

PRIVACIDAD Y DATOS PERSONALES DE LOS TRABAJADORES: CONVERGENCIA DE LAS SOLUCIONES LEGISLATIVAS Y JURISPRUDENCIALES EN EUROPA

PRIVACY AND PERSONAL DATA PROTECTION OF WORKERS:
CONVERGENCE OF LEGAL AND JUDICIAL SOLUTIONS IN
EUROPE

DAVID ORDÓÑEZ SOLÍS

Magistrado

Red de Especialistas en Derecho de la Unión Europea (REDUE)

Comisión Iberoamericana de Ética Judicial

d.ordonez@poderjudicial.es

RESUMEN

Los trabajadores también tienen derecho a que en su relación laboral se respete su vida privada y se protejan sus datos personales. Como si fuese una carrera frente a unas tecnologías cada vez más invasivas, la legislación y, en particular, la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea están aportando soluciones. La legislación europea, especialmente a partir de la aplicación del Reglamento General de Protección de Datos, resulta de gran importancia y así se deduce de la aprobación de leyes nacionales complementarias. En la aplicación de este marco normativo, integrado por normas europeas y nacionales, los tribunales deben tener en cuenta esta retroalimentación entre legislación y jurisprudencia en un ámbito donde se deja en manos de los jueces la tarea de garantizar adecuadamente el equilibrio de los derechos en juego del trabajador y del empleador.

Palabras clave: nuevas tecnologías, empleador, trabajador, derecho a la vida privada, derecho a la protección de datos, Tribunal Europeo de Derechos Humanos, Tribunal de Justicia de la Unión Europea, tribunales nacionales.

ABSTRACT

Workers are entitled to protect their rights in the working relations, notably the right to privacy and the right to protect their personal data. As a competition facing the new technologies' intrusion, European legislation and case-law, notably the European Court of Human Rights and the Court of Justice of the European Union, are focused on these issues. Especially after the entry into force of the General Data Protection Regulation, European legislation is of great interest in order to adopt complementary national norms. When implementing this legal framework, composed of European and national laws, national Courts must understand this feed-back between legislation and case-law where judges are committed to strike a fair balance between workers' and employers' rights at stake.

Keywords: new technologies, worker, employer, right to privacy, right to personal data protection, European Court of Human Rights, Court of Justice of the European Union, National Courts.

RESUMO

Os traballadores tamén teñen dereito a que na súa relación laboral se respecte a súa vida privada e se protexan os seus datos persoais. Como se fose unha carreira fronte a unhas tecnoloxías cada vez máis invasivas, a lexislación e, en particular, a xurisprudencia do Tribunal Europeo de Dereitos Humanos e do Tribunal de Xustiza da Unión Europea están a achegar solucións. A lexislación europea, especialmente a partir da aplicación do Regulamento xeral de protección de datos, resulta de gran importancia e así se deduce da aprobación de leis nacionais complementarias. Na aplicación deste marco normativo, integrado por normas europeas e nacionais, os tribunais deben ter en conta esta retroalimentación entre lexislación e xurisprudencia nun ámbito onde se deixa en mans dos xuíces a tarefa de garantir adecuadamente o equilibrio dos dereitos en xogo do traballador e do empregador.

Palabras chave: novas tecnoloxías, empregador, traballador, dereito á vida privada, dereito á protección de

datos, Tribunal Europeo de Derechos Humanos, Tribunal de Xustiza da Unión Europea, tribunais nacionais.

1. INTRODUCCIÓN. INTIMIDAD, PRIVACIDAD Y TRABAJADORES EN UN CONTEXTO TECNOLÓGICO AVANZADO

La aparición de nuevas tecnologías ha facilitado una alarmante invasión de la vida privada de las personas hasta el punto de haber acelerado, en respuesta, la creación de un nuevo derecho fundamental, complementario del derecho a la privacidad, como es la protección de los datos personales.

En el ámbito laboral la aplicación de este nuevo derecho fundamental ha venido matizado por la necesidad de tener en cuenta la especial relación que se produce entre empleador y empleado que, en realidad, puede exigir una ponderación apropiada de los intereses en juego. Esta relación especial debilita, en gran medida, la eficacia del consentimiento del trabajador para el tratamiento de los datos personales por el empleador, pero no exime a este de respetar un ámbito íntimo del trabajador y lo somete a un procedimiento de información y de justificación de la intromisión en su vida privada.

En estos momentos resulta relevante comprobar cómo se producen los cambios en la formulación constitucional, en la adopción de normas legislativas y, en fin, en las soluciones jurisprudenciales adoptadas. Para ello sería importante tomar como referencia la experiencia española, desarrollada en el marco europeo, donde se intentan cumplir las obligaciones europeas sobre privacidad y protección de datos en el ámbito laboral y ver cómo los tribunales, en particular el Tribunal Constitucional y los tribunales de lo social y de lo contencioso-administrativo, tratan de establecer parámetros claros de actuación.

En la primera parte, examino la regulación de la Unión Europea y su aplicación normativa en España; y en la segunda parte explico cuál ha sido el alcance de las intervenciones de los tribunales europeos, del Tribunal Europeo de Derechos Humanos y del Tribunal de Justicia de la Unión Europea, y la actitud de los tribunales españoles.

2. LA REGULACIÓN DE LA PROTECCIÓN DE LA VIDA PRIVADA Y LOS DATOS PERSONALES DE LOS TRABAJADORES EN LA UNIÓN EUROPEA Y EN ESPAÑA

El Consejo de Europa estableció en 2015 unos principios aplicables tanto al empleo privado como al público basados en la dignidad humana y los derechos y libertades fundamentales, al tiempo que marcaba las pautas a empleadores y trabajadores en cuanto a almacenamiento de los datos, a su uso interno, a su comunicación, a su transmisión, a los datos sensibles de los trabajadores o a las formas particulares de procesamiento de los datos (uso de Internet y comunicaciones electrónicas, videovigilancia y control, localización, datos biométricos, etc.)¹.

El 25 de mayo de 2018 entró en vigor el Reglamento General de Protección de Datos (RGPD)² que se aplica en todos los ámbitos excepto en el penal donde rige la regulación especial de la Directiva (UE) 2016/680 que debía incorporarse a las legislaciones nacionales y entrar en vigor el 6 de mayo de 2018³.

