El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679

Susana Rodríguez Escanciano

Catedrática de Derecho del Trabajo y de la Seguridad Social. Universidad de León

Extracto

La tutela de los derechos de los ciudadanos frente al uso ilegítimo de los datos personales es una necesidad que se deja sentir, con la mayor crudeza, en el ámbito de las relaciones laborales, dado el hecho incontestable de que la gestión informatizada del personal amplía la posibilidad de acumulación de referencias de los trabajadores, aumenta la capacidad de combinación a través de la formación de perfiles y multiplica exponencialmente las posibilidades de acceso y de transmisión a terceros.

Tratar de dar respuesta a los interrogantes generados por la protección de los datos personales de los trabajadores exige la difícil tarea de partir de las reglas jurídicas que ordenan con carácter general el tratamiento automatizado, ahora singularmente abanderadas por el Reglamento europeo 2016/679, para a partir de tales pilares construir pautas especiales que atiendan a las características propias del trabajo asalariado.

Palabras clave: datos personales; trabajadores; autodeterminación informativa; consentimiento; transparencia.

Fecha de entrada: 03-05-2018 / Fecha de aceptación: 07-05-2018

The right to protection of personal data in the employment contract: considerations at the sight of the European regulation 2016/679

Susana Rodríguez Escanciano

Abstract

The protection of the rights of persons against the illegitimate use of personal data is a need that is felt, with the utmost harshness, in the field of labor relations, given the indisputable fact that the computerized management of personnel extends the possibility of accumulation of references of workers, increases the capacity of combination through the formation of profiles and exponentially multiplies the possibilities of access and transmission to third parties.

Trying to answer the questions generated by the protection of the personal data of workers requires the difficult task of starting from the legal rules that order in a general way the automated processing, now singularly integrated by the European Regulation 2016/679, to take such regulations to guarantee the characteristics of salaried work.

Keywords: personal data; workers; self-determination information; consent; transparency.

Sumario

NOTA: Estudio realizado en el marco del proyecto de investigación DER2017-82192-C3-1-R titulado «Nuevos lugares, distintos tiempos y modos diversos de trabajar. Innovación tecnológica y cambios en el ordenamiento social», financiado por el Ministerio de Economía, Industria y Competitividad.

Este estudio constituye la base de la ponencia «Implicaciones de la normativa sobre protección de datos en la dimensión individual de las relaciones laborales» presentada en el «Congreso Internacional sobre el impacto del Reglamento Europeo de Protección de Datos: análisis nacional y comparado» (Universidad Jaume I, 17 y 18 de mayo de 2018), financiado con el proyecto MINECO «El impacto del nuevo Reglamento Europeo de Protección de Datos: análisis nacional y comparado» (DER2015-63635-R).

Cómo citar este estudio:

Rodríguez Escanciano, S. (2018). El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679. *RTSS.CEF, 423*, 19-62.

1. LA DISPOSICIÓN EMPRESARIAL DE GRANDES BANCOS DE DATOS DE LOS TRABAJADORES: LA AGRESIVIDAD INFORMÁTICA FRENTE A LOS DERECHOS FUNDAMENTALES

La tutela de los derechos de los ciudadanos frente al uso ilegítimo de los datos personales es una necesidad que se deja sentir, con la mayor crudeza, en el ámbito de las relaciones laborales, dado el hecho incontestable de que la gestión informatizada del personal amplía la posibilidad de acumulación de referencias de los trabajadores. Las nuevas formas de actividad en los modelos de industria 4.0 o en los sistemas cibercientíficos, intensivas en el uso de tecnologías de la información y comunicación y de otros adelantos (robótica, microelectrónica, virtualización, optométrica, ciberseguridad, nanotecnología, etc.), van a permitir no solo optimizar y agilizar el desempeño de la prestación profesional, sino también almacenar una cantidad enorme de información relativa a la persona del trabajador entremezclada con el quehacer laboral.

Sin duda, la gestión informatizada del personal facilita que todos los datos concernientes al desarrollo del contrato de trabajo, desde el momento de la selección de personal, pasando por la constitución del vínculo contractual hasta su resolución, sean incluidos en los soportes automatizados de la empresa. Y es que la incorporación de la persona del trabajador a la organización productiva favorece tanto una continua adquisición de noticias sobre extremos personales de diversa naturaleza como su minuciosa puesta al día, fundamentalmente por tres razones: de un lado, ante la exhaustividad en la información habitualmente obtenida o exigida en relación con las solicitudes de empleo, incluida –la mayoría de las veces– la realización de test indiscretos destinados a obtener trabajadores altamente productivos y sin defectos, permaneciendo los datos en poder de la entidad a la cual ha sido solicitado el trabajo incluso aunque el reclutamiento haya sido denegado (Tascón, 2008, p. 449); de otro, debido a la gestión de determinadas materias realizadas por las entidades empresariales en nombre de los trabajadores a su servicio (pago de cuotas de Seguridad Social, abono de ayudas para estudios del propio empleado o de sus hijos, concesión de otros auxilios familiares, etc.); en fin, teniendo en cuenta que los modernos métodos de dirección y control de mano de obra predisponen a los empresarios a contar con referencias exhaustivas sobre la formación y cualificación de los trabajadores, aptitudes físicas y psíquicas, ritmos de trabajo, dedicación, horas de entrada y salida, eventuales sanciones disciplinarias, movimientos en el interior de la empresa, relaciones con los compañeros, mayor o menor vulnerabilidad a las enfermedades... sin que el interesado sea consciente; todo ello, con el objetivo último de conseguir la máxima competitividad y rentabilidad, la conveniente adaptación de cada empleado a su puesto de trabajo y, al tiempo, una óptima planificación empresarial a medio y largo plazo (Rodríguez, 2009, p. 9), con el agravante de que, en la mayoría de las ocasiones, el trabajador carece de la oportunidad de defensa frente a las decisiones del empresario, produciéndose, también en el ámbito laboral, una «expropiación sin precedentes de la privacidad» (Sancho, 2017, p. 127).

Bajo tales premisas, entre los riesgos que entraña el poder informático para los derechos de los trabajadores pueden encontrarse los derivados de su capacidad de recopilar y de transmitir datos sobre su persona, así como de tratar la información recabada elaborando perfiles completos a través de los denominados análisis *multicriteria*, facilitados por las nuevas tecnologías, sobre todo, por el avance de los canales conocidos como *big data*, que permiten la valoración a gran escala de los datos procedentes de diferentes fuentes y que convertirán en estándar la toma de decisiones en tiempo real (Álvarez, 2017, p. 16).

2. EL RECONOCIMIENTO DE DERECHOS *ONLINE* A LOS TRABAJADORES: LA AUTODETERMINACIÓN INFORMATIVA

La informática permite un ilimitado e indiscriminado acarreo de circunstancias personales del ciudadano y, cómo no, del empleado o candidato a un empleo, facilitando que noticias anteriormente diseminadas aparezcan instantáneamente reunidas en un soporte digitalizado sin tener en cuenta su relevancia en relación con los requisitos de aptitud o con las obligaciones derivadas del contenido de la prestación laboral, posibilitando, además, métodos de recogida sin conocimiento por parte del trabajador afectado, de modo que el empresario puede acceder al contenido de los extremos personales con total ignorancia de este (Goñi, 2004b, p. 51).

En este contexto, el interés legítimo del trabajador se circunscribe no tanto a proteger un espacio propio cuanto a dominar sus datos personales insertos en los sistemas de comunicación empresariales porque solo así puede ejercer un control sobre el uso secundario de esos datos y evitar la afectación negativa durante la relación laboral o su postergación para un futuro empleo (Goñi, 2017, p. 23).

