sentido, la AEPD[4] subraya el riesgo que para la privacidad conllevan los dispositivos móviles inteligentes, como *smartphones* y tabletas, que permiten a los proveedores de servicios de geolocalización tener una visión muy cercana de los hábitos y patrones de movimiento del titular, de forma que se puede llegar a saber las preferencias de todo tipo, al igual que los motores de búsqueda que tratan un amplio abanico de datos –direcciones IP, *logs*, información que registran las *cookies*[5] o la información que el propio usuario aporta–, lo que hace posible obtener perfiles de hábitos de conducta.

No cabe desconocer, adicionalmente, que la digitalización implica la capacidad de hacer predicciones. Mediante técnicas como el aprendizaje automático supervisado y otras relacionadas, como el estudio de series temporales, y el estudio estadístico, cabe construir modelos predictivos capaces de estimar los valores más probables que tendrán estas métricas en el futuro próximo. Es posible analizar y predecir comportamientos futuros de las personas mediante la utilización de complejos algoritmos. Con el Big data se puede llegar a predecir

3 Se refiere a la tecnología para llevar puesta (*wearable computing*), –v. gr. relojes o gafas a las que se añaden sensores, cámaras o micrófonos que registran y transfieren datos al fabricante del dispositivo–, a los dispositivos capaces de registrar información relacionada con la actividad física de las persona y a la domótica . Vid. el Dictamen 8/2014 sobre Internet de las cosas, aprobado por el Grupo de Trabajo del Artículo 29, en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

4 AEPD: "Servicios de Internet y riesgos para sus datos personales", http://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2013/servicios_y_riesgos-ides-idphp.php

5 Las *cookies* son –como señala la AEPD en "Tus datos personales en Internet", www. agpd.es– ficheros que se almacenan en el ordenador del usuario, cuando navega por Internet, bien por los sitios web que visita el usuario o bien por terceros con los que se relaciona el sitio web, y permiten a éste conocer con detalle su actividad, por ejemplo: el lugar desde el que accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil) el sistema operativo y navegador utilizados, as páginas más visitadas, el número de clics realizados e infinidad de datos respecto al comportamiento del usuario en Internet.

determinadas conductas relacionadas con el comportamiento del consumidor, la seguridad o la salud; esto es, descubrir e identificar una serie de patrones de conducta de los clientes, determinar la propensión a padecer enfermedades, o la posibilidad de delinquir; en definitiva, se pueden extraer conclusiones sobre individuos con posibilidad de influir en el futuro de las personas.

En relación con el mundo de la empresa, la tecnología digital ha irrumpido con fuerza, provocando una disrupción notable en los modelos de negocio y comportando nuevos retos para la protección de los derechos fundamentales de los trabajadores. No es solo que el uso de las tecnologías vinculadas a la informática ha llegado a convertirse en una herramienta básica e imprescindible para la inmensa mayoría de las empresas por la necesidad de organizar de una manera más eficiente la actividad productiva; en los tiempos actuales, es casi inimaginable una empresa no conectada a la red o que no disponga de equipos informáticos dadas las ventajas competitivas que ello supone. Con independencia de ello, las empresas recurren a la tecnología digital porque es fuente de información y "la información personal adquiere cada vez un mayor valor económico". Muchas de las innovaciones en los productos y servicios tienen su origen en el análisis y explotación de datos por las propias u otras empresas. Big Data son una oportunidad para que las compañías mejoren su efectividad operacional a través de una mejor gestión de los datos de sus clientes y de sus empleados. Los Big data han adquirido un valor económico; es la nueva minería, el oro negro, y se comercia con ellos. En la actualidad, el comercio con los datos a gran escala es un negocio floreciente[6].

Refiriéndonos ahora al ámbito de las relaciones laborales, el uso de estas nuevas tecnologías ha traído consecuencias no del todo positivas para los trabajadores[7]. Es evidente que aportan beneficios también a los trabajadores como mejoras en el acceso a la información y en las comunicaciones para el desempeño de su trabajo y para estar más interconectados y resolver con prontitud situaciones personales. Pero, al mismo tiempo, las tecnologías vinculadas a la informática representan una amenaza potencial para el trabajador, en la medida en que registran cantidad de datos personales del trabajador. Datos que unas veces se aportan voluntariamente en servicios de redes sociales, otras involuntariamente al navegar en Internet, o al manejar cualquier instrumento de tecnología digital,

6 PÉREZ DE PABLOS, S., "Datos privados a la venta por 7 céntimos de euro", El País, 4 de mayo de 2017, p. 23, da cuenta de la existencia en Europa de más de 50 "data brokers" (empresas de comercio de datos") y de un número indeterminado a nivel mundial. Ahora bien, no cabe desconocer los riesgos que la digitalización representa. Amnistía Internacional revela la oferta por parte de una empresa estadounidense (Exact Data) de información de 1,8 millones de musulmanes por 138.380 dólares, a razón de 7,5 centavos por persona. Y es una de tantas ofertas que hace la compañía dentro de "un abanico de listas de contactos preconfigurados", en la que se incluye la de los "estadounidenses hispanos no asimilados" (en referencia a los que no están integrados en la sociedad de EE. UU., independientemente de su condición legal)"

7 Sobre los riesgos que entraña el poder informático para los derechos de los trabajadores, vid. RODRÍGUEZ ESCANCIANO, S., *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Bomarzo, Albacete, 2009, p. 5 y ss.

y que permanecen sin caer en el olvido, pudiendo acabar proporcionando información inferida[8].

El problema sustancial de la aplicación de las tecnologías vinculadas a la informática (cámaras de vídeo conectadas a Internet, sistemas de geolocalización, servicios de correo electrónico, dispositivos móviles (smartphones, tabletas) y aplicaciones, redes sociales, sistemas de mensajería instantánea, etc.) reside en que esa potencial aptitud para registrar y conservar datos sobre los más irrelevantes detalles del comportamiento del trabajador dentro y fuera del lugar de trabajo, puede ser utilizada para deducir información con finalidad distinta a la inicial e incluso discriminatoria. Y todo ello sin que el trabajador tenga, muchas veces, conocimiento ni control alguno de esa información.

Los nuevos sistemas tecnológicos posibilitan una vigilancia continua mientras dura la prestación y a veces después, lo que hace que el trabajador caiga en un estado de visibilidad permanente[9]. Tal es el caso de los equipos informáticos o sistemas de geolocalización que proporcionan a los Departamentos de Recursos Humanos abundante y constante información sobre sus empleados: no solo datos relativos a su actividad, pausas, rendimiento, evaluación del desempeño o trayectoria profesional, sino datos personales, concernientes a sus relaciones, amistades, salud, ideología, afectividad o comportamiento íntimo de la persona en el lugar de trabajo o fuera del mismo. La información de un empleado queda registrada en sistemas diferentes sin conexión entre sí. Pero nada impide interrelacionarlos para un análisis.

Con las nuevas tecnologías ya se pueden juntar todos esos datos para analizar, predecir escenarios futuros y anticiparse. Es posible "saber qué hará un empleado (comportamiento), qué conseguirá (rendimiento) y cómo estará (satisfacción)"[10]. Se pueden crear, así, sistemas para identificar a los profesionales con mejor desempeño, determinar qué perfiles encajarán en un determinado puesto o perfeccionar los mecanismos que miden la satisfacción de los empleados[11]. Con la consecuencia de que los datos transformados en conocimiento pueden conducir a veces a resultados en sí mismos inaceptables; piénsese, por ejemplo, si determinan la preferencia de un determinado sexo frente al otro, o el rechazo de determinadas personas con algunos componentes hereditarios o genéticos o con propensión a enfermar.

---

8 INNERARITY, D., "La reinvención de lo privado", El País, 4 de julio de 2014, p. 31.

9 Sobre la vigilancia potencial que acompaña como una sombra al trabajador, vid. MERCADER UGUINA, J., "Les libertés individuelles dans l'entreprise à l'epreuve des novelles techonologies. Observations à partir de la situation espagnole", AA. VV. (Dir. AUVERGNON, Ph.) *Les libertés individuelles et relations de travail: le possible, le permis et l'interdit?,* Presses Universitaires de Bordeaux, 2011, p. 148; COELHO MOREIRA, T., "A privacidade dos trabalhadores e a utilizaçao de redes sociais online: algunas questoes", *Questões Laborais*, nº 41, 2013, p. 46.

10 TABURET, L., La capacidad de predecir y comprender comportamientos humanos con Big Data https://www.linkedin.com/pulse/la-capacidad-de-predecir-y-comprender-comportamientos-laura-taburet

11 Vid. CASALDA, A., Gestión de personas. Algo más que 'big data' y algoritmos", Expansión, 12-4-2017 http://www.expansion.com/emprendedores-empleo/desarrollo carrera/2017/04/11/58ed0e00ca47414e2d8b45aa.html

La tecnología digital presenta, así, junto al riesgo de proporcionar al empresario, el conocimiento de aspectos de la vida privada del trabajador, el peligro evidente de suministrar una valoración o un perfil, a veces inaceptable desde el punto de vista del respeto a la dignidad y a los derechos fundamentales, que puede ser utilizado posteriormente con fines discriminatorios para la postergación del candidato o del trabajador en función del resultado y objetivos.

Otro importante efecto de la revolución digital estriba en el desvanecimiento de las fronteras entre la actividad profesional y la vida privada del trabajador[12]. Las nuevas tecnologías incorporan la posibilidad de estar conectado a cualquier hora del día, lo que facilita el desarrollo del trabajo fuera incluso de la jornada y del lugar de trabajo. La disponibilidad permanente se ha instalado en la cultura laboral, y recibir instrucciones del jefe a cualquier hora y contestar con inmediatez sus mensajes es una práctica habitual. La digitalización del trabajo ha acabado con la tradicional separación de tiempo y espacio[13], permitiendo una prolongación ilimitada de la jornada laboral con sobrecarga de trabajo y de esfuerzo, y, a la vez, una ampliación de las posibilidades de control de la actividad del trabajador por parte del empresario. La digitalización ha supuesto un paso atrás para la conciliación de su vida laboral y personal y para una mejor calidad de vida.