En España y hasta ahora la única medida legislativa que completa el RGPD es la Ley española de protección de datos personales y garantía de los derechos digitales, en vigor

¹ Comité de Ministros del Consejo de Europa (2015). [*Recommendation CM/Rec \(2015\) 5 on the processing of personal data in the context of employment*](#), 1 de abril de 2015, at the 1224th meeting of the Ministers' Deputies), Estrasburgo.

² Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (*DOUE* nº L 119, 4.5.2016, p. 1).

³ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (*DOUE* nº L 119, 4.5.2016, p. 89).

desde el 7 de diciembre de 2018⁴. En cambio, la Directiva de protección de datos en el ámbito penal sigue pendiente de transposición en España⁵.

En cuanto se refiere a la protección de la vida privada y los datos personales de los trabajadores habrá que estar al marco normativo establecido por el RGPD que, no obstante, confía en una colaboración de los legisladores nacionales, mediante leyes y otras normas, y de los interlocutores sociales, a través de regulaciones convencionales.

2.1. LA REGULACIÓN EUROPEA Y SU APLICACIÓN EN EL ÁMBITO LABORAL A PARTIR DE 2018

El RGPD se refiere expresamente a la regulación normativa o convencional del tratamiento de los datos personales de los trabajadores en el ámbito la laboral y ofrece una enumeración de ámbitos afectados que reproduce extensamente tanto en sus considerandos como en la parte dispositiva.

Así, en su considerando 155 el RGPD hace referencia a los ámbitos en los que pueden operar las normas y los convenios colectivos, a saber, «en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del

⁴ Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPD 2018) (BOE núm. 294, de 06/12/2018).

⁵ El 25 de julio de 2019 la Comisión Europea inició un procedimiento por incumplimiento contra España y pidió al Tribunal de Justicia de la Unión Europea «que imponga sanciones financieras en forma de una suma a tanto alzado de 21.321 euros al día entre el día posterior al vencimiento de la fecha límite del plazo de transposición que se establece en la Directiva y la fecha de cumplimiento por parte de España, o bien la fecha de pronunciamiento de la sentencia prevista en el artículo 260, apartado 3, del TFUE, con un importe mínimo a tanto alzado de 5.290.000 euros y una multa diaria de 89.548,20 euros desde el día de la primera sentencia hasta alcanzar el pleno cumplimiento o hasta la segunda sentencia del Tribunal» (véase el comunicado de prensa en [IP/19/4261](https://ec.europa.eu/commission/presscorner/detail/es/IP/19/4261)). El recurso por incumplimiento fue interpuesto ante el Tribunal de Justicia el 4 de septiembre de 2019, Comisión Europea / España, C-658/19.

consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral».

El artículo 88 RGPD se refiere al tratamiento en el ámbito laboral y, en esencia, reconoce la facultad de las autoridades nacionales para adoptar, mediante disposiciones legislativas o convenios colectivos, «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, 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».

El artículo 88.2 RGPD se refiere a los límites que se imponen a tales regulaciones del modo siguiente:

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.

El artículo 9.2.h) RGPD consagra una excepción a la prohibición del tratamiento de datos personales relativos a la salud cuando:

el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

En el artículo 9.3 RGDP se permite este tratamiento cuando sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes.

La Comisión Europea ha impulsado, primero a través del Grupo de Trabajo sobre Protección de Datos del Artículo 29 y ahora a través de la Comité Europeo de Datos Personales, el examen de la dimensión laboral de la privacidad y de la protección de datos personales.

En el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de 8 de junio de 2017, el Grupo del Artículo 29 «reevalúa el equilibrio entre los intereses legítimos de los empresarios y las expectativas razonables de privacidad de los trabajadores, describiendo los riesgos que plantean las nuevas tecnologías y evaluando la proporcionalidad de una serie de escenarios en los que podrían aplicarse»⁶.

A tal efecto, el Dictamen 2/2017 realiza un examen de los escenarios donde estarían en juego los derechos de los trabajadores, en particular, el tratamiento de datos personales durante el proceso de selección (consulta de perfiles disponibles de Internet), los derivados del examen en el empleo, la vigilancia del uso de las nuevas tecnologías de la información en el lugar de trabajo y fuera de él, el

⁶ En este dictamen se hace referencia a *Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral*, WP48, 13 de septiembre de 2001, y al *Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo*, WP55, 29 de mayo de 2002.

empleo del tiempo y la presencia en el trabajo, la videovigilancia, el control de vehículos de la empresa utilizados por el trabajador (a través del GPS, de vídeos, etc.), la comunicación de los datos de los trabajadores a terceros (por ejemplo, facilitando la foto del repartidor a los clientes) o las transferencias internacionales de estos datos. En este Dictamen 2/2017 del Grupo del Artículo 29 se subraya reiteradamente la escasa operatividad del consentimiento de trabajador para que su empleador utilice sus datos porque: «Los trabajadores casi nunca están en condiciones de dar, denegar o revocar el consentimiento libremente, habida cuenta de la dependencia que resulta de la relación empresario/trabajador. Dado el desequilibrio de poder, los trabajadores solo pueden dar su libre consentimiento en circunstancias excepcionales, cuando la aceptación o el rechazo de una oferta no tiene consecuencias» (apartado 6.2).

En definitiva, desde la perspectiva europea se han apuntado los problemas más específicos de la protección de la privacidad y de los datos personales de los trabajadores, al tiempo que se encomienda a los legisladores nacionales y a los interlocutores sociales su regulación específica.

2.2. LA REGULACIÓN ESPAÑOLA APLICABLE EN MATERIA LABORAL

La Constitución española de 1978 adivinó la importancia de las nuevas tecnologías pero sólo dejó apuntada la necesidad de regular tal cuestión: «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».

El ordenamiento constitucional español contiene una versión limitada o embrionaria del derecho a la protección de datos personales al referirse al derecho a la intimidad personal y familiar en estos términos: «Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen». En 1978 era difícil aventurar la deriva que tendría el vertiginoso desarrollo tecnológico y sus efectos en la vida privada de los ciudadanos.

En todo caso, la legislación española ha ido a remolque de la armonización legislativa europea a partir de la Directiva 95/46/CE y, desde luego, a partir de la unificación legislativa llevada a cabo a partir de 2018 por el RGPD.