De la defensa del núcleo básico de la intimidad, entendida como pretensión de no injerencia de terceros, se tiene que evolucionar hacia una nueva dimensión que faculte a cada sujeto a mantener el poder de disposición sobre el patrimonio informativo, surgiendo los derechos *online* de los trabajadores. Procede identificar, así, un nuevo derecho frente a sofisticadas formas empresariales de amenaza, el derecho a la libertad informática o el derecho a la autodeterminación informativa, reconocido por el Tribunal de Justicia de la Unión Europea[1] y por el texto constitucional español en el artículo 18.4[2], configurado como aquel que tiene por objeto:

> Garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos (*habeas data*); controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los asientos inexactos o indebidamente procesados; disponer sobre su transmisión (...); en definitiva, este derecho en-

[1] Sentencias del Tribunal de Justicia de la Unión Europea (SSTJUE) de 8 de abril de 2014, asunto Digital Rights Ireland, y 6 de octubre de 2015, asunto Schrems.

[2] Sentencias del Tribunal Constitucional (SSTC) 254/1993, de 20 de julio, y 290/2000 y 292/2000, de 30 de noviembre.

> traña una facultad de decidir sobre la revelación y el uso de los datos personales, en todas las fases de elaboración y utilización de los mismos, es decir, su acumulación, su transmisión, su modificación y cancelación[3].

Este derecho:

> Otorga a su titular un poder de disposición y de control sobre los datos personales que se concreta jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero. Y ese derecho de consentir el conocimiento y tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo y, por otro lado, el poder oponerse a esa posesión y uso[4].

Y ello con el propósito último «de impedir su tráfico ilícito y lesivo para la dignidad del afectado»[5].

El derecho a la protección de datos personales del artículo 18.4 de la Constitución española (CE), referidos no solo a informaciones confidenciales o relacionadas con la intimidad, sino a cualquier tipo de noticia, tanto subjetiva como objetiva, en forma de opiniones o apreciaciones sobre una persona[6], establece, a la postre, mecanismos de tutela frente a cualquier uso de las tecnologías de la información que vulnere el pleno ejercicio de los derechos fundamentales: intimidad del trabajador, derecho de huelga, libertad ideológica o religiosa, secreto de las comunicaciones, propia imagen, etc.

3. EL IMPULSO DEL REGLAMENTO EUROPEO EN CUANTO A LA PROTECCIÓN DE DATOS PERSONALES EN EL MARCO DEL TRABAJO ASALARIADO. A LA ESPERA DE LA REACCIÓN DEL ORDENAMIENTO ESPAÑOL

Advertida la agresividad de los dispositivos electrónicos, informáticos y visuales frente a la privacidad del individuo en el marco de la relación laboral, de lo que se trata es de fijar un punto de equilibrio entre la potestad empresarial a la hora de optimizar las posibilidades que le ofre-

[3] En la línea de la Sentencia del Tribunal Europeo de Derechos Humanos (STEDH) 2000/130, de 4 de mayo, asunto Rotaru.

[4] SSTC 206/2007, de 24 de septiembre; 70/2009, de 23 de marzo; 12/2012, de 30 de enero, y 96/2012, de 7 de mayo.

[5] Sentencia del Tribunal Constitucional (STC) 292/2000, de 30 de noviembre.

[6] Sentencia del Tribunal de Justicia de la Unión Europea (STJUE) de 20 de diciembre de 2017, asunto Peter Nowak.

cen las nuevas tecnologías, incluida la organización y el control de la mano de obra, y la preservación de los derechos y libertades fundamentales del trabajador; singularmente, el derecho a la protección de datos. En este intento, como casi siempre, el ordenamiento social, ante la ausencia de regulación específica, debía partir de las reglas jurídicas que ordenan con carácter general el tratamiento automatizado de datos personales, tanto en el ámbito internacional (Convenio 138 del Consejo de Europa, de 28 de enero de 1981; Recomendación número 89 (2), de 18 de enero de 1989, del Comité de Ministros del Consejo de Europa; art. 8 Carta de los Derechos Fundamentales de la Unión Europea; art. 16.1 Tratado de Funcionamiento de la Unión Europea, y Directiva 95/46, de 24 de octubre de 1995), como en el ámbito interno (Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal [LOPD], desarrollada por RD 1720/2007, de 21 de diciembre), para, a partir de las mismas –y como un plus mediante el cual valorar las circunstancias presentes en la relación laboral–, construir principios y reglas especiales para este sector del ordenamiento jurídico.

No obstante, y sin dudar de la aplicación de la normativa general al uso –algo indiscutible–, son numerosas las voces alzadas para reclamar una regulación propia y específica que atienda las múltiples y variadas peculiaridades existentes en los centros de trabajo. Semejante deseo ha tardado en encontrar respuesta concreta en instrumentos normativos, más allá de la Resolución R (89) del Comité de Ministros de los Estados miembros del Consejo de Europa sobre protección de datos de carácter personal utilizados con fines de empleo, la Recomendación práctica de la Organización Internacional del Trabajo (OIT) sobre protección de datos de los trabajadores de 1997 o cierta iniciativa de algún país de nuestro entorno, como, por ejemplo, las Directrices del Garante Italiano, de 23 de noviembre de 2006.

Recientemente, esta aspiración ha dado frutos tangibles, si bien parciales, de la mano del Reglamento (UE) n.º 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), que ha venido a derogar la Directiva 95/46/CE, y que concretamente introduce tres pasajes relevantes en el contexto laboral: en primer lugar, reconoce la posibilidad de poder establecer normas específicas relativas al tratamiento de datos personales en el ámbito laboral, sobre la base del consentimiento, del cumplimiento de obligaciones establecidas legalmente, de los fines de la contratación, de la ejecución del contrato, de la gestión, planificación y organización del trabajo y/o a efectos de la rescisión de la relación laboral (considerando 155). En segundo término, permite el tratamiento de categorías especiales de datos cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral, pero teniendo en cuenta no solo la legislación nacional, sino también los convenios colectivos y el derecho de la Unión Europea, y siempre y cuando se establezcan garantías adecuadas del respeto de los derechos fundamentales y de los intereses del afectado (art. 9.2 b). En tercer lugar, señala que: 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 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 ley o por 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 relacionadas con el empleo a efectos de extinción de la relación laboral (art. 88.1). Añade, además, que: 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 (art. 88.2).

En una primera aproximación, a la luz del tenor literal de esta disposición en la que se utiliza la expresión «podrán», parece que la Unión Europea otorga una facultad, que no una obligación, a los Estados miembros de legislar sobre la materia. Ahora bien, revisando el texto del artículo 88 en su conjunto, y sobre todo teniendo en cuenta su apartado 3 *in fine*, en realidad se establece un mandato legislativo de regular el derecho a la protección de datos en el contexto del trabajo, de modo que los Estados miembros se ven enfrentados a una doble tarea: por una parte, acomodar y concretar los principios generales de protección de datos en el marco de la relación laboral; por otra, adoptar medidas adecuadas para garantizar la dignidad y los derechos fundamentales de los trabajadores ante el ejercicio de posibles controles en el lugar de trabajo (Martínez, 2017, p. 414).

Esta norma obliga, por tanto, a proceder, antes del 25 de mayo de 2018, a la aprobación de un nuevo texto de ley orgánica en la materia que incorpore la pertinente traslación del derecho de la protección de datos personales al ámbito laboral, tal y como ya se ha realizado por otros Estados de nuestro entorno: Alemania, a través de la *Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directiva (EU) 2016/680,* de 30 junio de 2017; Bélgica, mediante el texto consolidado de la *Loi relative a la protection de la vie privée á légard des traitements de données à caractère personnel*, de 8 de diciembre de 1992; Francia, adaptando algunas disposiciones de la *Loi 78-17 du 6 janvier* relativa a *l'informatique, aux fichiers et aux libertés* y de la *Loi n.º 2016-1321 du 7 octobre 2016 pour une République numérique*; Italia, incluyendo el texto consolidado del *Codice in materia di protezione dei dati personali*, aprobado mediante Decreto legislativo en 2003; o Gran Bretaña, tramitando en el Parlamento la *Data Protection Bill*.