Por último, los dispositivos digitales presentan importantes ventajas desde el punto de vista de gestión del personal y del ejercicio de las facultades del poder de dirección por el empleador. Dichos dispositivos se caracterizan por ser un medio excelente para la vigilancia de la ejecución normal de la actividad laboral; permiten ver lo que muchas veces no está al alcance del ojo humano. Pero no solo son instrumentos verificadores de cumplimiento laboral, sino que son también magníficos medios de prueba, que permiten acreditar el incumplimiento de sus obligaciones laborales por el trabajador en el proceso laboral. Los instrumentos tecnológicos pueden ser preordenados con un fin disciplinario; en la casuística de los tribunales se encuentran a menudo casos de utilización de las cámaras de video-vigilancia o de dispositivos de geolocalización para obtener la prueba de alguna conducta irregular del trabajador en el desempleo de su actividad laboral sea dentro o fuera de la empresa.

2. INTERESES JURÍDICOS AFECTADOS: ¿INTIMIDAD O PRIVACIDAD DEL TRABAJADOR?

Bajo la perspectiva examinada, cabe preguntarse ahora por los concretos derechos que se ven especialmente afectados por el uso de las nuevas tecnologías

12 RODRÍGUEZ-PIÑERO ROYO, M., *Las nuevas tecnologías en la empresa*, Consejo de Relaciones Laborales, Sevilla, 2006, p. 14.

13 Vid. ALEMAN PAEZ, F., "El derecho de desconexión digital. Una aproximación conceptual crítica y contextualizadora al hilo de la Loi travail Nº 2016-1088", pendiente de publicación en la Revista Trabajo y Derecho.; VALLECILLO GÁMEZ, M.R., "El derecho a la desconexión: ¿novedad digital o esnobismo del viejo derecho al descanso", TESS, CEF, nº 408, 2017, p. 172.

digitales en el ámbito laboral. Por lo general, se tiende a señalar la intimidad y el secreto de las comunicaciones. Y es bastante coherente, porque las nuevas tecnologías permiten, como se ha podido comprobar, que se pueda llegar incluso al núcleo más sagrado de la vida privada, bien de forma indirecta o bien de forma directa con total intencionalidad, comprometiendo ese ámbito personal y reservado de los trabajadores que garantiza el art. 18.1 CE, y el secreto de las comunicaciones que protege el art. 18.4 CE. El trabajador cuando utiliza el ordenador o dispositivos móviles de la empresa o propios para la ejecución de la prestación, se expone a que los mensajes que emite y las huellas que deja acerca de su localización o comportamiento, puedan ser supervisados, porque esas herramientas tecnológicas registran e incorporan aspectos personales vinculados a la subjetividad del ser humano. Existe, por tanto, el riesgo de que la intimidad quede al descubierto.

Pero el objeto de tutela no es solo o principalmente la intimidad del trabajador, porque el concepto de intimidad adquiere un valor relativo en el contexto actual de las nuevas tecnologías digitales.

Y ello, en primer lugar, porque la prestación se realiza muchas veces en el propio medio tecnológico, y el empresario tiene derecho a comprobar si su uso se ajusta o no al fin profesional. En estas formas de trabajo el cumplimiento laboral se presenta conectada de forma inescindible a la actividad de la persona del trabajador. La tutela de la intimidad es un interés sacrificable en aras a permitir que el empresario pueda verificar el cumplimiento por el trabajador de sus obligaciones laborales (art. 20.3 ET). Se debe permitir al empresario hacer una cierta exploración en el caudal informativo (profesional e íntimo) que el trabajador va dejando en el ordenador o en la red, mientras ejerce sus funciones, para que aquél pueda ejercer su poder de mando sobre el trabajador. Es sabido que los derechos fundamentales pueden experimentar ciertas modalizaciones en el seno de las relaciones laborales, en función de los requerimientos de la organización productiva, de forma que, ciertas manifestaciones de ejercicio del derecho a la intimidad que serían legítimas y procedentes en otro contexto pueden no serlo en el marco de la relación laboral (STC 126/2003). Y esto es lo que ocurre cuando el empleado maneja como instrumento de realización de su prestación los medios telemáticos o digitales: que lo que no es lícito conocer en general, puede serlo en el caso del empleador porque el control de la actividad laboral del trabajador solo es posible penetrando de alguna manera en su intimidad.

En segundo lugar, la tutela de la intimidad resulta disminuida por la propia voluntad de la persona, que acota un ámbito cada vez más reducido de su propia intimidad. A lo anterior se añaden las transformaciones que se están produciendo en la actitud de las personas ante el mundo digital. Al utilizar las nuevas tecnologías, corresponde a cada persona decidir lo que desea desvelar. La tendencia actual es justamente la opuesta al "*right to be let alone*", que imperaba en

otros tiempos. Internet es un espacio en el que cada vez más personas tienden a compartir sus informaciones personales –curriculum vitae, comentarios, fotografías, aficiones–, en plataformas virtuales –blogs, redes sociales, etc.–, y ello de manera muchas veces abierta al público, lo que se hace también desde el lugar de trabajo con las herramientas del empresario. El individuo se exhibe ante el mundo virtual a través de las nuevas posibilidades tecnológicas. Quiere darse a conocer y tener muchos amigos en las redes sociales con los que interactuar, renunciando voluntariamente a sus propios espacios de intimidad.

En tercer lugar, no cabe desconocer la servidumbre que comportan las nuevas tecnologías, al exigir como condición de acceso a la red el deber de facilitar información personal. Las nuevas tecnologías sitúan al usuario ante la necesidad de tener que dar información acerca de sí mismo para entrar en determinadas páginas o poder interactuar. La ampliación de la propia persona no siempre es una decisión voluntaria. Las nuevas tecnologías ofrecen enormes ventajas, pero a cambio exigen proporcionar datos personales, al registrarse de alta como usuario en portales de compra, o redes sociales, servicios de mensajería, o al navegar por Internet, datos que pueden revelar información del entorno, la familia, o sobre los hábitos, estilos de vida, o la salud. Es el nuevo paradigma que ha arraigado con la llegada de Internet.

En este nuevo contexto, la intimidad, entendida como "ámbito propio y reservado frente al conocimiento de los demás", constituye una realidad en declive. En la actualidad su importancia es decreciente porque lo que se incentiva es una forma de relacionarse colaborativa que obliga a compartir y a salir del anonimato. Hay una necesidad de conectividad y de derribar los muros individuales tanto para crear "una inteligencia colectiva"[14] accesible a mucha gente desde cualquier lugar, como para llegar a conocer las pretensiones individuales de las personas y ofrecer una satisfacción a esas pretensiones individualizadas. La nueva era comunicativa que inauguran las TIC es de todo punto diversa al mundo cerrado y sustraído a la publicidad, que preconiza el derecho a la intimidad en su vertiente negativa, por lo que su reivindicación y defensa en el mundo digital ha perdido gran parte de su sentido.

El reto que suponen las nuevas tecnologías de la información va más allá de la necesidad de protegerse de las indiscreciones y de las curiosidad ajenas que garantiza el derecho a la intimidad. La sociedad de la información ha provocado un cambio en la concepción de la intimidad y obliga a pensar y defender lo privado de manera diferente. La sociedad está ahora sensibilizada con un fenómeno más complejo que el de un ámbito de protección específico, cual es el control de su identidad. El usuario de las nuevas tecnologías lo que quiere es no perder el control de los datos personales y de cuanta información se recoge o se

14 COELHO MOREIRA, T., "A privacidade dos trabalhadores e a utilizaçao de redes sociais online: algunas questoes", cit., p. 51.

trata a través de la actividad *on line*. En la sociedad de las redes lo que adquiere valor es la privacidad en sentido amplio, entendido como concepto que permite a la persona conocer cómo y con qué fines se están utilizando sus datos y decidir en consecuencia con el propósito de impedir su tráfico ilícito y lesivo de dus derecho a la dignidad.

No tiene mucho sentido luchar contra la capacidad de las nuevas tecnologías de recolectar información y de generar información derivada porque el proceso es imparable. La defensa de los derechos de la persona estriba en tener la oportunidad de seguir siendo dueña de su propia identidad, disponiendo, de una manera transparente, de toda la información sobre la recogida y tratamiento de sus datos. En suma, el interés legítimo del trabajador se circunscribe no tanto a proteger un espacio propio, cuanto a controlar sus datos personales insertos en los sistemas de comunicación, porque solo así puede ejercer un control sobre el uso secundario de esos datos y evitar las discriminaciones o exclusiones en el acceso al empleo o durante la relación laboral.

3. MARCO REGULADOR DE LAS FACULTADES DE VIGILANCIA DEL EMPRESARIO: EL REGLAMENTO DE LA UE DE 2016 SOBRE PROTECCIÓN DE DATOS

El conflicto jurídico suscitado por las nuevas tecnologías digitales se mantiene huérfano de solución en nuestro ordenamiento jurídico laboral. No existe una normativa específica que contemple de alguna manera los problemas derivados de la utilización de los medios técnicos como mecanismos de control en el lugar de trabajo[15]. El legislador ha omitido sistemáticamente en todas las reformas laborales, el tratamiento de los nuevos derechos vinculados al desarrollo de las TIC, pese a los delicados problemas aplicativos suscitados[16].

Sólo se cuenta con el parvo instrumental que proporciona el art. 20.3 del Estatuto de los Trabajadores, que faculta al empresario a "*adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida de su dignidad humana*". El precepto reconoce, así, al empresario un amplísimo poder de vigilancia y control, solo limitado por el respeto a la dignidad humana del trabajador. Es una genérica declaración, que comporta evidentes dudas aplicativas sobre los límites del poder de control empresarial.