En estos momentos la Ley española de protección de datos personales y garantía de los derechos digitales (2018) ha consagrado una serie de derechos de gran interés en el ámbito laboral referidos al uso de dispositivos digitales, el derecho a la desconexión digital, el uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo o los sistemas de geolocalización.

Los derechos consagrados se aplican a todo tipo de trabajadores y empleados públicos. De hecho, la Ley de 2018 modifica simultáneamente el Estatuto de los Trabajadores y el Estatuto Básico del Empleado público con la misma finalidad.

La propia Ley de 2018 modifica el Estatuto de los Trabajadores, añadiendo un artículo 20bis, con el fin de introducir una regulación específica de los derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.

También la Ley de 2018 modifica el Estatuto Básico del Empleado Público con el fin de consagrar, en el artículo 14.jbis), 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».

En primer lugar y por lo que se refiere al uso de dispositivos digitales, el artículo 87 reconoce el derecho a la protección de la intimidad frente a ellos y al empleador. No obstante, prevé el acceso del empleador «a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos».

Este acceso exige de los empleadores que establezcan «criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de

protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores». También se prevé la necesidad de especificar los usos autorizados y exige que se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Asimismo, la Ley española dispone: «los trabajadores deberán ser informados de los criterios de utilización».

El artículo 88 proclama el derecho a la desconexión digital en el ámbito laboral con el fin de «garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar».

El alcance de este derecho depende de «la naturaleza y objeto de la relación laboral» y con el mismo se pretende potenciar «el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores».

El procedimiento de regulación corresponde al empleador quien, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

El artículo 89 de la Ley española pretende una regulación del uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

Por una parte, permite a los empleadores «tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras 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. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida».

Por otra parte, la Ley española resuelve un caso especial que enuncia en estos términos: «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». La efectividad de tales pruebas exige que, por lo menos, se haya colocado un dispositivo informativo en lugar suficientemente visible que identifique la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos, pudiendo hacerlo mediante un código de conexión o dirección de internet a esta información.

Ahora bien, la Ley española establece un límite absoluto a la «instalación de sistemas de grabación de sonidos [o] de videovigilancia»: cuando se trate de «lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos».

También se establecen garantías adicionales de modo que «la utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley».

Por último, el artículo 90 se refiere a la utilización de sistemas de geolocalización en el ámbito laboral que pueden instalar los empleadores bajo ciertas condiciones.

Por una parte, el tratamiento de los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, debe realizarse siempre dentro de su marco legal y con los límites inherentes.

Por otra parte, se requiere la información previa por parte de los empleadores de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

El artículo 91 deja un ámbito de regulación a la negociación colectiva de modo que «los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral».

3. LA JURISPRUDENCIA EUROPEA SOBRE LA PROTECCIÓN DE LA VIDA PRIVADA Y LOS DATOS PERSONALES DE LOS TRABAJADORES EN EL MARCO TECNOLÓGICO ACTUAL

El desarrollo vertiginoso de las nuevas tecnologías permite rastrear en los últimos años una evolución de la jurisprudencia europea y de la jurisprudencia de los tribunales españoles en materia de privacidad y datos personales de los trabajadores en general y de los empleados públicos en particular. De hecho, se comprueban las titubeantes respuestas de los tribunales en los distintos niveles, europeo y nacional, y la atención del legislador a resolverlos con opciones legislativas claras.

El examen debe tener en cuenta los desarrollos en Estrasburgo a cargo del Tribunal Europeo de Derechos

Humanos, en Luxemburgo por obra del Tribunal de Justicia de la Unión Europea y en los tribunales españoles.

3.1. LA JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

El Tribunal Europeo de Estrasburgo ha elaborado una jurisprudencia sólida en materia de protección de la privacidad y de los datos personales que es aplicable en el ámbito laboral.

Recientemente se han adoptado dos sentencias de particular trascendencia: *sentencia Bărbulescu c. Rumanía* (2017)⁷ y *sentencia López Ribalda y otros c. España* (2019)⁸. En estos dos casos se muestra la división existente en el propio Tribunal de Estrasburgo que, primero, en una Sala, considera que ha habido violación de derechos fundamentales o que no la ha habido, mientras que, a continuación, la Gran Sala llega a la interpretación contraria.

En la *sentencia Bărbulescu c. Rumanía* la Gran Sala corrige en 2017 la sentencia de 2016 de la Sala. En la primera sentencia se dice que no hubo violación del artículo 8 por seis votos a uno; en cambio, la Gran Sala consideró que hubo violación del derecho a la vida privada por 11 votos frente a 6. Sumando los votos de ambas instancias se puede comprobar que, en teoría, habría habido empate entre los jueces que participaron en la deliberación de ambas sentencias.

Los hechos se refieren al despido de un ingeniero de una empresa rumana por el uso de *Yahoo Messenger* durante el trabajo para el intercambio de mensajes que había mantenido con su novia y con su hermano.

⁷ TEDH (Gran Sala), sentencia de 5 de septiembre de 2017, *Bărbulescu c. Rumanía*, procedimiento nº 61496/08 (despido del empleado por el uso de un servicio de mensajería en línea de la empresa). La Sala se había pronunciado en este asunto en virtud de la sentencia de 12 de enero de 2016.

⁸ TEDH (Gran Sala), sentencia de 17 de octubre de 2019, *López Ribalda y otros c. España*, procedimientos nº 1874/13 y 8567/13 (videovigilancia de empleados sin ser advertidos). La Sala se había pronunciado en la primera sentencia el 9 de enero de 2018.

La Sala se apoyó, fundamentalmente, en la comisión de una falta disciplinaria del trabajador al haber utilizado *Yahoo Messenger* para usos privados.

La Gran Sala matiza, en cambio, su respuesta para llegar a la conclusión de que hubo violación del artículo 8 CEDH. Su punto de partida es la existencia de un contrato de trabajo, la falta de consenso en las legislaciones nacionales para resolver esta cuestión y la rápida evolución en este ámbito.

El contrato de trabajo determina que se mantenga, por una parte, el derecho del trabajador al respeto de su vida privada; pero, a juicio del Tribunal Europeo, ha de tenerse en cuenta el derecho de control, incluidas las prerrogativas disciplinarias, que ejerce el empleador para asegurar el buen funcionamiento de la empresa (§ 124).