En la actualidad, en nuestro país, se está tramitando el proyecto de ley orgánica de protección de datos de carácter personal (PLOPD), si bien, a la espera del texto definitivo, las referencias explícitas relativas al ámbito de las relaciones laborales son ciertamente escasas, pues únicamente se encuentran en el artículo 9 en relación con los datos relativos a la afiliación sindical; en el artículo 19, referido a los datos de contacto de las personas físicas que presten servicios en una persona jurídica; en el artículo 22.5, alusivo a los sistemas de control de la prestación de trabajo a través de cámaras; y en el artículo 24 por lo que hace a la obligación empresarial de informar a los empleados acerca de la existencia de sistemas de denuncias de terceros sobre posibles ilícitos.

Así pues, la previsible promulgación de una norma específica en materia de protección de datos con tan escueto contenido en materia laboral va a obligar a seguir aplicando, de un lado, el marco jurídico común de la protección de datos y, de otro, aquellas otras muchas instituciones propias del

derecho del trabajo que, por su carácter tuitivo, puedan servir para proporcionar protección frente a situaciones concretas de abuso, mostrándose, empero, cierta dificultad, en tanto en cuanto pueden entrar en contradicción dos sectores del ordenamiento jurídico inspirados en postulados distintos, máxime cuando la legislación de protección de datos aporta una regulación compleja que no adopta como norte el principio *pro operario*, no solo por los intereses que tutela, sino también por las técnicas normativas que utiliza: conviven preceptos que normativizan principios generales (que se refieren a la calidad de los datos) con disposiciones que regulan los procedimientos que deberán observarse si se quiere que la recogida y tratamiento sean legítimos, y con otros pasajes que reconocen al afectado un conjunto de derechos que refuerzan su posición (derecho de defensa), delineando, a la postre, una serie de figuras que confluyen en la materia: responsable del tratamiento, encargado del tratamiento, delegado de protección de datos y autoridades de control.

4. PRINCIPIOS E INSTRUMENTOS BÁSICOS DE TUTELA. ALGUNAS DUDAS SOBRE SU ENCAJE EN EL ÁMBITO DE LA PRESTACIÓN DE SERVICIOS POR CUENTA AJENA

En tanto en cuanto las nuevas tecnologías amplían las posibilidades de acumulación de datos de los trabajadores, aumentan la capacidad de combinación de los mismos a través de la formación de «perfiles» y multiplican exponencialmente las posibilidades de acceso y de transmisión a terceros de dicha información, no cabe duda de que debe ser de aplicación la legislación sobre protección de datos personales en los centros de trabajo con el intento por encontrar garantías adecuadas, tendentes a determinar cuándo, cómo, a quién, para qué y qué información puede ser tratada.

Parte sustancial del contenido del RGPD y también del PLOPD, al igual que en la Ley orgánica 15/1999, viene delimitado por una serie de principios generales que definen las pautas a las que deben atenerse la recogida, el registro y el uso de los datos personales (licitud, transparencia, finalidad, adecuación, pertinencia, exactitud y actualización, temporalidad, seguridad a través de la confidencialidad, seudonimización o cifrado, evaluación de impacto y responsabilidad proactiva) y por una serie de garantías de la persona que se configuran como derechos subjetivos encaminados a hacer operativos los principios genéricos (información, acceso, rectificación, supresión, bloqueo, limitación del tratamiento, portabilidad u oposición).

Como fácilmente puede colegirse, todos estos parámetros alcanzan plena virtualidad en el ámbito laboral, no ya solo por el necesario flujo de información entre el trabajador o candidato a un empleo y el empresario (los inevitables datos personales que los primeros han de revelar a los segundos o que estos últimos pueden obtener fácilmente), sino por el carácter personalísimo de la prestación del contrato de trabajo en la que se ponen en juego valores esenciales de la persona, circunstancias capaces de convertir el ámbito laboral en especialmente propicio para el surgimiento de violaciones de los derechos fundamentales derivados del uso y tratamiento de la información (Goñi, 2004a, p. 55).

Atendiendo al objeto y finalidad de la normativa de protección de datos, cual es garantizar la tutela de los derechos capaces de resultar afectados por la potencialidad lesiva de la informática aplicada al tratamiento de datos personales, procede reconducir sus minuciosas reglas, agrupándolas en una serie «macroprincipios», descendiendo al detalle de su juego en el marco de las relaciones laborales.

4.1. CONSENTIMIENTO EXPLÍCITO: MATIZACIONES A SU EXIGIBILIDAD

Entre los principios de tutela que incorpora el ordenamiento de protección de datos:

> El de la autodeterminación informativa protegería el derecho de los empleados a ser informados de que precisamente, por medio de ficheros de datos, la empresa va a poder verificar el cumplimiento de sus obligaciones laborales y otros extremos de su interés (...), debiendo conocer el contenido de la información, la procedencia de la misma, así como la existencia del propio fichero o tratamiento, la finalidad de la recogida de los datos, los destinatarios de la información (...), la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y la identidad y dirección del responsable del tratamiento (...)[7].

Item más, de conformidad con las normas y principios jurídicos que rigen la protección de datos, solo se justificará el almacenamiento cuando concurra una finalidad lícita debidamente conocida por el interesado y, por tanto, únicamente podrían conservarse aquellos extremos que resulten imprescindibles y por el tiempo necesario para cumplir con la finalidad perseguida con la adopción de dichos instrumentos.

Desde tal perspectiva, el gran postulado a partir del cual aparece vertebrada la regulación de protección de datos es, sin duda, la exigencia de una manifestación de voluntad libre, específica, informada e inequívoca por la que se acepta, mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales (arts. 4.11 y 6 RGPD y 6 PLOPD), quedando eliminada cualquier posibilidad de oposición tácita[8]. El consentimiento se podrá otorgar mediante una declaración escrita, ya sea utilizando medios tradicionales o electrónicos, incluso mediante la marcación de una casilla, o a través de una enunciación verbal; en ambos casos, de forma individualizada atendiendo a todos y cada uno de los fines perseguidos.

En efecto, como regla general, el interesado o afectado ha de prestar su conformidad explícita para la recogida o tratamiento de sus datos personales. También, como pauta general, el respon-

[7] Sentencia del Tribunal Superior de Justicia (STSJ) de Cantabria (Sala de lo Contencioso-Administrativo) de 16 de mayo de 2003 (rec. 630/2002).

[8] La doctrina constitucional atribuye al consentimiento del afectado un valor fundamental (SSTC 202/1999, de 8 de noviembre; 144/1999, de 22 de julio; 223/1998, de 24 de noviembre, o 106/1998, de 18 de mayo).

sable del tratamiento deberá proporcionarle información sobre el objeto y fines de esas operaciones, así como sobre los derechos subjetivos de los que dispone ante dicho tratamiento. Acontece, así, una unión inescindible entre ambos requisitos (consentimiento e información) a partir de la cual queda abonado el campo para hablar en este ámbito de la aparición de una verdadera especie del género «consentimiento informado» (Tascón, 2005, p. 103). Es más, se ha de garantizar al interesado la posibilidad de retirar su aquiescencia en cualquier momento (art. 7.3 RGPD).