El marco legal presenta, así, claros síntomas de insuficiencia, porque no ofrece concreción alguna respecto de los delicados conflictos entre el interés del

15 GOÑI SEIN, J.L., "Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?, en AA. VV. *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social, XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social,* AEDTSS- Cinca, Madrid 2014, p. 31.

16 Una breve descripción de los problemas que genera la deficiente regulación laboral en esta materia puede verse en RODRÍGUEZ-PIÑERO ROYO, M., *Las nuevas tecnologías en la empresa,* cit., p. 16.

empresario por la supervisión de la actividad laboral y los derechos fundamentales principalmente afectados, el derecho a la intimidad [art. 4.2.e) ET], la privacidad (art. 18.4 CE) y el secreto de las comunicaciones (art. 18.3 CE).

Ello obliga a los jueces y tribunales a hacer de intérpretes de los límites al poder de control empresarial que derivan del referido principio de respeto de la dignidad, y a buscar criterios de solución de los conflictos planteados. En este sentido, resulta un lugar común afirmar que la jurisprudencia, especialmente la constitucional pero también la casacional, ha desempeñado, animado por un cierto activismo judicial, un papel muy relevante en la apreciación de los límites del poder de control empresarial, haciendo un loable esfuerzo de cobertura de vacío normativo[17].

No obstante, y aunque el papel del Tribunal Constitucional y Tribunal Supremo ha sido trascendente especialmente en el restablecimiento del juego de los derechos fundamentales en el uso de las nuevas tecnologías en el ámbito laboral y en la delimitación del alcance del poder de vigilancia y control del empresario, y así hay que reconocerlo, los resultados de tal intervención jurisdiccional a veces "*no dejan de resultar … inquietantes en la medida en que no siempre son coherentes ni previsibles*"[18], pues en algunos casos se ha llegado a soluciones tan peculiares como arbitrarias, cuando no a una "guerra de Tribunales", como habrá ocasión de comentarlo más adelante.

En todo caso, es de esperar que este panorama de anomia e indiferencia del legislador hacia el papel de los derechos fundamentales en el ámbito de las facultades de control empresarial cambie, en breve, al menos con relación al derecho a la protección de datos de carácter personal. Se ha de recordar que el recién aprobado Reglamento UE 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de las personas[19], que ha venido a derogar la Directiva 95/46/CE, obliga al Estado español a adoptar antes del 25 de mayo de 2018, las normas de implementación del derecho a la protección de datos en el ámbito laboral.

Específicamente, en el art 88 del RGPD se señala que:

"1. *Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de*

17 Vid. RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., "Del *Statuto dei lavoratori* al Estatuto de los trabajadores. Dos experiencias en contraste", AA. VV., *El Estatuto de los trabajadores italiano veinte años después,* Ministerio de Trabajo y Seguridad Social, Madrid, 1993, p. 153

18 GOERLICH PESET, J.M., "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas", AA. VV., *El derecho a la privacidad en el nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional,* Tribunal Constitucional y Centro de Estudios Constitucionales, Madrid, 2016, p. 126.

19 DOUE de 4 de mayo de 2016.

los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

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

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas".

El tenor literal del precepto, si bien solo faculta a los Estados miembros a legislar sobre la materia, como denota el término "podrán", comporta, sin embargo, un mandato al legislador y a los agentes sociales para que regulen sobre la materia, ya que los Estados miembros están obligados a presentar ante la Comisión antes del 25 de mayo las disposiciones legales de implementación del derecho a la protección de datos en el ámbito laboral.

EL Reglamento pone a los Estados miembros ante el difícil reto de realizar una acomodación y concreción de los principios del Reglamento en un ámbito extenso de materias de la relación laboral. Establece que sus normas sean especificadas en las siguientes materias: contratación, ejecución del contrato laboral, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

Importa destacar que el art. 88 obliga a contemplar concretamente, dentro de las "*medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales",* una regulación legal o convencional directa de *"los sistemas de supervisión en el lugar de trabajo",* así como de" *la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta".*

Esa labor de determinación específica se antoja difícil y compleja, pues cada uno de los Estados debe acometer la concreción sin que previamente se hayan

desplegado unas mínimas bases de acomodación, más allá del respeto al espíritu y los principios del Reglamento. Cada uno de los Estados debe especificar, según su capacidad de entendimiento, el contenido y alcance del derecho fundamental en el ámbito laboral. Puede ocurrir que en un primer momento, lejos de alcanzar la uniformidad deseada por el Reglamento, se origine una disparidad de regímenes jurídicos, y en vez de proporcionar seguridad jurídica y transparencia a los operadores económicos, señaladamente a las microempresas y las pequeñas y medianas empresas, se termine obligando a éstas a satisfacer los diferentes requisitos de protección de datos de cada Estado miembro como sucedía hasta ahora. Pero para conjurar ese riesgo de disgregación está el Comité Europeo de Protección de Datos, que tiene, entre otras funciones, la de garantizar la aplicación coherente del Reglamento.

Por lo demás, interesa señalar que el Reglamento entró en vigor a los 20 días de su publicación (25 de mayo de 2016), pero únicamente será de obligado cumplimiento a los dos años desde la publicación. No comenzará a aplicarse, pues, hasta pasados dos años, el 25 de mayo de 2018. Hasta entonces, tanto la Directiva 95/46 como las normas nacionales que la trasponen, entre ellas la española, seguirán siendo plenamente válidas y aplicables.

A la finalización del referido plazo (25 de mayo de 2018) el Reglamento será de aplicación directa en todos los Estados miembros de la UE y los problemas de convivencia entre la redacción actual de la LOPD y su norma de desarrollo, por un lado, y el RGPD, por otro lado, se solventarán a favor de la norma comunitaria. El Reglamento será la opción prevalente a la hora de interpretar el contenido y alcance del derecho fundamental a la protección de datos y ninguna disposición nacional podrá ser aplicable si resulta incompatible con el RGPD[20].

4. LA DOBLE PERSPECTIVA DE ANÁLISIS DEL CONFLICTO TECNOLÓGICO LABORAL

A falta de unos principios específicos en el ordenamiento jurídico laboral, el debate sobre la identificación de los límites del poder de control empresariales a través de las nuevas tecnologías, se sustancia en una doble instancia -por una parte, en sede jurisdiccional[21] y por otra, ante la autoridad de control del derecho a la protección de datos-, con notables divergencias de planteamiento, dando lugar a espacios de inseguridad jurídica.

Aunque el conflicto es único e indivisible, las instancias jurisdiccionales y la autoridad de control del derecho fundamental a la protección de datos enfocan

20 GARCÍA MEXIA, P., "La singular naturaleza jurídica del Reglamento General de Protección de datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en AA. VV. (Dir. PIÑAR MAÑAS, José Luis): *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Editorial Reus, S. A., Madrid, 2016, pp. 25-27.

21 TASCÓN LÓPEZ, R., *El tratamiento por la empresa de datos personales de los trabajadores (Análisis del estado de la cuestión)*, Thomson-Civitas, APDCM, Navarra, 2005, p. 138.

el problema desde perspectivas distintas. Por una parte, el Tribunal Supremo y el Tribunal Constitucional no dejan de observarlo como un problema que afecta en exclusiva a la expectativa de la intimidad del trabajador y al secreto de las comunicaciones. Por su parte, la Agencia Española de Protección de datos lo analiza en clave diferente, bajo la protección de datos personales. De modo que, acerca de la valoración de los límites del poder de control tecnológico se confrontan dos posiciones de signo diverso, encerrados, más o menos, cada uno en una burbuja, dejando al operador jurídico y al empresario amplios márgenes de duda respecto del canon de enjuiciamiento aplicable a los mecanismos de control tecnológico empresarial en el ámbito de la relación laboral.

4.1. EL CRITERIO JURISPRUDENCIAL: EXPECTATIVA DE CONFIDENCIALIDAD

En la jurisprudencia, el conflicto entre el interés del empresario por vigilar y controlar la actividad laboral del trabajador y el respeto a los derechos fundamentales de los trabajadores en el entorno de las nuevas tecnologías, se tiende a enjuiciar en la mayoría de las ocasiones desde la perspectiva del derecho a la intimidad (art. 18.1 CE) y el secreto de las comunicaciones (art. 18.3 CE), como únicos derechos afectados. No se puede decir, con todo, que sea el único criterio adoptado por los Tribunales, porque a veces resulta de aplicación también el principio de proporcionalidad.

Centrándonos en el ámbito del control del ordenador, que es en donde se ha producido fundamentalmente el debate, y sin perjuicio de lo que más adelante se comentará sobre la video-vigilancia, que constituye un caso aislado en la jurisprudencia, cabe observar que la doctrina jurisprudencial ha experimentado una importante evolución.

El Tribunal Supremo y el Tribunal Constitucional han sentado en esta materia un criterio diverso al canon clásico de enjuiciamiento de la legitimidad de las medidas empresariales restrictivas de los derechos fundamentales del trabajador basado en el principio de proporcionalidad (SSTC 98/2000 y 186/2000). Se advierte un cierto abandono del método ponderativo del principio de proporcionalidad[22]. El conflicto no se examina exclusivamente desde la perspectiva del carácter indispensable de la inspección empresarial en el ordenador del trabajador (o principio de proporcionalidad).