En este sentido, concluye el Tribunal Europeo: «las instrucciones de un empleador no pueden reducir a la nada el ejercicio de la vida privada social en el lugar de trabajo. El respeto de la vida privada y de la confidencialidad de las comunicaciones continúa exigiéndose, incluso si estas últimas pueden limitarse en la medida que sea necesario» (§ 80).

A tal fin, el Tribunal Europeo procedió a una sistematización de los criterios que debía tener en cuenta para enjuiciar estos casos en los siguientes términos:

- 1) El empleado debe ser informado claramente y con carácter previo a su instalación de la posibilidad de que el empleador adopte medidas de vigilancia de su correspondencia y sus comunicaciones.
- 2) Es importante la amplitud de la vigilancia del empleador y el grado de injerencia en la vida privada del empleado, debiendo distinguirse entre el flujo de comunicación y su contenido.
- 3) Corresponde al empleador la justificación de los motivos legítimos del uso de la vigilancia y de su alcance y de sus límites.
- 4) Debe analizarse la posibilidad de alcanzar el fin legítimo a través de medios y de medidas menos invasivas para el contenido de las comunicaciones del trabajador.

5) Deben tenerse en cuenta las consecuencias de la vigilancia para el empleado pudiendo controlarse su proporcionalidad, es decir, la utilización para el fin pretendido que haga el empleador de tales datos.

6) El empleador debe ofrecer al trabajador garantías adecuadas especialmente si las medidas son invasivas (§ 121).

En el examen del caso concreto la Gran Sala subraya los defectos que observa en el enjuiciamiento de los tribunales rumanos, a saber y por una parte, no verificaron si el trabajador había sido advertido con carácter previo de la posibilidad de vigilar sus comunicaciones de Yahoo Messenger; y, por otra, el trabajador no había sido informado de la naturaleza ni del alcance de la vigilancia. Además, los tribunales rumanos tampoco determinaron las razones que justificaban la aplicación de medidas de control, ni si el empleador podría haber utilizado medidas menos invasivas para la vida privada y su correspondencia, ni, en fin, si el acceso al contenido de las comunicaciones hubiese sido posible sin su conocimiento (§ 140).

Ahora bien, la Gran Sala no concede indemnización alguna al trabajador sino que, simplemente, considera que la constatación de la violación supone una satisfacción suficiente del daño moral que se le habían causado.

En el *asunto López Ribalda* se planteaba la cuestión de la vulneración de los derechos de las empleadas de un supermercado videovigilado sin que hubiesen sido advertidas del alcance del control dado que algunas de las cámaras estaban ocultas. El propio Tribunal Europeo se refiere a un antecedente propio, la *decisión Köpke* (2010) referida a un supuesto similar en Alemania⁹.

⁹ TEDH, decisión de 5 de octubre de 2010, *Karin Köpke c. Alemania*, recurso nº 420/07 (cámara oculta en un supermercado para detectar si se habían producido hurtos). En este caso se acordó la inadmisibilidad del recurso y se consideró, en esencia, que los tribunales alemanes habían ponderado el derecho de propiedad del empleador, que no tenía otro medio efectivo de protegerse contra los hurtos en el establecimiento de su propiedad, en relación con el derecho de la empleada a que se respetase su vida privada.

Ante los tribunales españoles, cinco cajeras de un supermercado de Mercadona en Granollers (Barcelona) fueron despedidas por haberse comprobado, después de que la empresa hubiese colocado videocámaras, algunas visibles pero otras ocultas, estas últimas enfocaban a las cajas sin haberlo advertido a las trabajadoras que escaneaban los productos y luego cancelaban las compras de clientes, compañeros y las suyas propias o dejaban salir con los productos sin pagar. Las trabajadoras despedidas reconocieron los hechos pero alegaron la vulneración de su derecho a la intimidad en el trabajo.

El Juzgado de lo Social de Granollers y la Sala de lo Social del Tribunal Superior de Justicia de Cataluña desestimaron las demandas frente a los despidos; la Sala de lo Social del Tribunal Supremo y el Tribunal Constitucional inadmitieron la casación y el recurso de amparo.

En cambio, la primera sentencia de 2018 del Tribunal Europeo condenó a España basándose en el enjuiciamiento realizado por los jueces españoles; no obstante, en 2019 la sentencia de la Sala cambia de criterio y desestima el recurso.

En ambas sentencias, el Tribunal Europeo recuerda su jurisprudencia sobre el derecho a la vida privada conforme a la cual «la expectativa razonable de una persona respecto a su intimidad es un factor revelador pero no necesariamente concluyente».

Asimismo, en el caso concreto, el Tribunal de Estrasburgo subraya que «la videovigilancia encubierta de un empleado en su lugar de trabajo debe considerarse, en sí misma, como una importante intromisión en su vida privada».

En fin, el Tribunal Europeo comprueba que la legislación española ya obligaba a informar a los clientes y a los trabajadores sobre el uso de la videovigilancia encubierta por un tiempo prolongado. No obstante, a juicio del Tribunal Europeo la utilización en el procedimiento judicial del material grabado en secreto no se opone a las exigencias de equidad garantizadas por el artículo 6.1 del Convenio.

Ahora bien, la sentencia de 2018 el Tribunal Europeo reprocha a los tribunales españoles no haber alcanzado un equilibrio equitativo entre el derecho de las trabajadoras al

respeto de su vida privada con arreglo al artículo 8 del Convenio y el interés de su empleador en la protección de sus derechos patrimoniales. De esta solución discrepó el juez Dedov al considerar que «el fallo de la mayoría contradice el principio general del derecho: no se debe permitir que los demandantes se beneficien legalmente de sus propios actos ilícitos». El Tribunal de Estrasburgo concede a cada una de las cinco empleadas una indemnización por daños morales de 4.000 euros. No obstante, dos de los siete jueces europeos consideraron que la propia sentencia hubiese sido satisfacción bastante.

En cambio, la sentencia de 2019 de la Gran Sala llega a la conclusión contraria, por 14 votos a 3, de modo que decide que España no habría vulnerado el artículo 8 del Convenio.