Así pues, el trabajador ha de poder negarse a prestar el consentimiento y ha de contar con la posibilidad de rectificar posteriormente sin verse perjudicado por ello (Mercader, 2018a, p. 757)[9]. Ninguna duda cabe –como botón de muestra– sobre la necesaria concurrencia de consentimiento específico de los trabajadores para que la empresa pueda publicar en la página web corporativa su nombre, apellidos, foto, perfil profesional y aficiones, así como los resultados de la evaluación por los clientes[10]. Al igual que debe concurrir tal consentimiento para que la empresa pueda comunicar el rendimiento obtenido por un trabajador a sus compañeros, de forma que en los procesos de reestructuración en los que los criterios de selección de los afectados por los despidos se anudan a la productividad, la empresa debe adoptar las debidas cautelas en el periodo de consultas[11].

No obstante, teniendo en cuenta las dificultades que la obtención del consentimiento puede implicar, el propio ordenamiento de protección de datos establece algunas excepciones de interés en el marco de las relaciones laborales (art. 6.1 c) RGPD):

1. La primera contempla «el cumplimiento de una obligación legal aplicable al responsable del tratamiento», lo cual justifica –en paradigmático ejemplo– la disposición en la nómina sin necesidad de ningún tipo de *placet* por parte del trabajador de datos personales como el número de hijos, la existencia de discapacidad o la obligación de satisfacer determinadas prestaciones económicas por resolución judicial. Como agravante, procede tener en cuenta que la confección de los recibos de salarios normalmente se encomienda por la empresa a terceros (gestorías, asesorías, gabinetes jurídicos...), a los cuales se remiten, vía *e-mail*, los datos mes a mes, siendo necesario –eso sí– que dicha información se envíe encriptada o cifrada, utilizando cualquier medio capaz de impedir que la misma sea manipulada.

   Sobre el empresario pesa también la obligación legal de entregar copia básica a los representantes de los trabajadores de todos los contratos que deban ser celebrados por escrito, con la excepción de los relativos a la relación laboral de alta dirección. Tal entrega no requiere –*ex lege*– consentimiento expreso y específico del trabajador contratante, pues razones de interés público (básicamente fundadas en la cons-

[9] Grupo de trabajo del artículo 29 –GT29–. *Opinion 15/2011*.

[10] Informe de la Agencia Española de Protección de Datos –Informe AEPD– 2010-0039.

[11] Informe AEPD 0529-2009.

tatación jurídico-práctica de que el trabajador asume de ordinario la condición de contratante más débil) llevan a pensar al legislador que la exigencia del consentimiento previo del trabajador supondría, en realidad, un elemento decisivo para la inefectividad del deber, habida cuenta la incontestable y ya reseñada posición de supremacía contractual del empresario. El contenido de este documento puede suscitar importantes problemas de interpretación a los efectos de este estudio; no en vano, la revelación de ciertos datos del contrato también podría suponer un atentado a la intimidad del trabajador. En efecto, el problema jurídico puede surgir cuando colisionan dos derechos constitucionales como son el individual del trabajador contratado a su privacidad (art. 18.1 CE) y el colectivo de los representantes de los trabajadores (fundado en un interés legítimo derivado de las funciones representativas reconocidas por el art. 129.2 CE, en relación con los arts. 7, 9.2 y 28.1 CE y con las normas dictadas en su desarrollo) a evitar cualquier contratación irregular. Si la finalidad de la entrega de la copia básica encuentra justificación legal en la verificación de que el contrato cumple con la legalidad vigente para, si apreciada la inadecuación, efectuar las denuncias oportunas tendentes a facilitar la actuación inspectora de la Administración, es lógico pensar que los datos contenidos deben ser únicamente aquellos que pueden ser objeto de la actuación inspectora, ciñéndose al momento preciso en el cual aquel contrato fue concertado.

Igualmente, resultan almacenables los datos personales cuyo conocimiento por el empresario sea necesario por la índole del contrato (titulación del trabajador para concertar un vínculo en prácticas, por ejemplo) (San Martín, 2014, p. 220).

2. Otras excepciones se refieren a aquellos supuestos en los cuales «se trata de cumplir un fin de interés público» (tal y como sucede, por ejemplo, con la proyectada creación de la «tarjeta social universal», en la que se recogerán los datos relativos a prestaciones sociales públicas de contenido económico de una determinada persona física), o de facilitar «el ejercicio de poderes públicos conferidos al responsable del tratamiento» (el Tribunal Supremo ha entendido que la empresa saliente ha de informar a la entrante si algún trabajador carece de la habilitación necesaria en un supuesto de cesión de contratas de vigilancia y seguridad)[12] o, en fin, «para la satisfacción de intereses legítimos», respecto de los cuales es necesario realizar una evaluación aplicando el principio de proporcionalidad. Se nota aquí la falta de adaptación específica del ordenamiento de protección de datos al mundo laboral, pues muy bien pudiera haberse previsto algún tipo de información a los representantes unitarios o sindicales de los trabajadores, quienes quedaron completamente olvidados por la regulación anterior y por la presente.

3. Mención separada merece la previsión introducida en el artículo 7 del RGPD y en el artículo 6.3 del PLOPD relativa a que no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que

[12] Sentencia del Tribunal Supremo (STS) de 28 de septiembre de 2011 (rec. 4376/2010).

no guarden relación con el mantenimiento, desarrollo o control de la relación contractual. Se está reconociendo, por tanto, la posibilidad de entender que el consentimiento de los trabajadores estaría viciado si el asentimiento a la utilización de sus datos personales se incluye, como una cláusula contractual indiferenciada, entre las condiciones laborales.

Por su parte, el artículo 19 del PLOPD sienta que estará amparada como excepción al consentimiento la utilización de aquellos datos de contacto de las personas físicas que presten servicios en una persona jurídica siempre que «el tratamiento se refiera únicamente a los datos necesarios para su localización profesional». Esta posibilidad debe ser interpretada en sentido estricto, quedando extramuros de la misma los datos relativos al teléfono móvil, dirección de correo electrónico particular de los trabajadores o claves de acceso a las redes sociales, pues, como ha reconocido la Audiencia Nacional, son nulas las cláusulas contractuales en las que se obligue al trabajador a disponer de medios propios (móvil e internet) y proporcionar los enlaces a la empresa para que esta pudiera efectuar cualquier comunicación referida a la relación laboral, siendo necesario que el empleado manifieste expresamente su consentimiento a tales efectos; no en vano, la LOPD no solo protege datos íntimos, sino también datos de carácter personal, impidiendo su tráfico ilícito y lesivo para la dignidad del afectado, de modo que estos solo pueden ser tratados y cedidos con su aquiescencia[13]. En este mismo sentido, el Tribunal Supremo ha reconocido recientemente que las direcciones IP, al contener información concerniente a personas físicas «identificadas e identificables», son datos personales que no pueden usarse sin el consentimiento de sus titulares[14].

4.2. TRANSPARENCIA

Tampoco hace falta prestar el consentimiento cuando el tratamiento sea necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación, a su petición, de medidas precontractuales (art. 6.1 b) RGPD). Aun en términos estrictos, la proyectada normativa, al igual que hacía la LOPD, parte de la idea de que el consentimiento va implícito en la mera aceptación de la oferta o en la perfección del contrato, pues reconoce en el artículo 19, como excepción al consentimiento: «Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios». Como ha señalado el Tribunal Constitucional, «no hay habilitación legal expresa para la omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales»[15].

[13] Sentencia de la Audiencia Nacional (SAN) de 28 de enero de 2014 (rec. 428/2013).

[14] STS (Sala de lo Contencioso-Administrativo) de 3 de octubre de 2014 (rec. 6153/2011).

[15] STC 29/2013, de 11 de febrero.