El TS y el TC analizan los diversos supuestos de control tecnológico desde la posible expectativa de confidencialidad que puede derivar de las reglas de uso

22 ÁLVAREZ ALONSO, D., "Modulación laboral de los derechos fundamentales, ponderación y principio de proporcionalidad. ¿Un paradigma en retroceso?", en AA.VV. *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social, XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social,* AEDTSS-Cinca, Madrid 2014, incluye CD, p. 11 de la Comunicación, se pregunta si el Tribunal Constitucional está abandonando el método ponderativo y virando hacia el de la delimitación de los derechos fundamentales como forma de acotar su alcance en el contexto laboral; si estos modelos son antagónicos o incompatibles entre sí, o si, por el contrario, cabe una aplicación complementaria de ambos.

de los medios informáticos y del deber de información previa al trabajador. En realidad, el deber de información previa (la existencia de unas reglas sobre el uso de los medios informáticos y del conocimiento de tales reglas por los trabajadores[23]) se convierte en el primer y principal requisito para legitimar el registro en el ordenador [correos electrónicos, navegación por Internet y cualquier vía de mensajería (Skype, Messenger, etc.)] .

En la primera aproximación al asunto, el Tribunal Supremo, en su sentencia de 26 de septiembre de 2007, establece que lo que debe hacer la empresa, de acuerdo con las exigencias de la buena fe, es fijar previamente las reglas de uso de los medios, con prohibiciones absolutas o parciales e informar a los trabajadores de que va a existir control y de los medios que han de aplicarse en orden a la comprobar la corrección de usos. La doctrina fijada en esta Sentencia del TS y en las de 8 de marzo de 2011, 6 de octubre de 2011 y Sentencias del TC 241/2012 y 170/2013 atiende, de este modo, a las prohibiciones establecidas o no de uso con fines personales de los medios informáticos, construyendo en función de las condiciones de uso el derecho del trabajador a tener, en su caso, una "*expectativa general de confidencialidad*" de los eventuales usos privados y de sus comunicaciones. Esta expectativa de confidencialidad se reconoce cuando no se establecen reglas de uso o se permite su utilización con fines personales. Se considera que en tales supuestos se genera una expectativa que "*no puede ser desconocida, aunque tampoco puede convertirse en un impedimento permanente de control empresarial*" (STS 26 de septiembre de 2007).

No obstante, en las sucesivas sentencias, el TS y el TC han ido reduciendo las posibilidades de invocación del derecho a la confidencialidad, pues se ha ido suavizando el nivel de exigencia del deber de información previa. De un criterio inicial garantista mantenido en la primera sentencia, que viene a exigir a la empresa una política explícita no solo sobre el uso, sino también sobre el control de las herramientas puestas a su disposición, incluso la adopción de medidas preventivas, se ha pasado a otro más permisivo que consagra como único criterio definidor de las expectativas de intimidad en el centro de trabajo, la mera política sobre el uso. La jurisprudencia ha excluido la necesidad de una previa información sobre los mecanismos de control, que opere como límite a la discrecionalidad del empresario, permitiendo incluso el acceso clandestino y sorpresivo, una vez establecidas las pautas de prohibición absoluta. Así, en la sentencia del TS de 6 de octubre de 2011, donde no opone reparo alguno a que se utilice un programa espía para el control de la actividad del trabajador.

Pero el Tribunal Constitucional ha ido incluso más lejos, desvirtuando casi por completo el inicial esquema garantista de la STS de 26 de septiembre de 2007, al

23 RODRÍGUEZ ESCANCIANO, S., *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas"*, cit., p. 55.

considerar suficiente una simple previsión de prohibición de uso personal establecido en un convenio colectivo, para acceder al correo electrónico del trabajador. Ello se produce con la STC 170/2013 en que se analiza el caso de una empresa, que sin haber establecido previamente prohibición alguna de uso privado, procede a interceptar el contenido de los correos electrónicos de un trabajador registrados en el ordenador ante las sospechas de revelación de información confidencial a otra empresa. El TC avala tal acceso, porque considera que la tipificación en el Convenio colectivo aplicable, como falta leve de "la utilización de medios informáticos propiedad de la empresa para fines distintos de los relacionados con el contenido de la prestación laboral", impide albergar cualquier expectativa razonable de privacidad y, por tanto, entiende legitimo el control empresarial del ordenador y teléfono móvil llevado a cabo al amparo de la misma[24].

Esta jurisprudencia constitucional se ha extendido, además, a "supuestos en los que pudiera ser aplicable una protección constitucional más fuerte: la derivada del secreto de las comunicaciones"[25] (art. 18.3 CE). De este modo, se acepta el control no solo del uso del correo electrónico y la navegación por internet, sino de los programas de mensajería instantánea ubicados por el trabajador en los ordenadores, permitiendo la interceptación de las conversaciones electrónicas de los trabajadores. Ello ocurre en la STC 241/2012, a propósito de un caso de utilización de un programa informático denominado "Trillian" de mensajería instantánea, instalado en ordenador de uso común, en clara contravención de una orden expresa de la empresa, y desde el que se vierten comentarios despectivos, críticos e insultantes hacia sus compañeros y superiores; en ella se afirma que no existe una expectativa razonable de confidencialidad derivada de la utilización del programa instalado al tratarse de una forma de comunicación abierta, y que, por tanto, las conversaciones realizadas por estos trabajadores no están garantizadas por el secreto de las comunicaciones[26].

Este posicionamiento de la Sala 4ª del TS y del TC ha sido objeto de una fuerte crítica por parte de la Sala 2ª del Tribunal Supremo. En su sentencia de 16 de junio de 2014 (R. nº 2229/2013) sostiene, por el contrario, la necesidad de la autorización judicial previa para acceder al contenido de una cuenta de correo o mensajes del trabajador. Recuerda que el artículo 18.3 de la Constitución "*no contempla (...) ninguna posibilidad ni supuesto, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc. propiedad de tercero ajeno al comunicante) ni del carácter del tiempo en el que se utiliza (jornada laboral),*

24 En relación con esta sentencia, vid. APARICIO TOVAR, J., "Los derechos fundamentales y el juicio de proporcionalidad degradados a mera retórica. A propósito de la STC 170/2013, de 17 de octubre de 2013", *Revista de Derecho Social,* nº 64, 2014.

25 GOERLICH PESET, J. M., "Protección de la privacidad de los trabajadores en el nuevo entorno tecnológico: inquietudes y paradojas", cit., p. 145.

26 A propósito de esta sentencia, vid. CARDONA RUBERT, M. B., Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás. Comentario a la STC 241/2012, de 17 de septiembre*", Revista de Derecho Social,* nº 60, 2012, pp. 169 y ss.

ni tan siquiera, de la naturaleza del cauce empleado ("correo corporativo"), para excepcionar la necesaria e imprescindible reserva jurisdiccional en la autorización de la injerencia".

Esta tesis ha abierto una clara brecha entre los "ámbitos penal y laboral"[27], aunque la propia Sala 2ª ha matizado un poco la exigencia de la autorización judicial al dejar fuera los "datos de tráfico" (circunstancias de tiempo, líneas utilizadas, duración de la comunicación, etc.) y los mensajes una vez recibidos y abiertos por el trabajador, así como la información sobre accesos a otros servicios de la red como las páginas web visitadas, que no forman parte de la comunicación propiamente dicha, y dejan de estar protegidos por el secreto de las comunicaciones. De todas formas, el que no estén cubiertos por el art. 18.3 CE no impide, al decir de la propia sentencia, que a los correos leídos no haya que aplicarles los principios de protección y conservación de datos (art. 18.4 CE) y en consecuencia sea exigible la información previa sobre la revisión y tratamiento de los datos obtenidos (duración, fines, etc.)[28] y los derechos de intimidad documental en sentido genérico (art. 18.1 CE).

Paradojas y disputas aparte, se debe dejar constancia, no obstante, de que se ha producido un cambio significativo en la doctrina del Tribunal Constitucional en los últimos tiempos, al menos en lo que respecta a la utilización de las cámaras de video para el control del cumplimiento de la actividad laboral. En la STC 29/2013 se valora por primera vez la prueba de la video vigilancia desde la perspectiva de protección de datos. El criterio dirimente utilizado hasta la fecha consistía en el principio de proporcionalidad; que comportaba un análisis de la medida de instalación de las cámaras desde la perspectiva de idoneidad para la finalidad pretendida por la empresa, necesidad y estricta proporcionalidad en relación con los objetivos de la empresa (STC 186/2000). En la referida sentencia, el centro de la valoración se sitúa, sin embargo, en otro elemento distinto, en concreto, la información previa, en atención a que la video-vigilancia implica tratamiento de datos personales y resulta, por ende, aplicable la normativa de protección de datos personales.

Tal solución supone un tímido intento de admisión de los principios de protección de datos como canon de enjuiciamiento constitucional cuando se trata de analizar una medida empresarial de control que comporte tratamiento de datos personales del trabajador, y, aunque va referida a la videovigilancia, no hay motivo aparente para no extenderla a otros supuestos de control tecnológico[29].

27 FERRANDO GARCÍA, M.F., "Vigilancia y control de los trabajadores y derecho a la intimidad en el contexto de las nuevas tecnologías", *RTSS, CEF*, nº 399 (junio 2016), p. 57.

28 Ibídem.

29 Tal orientación ha sido mantenida posteriormente, también, por el Tribunal Supremo. En la STS de 13 de mayo de 2014 ha rechazado la utilización de las cámaras de video vigilancia, instaladas con la finalidad exclusiva de evitar robos por parte de clientes, para sancionar a una trabajadora por incumplimiento de sus obligaciones laborales. Considera que la utilización para un fin distinto del expresamente señalado por la empresa vulnera los principios de protección de datos del art. 18.4 CE.

4.2. EL CRITERIO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS

Por otra parte, la Agencia Española de Protección de Datos se sitúa en otra perspectiva. Considera que las operaciones de vigilancia tecnológica constituyen tratamiento de datos. Frente a la consideración única de la expectativa de la confidencialidad mantenida por el TS y TC, el enjuiciamiento resulta más amplio en el ámbito de la AEPD. El conflicto es analizado desde el punto de vista del derecho a la privacidad que implica un contenido más extenso.