El Tribunal Europeo se basa expresamente en la *decisión Köpke* y en la *sentencia Bărbulescu*, siguiendo las mismas indicaciones, vuelve a repetir los elementos que deben determinar la proporcionalidad de las medidas de videovigilancia:

- 1) El empleado debe ser informado claramente y con carácter previo a su instalación de la posibilidad de que el empleador adopte medidas de videovigilancia.
- 2) Resulta importante tener en cuenta la amplitud de la videovigilancia del empleador y el grado de injerencia en la vida privada del empleado: lugares más o menos privados, límites espaciales y temporales, y número de personas que tienen acceso a los datos.
- 3) Es necesaria la justificación por el empleador de los motivos legítimos del uso de la videovigilancia y de su alcance, de tal modo que cuanto más invasiva sea la videovigilancia, más exigente debe ser su justificación.
- 4) Debe considerarse la posibilidad de alcanzar el fin legítimo a través de medios y de medidas menos invasivas en la vida privada del asalariado.
- 5) Han de tenerse en cuenta las consecuencias de la videovigilancia para el empleado pudiendo controlar la utilización que haga el empleador de tales datos en función de la finalidad perseguida.

6) El empleador debe ofrecer al empleado las garantías adecuadas, directamente, a través de sus representantes, bajo el control de un organismo independiente o si hay posibilidad de presentar reclamaciones, especialmente cuando las medidas son invasivas (§ 116).

Finalmente, la Gran Sala del Tribunal Europeo llega a la conclusión de que no hubo violación del artículo 8 del Convenio, debido a las garantías que ofrecía la normativa española, teniendo en cuenta el enjuiciamiento detallado hecho por el Juzgado de Granollers y por la Sala de lo Social de Barcelona del que se deducía la justificación y proporcionalidad de las medidas de videovigilancia y, en fin, en atención a las vías de recurso ante la Agencia Española de Protección de Datos y ante otros tribunales que, sin embargo, las empleadas no utilizaron (§ 137).

En cambio, el voto disidente que pretendía constatar la violación del artículo 8 reprochaba a la legislación española que no hubiese previsto más que una única garantía específica al régimen de videovigilancia, la obligación de advertir con carácter previo a los empleados de la instalación y utilización de la vigilancia, sin que se estableciese ninguna otra excepción (§ 4); lo que no se habría producido en el caso de las cámaras ocultas y, en consecuencia, hubiese determinado, dice el voto discrepante, la vulneración por España del derecho fundamental a la privacidad de los trabajadores.

En suma, puede observarse que la jurisprudencia de Estrasburgo es oscilante y no termina por decantarse por una solución única. No obstante, los elementos fundamentales de la jurisprudencia están ya diseñados.

3.2. LA JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

La Unión Europea ha respondido legislativamente de una manera apropiada frente a los desafíos de las nuevas tecnologías en la vida privada y en la protección de datos personales. Ahora bien, en el caso de los trabajadores, la jurisprudencia de Luxemburgo no es, hasta ahora,

particularmente significativa. Sin embargo, ofrece algunos elementos que merecen destacarse.

En la *sentencia Österreichischer Rundfunk y otros* (2003) el Tribunal de Justicia aborda la cuestión de la conformidad con el derecho a la protección de datos del control que corresponde al Tribunal de Cuentas y otros organismos públicos sobre los ingresos de determinados empleados de la televisión pública austriaca y otros entes territoriales y empresas públicas¹⁰.

El Tribunal de Justicia considera que cabe una amplia divulgación del importe de los ingresos anuales y, cuando estos superan un límite determinado, del nombre de las personas empleadas por las entidades sujetas al control del Tribunal de Cuentas, si es necesaria y apropiada para lograr el objetivo de buena gestión de los recursos públicos.

La *sentencia Worten* (2013) se pronuncia sobre las cuestiones del registro del tiempo de trabajo, con la indicación de las horas en que cada trabajador inicia y finaliza la jornada y las pausas de descanso, y considera que está comprendido en el concepto de «datos personales» aplicándose la legislación europea al efecto, en aquel entonces la Directiva 95/46/CE¹¹.

La cuestión prejudicial planteada por un tribunal de trabajo portugués pretendía saber si era conforme con el Derecho de la Unión europea la imposición de una multa a una empresa que no había permitido que la Inspección laboral procediera a la consulta inmediata del registro del tiempo de trabajo de los trabajadores de un establecimiento de la empresa Worten.

A pesar de las garantías en materia de protección de datos, la legislación europea no impide que se aplique la Directiva

¹⁰ TJCE, sentencia de 20 de mayo de 2003, *Österreichischer Rundfunk y otros*, C-465/00, C-138/01 y C-139/01, EU:C:2003:294 (divulgación de datos sobre los ingresos de empleados de entidades sujetas al control financiero externo).

¹¹ TJCE, sentencia de 30 de mayo de 2013, *Worten — Equipamentos para o Lar, S.A. / Autoridade para as Condições de Trabalho (ACT)*, C-342/12, EU:C:2013:355 (acceso de la inspección de Trabajo para la supervisión de las condiciones de trabajo).

2003/88/CE relativa a determinados aspectos de la ordenación del tiempo de trabajo. La efectividad de esta Directiva puede establecer la obligación del empleador de proporcionar a una autoridad de control laboral el acceso inmediato al registro del tiempo de trabajo dado que esta obligación puede resultar necesaria si contribuye a una aplicación más eficaz de la normativa en materia de condiciones de trabajo.

Este enfoque ha sido confirmado por la *sentencia Federación de Servicios de Comisiones Obreras (CCOO) / Deutsche Bank* (2019), en la medida en que el Tribunal de Justicia considera necesario garantizar el efecto útil de los derechos recogidos en la Directiva 2003/88 y el artículo 31.2 de la Carta de todo trabajador a la limitación de la duración máxima del trabajo y a períodos de descanso diarios y semanales, así como a un período de vacaciones anuales retribuidas, de tal modo que las autoridades nacionales están obligadas a «imponer a los empresarios la obligación de implantar un sistema objetivo, fiable y accesible que permita computar la jornada laboral diaria realizada por cada trabajador»¹².

La *sentencia Nowak* (2017) aplica la Directiva 95/46 a un examen profesional hecho en el Colegio de censores jurados de cuentas de Irlanda¹³. A juicio del Tribunal de Justicia, «las respuestas por escrito dadas por un aspirante en un examen profesional y las eventuales anotaciones del examinador referentes a esas respuestas son datos personales» (apartado 62).