Particularmente significativo es el pronunciamiento judicial, que reconoce que:

> La transmisión de datos por una empresa del sector telemarketing a otra entidad aseguradora de automóviles, que se limitan a la cesión del nombre, apellidos y DNI del trabajador adscrito al cometido de la gestión telefónica de los siniestros asegurados por la segunda, viene exigida por el propio vínculo suscrito entre ambas patronales, pues la actividad de telemarketing, prestada por la primera a favor de la aseguradora, y que fue el objeto del contrato, precisa el acceso por el trabajador a datos sensibles de la empresa cliente, y por ello, y por propia seguridad, esta última puede necesitar y exigir conocer quién utiliza y entra en sus sistemas, asignando claves de usuario de forma personalizada, para lo que se han de aportar el nombre, los apellidos y el número del DNI del trabajador adscrito a tales cometidos (...), [máxime si] de conformidad con el número 2 del art. 6 LOPD «no será preciso el consentimiento cuando los datos de carácter personal (...) se refieran a las partes de un contrato de trabajo o precontrato de una relación negocial o laboral (...)»[16].

Ahora bien, aunque no se exija el consentimiento del trabajador, sigue siendo necesario que el titular de la recogida de datos observe el deber de información sobre la recogida, tratamiento, uso, plazo de conservación y destino (arts. 13 y 14 RGPD y 11 PLOPD), distinguiendo si los datos personales se obtienen o no del interesado. Aun cuando no se exige la preceptiva formalización por escrito del traslado de las pertinentes referencias que integran el deber de transparencia, lo cierto es que ha de realizarse a través de un medio que permita acreditar su cumplimiento, siendo muchas veces insuficiente la comunicación verbal, máxime cuando además de la información básica se le ha de indicar una dirección electrónica u otro medio que permita al interesado acceder de forma sencilla e inmediata a las restantes circunstancias[17].

Dentro del catálogo de extremos que componen este principio de transparencia se encuentra el destinatario, se trate o no de un tercero, expresión esta última que incluye a los propios encargados del tratamiento, definidos en el propio RGPD como toda «persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento» (art. 4.8), entendiendo que en este ámbito también hay cesión de datos (De Miguel, 2018, p. 1)[18].

Así pues, el empresario ha de informar con carácter previo y de modo expreso, preciso e inequívoco de la existencia del fichero, del objeto y finalidad para el que se ha creado, de cuál va a ser su posterior utilización, de la identidad y dirección del encargado del tratamiento y de la dis-

[16] STSJ de Madrid de 30 de junio de 2008 (rec. 2351/2008).

[17] Resoluciones AEPD 00500/2009 y 01823/2008.

[18] *Guidelines on transparency under Regulation* 2016/679 (WP260).

posición que sobre los datos va a tener el trabajador y del modo en que el afectado podrá hacer uso de los derechos que el ordenamiento de protección de datos le confiere, de suerte que si este no es alertado de manera completa sobre las circunstancias particulares, así como del alcance y ámbito de actuación, el procedimiento deberá reputarse ilegal (Thibault, 2009, p. 219). Asimismo, la Audiencia Nacional se ha pronunciado sobre el alcance de la obligación de informar en una reciente sentencia en la cual una empresa había solicitado determinados datos de identificación de empleados, transportistas autónomos o personal de empresas de servicios, con la finalidad de establecer una tarjeta de identificación que sirviera de credencial ante los clientes. La recogida de información se efectuó por medio de una ficha manual. La entidad alegó que los trabajadores conocían en todo momento la existencia del fichero porque había sido objeto de una publicación interna y se había informado al comité de empresa. Sin embargo, el órgano juzgador considera que la corporación no cumplió con la obligación de información, pues, aunque se admitiera que los afectados conocían la finalidad de los datos que figuraban en la ficha, la ley exige que la actividad informativa sea más precisa y se ponga en conocimiento de los afectados, además de la existencia del fichero y de su finalidad, el carácter obligatorio o facultativo de las respuestas, las consecuencias de la facilitación de los datos o de la negativa a suministrarlos, la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación y, por último, la identidad y dirección del responsable del fichero[19].

4.3. LICITUD Y FINALIDAD

Como es obvio, la exigencia de un tratamiento lícito, leal y transparente que incorpora el artículo 5.1 a) del RGPD tiene un *prius* lógico en cuanto a los medios a través de los cuales los datos pueden ser obtenidos: la utilización de vías fraudulentas, desleales o ilícitas viciará de raíz la información y, sin perjuicio de las responsabilidades de otro tipo a las que pudiera dar lugar (singularmente penales), queda terminantemente prohibido su tratamiento automatizado, en este caso, por el titular de la organización productiva.

Tal sucederá, por ejemplo, con determinadas investigaciones privadas a través de detectives con nula incidencia en el desarrollo de la actividad laboral o con la obtención de información sobre comportamientos de los trabajadores utilizando cauces lesivos de sus derechos fundamentales, lo que va a conducir a la inadmisión de la prueba aportada o, en su caso, a su no valoración en el juicio si en su momento fue admitida de forma provisional. La inutilidad de una prueba ilegal es, por tanto, doble: ni se debe admitir la práctica de dicha prueba (decisión judicial de inadmisión) ni se deben aceptar por el juez sus resultados fácticos en el caso de haberse practicado dentro o fuera del proceso (decisión judicial de exclusión de sus resultados a la hora de su valoración).

De forma harto ilustrativa, el artículo 5.1 b) del RGPD establece también que los datos habrán de ser «recogidos con fines determinados, explícitos y legítimos», sin que puedan ser tratados posteriormente «de manera incompatible con dichos fines». Debe existir, por tanto, un motivo determina-

[19] SAN de 30 de noviembre de 2011 (rec. 415/2000).

do, explícito, justificado y legítimo para la recogida de los datos y su clasificación, de modo que las informaciones de carácter personal no podrán utilizarse para finalidades «incompatibles» con aquellas para las que hubieran sido recogidas, lo que no significa, sin embargo, que no puedan utilizarse para finalidades diferentes (AEPD-ISMS Forum, 2017, p. 11). A la hora de valorar la compatibilidad de usos posteriores con la finalidad original, procede tener en cuenta los siguientes criterios: debe existir una relación entre la finalidad original y la finalidad o finalidades ulteriores; el tratamiento posterior debe encontrarse dentro de las expectativas razonables del interesado; han de tenerse en cuenta la naturaleza de los datos objeto de tratamiento y la sensibilidad de los mismos; es menester considerar el impacto que este tratamiento va a tener en los interesados, y deben atenderse las medidas de protección que el responsable del tratamiento establece, en particular, las medidas técnicas y organizativas: encriptación, seudonimización, separación funcional, transparencia u oposición al tratamiento[20].

Tanto la Recomendación número 89 del Consejo de Europa como el Código de Conducta aprobado por la OIT entienden, además, que la utilización de las informaciones personales para otras finalidades puede ser compatible con la inicial solo cuando se deriven beneficios para el trabajador o no se rompan las garantías. Lo importante es que el nuevo uso se justifique también en función del contrato de trabajo y que el empleado sea debidamente informado para que pueda ejercer sus derechos. Así, se ha considerado finalidad legítima la obligación de los trabajadores de un banco con información privilegiada de comunicar las operaciones financieras realizadas por ellos y por sus familiares, valorando que se trata de una medida dirigida a garantizar la imparcialidad e independencia en sus quehaceres laborales[21]. También la práctica de una empresa de hacer constar en los tiques, resguardos o justificantes de compra que se entregan a los clientes el nombre y apellido del trabajador vendedor que interviene en la operación de venta, así como las expresiones «Sr./Srta.»[22]. Igualmente, la utilización del dato sobre la afiliación sindical del trabajador para conceder el trámite de audiencia a los representantes sindicales en un despido, pese a que ese extremo se proporcionó para el descuento de la cuota sindical[23]. O la utilización de los datos personales (nombre y apellidos) de los trabajadores por parte de su antigua empleadora, previo cese voluntario de los mismos, para la creación por ellos de una nueva empresa, con el fin de advertir a los clientes sobre la terminación de la relación laboral y la inexistencia de vinculación con la entidad[24].