La doctrina expresada por la AEPD en cuanto a los controles basados en el uso de las tecnologías de la información, no se detiene solo en las expectativas de confidencialidad, sino que se concentra en el conjunto de principios de protección de datos. Se sitúa así, en una lógica diversa, exigiendo un deber de adecuación al derecho fundamental de protección de datos (art. 18.4 CE).

En la Guía editada sobre "La protección de datos en las relaciones laborales"[30], la AEPD subraya la necesidad de cumplir con los deberes de protección de datos, señaladamente los de proporcionalidad, finalidad y de información a los trabajadores. La Agencia somete al empresario, cuando decide adoptar algún mecanismo de control tecnológico, a la carga de la prueba de la observancia de los principios de protección de datos, lo que implica un juicio de valoración más amplio que la simple constatación de un deber de información estereotipado.

Así, por ejemplo, cuando se trata de la instalación de los servicios de geolocalización en los dispositivos móviles o en los vehículos del trabajador, la AEPD maneja un criterio mucho más riguroso que los órganos judiciales. Permite la instalación solo si concurre una necesidad específica de la empresa, excluyendo cuando los empleados puedan organizar libremente sus planes de viajes o cuando se lleve a cabo con el único fin de controlar el trabajo de un empleado, siempre que pueda hacerse por otros medios. Impone a los responsables el deber de información previa a los trabajadores de la existencia de tal mecanismo en el vehículo o en el teléfono móvil, así como de la finalidad de recogida de los datos. Obliga a tener algún dispositivo que permita desactivar el sistema fuera de las horas de trabajo; impide la utilización de datos obtenidos para un uso divergente de la finalidad originaria; exige que los datos se conserven exclusivamente durante el oportuno en función de la finalidad que justifique su tratamiento, y, en fin obliga a adoptar todas las cautelas necesarias para garantizar la seguridad de los datos (Informe Jurídico 613/2009). La Agencia no se conforma con exigir una mera información a los trabajadores de la instalación de la instalación de estos controles, como cabría deducir de las resoluciones del TS y TC.

Respecto del control del correo electrónico del trabajador, la Agencia se muestra, asimismo, igual de rigurosa en la determinación de las condiciones de licitud. La

30 Disponible en http://www.agpd.es

AEPD entiende que "el artículo 2.3 ET no legitima por sí solo el ejercicio del control de las herramientas de trabajo" (Informe Jurídico 6/2009) y concede gran importancia al cumplimiento del deber de información por constituir uno de los elementos esenciales para garantizar el derecho fundamental de protección de datos. Tiene declarado que el deber de informar "resulta particularmente relevante cuando se trate de controles de uso de Internet y/o del correo electrónico" y que se debe describir de forma pormenorizada en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales, informando también sobre la finalidad de la vigilancia, y las medidas de vigilancia adoptadas[31]. En este sentido, ha llegado a sancionar a una empresa con una multa de 60.102 euros por no haber informado previamente de la posibilidad de control; así en el Procedimiento Sancionador PS 355/2010, seguido contra una empresa que accedió al correo electrónico de los trabajadores, sin haber establecido las reglas de uso y control. Y cuando en los procedimientos de sanción se invoca la doctrina flexible del TS y TC sobre las políticas de uso de los medios, la AEPD se encarga de recordar que dicha doctrina no les exime del deber de cumplir con la normativa de protección de datos (Resolución AEPD R/01755/2013 Procedimiento A/00060/2013)[32].

En consecuencia, el criterio interpretativo o de enjuiciamiento del conflicto empleado por la AEPD es más rico en exigencias, porque analiza no solo desde un perfil negativo (*ius excludendi*), sino del positivo de control de los propios datos[33]. Los requisitos a que se condicionan los controles empresariales y que pueden justificar eventuales monitorizaciones de los instrumentos de información y comunicación de los trabajadores, se enmarcan dentro de un ámbito más preciso y extenso de los principios de protección de la privacidad, donde la intimidad *strictu sensu* recibe también su protección.

5. ENJUICIAMIENTO A LA LUZ DEL REGLAMENTO DE LA UE 2016 DE PROTECCIÓN DE DATOS

En la doctrina de los Tribunales y de la Agencia se han consolidado, así, dos direcciones interpretativas paralelas no por ello contradictorias, lo que no deja de suscitar cierta perplejidad, pues, a nivel ontológico, difícilmente pueden separarse los dos perfiles de constitucionalidad de este único conflicto. El intento de separación compromete la seguridad jurídica y repercute negativamente en la efectividad de los derechos fundamentales reconocidos a los trabajadores.

31 AEPD "La protección de datos en las relaciones laborales", cit.

32 Vid. ABERASTURI GORRIÑO, U., "Control empresarial del correo electrónico del empleado y relevancia de la información previa a los trabajadores como garantía mínima para ejercer ese control, a la luz de las STC 7 octubre 2013"NREDT, 2015, nº 180, pp. 207-8.

33 Véase al respecto el criterio interpretativo mantenido por La Agencia Catalana de Protección de Datos en su Dictamen 1/2013 sobre la problemática de privacidad d en el uso del correo electrónico en el entorno laboral.

Entre el derecho a la intimidad (ex art. 18.1 CE) y el derecho a la privacidad (ex art. 18.4 CE), hay un ámbito concurrente. La intimidad forma parte del núcleo más protegido de la privacidad. Aquellos datos que por su naturaleza son especialmente sensibles y que pertenecen a la intimidad, se hallan especialmente protegidos por el derecho de protección de datos. El derecho a la privacidad consagra implícitamente el respeto a lo más íntimo de la persona, prohibiendo también la interceptación o el conocimiento antijurídico de aspectos íntimos. La intimidad conforma un círculo más reducido y encuentra también protección dentro de la privacidad. No es solo que haya un punto de interconexión entre estos derechos. Es que, como han señalado Diego Córdoba Ignacio Díez-Picazo, la privacidad o el derecho a la protección de datos se ha comido a la intimidad[34].

La resistencia de los Tribunales –Supremo y Constitucional– a reconocer relevancia al derecho fundamental a la protección de datos en el ámbito de la valoración de los límites a los poderes de control tecnológico del empresario, no tiene fácil explicación.

El Grupo de Trabajo del Artículo 29 (integrado por las Autoridades Europeas de protección de datos)[35] ha manifestado en varios Dictámenes que el marco jurídico aplicable a cualquier sistema tecnológico de tratamiento de datos en el lugar de trabajo es la Directiva de Protección de Datos 95/46/CE en combinación con la Directiva 2002/58/CE de Privacidad y Comunicaciones Electrónicas. En su Dictamen 8/2001 de 13 de septiembre de 2001 sobre "*el tratamiento de datos de carácter personal en el contexto profesional*", dejó bien claro que "*las disposiciones relativas a la protección de datos se aplican a la vigilancia y control de los trabajadores, tanto en términos de utilización del correo electrónico, acceso a Internet, cámaras de vídeo o datos de localización*". Y lo ha reiterado con posterioridad en varias ocasiones en que se ha pronunciado sobre las concretas formas de vigilancia tecnológica por parte del empresario. Así, en el "*Documento de Trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo*", adoptado el 29 de mayo de 2002 y en el "*Dictamen 4/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, adoptado el 11 de febrero de 2004*".

Por otra parte, el nuevo Reglamento 679/2016 de Protección de Datos de la UE sanciona de manera explícita en el art. 88 esta inserción de cualquier tratamiento de datos en el ámbito laboral en el marco de los principios de protección de datos, toda vez que habilita de forma específica al Estado, para que, a través de

34 CÓRDOBA CASTROVERDE, D., DÍEZ-PICAZO GIMÉNEZ, I., "Reflexiones sobre retos de la protección de la privacidad en un entorno tecnológico", AA. VV., *El derecho a la privacidad en el nuevo entorno tecnológico, XX Jornadas de la Asociación de Letrados del Tribunal Constitucional,* Tribunal Constitucional y Centro de Estudios Constitucionales, Madrid, 2016, p. 105.

35 El *Grupo de Trabajo del Art. 29* es un organismo de la Unión Europea constituido en virtud del art. 29 de la Directiva 95/4/EC con el fin de contribuir a la aplicación uniforme de las Directivas en materia de protección de datos en los Estados miembros. Es un grupo consultivo compuesto por representantes de las autoridades de protección de datos de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea.

disposiciones legislativas o convenios colectivos, establezca normas de garantía de los derechos fundamentales en relación con el tratamiento de los trabajadores en el ámbito laboral, prestando, además, especial atención a la "transparencia del tratamiento" y a los "sistemas de supervisión en el lugar de trabajo".

En consecuencia, una lectura conforme a los nuevos retos planteados por las nuevas tecnologías debería llevar a encuadrar el conflicto en la disciplina del derecho a la protección de datos que garantiza la Constitución, aplicándose los límites conexos a tal derecho y condicionando la legitimidad de la medida de control empresarial a la valoración de todos los derechos afectados[36].

5.1. CONTROL DE LAS COMUNICACIONES ELECTRÓNICAS DEL TRABAJADOR

Volviendo a la doctrina de la Sala 4ª del TS y del TC sobre la facultad de acceso empresarial a las herramientas informáticas y comunicaciones electrónicas del trabajador, cabe observar que dista bastante de ajustarse a los principios de protección de datos de carácter personal.

La compatibilidad del poder de la vigilancia de las comunicaciones electrónicas del trabajador y sus derechos fundamentales se halla anclada, como se ha señalado, en la tutela de la intimidad en su vertiente negativa (*ius excludendi*). Sólo se toma en consideración el ámbito protegido por la intimidad o el secreto de las comunicaciones y ninguna relevancia asume el derecho a la protección de la privacidad en su dimensión positiva de poder de control y disposición sobre los propios datos (ex art. 18.4 CE). El corpus doctrinal del TS y del TC justifica la licitud sin hacer cuestión ni objeción de la libertad de disposición de sus datos por parte de los sujetos controlados.