No obstante, el Tribunal de Justicia considera que, transcurrido un plazo determinado, puede haber interés en que tales exámenes se destruyan teniendo presentes los derechos de terceros. En efecto, el Tribunal de Justicia subraya expresamente que un aspirante tendría derecho a

¹² TJUE (Gran Sala), sentencia de 14 de mayo de 2019, Federación de Servicios de Comisiones Obreras (CCOO) / Deutsche Bank, S.A.E., C-55/18, EU:C:2019:402 (sistema de registro de la jornada laboral diaria realizada por sus trabajadores).

¹³ TJUE, sentencia de 20 de diciembre de 2017, Nowak, C-434/16, EU:C:2017:994 (anotaciones en un examen profesional como datos personales).

solicitar al responsable del tratamiento de datos que, transcurrido un determinado período de tiempo, se supriman sus respuestas al examen y las correspondientes anotaciones del examinador, es decir, que se destruyan. A lo que añade el Tribunal de Justicia: «habida cuenta de la finalidad de las respuestas del aspirante en un examen y de las correspondientes anotaciones del examinador, su conservación en una forma que permita la identificación del aspirante ya no parece necesaria a priori, una vez que el procedimiento de examen está definitivamente concluido y no puede ser objeto de recurso, de tal modo que tales respuestas y anotaciones han perdido cualquier valor probatorio» (apartado 55).

Y de manera muy clara el Tribunal de Justicia insiste en las limitaciones que tanto la Directiva 95/46 como el Reglamento 2016/679, que sustituyó a dicha Directiva, establecen a esos derechos (apartado 59).

Los desarrollos en otros ámbitos del derecho a la protección de datos personales y el uso de Internet¹⁴ o la protección de datos biométricos¹⁵ pueden arrojar luz al ámbito propiamente de las relaciones entre empleadores y trabajadores.

3.3. LA JURISPRUDENCIA DE LOS TRIBUNALES ESPAÑOLES

En España las cuestiones relativas a los derechos de privacidad y de protección de datos de los trabajadores se resuelven tanto en la jurisdicción social cuando conoce de

¹⁴ TJUE (Gran Sala), sentencia de 24 de septiembre de 2019, Google / Comisión Nacional de Informática y Libertades de Francia, C-507/17, EU:C:2019:772 (alcance territorial del derecho al olvido en Internet); TJUE (Gran Sala), sentencia de 1 de octubre de 2019, Planet49, C-673/17, EU:C:2019:801 (consentimiento sobre datos personales en Internet y *cookies*); TJUE, sentencia de 3 de octubre de 2019, Eva Glawischnig-Piesczek / Facebook Ireland Limited, C-18/18, EU:C:2019:821 (obligaciones de una red social a bloquear o a suprimir datos almacenados y declarados judicialmente ilícitos).

¹⁵ TJUE, sentencia de 3 de octubre de 2019, Staatssecretaris van Justitie en Veiligheid / A y otros, C-70/18, EU:C:2019:823 (registro de datos biométricos de trabajadores turcos).

los litigios entre trabajadores y empresarios como en la jurisdicción contencioso-administrativa cuando quedan afectados los empleados públicos (el acceso de los todos al empleo público, incluido el personal laboral, y las vicisitudes laborales de los funcionarios y del personal estatutario).

Todo parece indicar una convergencia en las soluciones de la jurisdicción social y de la jurisdicción contencioso-administrativa producida no solo por la jurisprudencia europea antes referida sino también por la jurisprudencia constitucional. De hecho, el Tribunal Constitucional, intérprete supremo de la Constitución y que protege de manera especial determinados derechos fundamentales por vía de amparo, en particular tal como resultan del artículo 18 de la Constitución, actúa como punto de referencia de las jurisdicciones implicadas.

No es posible un examen exhaustivo de la jurisprudencia de los tribunales españoles por lo que se han elegido algunas sentencias que marcan la tendencia en la jurisdicción constitucional y en la jurisdicción ordinaria, social y contencioso-administrativa.

3.3.1 Tribunal Constitucional

El Tribunal Constitucional se pronunció en la sentencia 39/2016 en un recurso de amparo formulado por una trabajadora de una tienda de moda Bershka, del Grupo Inditex, en León que había sido despedida como consecuencia de las imágenes captadas por una cámara de videovigilancia instalada sin comunicación previa a la trabajadora, aunque había aviso en la tienda de instalación de cámaras, y de las que se deducían que se había apropiado de 189,92 euros de la caja¹⁶. Tanto el Juzgado como la Sala de lo Social habían desestimado la impugnación del despido disciplinario de la trabajadora.

Sobre este particular, el Tribunal Constitucional se refiere, en primer lugar, al consentimiento y señala: «En el ámbito

¹⁶ TC (Pleno), sentencia 39/2016, de 3 de marzo, ponente: Roca Trías (despido basado en las imágenes captadas por una cámara de videovigilancia instalada sin comunicación previa a la trabajadora de Bershka).

laboral el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes». No obstante, precisa: «el consentimiento de los trabajadores afectados sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato».

En segundo lugar, el Tribunal Constitucional se pronuncia sobre el deber de información que pesa sobre el empleador en este sentido: «El deber de información previa forma parte del contenido esencial del derecho a la protección de datos, pues resulta un complemento indispensable de la necesidad de consentimiento del afectado».

En tercer lugar, el Tribunal Constitucional prevé excepciones a los dos supuestos anteriores en estos términos: «el incumplimiento del deber de requerir el consentimiento del afectado para el tratamiento de datos o del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada». En el caso concreto, el Tribunal Constitucional desestima el recurso de amparo por considerar que se había respetado el principio de proporcionalidad en sus tres dimensiones (juicio de necesidad, juicio de idoneidad y proporcionalidad en sentido estricto), a saber:

la medida de instalación de cámaras de seguridad que controlaban la zona de caja donde la demandante de amparo desempeñaba su actividad laboral era una medida justificada (ya que existían razonables sospechas de que alguno de los trabajadores que prestaban servicios en dicha caja se estaba apropiando de dinero); idónea para la finalidad pretendida por la empresa (verificar si algunos de los trabajadores cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la

grabación de imágenes se limitó a la zona de la caja), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE (FJ 5).