La finalidad debe definirse, además, de la manera más precisa posible: se prohíbe la creación de grandes bancos de datos personales alimentados para fines más o menos indeterminados, de modo que no será acorde con la norma una definición o descripción vaga del objeto del tratamiento, como «fines laborales», por ejemplo, sino que el empresario deberá precisar cuál es la decisión profesional

[20] GT29. *Opinion 03/2013 on purpose limitation* (2 April 2013).

[21] STS de 7 de marzo de 2007 (rec. 132/2005).

[22] STS de 18 de diciembre de 2006 (rec. 112/2005).

[23] Informe AEPD. Utilización de la afiliación sindical en los procedimientos de despido. 2002.

[24] SAN de 15 de junio de 2005 (rec. 669/2003).

última que justifica un tratamiento: selección de personal, contabilidad, gestión de horarios, carrera profesional, formación, seguridad, control, etc. Aun cuando aparentemente podría entenderse autorizado un uso «plurifuncional» de los datos, ante la indeterminación de cuáles son los «fines incompatibles», en realidad se trata de una exigencia para las partes del contrato laboral de actuar en el proceso de captación de datos de buena fe, evitando todo tipo de estrategias engañosas tendentes a recabar referencias personales que bien trascienden el marco profesional de la prestación debida y recaen sobre la misma persona del trabajador, o bien resultan excesivas para verificar el cumplimiento por este de sus obligaciones y deberes en el marco de la prestación de servicios (Thibault, 2006, p. 25).

En paradigmático ejemplo, si se anotan «partes de baja» para el cuidado de la salud de los trabajadores, no pueden usarse después, como ha señalado el Tribunal Constitucional, para adoptar medidas de control del absentismo laboral[25], al igual que tampoco puede cederse el reconocimiento médico practicado por una empresa o una mutua para la elaboración de un informe sobre el mismo trabajador destinado a otra empresa, que provocó la extinción del contrato en periodo de prueba[26], ni, por idéntico motivo, pueden crearse archivos donde aparezca solo la fecha de la baja a los efectos de controlar el absentismo[27]. En este mismo sentido, se considera ilegítimo el descuento empresarial de los salarios a todos los trabajadores respecto de los que constaba la afiliación a los sindicatos convocantes de la huelga sin verificar previamente su participación en esta y pese a que los datos se habían proporcionado exclusivamente para el descuento de la cuota sindical[28]. También se ha considerado incompatible la utilización de los datos del fichero denominado «gestión de personal» para realizar un proyecto de investigación sobre los niveles de comunicación existentes en la empresa, por medio de un cuestionario que ella misma aprobó y que incluía preguntas sobre el estado de salud y la ideología de los trabajadores[29].

4.4. PERTINENCIA, ADECUACIÓN Y LIMITACIÓN: MINIMIZACIÓN DE LOS DATOS ANTE EL PODER DE CIBERVIGILANCIA EMPRESARIAL

La información que por vía automatizada se pretende recabar o acumular ha de ser adecuada, pertinente y proporcional (art. 5.1 c) RGPD); esto es, no solo debe ser legítima en el sentido antes apuntado, sino conforme a la finalidad pretendida (en lógica exigencia de congruencia) y también proporcionada, entendiendo por tal la acreditación de un nivel de recogida y almacenamiento de datos «no excesivo» respecto a dicha finalidad.

25 STC 202/1999, de 16 de diciembre.

26 Resolución AEPD 00740/2005.

27 STS (Sala de lo Contencioso-Administrativo) de 5 de marzo de 2012 (rec. 1104/2009).

28 SSTC 11/1998, 33/1998, 45/1998, 60/1998, 77/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 125/1998, 126/1998, 158/1998, 223/1998, 30/1999, 44/1999 y 45/1999.

29 SAN de 8 de marzo de 2002 (rec. 948/2000).

La ausencia de mayor precisión y de jurisprudencia consolidada a este respecto no impide poder colegir cuáles serán los parámetros generales para medir la pertinencia y la proporcionalidad de los datos informáticos requeridos o acumulados en el marco de las relaciones laborales. En cuanto a la fase de selección se refiere, quedará prohibida la recogida de aquellos extremos no estrictamente necesarios para llevar a cabo la valoración de la capacidad profesional del candidato, siendo «excesiva» (y, en consecuencia, prohibida) cualquier otra averiguación sobre hechos no imprescindibles para su determinación, en cuanto supone –en esa medida– un abuso en el proceso de obtención de información del trabajador. En lo relativo a la recogida o acumulación de datos informáticos durante la vida laboral del trabajador, parece clara la exigencia de que obedezca a efectivas y reales exigencias organizativas, productivas o de seguridad en el trabajo, es decir, a un interés empresarial serio y, por tanto, legítimo, siempre y cuando no lleve aparejado un abuso o invasión injustificada en la esfera privada del individuo (Tascón, 2008, p. 455).

La AEPD, en respuesta a una consulta efectuada sobre la legalidad del control de la productividad, ha declarado que:

> En el ámbito de la relación jurídica que existe entre los empleados y la empresa en la que prestan sus servicios, debe entenderse adecuado que el empleador recabe los datos que sean precisos para el normal desenvolvimiento de la misma y, dentro de estos datos, parece adecuado que se obtengan del empleado los correspondientes a su identidad a efectos de comprobar el grado de cumplimiento de las obligaciones que competen a los empleados (Goñi, 2017, p. 23).

Ahora bien, los nuevos sistemas tecnológicos permiten registrar y conservar datos sobre los más irrelevantes detalles del comportamiento de un trabajador dentro o fuera del lugar de trabajo, sin que la mayoría de las veces el trabajador tenga conocimiento alguno de esa información, que puede referirse no solo a datos relativos a su actividad, pausas, rendimiento, evaluación del desempeño o trayectoria profesional, sino a circunstancias concernientes a sus relaciones, amistades, salud, ideología, afectividad o comportamiento íntimo. Hasta el momento, en el ordenamiento jurídico español solo se cuenta con el escueto enunciado del artículo 20.3 del Real Decreto legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido del Estatuto de los Trabajadores (ET), 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 a su dignidad». Este precepto utiliza una genérica declaración que comporta evidentes dudas sobre los límites aplicables, provocando una constante intervención de los órganos judiciales que vienen realizando un loable esfuerzo de cobertura del vacío normativo.

Ciertamente, el RGPD, en su artículo 88, obliga a contemplar concretamente, dentro de «las medidas adecuadas y específicas para preservar la dignidad humana de los interesados, así como los intereses legítimos y sus derechos fundamentales», una regulación legal o convencional directa de «los sistemas de supervisión en el lugar de trabajo», lo cual implica la aplicación de la normativa de protección de datos personales y, en concreto, el principio de minimización

en el tratamiento, cualquiera que sea el método utilizado para descubrir posibles incumplimientos laborales de los trabajadores: sobre los accesos o desplazamientos del trabajador en el lugar de trabajo a través de puertas gobernadas electrónicamente y con un lector conectado a un ordenador (*badges* con códigos de identificación personal), sobre las llamadas telefónicas efectuadas gracias a la imbricación del teléfono utilizado por el trabajador con una centralita «computerizada» y sobre el uso del correo electrónico, sobre la navegación por páginas web o el alojamiento en Dropbox o la interacción en redes sociales, no siendo infrecuentes tampoco la instalación de programas espía, los controles biométricos o por infrarrojos, los test sobre el patrón de consumo de alcohol y drogas, los identificadores por radiofrecuencia como instrumentos de localización a distancia, las webcam conectadas a un ordenador gracias al protocolo TCP/IP, los microchips y otros sistemas de videovigilancia (Tascón, 2005, p. 131).