Y en este sentido se observa un claro contraste con respecto a la exigencia de encuadramiento propio dentro de los principios de protección de datos que recoge la doctrina del Tribunal Europeo de Derechos Humanos en el asunto Barbulescu (Sentencia de 12 de enero de 2016, Barbulescu v. Rumania). El poder de control del empresario se justifica, según el Tribunal Europeo, a la luz de un doble criterio hermenéutico: en primer lugar, la expectativa de la intimidad y, en segundo lugar, la protección de datos. El TEDH parte de que la conducta de vigilancia y control de las comunicaciones electrónicas del trabajador implica recogida y tratamiento de datos personales. Por ello considera que es un comportamiento que cae dentro del concepto de protección de datos, y, por tanto, de la normativa de protección de datos. La determinación de la legitimidad del control de las comunicaciones electrónicas no puede prescindir de esta otra referencia.

La posición del TS y TC está, por tanto, en una perspectiva alejada de los principios de protección de datos a los que se conecta la vigilancia de las comunicaciones

36 Tesis que he mantenido, en diversos trabajos, entre otros: GOÑI SEIN, J. L. "Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos", *Justicia Laboral*, nº 39, 2009, pp. 19 y ss;

electrónicas de los empleados en la doctrina del Tribunal de Estrasburgo. Lo que resulta, además, poco comprensible y contradictorio si se compara con la video vigilancia en que el TC impone el efectivo cumplimiento de las reglas generales de protección de datos en los supuestos de vigilancia mediante videocámaras, señaladamente el deber de información previa (así en la STC 29/2013 y STC 39/2016).

En efecto, cuando el TC enjuicia la videovigilancia empresarial de los trabajadores no permanece encerrada en la única perspectiva de la intimidad sino que efectúa una ponderación más abierta, tomando en consideración la normativa de protección de datos, valorando incluso una Instrucción dictada por la Agencia Española de Protección de datos (Instrucción 1/2006). La no toma en consideración por parte del TS (en la STS 6.10.11 el justiciable invoca el derecho a la protección de datos y no recibe la más mínima respuesta) y del TC de este otro aspecto constitucional de la medida de control, cuando se trata de comunicaciones electrónicas carece de justificación, por cuanto todas las medidas indicadas de control empresarial comprometen la protección de datos. Como destaca el "Grupo de Trabajo" del art. 29 en su Dictamen 8/2001, de 13 de septiembre de 2001 sobre el "tratamiento de datos de carácter personal en el contexto profesional" (citado en la Sentencia Barbulescu), "las disposiciones relativas a la protección de datos se aplican a la vigilancia y control de los trabajadores, tanto en términos de utilización del correo electrónico, acceso a Internet, cámaras de video o datos de localización"[37].

Se perciben igualmente diferencias en lo que hace referencia a la política de la empresa en relación con las condiciones de uso de las herramientas informáticas y las medidas de control de la actividad de los trabajadores, en particular sobre el deber de información. Perplejidad absoluta suscita la doctrina establecida por el TC en la Sentencia 170/2013 (sin voto particular), según la cual una mera prohibición de uso personal de las herramientas de trabajo establecida en convenio colectivo se considera suficiente para legitimar el control de las comunicaciones electrónicas y de cualquier otro documento hallado en el ordenador o dispositivo facilitado al trabajador por la empresa. Se afirma en la sentencia que la tipificación, prevista en el convenio como falta leve, de la utilización de los medios informáticos de propiedad de la empresa para fines distintos de los relacionados con la prestación laboral, aun sin advertencia previa alguna, impide albergar expectativa razonable de privacidad.

Tal conclusión resulta criticable, ante todo, porque entraña el riesgo de vaciar el derecho fundamental a la intimidad del trabajador en el contexto de las nuevas tecnologías, de un contenido aplicativo identificable. No puede atribuirse al convenio o a la empresa una facultad de determinación tan amplia, que degrade

37 Así también la AEPD Resolución R/01755/2013: *"la actuación de una empresa de filtrar, controlar y acceder al contenido de una cuenta de correo electrónico corporativa, aún en el sentido del artículo 20.3 del Estatuto de los Trabajadores aprobado por el Real Decreto Legislativo 1/1995, de 24 marzo (ET), supone un tratamiento de datos"*

a mero protocolo, carente de una incidencia real y un alcance efectivo, el derecho a la intimidad en el ámbito del control laboral. Incluso en la hipótesis de una prohibición absoluta, cabe invocar este derecho, pues el empresario no pueda abusar de las facultades de control, comprometiendo, más allá de los límites razonables, la sujeción del trabajador. La prohibición de uso personal no le confiere el empresario un derecho a realizar controles indiscriminados, abusivos o tendentes a obtener unos perfiles específicos de la persona.

Al margen de ello la doctrina del TC tropieza con un principio básico en materia de protección de datos, cual es el de información previa o de transparencia (art. 5 LOPD) que aparece notablemente reforzado en el Reglamento 679/2016, de 27 de abril de la UE, al configurarse como derecho del interesado y no como obligación del responsable e incrementar, en los apartados 1 y 2 del art. 13 del Reglamento, respecto de la Directiva 95/46, la información que habrá de facilitarse.

No se debe olvidar que el acceso a las conversaciones electrónicas, aun cuando se consideren realizadas en nombre de la empresa y, por tanto, revistan carácter profesional, constituyen también un tratamiento de datos del trabajador a efectos de aplicar la normativa de protección de datos, en la medida en que dichos instrumentos memorizan información y datos personales del trabajador susceptible de ser tratados. La doctrina constitucional, al observar que con la prohibición convencional de uso personal decae la necesidad de una información previa a los trabajadores, autoriza a inferir que el empresario en su actividad de control empresarial no está obligado a cumplir determinadas exigencias de la normativa de protección de datos. Esto es, que la falta de información previa no es óbice para la validez y eficacia del acto de intervención en el proceso de comunicación.

Sin embargo, esto no es lo que emerge de la Sentencia del TEDH en el asunto Barbulescu, ni de los principios de protección de datos. La Sentencia Barbulescu condiciona la legitimidad del control a un requisito procedimental básico, cual es la información previa. En efecto, aun cuando en la sentencia se establece una doctrina incierta y llena de lagunas sobre el alcance sobre las medidas de control de la actividad laboral en las comunicaciones electrónicas, lo cierto es que la jurisprudencia del Tribunal Europeo parece haber acogido, al menos, la necesidad de establecer una información previa sobre la política de uso de los medios informáticos, esto es, la obligación de comunicar a los trabajadores la política de uso profesional o personal de Internet y en general de los instrumentos de comunicación electrónica.

Hay que tener en cuenta que la información previa posee una relevancia decisiva por cuanto, como indica el propio TC en la Sentencia 29/2013 “este deber permite al afectado ejercer los derechos de acceso, rectificación, cancelación y oposición y conocer la dirección del responsable del tratamiento o en su caso, del representante (art. 5 LOPD)”. El art. 5.1 de la LOPD exige que se informe de “modo expreso, preciso e inequívoco”. Y en una línea más contundente, el nuevo

Reglamento establece que a la persona física le "debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados"(Considerando 39). No se puede seguir, por tanto, manteniendo que sea suficiente con una genérica prohibición de uso personal de los medios informáticos establecida en el convenio colectivo aplicable, para entender cumplido el deber de informar. Eso hace irreconocible el derecho a la transparencia del trabajador.

Por otra parte, e independientemente de garantizar a los trabajadores el conocimiento y de proporcionarles el control de su información digital, hay otro elemento clave en el deber de información, que no debe pasar desapercibido, cual es la seguridad. El aumento de la ciberdelincuencia se ha identificado como una cuestión crítica que compromete el desarrollo de los servicios en Internet. La empresa debe preservar, junto la privacidad, el secreto y la seguridad de los datos personales, sean de trabajadores o de clientes o de quienes accedan o pasen por la empresa, adoptando las medidas técnicas y organizativas imprescindibles para evitar el mal uso, la alteración, el acceso no autorizado o el robo de los datos facilitados. En este sentido es preciso recordar que el art. 89 del Real Decreto 1720/2007 (Reglamento de Protección de Datos) obliga al responsable (empresa) a establecer en el Documento de Seguridad, claramente definidas, las funciones y obligaciones de cada uno de los usuarios con acceso a datos personales y a los sistemas de información, y además a que sus empleados conozcan dichas normas de seguridad y de las consecuencias de su incumplimiento.

No se puede trasladar la idea de que basta con que el convenio colectivo establezca una prohibición de uso personal para que se legitime cualquier registro de las conversaciones o de los correos, porque eso supone trivializar el principio de seguridad, que es clave en la protección de datos personales. En una organización debe haber una clara y explícita política de privacidad y de seguridad, de forma que todo el personal conozca los términos de uso y de control de las herramientas informáticas y tecnológicas que maneja cada cual. No cabe configurar una verdadera política de seguridad de una empresa desde meras generalidades o cláusulas convencionales.

5.2. VIGILANCIA POR MEDIO DE CÁMARAS

Los límites a la utilización de las cámaras de vídeo en la vigilancia empresarial constituye otro de los grandes puntos de controversia en materia de control empresarial, La evolución interpretativa de la doctrina de los tribunales, y especialmente la del TS y Tribunal Constitucional, es hacia una mayor consideración de los derechos fundamentales y señaladamente del derecho de protección de datos, aunque en su última resolución el TC parece haber retrocedido en sus posiciones garantistas.