A esta sentencia se formularon dos votos particulares, firmados por tres de los once magistrados del Tribunal Constitucional, en los que proponen la solución contraria. Por una parte, el voto suscrito por el magistrado Valdés Dal-Ré, catedrático de Derecho del Trabajo, considera: «el despido debió calificarse como nulo, por no haberse cumplido el deber de información que impone al empresario el art. 18.4 CE» que reniega enérgicamente por una interpretación en la que «ni los poderes o facultades empresariales son, sin excepción y de manera universal, expresiones directas e indefectibles de los arts. 33 y 38 CE que quepa confrontar de manera mecánica y sin mayor fundamentación con los derechos fundamentales de los trabajadores; ni, en fin, las facultades del empresario y, menos aún si se ejercen de modo irregular o desviado, como más adelante tendré ocasión de razonar, pueden restringir aquellos derechos en el ámbito de las organizaciones productivas, incluidos, claro está, los formulados en el art. 18 CE».

El otro voto particular, del magistrado Xiol Ríos, adopta la misma postura e insiste en que la información al público no sea suficiente sino que debe informarse a los trabajadores. Además, su voto revela lo ajustado de la solución al proponer que se estimase el amparo pero se mantuviesen las sentencias previas dado que «tanto en primera instancia como en suplicación se hace constar por los respectivos tribunales que existen otros elementos de prueba independientes de la videovigilancia suficientes para entender probados los hechos que dieron lugar al despido». El sentido de la sentencia responde, con toda probabilidad, a la influencia de la solución dada en la primera *sentencia Bărbulescu* (2016), que no había apreciado la violación del derecho a la vida privada. Aunque, ha de recordarse que a la luz de la segunda *sentencia Bărbulescu* (2017), dictada seis meses después, la sentencia podría haber sido estimatoria. En cambio, a la luz de la primera *sentencia*

López Ribalda (2018), la solución del Tribunal Constitucional hubiese sido más controvertida que desde la perspectiva de la segunda *sentencia López Ribalda* (2018) en que la solución de Estrasburgo y de Madrid parecen sincronizarse. Aun cuando no sea en el ámbito laboral, es importante tener en cuenta la sentencia 97/2019 donde el Tribunal Constitucional se refiere al uso de datos de la denominada *lista Falciani*¹⁷ y confirma las sentencias de instancia y de casación que habían condenado por delito contra la Hacienda pública en la declaración del impuesto de la renta de 2005 y en la de 2006 a un empresario domiciliado en Madrid¹⁸.

El Tribunal Constitucional deniega el amparo porque «los datos que son utilizados por la Hacienda Pública española se refieren a aspectos periféricos e inocuos de la llamada “intimidad económica”. No se han introducido dentro del proceso penal datos, como podrían ser los concretos movimientos de cuentas, que puedan revelar o que permitan deducir los comportamientos o hábitos de vida del interesado [...] Los datos controvertidos son, exclusivamente, la existencia de la cuenta bancaria y el importe ingresado en la misma. El resultado de la intromisión en la intimidad no es, por tanto, de tal intensidad que exija, por sí mismo, extender las necesidades de tutela del derecho sustantivo al ámbito del proceso penal, habida cuenta que, como ya se ha dicho, éste no tiene conexión instrumental alguna con el acto de injerencia verificado entre particulares».

Estas dos vías de aproximación, el carácter más o menos periférico e inocuo de los datos tenidos en cuenta así como la existencia de un ilícito previo, especialmente si es grave, determinan en gran medida las soluciones que deben alcanzar los tribunales.

¹⁷ TC (Pleno), sentencia 97/2019, de 17 de julio de 2019, ponente: Montoya Melgar (uso de datos de la *lista Falciani* para la persecución de delitos de defraudación tributaria).

¹⁸ TS (Sala 2ª), sentencia de 23 de febrero de 2017, recurso nº 1281/2016, ES:TS:2017:471, ponente: Marchena Gómez (delito fiscal y *lista Falciani*).

3.3.2 La jurisprudencia social y contencioso-administrativa del Tribunal Supremo

En primer lugar y por lo que se refiere a la jurisdicción social, la sentencia de 2 de febrero de 2017, del Pleno de la Sala Social acepta la legitimidad de pruebas videográficas obtenidas en la entrada y espacios comunes de un gimnasio sin que el Tribunal Supremo exija haber comunicado que su uso podría hacer en procedimientos disciplinarios¹⁹.

Un trabajador había sido despedido, entre otras razones por colar a clientes sin entrada, para lo tanto el Juzgado como la Sala de lo Social de Barcelona habían declarado la improcedencia del despido por las pruebas de que se había valido el empleador.

En cambio, el Tribunal Supremo aceptó las pruebas videográficas y consideró que «el uso de la videocámara revistió carácter razonable y proporcionado a su objeto sin que por el lugar de su instalación exista riesgo para la vulneración del derecho al honor a la intimidad personal y familiar ni por las circunstancias de tiempo y oportunidad lo haya tampoco para el pleno ejercicio de sus derechos al haber actuado el demandante como lo ha hecho siendo conocedor de que su conducta estaba siendo grabada y de que por lo que respecta a las cámaras de la entrada el acceso indebido con auxilio interno ya había sido objeto de sanción».

El Tribunal Supremo acoge, en su sentencia de 23 de febrero de 2017 la *jurisprudencia Barbulescu* en el ámbito social considerando que está en sintonía con la jurisprudencia constitucional²⁰. La cuestión se planteaba respecto del rechazo de determinadas pruebas que habían justificado el despido de un trabajador.

¹⁹ TS (Sala 4ª, Pleno), sentencia de 2 de febrero de 2017, recurso nº 554/2016, ES:TS:2017:817, ponente: Calvo Ibarlucea (validez de pruebas videográficas en la entrada y espacios públicos sin que se avisase a los trabajadores de su uso a efectos disciplinarios).

²⁰ TS (Sala 4ª), sentencia de 8 de febrero de 2018, recurso nº 1121/2015, ES:TS:2018:594, ponente: De Castro Fernández (plena validez procesal de la prueba utilizada por Inditex y derivada del examen del correo electrónico existente en ordenador del trabajador).

En suplicación, la Sala de Galicia había desechado las pruebas ilícitamente obtenidas a través del control del correo electrónico del trabajador de Inditex, aunque, a la vista de otras pruebas, confirmó el despido.