De toda esta urdimbre de instrumentos tecnológicos, particular atención merecen los siguientes:

1. El RGPD y el PLOPD regulan los tratamientos con fines de videovigilancia realizados por los empleadores[30], exigiendo el artículo 22.5 del PLOPD que los datos obtenidos a través de sistemas de cámaras para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 del ET se lleven a cabo dentro del marco legal y con los límites inherentes, siendo necesario como regla general informar a los trabajadores sobre esta medidas.

   Los límites a la utilización de las cámaras de vídeo en la vigilancia empresarial es uno de los grandes puntos de controversia judicial, por cuanto este instrumento es susceptible de ampliar los grandes poderes del empresario y de comprimir claramente los derechos de los trabajadores. La videovigilancia, en cuanto permite la captación y grabación en un soporte físico de la imagen, así como la repetición ilimitada y el análisis detenido de los fotogramas conservados, constituye no solo un instrumento de supervisión del cumplimiento de la actividad laboral del trabajador y un valioso instrumento de prueba de los incumplimientos, sino una herramienta que permite crear una base de datos de información personal (*data vigilancia*) y obtener perfiles sociales de los trabajadores afectados (Goñi, 2009, p. 11).

   Lógico es pensar que, atendiendo al principio de buena fe contractual, si el empresario no informa al trabajador de que está siendo controlado, entonces la injerencia empresarial debe ser considerada ilícita, máxime si se atiende a dos recientes pronunciamientos del Tribunal Europeo de Derechos Humanos: uno, de 28 de noviembre de 2017 (asunto Antovic and Mirkovic contra Montenegro)[31], que consi-

[30] La garantía del derecho a la protección de datos personales en los supuestos de videovigilancia se ha reconocido en la STJUE de 11 diciembre 2014, asunto Rynés.

[31] *Aplicattion* núm. 70838/13.

dera inadecuada la instalación de cámaras en los auditorios universitarios donde se imparten clases por invadir el derecho a la vida privada de los profesores demandantes, quienes no autorizaron dicha grabación y únicamente conocieron la instalación por el informe que proporcionó el decano en la junta de facultad con el fin de garantizar la seguridad de los bienes y las personas, incluidos los estudiantes y la vigilancia de la enseñanza; otro, de 9 de enero de 2018 (asunto López Ribalda contra España)[32], que entiende ilícita, por vulnerar el artículo 8 del Convenio Europeo de Derechos Humanos, una vigilancia continua no informada a través de cámaras ocultas sobre unas cajas de un supermercado demostrativa de la comisión de hurtos sucesivos por parte de algunas trabajadoras, reconociendo además una indemnización de daños morales y recordando la obligación de los Estados miembros del Consejo de Europa de tomar medidas para garantizar el respeto a la vida privada de los ciudadanos, extremo no observado por el Estado español (Rojo, 2018, p. 135). Considera que el interés legítimo del empleador podría haberse tutelado de una forma menos intrusiva, informando de forma previa y específica, no de manera equívoca o genérica y, mucho menos, presunta (Molina, 2018a, p. 134). Entiende, sin embargo, que los tribunales españoles no vulneraron el derecho de las afectadas a un proceso justo, al haber valorado también otras pruebas.

Estas conclusiones, sin embargo, no son plenamente coincidentes con la tesis mantenida por la STC 39/2016, de 3 de marzo, que admite como prueba lícita, justificativa de un despido derivado de la apropiación de dinero en una caja registradora, las grabaciones de una cámara de vigilancia instalada ante la existencia de sospechas previas y ello pese a que no se informó expresamente a la trabajadora de la colocación ni la finalidad del sistema de control. Entiende el máximo intérprete de la Constitución que el deber empresarial de información se vio cumplido mediante la simple visualización del correspondiente distintivo informativo (el cartel indicativo de «zona videovigilada») en un lugar visible.

Como único avance normativo dentro de una imperante inseguridad, el artículo 22.5 del PLOPD exige información por parte de los empleadores a los trabajadores acerca del sistema de videovigilancia, si bien, lo que no deja de causar perplejidad, en el supuesto de que «las imágenes hayan captado la comisión flagrante de un acto delictivo, la ausencia de la información a la que se refiere el apartado anterior no privará de valor probatorio a las imágenes, sin perjuicio de las responsabilidades que pudieran derivarse de dicha ausencia». Todo ello sin olvidar que el artículo 22.3 exige que los datos sean suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones.

Cabe preguntarse, a la luz de las novedades normativas singularmente derivadas del RGPD y de las decisiones del Tribunal Europeo de Derechos Humanos, si la

[32] *Aplicattions* núms. 1874/13 y 8756/13.

existencia de cámaras de videovigilancia en el interior de un centro de trabajo, cuya finalidad es asegurar la seguridad del mismo frente a robos y otros hechos ilícitos, con un rótulo informativo de tal finalidad, permite utilizar las imágenes de los trabajadores así obtenidas para fines distintos a la seguridad, como son el control de la actividad laboral y, de añadido, se usa como prueba en un proceso ulterior en contra del titular de dichos datos, todo ello sin contar con la autorización judicial previa para el acceso particular a unos ficheros de imágenes obtenidos para fines distintos (Preciado, 2017, p. 184).

2. No menos controvertida es la cuestión relativa a los registros sobre el ordenador utilizado por el trabajador, recurriendo muchas veces a programas espías (*web bugs*), que permiten el acceso subrepticio al ordenador del trabajador sin violar su *password*, o «registradores de teclas» que facilitan la averiguación de las contraseñas, sobre todo para inspeccionar el sistema de mensajería o los accesos a internet (Miñarro, 2004, p. 13). Todos estos supuestos constituyen también un tratamiento de datos del trabajador, pues se memoriza una información del trabajador susceptible de ser tratada.

   El registro directo de los terminales informáticos utilizados por los trabajadores (*hardware*) y el control del uso de internet y del correo electrónico ha dividido a la doctrina y a la jurisprudencia sin que todavía hoy se haya alcanzado una postura claramente asentada, si bien cabe mencionar, como último hito importante, el pronunciamiento en Gran Sala del Tribunal Europeo de Derechos Humanos el 5 de septiembre de 2017 (Bărbulescu II), en el que se reconoce que los tribunales rumanos no verificaron si, pese a la existencia de instrucciones del empleador sobre el uso de los dispositivos, el trabajador había sido advertido con anterioridad de la vigilancia que iba a llevarse a cabo de las comunicaciones electrónicas efectuadas desde su cuenta profesional ni tampoco hasta qué punto se ha producido una intromisión en la vida privada del trabajador en el ámbito de la relación de trabajo que hubiera podido alcanzarse por vías menos invasivas (Cuadros, 2017, p. 139). Considera que no es suficiente, atendiendo al Código de buenas prácticas para la protección de los datos personales del trabajador de 1999 y a la Recomendación del Comité de Ministros del Consejo de Europa (CM/Rec. 2015), sobre tratamiento de datos personales en el ámbito de la relación laboral, que la empresa hubiera remitido una notificación a sus empleados en la que se ilustraba sobre el despido de una trabajadora por motivos disciplinarios, después de haber utilizado para fines privados internet, el teléfono y la fotocopiadora, sino que es necesario un aviso previo, antes de que comience la supervisión. De este pronunciamiento pueden extraerse interesantes conclusiones: a) el trabajador ha de ser informado de las medidas que el empresario adopte a fin de controlar los medios de comunicación; b) es necesario diferenciar los flujos de comunicación de su contenido; c) el segundo control, el de los contenidos, exige justificaciones claras y, de producirse, han de instrumentarse mediante el establecimiento de unas efectivas garantías a favor del trabajador; d) la información facilitada al trabajador ha de efectuarse con claridad y transparencia,

y e) ha de realizarse, adicionalmente, con anterioridad a que se active y comience el control (Valdés, 2017, p. 34). Muy significativa es la consideración que alerta sobre que:

> Las instrucciones de un empleador no pueden reducir la vida social privada en el lugar de trabajo a cero, el respeto de la vida privada y de la confidencialidad de la correspondencia, que siguen existiendo, aun cuando pudieran estar restringidos en la medida de lo necesario (Gallardo, 2017, p. 154)[33].