Durante mucho tiempo, los tribunales estuvieron aplicando un criterio muy permisivo respecto del uso de la videovigilancia en la relación laboral. Esa posibilidad se consideraba enmarcada dentro de las facultades de control del empresario del art. 20.3 ET y apenas conocía límites en nuestra jurisprudencia. La instalación de cámaras era una práctica empresarial tolerada por los tribunales en las dependencias donde se desarrollaba la actividad laboral, salvo en los lugares de aseo, descanso o comedores.

A partir de las SSTC 98/2000 y 186/2000 empezó a hablarse de límites al uso de la videovigilancia en el lugar de trabajo y se establece el principio de proporcionalidad. En la primera de las sentencias se analiza la instalación con conocimiento de los trabajadores y del comité de empresa de micrófonos (vigilancia auditiva) en las dependencias del Casino de la Toja (vigilancia en el puesto de trabajo), que permitía la audición continuada e indiscriminada de todo tipo de conversaciones tanto de los propios trabajadores, como de los clientes. El TC, después de desechar la concepción espacial de la intimidad y hacer un reconocimiento general del derecho a la intimidad "en el ámbito del desempeño de las tareas profesionales", establece que la adopción de las medidas de vigilancia audio-visual debe quedar sujeta al estrecho margen que impone el criterio de lo estrictamente necesario para garantizar el interés empresarial merecedor de tutela, y rechaza la instalación microfónica adoptada por la empresa, por considerarla una intromisión ilegítima en el derecho a la intimidad, al no quedar acreditado que el uso de las micrófonos resultase indispensable para la seguridad y el buen funcionamiento del casino, que ya contaba con un sistema de cámaras.

En la segunda sentencia (STC 186/2000) se enjuicia el caso de la instalación de cámaras ocultas para controlar una zona concreta (las cajas registradoras y el mostrador de paso de mercancías) de un economato, donde las trabajadoras prestaban su actividad laboral, ante las sospechas de hurto que se venían produciendo, con el objeto de obtener la confirmación y prueba del ilícito. El TC declara que la legitimidad se debe determinar en función de la superación del triple test de proporcionalidad –juicio de idoneidad, necesidad y de proporcionalidad en sentido estricto– ya comentado anteriormente. En este sentido el TC consideró que la medida de instalación de un circuito cerrado de televisión era una medida ajustada al principio de proporcionalidad y, por tanto, legítima, ya que no resultaba arbitraria, ni caprichosa, sino que se trataba de "verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes"; era además, necesaria, "ya que la grabación serviría de prueba de tales irregularidades, pues la grabación de imágenes se limitó a la zona de la caja y a una duración limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada".

El panorama jurisprudencial descrito experimenta, sin embargo, un cambio, a raíz de la STC 29/2013, de 11 de febrero, en que se adopta un nuevo enfoque de

análisis. El Tribunal Constitucional empieza a enjuiciar el uso de las cámaras de video-vigilancia desde la perspectiva de los principios de protección de datos. En ella se juzga la validez de la prueba videográfica aportada por la empresa (Universidad de Sevilla) para acreditar el incumplimiento horario de un empleado y para sancionarle. El trabajador firmaba las hojas de control de entrada y salida en horarios muy distintos a los que correspondían en realidad, y la Universidad, para acreditar dicho incumplimiento, se sirvió de las grabaciones videográficas efectuadas por varias cámaras, que tenía instaladas para controlar los accesos al recinto con la debida señalización y advertencia públicas. El Tribunal Constitucional no admite esa prueba videográfica, porque considera que las imágenes grabadas mediante las cámaras de vídeo-vigilancia instaladas en el recinto universitario eran utilizadas para un fin (la supervisión laboral) distinto al expresamente declarado, sin haber advertido a los trabajadores de que esas imágenes podían ser utilizadas a efectos del control laboral-, lo cual vulnera el art. 18.4 CE, y, en consecuencia, procede a anular las sanción de suspensión de empleo y sueldo durante tres meses impuesta al trabajador.

En dicha Sentencia, el Tribunal Constitucional realiza varias declaraciones muy importantes, a saber: 1.- "*Está fuera de toda duda que las imágenes grabadas en un soporte físico, (…) constituyen un dato de carácter personal que queda integrado en la cobertura del art. 18.4 CE, ya que el derecho fundamental amplía la garantía constitucional a todos aquellos datos que identifiquen o permitan la identificación de la persona (…), lo cual, como es evidente, incluye también aquellos que facilitan la identidad de una persona física por medios que, a través de imágenes, permitan su representación física e identificación visual u ofrezcan una información gráfica o fotográfica sobre su identidad*". 2.- La "*captación de las imágenes de las personas constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa*" de protección de datos (LOPD), 3.- Un "*elemento caracterizador de la definición constitucional del art. 18.4 CE, de su núcleo esencial,* (es) *el derecho del afectado a ser informado de quién posee los datos personales y con quién*". 4.- "*No hay una habilitación legal expresa para (la) omisión del derecho de información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales, y que tampoco podría situarse su fundamento en el interés empresarial de controlar la actividad laboral a través de sistemas sorpresivos o no informados de tratamiento de datos que aseguren la máxima eficacia en el propósito de vigilancia. Esa lógica fundada en la utilidad o conveniencia empresarial haría quebrar la efectividad del derecho fundamental, en su núcleo esencial*". Desarrollando el iter argumental expuesto, el TC concluye afirmando que el deber de información previa en el uso de las cámaras en el lugar de trabajo no se satisface solo con la colocación del cartel distintivo y la notificación de la creación del fichero a la Agencia española de Protección de Datos, sino que requiere además "*la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral*

a la esta captación podía ser dirigida", y, al no haber constancia de ello, rechaza la prueba vidográfica[38].

Con posterioridad, el TC ha vuelto sobre la cuestión controvertida y ha fijado en la STC 39/2016, de 3 de marzo, adoptada en Pleno, un nuevo criterio que viene a recortar el alcance indiscutible que había adquirido la exigencia relativa al deber de información previa del art. LOPD en el pronunciamiento anterior[39]. La Sentencia trata sobre la validez de la grabación de vídeo aportada por la empresa (una conocida marca de tiendas, Bershka de INDITEX) para justificar el despido de una trabajadora que fue sorprendida, mediante cámaras instaladas al efecto y con distintivo informativo, apropiándose dinero y realizando, para ocultar dicha apropiación, operaciones falsas de devolución de venta de prendas. La recurrente en amparo considera vulnerado el art. 18.4 CE porque, si bien tenía conocimiento de la existencia de las cámaras de vídeovigilancia, no había sido informada previamente de la misma en los términos de la doctrina contenida en la STC 29/2013, esto es, de una manera expresa, precisa, clara e inequívoca a los trabajadores sobre la captación de imágenes, su finalidad de control de la actividad laboral y su posible utilización para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo.

El núcleo del problema se contrae, así, a determinar si es suficiente la información general o, por el contrario, debe existir una información específica. Frente a la tesis sostenida en la STC 29/2013 de la exigibilidad de una información específica sobre la finalidad de control de la actividad laboral y posible uso para la imposición de sanciones, el TC declara que basta con que los trabajadores tengan conocimiento genérico de la existencia de las cámaras de vídeo a través del distintivo informativo conforme a lo dispuesto en la Instrucción 1/2006 de la AEPD, que obliga a incorporar una referencia a la LOPD, a la finalidad para la que se tratan los datos ("Zona videovigilada") y a la identificación del responsable ante quien puedan ejercitarse los derechos del art. 15 y ss. de la LOPD. Y sentado lo anterior resuelve que en el caso enjuiciado no hubo vulneración del art. 18.4 CE, porque la trabajadora podía conocer mediante el correspondiente

38 La doctrina del Tribunal Constitucional se aplica en la STS de 13 de mayo de 2014, rec. 1685/2013, que declara asimismo vulnerado el derecho fundamental del art. 18.4 CE, en un caso de utilización no consentida ni previamente informada de un sistema de cámaras de videovigilancia de carácter permanente para sancionar a una cajera de un supermercado (Champion) por no registrar ni cobrar ciertos productos retirados por su pareja, cuando la finalidad declarada era la de evitar robos por parte de los clientes. El TS confirma la nulidad del despido de la trabajadora, porque no se dio información a la trabajadora sobre la posibilidad de su uso con fines de control laboral y por cuanto el mero hecho del conocimiento de la existencia de las cámaras de grabación no puede comportar la consecuencia de entender que podía utilizarse para el control de la actividad laboral. Un sector doctrinal DESDENTADO BONETE A. y MUÑOZ RUIZ, A.B., "Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia", *Revista General del Derecho del Trabajo y de la Seguridad Social,* nº 39 (2014), p. 15. se ha mostrado crítico con la aplicación de la misma solución por considerar que existe una diferencia importante con la STC 29/2013: mientras en ésta se trataba de un incumplimiento laboral, en la analizada por el TS la acción captada es de naturaleza penal. Vid. la STSJ de Madrid de 16 de febrero de 2015, rec. 935/2014.

39 Vid. D. TOSCANI GIMÉNEZ, "Las facultades de la empresa de videovigilancia de sus trabajadores. Comentario a la STC 39/2016, de 3 de marzo", *Revista de Derecho Social,* nº 74, pp. 163 y ss.

distintivo colocado en el escaparate de la tienda donde trabajaba la existencia de las cámaras y la finalidad para la que habían sido instaladas. Por otra parte, tampoco aprecia vulneración del art. 18.1 CE igualmente invocada por la recurrente en amparo, porque considera que la medida de instalación de cámaras de seguridad para el control de la zona de caja era, de acuerdo con la doctrina de la STC 186/2000, una medida justificada, idónea, necesaria y equilibrada.