En cambio, la Sala de lo Social del Tribunal Supremo refuerza el poder de control del empresario en un supuesto en el que «si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de intimidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo». A tal efecto, el Tribunal Supremo reproduce los mismos argumentos del Tribunal Europeo y se refiere resumidamente a los criterios establecidos en Estrasburgo y que giran en torno a los siguientes elementos: «a) el grado de intromisión del empresario; b) la concurrencia de legítima razón empresarial justificativa de la monitorización; c) la inexistencia o existencia de medios menos intrusivos para la consecución del mismo objetivo; d) el destino dado por la empresa al resultado del control; e) la previsión de garantías para el trabajador».

Por lo que se refiere a la jurisprudencia contencioso-administrativa del Tribunal Supremo, no es muy abundante en relación con la protección de la vida privada y de los datos personales de los empleados públicos (funcionarios y personal estatutario).

La sentencia de 2 de julio de 2007 se refiere a la protección de los derechos fundamentales de integridad física y datos personales frente a la implantación de un sistema de control horario para empleados públicos en Cantabria mediante la lectura biométrica de la mano²¹.

²¹ TS (Sala C-A, Sección 7ª), sentencia de 2 de julio de 2007, recurso nº 5017/2003, ES:TS:2007:5200, ponente: Lucas Murillo de la Cueva (control de horario mediante la captación de la imagen tridimensional de la mano en Cantabria).

El Tribunal Supremo considera que se trata de datos personales cuyo registro está sometido a la normativa aplicable en la materia; sin embargo, a su juicio «la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos».

4. CONCLUSIÓN

La respuesta a los desafíos que las nuevas tecnologías representan para la privacidad y la protección de los datos personales de los trabajadores se basa en una decantación del derecho fundamental a la vida privada y a la protección de los datos personales.

La Constitución española apenas pudo adivinar en 1978 los cambios que produciría la técnica. Sin embargo, han sido la adopción de la Carta de los derechos fundamentales y su desarrollo legislativo por la Unión Europea, especialmente a través del vigente Reglamento General de Protección de Datos, los que han establecido un marco normativo apropiado que, no obstante, está en constante desarrollo. En este sentido será preciso confiar una mayor participación de los interlocutores sociales en la adopción de normas convencionales que clarifiquen el alcance del poder de autoorganización de los empleadores y el ámbito íntimo irreductible de los trabajadores.

La jurisprudencia europea, especialmente desde Estrasburgo, ha reflexionado sobre esta cuestión que, en realidad, se revela especialmente difícil como se deduce de las sentencias *Bărbulescu* y *López Ribalda*, con soluciones contradictorias y debates especialmente controvertidos entre los mismos jueces del Tribunal Europeo.

Desde España la atención y el seguimiento de esta jurisprudencia europea han sido especialmente intensos sin que, hoy por hoy, se haya determinado una solución unívoca. No obstante, parece que habrá una convergencia entre las soluciones adoptadas por los jueces españoles de lo laboral y de lo contencioso-administrativos por efecto de la jurisprudencia europea y de la jurisprudencia constitucional.

Ahora bien, todo parece indicar que, si bien el consentimiento del trabajador no es relevante en este ámbito, la mayor o menor información de los trabajadores sobre el alcance del control del empresario justificará determinadas invasiones y limitaciones en la privacidad y en la protección de los datos de los trabajadores. Ciertamente, será necesario superar un enfoque exclusivamente procedimental para tener en cuenta los aspectos sustantivos de la vida privada de los trabajadores. En este sentido, la mayor o menor afectación de la intimidad de los trabajadores será un elemento decisivo para determinar la legalidad de la actuación empresarial porque, como señala, el Tribunal Europeo de Derechos Humanos: «las instrucciones de un empleador no pueden reducir a cero el ejercicio de la vida privada social en el lugar de trabajo»²².

5. BIBLIOGRAFÍA

- Comité de Ministros del Consejo de Europa (2015). [*Recommendation CM/Rec \(2015\) 5 on the processing of personal data in the context of employment*](#), 1 de abril de 2015, at the 1224th meeting of the Ministers' Deputies), Estrasburgo.
- Delgado Martín, J. (2019), "Reflexiones sobre la protección de datos personales en la Administración de Justicia", *Diario La Ley* Nº 9363, Madrid.
- González González, C. (2019). "Control empresarial de la actividad laboral mediante la videovigilancia y colisión con los derechos fundamentales del trabajador. Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales", *Revista Aranzadi Doctrinal* Nº. 4, Navarra.

²² TEDH (Gran Sala), sentencia de 5 de septiembre de 2017, *Bărbulescu c. Rumanía*, procedimiento nº 61496/08, antes citada, § 80; la versión inglesa dice literalmente: «an employer's instructions cannot reduce private social life in the workplace to zero»; la versión francesa reza así: «les instructions d'un employeur ne peuvent pas réduire à néant l'exercice de la vie privée sociale sur le lieu de travail».

- Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2017). *Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, de 8 de junio de 2017*, [Comisión Europea](#), WP 249, Bruselas.
- Jiménez Asensio, R. (2019). *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*, Instituto Vasco de Administración Pública, Oñate.
- Mangan, D. (2019). "Beyond Procedural Protection: Information Technology, Privacy and the Workplace", *European Law Review*, August, pp. 559-571.
- Ordóñez Riaño, M. (2019). "Los derechos fundamentales de los trabajadores y el impacto de las nuevas tecnologías", *Diálogos Jurídicos 2019. Anuario de la Facultad de Derecho de la Universidad de Oviedo*, Universidad de Oviedo, Thomson Reuters Aranzadi, Navarra, pp. 217-232.
- Ordóñez Solís, D. (2014). *La protección judicial de los derechos en Internet en la jurisprudencia europea*, Editorial Reus, Madrid.
- Pérez Miras, J. (2019). *El derecho a la protección de datos y a la privacidad: una perspectiva comparada entre la Unión Europea y Estados Unidos*, Tesis doctoral dirigida por Marycruz Arcos Vargas (dir. tes.). Universidad de Sevilla (2019).
- Rallo Lombarte, A. (2019). *Tratado de protección de datos. Actualizado con la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant lo Blanch, Valencia.
- Rodríguez Escanciano, S. (2019). "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales", *Diario La Ley* Nº 9328, Madrid.
- Rojas Rosco, R. y López Carballo, D. (2018). "El impacto del RGPD en el ámbito del control laboral y la era de la innovación", *Actualidad civil* Nº 5, 2018 (Ejemplar dedicado a: Protección de datos: entre el RGPD y la nueva LOPD), Madrid.