La nueva orientación derivada de la STC 39/2016, aunque persiste en proclamar la necesidad de analizar la utilización de las imágenes obtenidas de cámaras de video en el ámbito laboral desde la perspectiva de la tutela constitucional del art. 18.4 CE, convierte el requisito esencial del deber de información previa del derecho fundamental del art. 18.4 CE en un puro formalismo, garantizando al trabajador un reconocimiento meramente nominal del derecho fundamental de protección de datos. Porque entender, como hace la Sentencia, que el deber de información se cumple suficientemente con los requisitos de la Instrucción 1/2006, de 8 de noviembre de la Agencia española de Protección de Datos, sobre tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, es decir, advirtiendo mediante un cartel distintivo de la existencia de cámaras en el establecimiento, equivale, como destaca el Magistrado Xiol Rios en su voto particular, a hacer ineficaz, carente de sentido práctico e irreconocible el derecho fundamental a la protección de datos, porque hace que la colocación de un cartel distintivo facultaría a la empresa para grabar imágenes de la actividad laboral del trabajador y servirse de las mismas para acreditar cualquier incumplimiento o comportamiento.

Respecto de lo razonado por la sentencia, es preciso realizar algunas puntualizaciones:

De entrada, resulta llamativo que el Supremo Intérprete Constitucional acoja sin más, sin hacer un juicio previo de ajuste constitucional, como "parámetro o canon de constitucionalidad" del tratamiento de datos derivado de la vigilancia por medio de cámaras de vídeo, la referida Instrucción 1/2006 de la AEPD; el TC da carta de naturaleza a un texto que no deja de ser una instrucción y que, en la medida en que delimita un componente básico de un derecho fundamental, reclama una mínima valoración a la luz de los principios constitucionales de reserva de ley que establece nuestra Constitución[40] y de los del art. 5 LOPD.

En segundo lugar, la suficiencia de la mera colocación de un cartel anunciador con las menciones contenidas en el ANEXO que exige la Instrucción 1/2016, si bien resulta admisible cuando se trata de instalación de videocámaras dirigidas a público general, porque se está ante un control cuyo destino es un colectivo desconocido, no parece aceptable en el caso de los trabajadores. No hay razón alguna para que el deber de información no se cumpla, como en los demás pro-

40 VILLALBA SÁNCHEZ, A., "Los derechos fundamentales del trabajador frente a los nuevos instrumentos de control empresarial", *Revista de Derecho Social y empresa,* , nº 6, 2016, p. 12

cedimientos de recogida de datos del trabajador por el empresario, ajustándose al cumplimiento íntegro de los requisitos exigidos por el art. 5 LOPD, entre los cuales se cuenta el deber de informar al interesado sobre la existencia del tratamiento de datos, la finalidad para la que se recogen y los destinatarios de la información, así como las consecuencias de la obtención de los datos o de su negativa a suministrarlos y la identidad y dirección del responsable del tratamiento.

En tercer lugar, la validez otorgada a la mera instalación de un cartel puede llevar a justificar la instalación permanente de las cámaras de vídeo para fines indeterminados[41], incluido el control directo de los propios trabajadores. Sin embargo, no parece que, en la instalación de las cámaras de vídeo en el lugar de trabajo, pueda prescindirse de un análisis objetivo de la concurrencia de un interés justificado en cada caso. Nótese que el TC, la OIT, el "Grupo del Artículo 29" de la UE, o la propia AEPD, tienen establecido que no cabe, como regla general, el control directo e indiscriminado sobre los trabajadores. En las SSTC 98/2000 y 186/2000 se señala que el uso de estos medios no puede justificarse en "*la mera utilidad o conveniencia para la empresa*", ni emplearse para un propósito de vigilancia y control genérico del cumplimiento laboral; el "Grupo del Artículo 29" de la UE, en su Dictamen 4/2004 afirma que "*por regla general no debe estar permitida la video vigilancia para el control directo de los trabajadores*"; y la propia Instrucción 1/2006 señala que "*se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de la persona*".

Por lo demás, entiendo que la nueva doctrina crea más problemas que soluciones interpretativas. Comparto la afirmación hecha en el primer voto particular por los Magistrados Fernando Valdés y Adela Asúa, "*de que los diversos intereses legítimos y constitucionales, enfrentados en este concreto conflicto, pudieron quedar perfectamente garantizados sin el sacrificio que la presente Sentencia lleva a cabo respecto de los derechos involucrados en el art. 18.4 CE de titularidad de quienes prestan un trabajo por cuenta ajena y dependiente*". Ciertamente no era necesario introducir recortes en la doctrina general sobre el deber de información sentada en la STC 29/2013, para resolver el caso planteado en esta sentencia. Se trata de un supuesto muy parecido al de la STC 186/2000, y se podía haber resuelto aplicando la doctrina establecida en ella, y si acaso precisando un poco más algunos aspectos del razonamiento jurídico de esta sentencia que han dado pie a interpretaciones poco ajustadas a la misma[42].

41 En esta línea el TS está admitiendo la validez de las pruebas de video vigilancia utilizadas para justificar el despido de los trabajadores, a pesar de presentar defectos informativos: SSTS de 31 de enero de 2017, rec. 3331/2015; 1 de febrero de 2017, rec. 3252/2015; 2 de febrero de 2017, rec. 554/2016.

42 Los Tribunales ordinarios han aplicado esta doctrina también a la instalación de cámaras con carácter permanente en el lugar de trabajo y con justificación bastante distinta a la de la STC 186/2000. Vid. las STSJ de Andalucía (Sevilla) 9 de marzo de 2001, STSJ de 22 de diciembre de 2005, rec. 5549/2005, STSJ Castilla y León (Valladolid) de 18 de septiembre de 2006, rec. 1479/2006, STSJ de Madrid de 17 de abril de 2009, rec. 5665/2008, STS Andalucía (Granada) de 25 de enero de 2012, rec. 2924/2011 o del TSJ de Asturias de 14 de diciembre de 2012, rec. 2691/2012. TALENS VISCONTI, E., "Observatorio temático de jurisprudencia Vídeovigilancia en el trabajo: una vuelta a la jurisprudencia clásica", *Trabajo y Derecho,* nº 21, 2016

La sentencia TC 39/2016 resuelve en el fondo de la misma manera que aquella, enjuiciando a la luz del triple test de proporcionalidad y utilizando la misma argumentación en cuanto a la no vulneración del derecho a la intimidad. Con ese solo enjuiciamiento tal vez hubiera bastado para decidir sobre la licitud de las cámaras instaladas para la obtención de pruebas de unos hechos ilícitos antes las sospechas existentes. Al entrar en otro tipo de consideraciones relacionadas con los principios de protección de datos, el TC ha venido a establecer una doctrina regresiva y perjudicial para ambas partes de la relación laboral:

Por una parte, respecto de los trabajadores, representa una "devaluación" del contenido del derecho a la información consagrado en la STC 29/2013, en cuanto al derecho a saber en qué casos las grabaciones pueden ser examinadas, durante cuánto tiempo y con qué propósitos y si pueden llegar a ser utilizados para imponer sanciones disciplinarias. En realidad se priva, como bien observa el Magistrado Preciado Domenech, al interesado de la necesaria información clara, precisa y específica que es contenido esencial del derecho de protección de datos y presupuesto del ejercicio de los derechos ARCO;[43]. Este derecho de información ahora, ya no será invocable por el trabajador a la hora de instalar una videocámara por el empresario. Aunque este escenario es difícil de mantener a la luz del Reglamento 679/2016, porque refuerza aun más el deber del responsable de tratamiento de datos, exigiendo en todo caso que queden totalmente claras las condiciones de tratamiento de los datos personales, dando cuenta de los fines a que se destinan los datos personales y de la existencia en su caso de las decisiones automatizadas como la elaboración de perfiles.

Y, por otra parte, resulta también regresiva para los empresarios, porque parece introducir un nuevo requisito procedimental en relación con la adopción de medidas de videovigilancia empresarial ante sospechas de ilícitos graves, no previsto en la STC 186/2000, cual es el deber de información previa de la existencia de las cámaras de vídeo mediante los referidos carteles distintivos, toda vez que justifica la licitud de la instalación de las cámaras desde la observancia del derecho de información previa. En este sentido señala el TC que "*Se ha cumplido en este caso con la obligación de información previa pues basta a estos efectos con el cumplimiento de los requisitos específicos de información a través del distintivo, de acuerdo con la Instrucción 1/2006*". Pero cabe preguntarse si en tales casos es verdaderamente necesario informar de la instalación de las cámaras de vídeo. Desde luego, es obvio que como regla general debe cumplirse con tal requisito de transparencia informativa (art. 5 LOPD), pero no parece que tenga mucho sentido cuando tiene por objeto, como ocurre en el caso enjuiciado en la sentencia, acreditar un ilícito laboral por determinada persona de la que se tienen sospechas, y no exista otro medio alternativo de obtención de una prueba de tales ilícitos. El previo aviso haría prácticamente inútil la medida de control

43 PRECIADO DOMÉNECH, C. H., "La video vigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal", *Revista de Derecho Social* nº 77, enero-marzo, 2017, p. 165

audiovisual, y "*dejaría* –como ha señalado Falguera[44]– *en la práctica indefensa*" a la empresa. En consecuencia, no se debe descartar por completo la posibilidad de instalación de cámaras ocultas. La OIT en el Repertorio de Recomendaciones Prácticas de Protección de los datos personales de los Trabajadores (Punto 6.4.2) lo admite, pero solo "*cuando existan sospechas suficientes de actividad delictiva y otras infracciones graves*". Lo interesante hubiera sido que el TC nos hubiera arrojado algo de luz en esta sentencia sobre los motivos razonables de sospecha que pueden dar lugar a la lícita instalación de cámaras ocultas en el lugar de trabajo[45].

44 Vid. FALGUERA BARÓ, M.A., "Nuevas tecnologías y trabajo (II): perspectiva constitucional", cit., p. 51.

45 Sobre el tema, vid. GOÑI SEIN, J.L., *La videovigilancia empresarial y la protección de datos personales*, Thomson/Civitas APDCM, Pamplona, 2007, pp. 129 y ss.