Por lo tanto, para ser legítimo, el control debe superar, primero, el test de transparencia en cuanto a la información previa y, segundo, el de proporcionalidad en lo que respecta a la preferencia de controles menos invasivos frente a los más intrusivos, solo admitidos siempre que no exista otra opción real y no una mera comodidad o conveniencia empresarial (Molina, 2017, p. 293). En definitiva, aunque el tribunal reconozca que el empleado tiene un interés legítimo en garantizar el buen funcionamiento de la empresa, y que esto puede hacerse mediante el establecimiento de mecanismos para verificar que sus empleados cumplan con sus deberes profesionales de mantera adecuada y con la diligencia necesaria, concluye que, tras un examen de los factores concurrentes, se vulneró la legislación aplicable internacional y europea en materia de protección de datos y los tribunales nacionales no establecieron un equilibrio justo entre los intereses del empresario y los derechos del trabajador (Martínez, 2017, p. 423).

3. En los momentos actuales,

> Cualquier utensilio conectivo, sean correos electrónicos, móviles, tabletas, teléfonos inteligentes, etc., transmuta los escenarios de desenvolvimiento de las ocupaciones laborales pues ubican a los trabajadores fuera de las unidades productivas típicas: empresas, centros y puestos. La unidad locativa por excelencia, o sea, el puesto de trabajo, se antoja movible, abierto, multifuncional y desespacializado (Alemán, 2017, p. 12).

Gracias a los sistemas de videoconferencias, del correo electrónico, el WhatsApp, las redes sociales, el alojamiento en la nube y todo un sinfín de herramientas de trabajo colaborativo disponibles a través de internet, los trabajadores pueden recibir órdenes e instrucciones del empresario cualquier día de la semana o del año y a cualquier hora del día o de la noche (*anywhere, anytime*).

[33] *Cfr*. ordinal 80 Bărbulescu II.

Ante esta «disrupción tecnológica» (Mercader, 2017, p. 24), debe ir cobrando fuerza el conocido «derecho de desconexión» del trabajador en aras de no perjudicar su bienestar. En paralelo, la expansión de distintas plataformas de internet, conocidas como redes sociales, amplían el concepto lugar de trabajo como presupuesto de la comisión de infracciones en materia laboral, pues los nuevos dispositivos permiten conectarse desde cualquier ubicación y en cualquier momento, quedando seriamente desdibujado el concepto de *locus laboris*. En estos nuevos contextos productivos, la aplicación del principio de minimización en el manejo de los datos debe adquirir un protagonismo esencial.

Resulta preocupante también –y en contrapartida– el hecho de que los tribunales pierdan de vista, a veces, que «la empresa no es una fortaleza inexpugnable frente a los valores y derechos constitucionales» (Carrillo, 2016, p. 1) y olviden, en ocasiones, la ilicitud de aquellos sistemas de control de tiempos de trabajo excesivamente rigurosos y exhaustivos, es decir, aquellos que permiten controlar minuto a minuto la actividad laboral y las más irrelevantes pausas y ausencias, sin dejar «el más mínimo espacio vital» dentro de la corporación. Sistemas de control de esta naturaleza, salvo que se justificara su carácter indispensable para el necesario desarrollo del proceso productivo y no tuviera cabida otro método menos gravoso para los derechos del trabajador, deberían considerarse por los órganos judiciales atentatorios a la dignidad y libertad del operario, máxime cuando no cabe una identificación absoluta entre «vida íntima» y «vida privada» (entendida esta como «no laboral») a través de la cual negar la existencia –y consiguiente exigencia para el empresario– del derecho a la intimidad del trabajador en el centro de trabajo, sobre todo cuando aquel no está realizando la prestación laboral (descansos, por ejemplo), pero con necesaria extensión a otros lugares (lavabos, vestuarios, aseos...), cuyo control y vigilancia (continua o esporádica) por medios audiovisuales suponen –de ordinario– un ataque frontal al derecho a la intimidad[34]; como también lo son, sin duda, las intromisiones mediante otros medios técnicos en comportamientos, actitudes o gestos del trabajador durante la jornada de trabajo verdaderamente irrelevantes a la hora de valorar la prestación laboral pero cuya posesión por el empresario puede ocasionarle consecuencias negativas (*licenza comportamentali*).

Un examen tan exhaustivo y permanente que llegue a acabar con cualquier resquicio de intimidad y autonomía en el lugar de trabajo supondría situar el poder de vigilancia en una dimensión inhumana, capaz de poner en peligro no solo la liber-

[34] STSJ de Madrid de 17 de abril de 2009 (rec. 5665/2008). Digna de especial mención es la STSJ de Madrid de 20 de diciembre de 2006 (rec. 3688/2006), que entiende como el módulo de espera o de descanso del personal de asistencia en tierra en un aeropuerto es un ámbito privado en el que no cabe instalar un sistema de vigilancia con grabación de imagen y sonido y con presencia de un detective camuflado, pese a que se acredita que en el módulo se produce el consumo de bebidas alcohólicas y drogas, se juega al fútbol utilizando cajas y deteriorando el mobiliario, se consumen productos de alimentación de aviones entregados por una azafata y un empleado del *catering* y se ensucia el local.

tad y la dignidad del trabajador, sino también su propio equilibrio psíquico, y de elevar el poder empresarial al grado de omnipotente, anónimo e invisible.

4. Lógicamente, el empresario podrá realizar un cierto control extramuros del centro de trabajo cuando la prestación se realice fuera de él a través de los dispositivos de geolocalización, siendo de aplicación las disposiciones de protección de datos (Molina, 2018b, p. 137); no en vano, el artículo 2 de la Directiva 2001/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, define los datos de localización como «cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público».

   La AEPD, en su Informe 193/2008, establece, igualmente, que los extremos obtenidos a través del sistema de geolocalización (rutas seguidas, tiempos de parada, velocidad, consumo de combustible del vehículo, etc.) están asociados a información concerniente a una persona física identificada o identificable a través de los lugares que frecuenta, de modo que, según el artículo 3 a) de la LOPD, se consideran datos de carácter personal, merecedores de todo el entramado garantista previsto en esta ley. Por tal motivo, en vía judicial, además de cumplir el principio de proporcionalidad, el control mediante GPS «totalmente camuflado», «con difícil acceso» y «sin advertencia a los trabajadores de su instalación» se ha calificado como una infracción de la buena fe empresarial[35]. Asimismo, se considera inválido el control de una trabajadora por GPS fuera de su jornada laboral, pues ha sido informada de que su vehículo dispone de un control de geoposicionamiento, cuyo objeto es «garantizar la seguridad y coordinación de los trabajos», siendo impertinente la vigilancia realizada durante los fines de semana y también durante una baja laboral[36].

   En esta misma línea, algún pronunciamiento judicial considera que efectivamente queda afectado el derecho a la intimidad del trabajador si el empresario utiliza un canal de control del trabajo de sus empleados que se desarrolla fuera de sus dependencias a través de un sistema de localización permanente del teléfono móvil (GMS) facilitado como instrumento de trabajo, sin consentimiento ni conocimiento de los trabajadores, máxime si estos han de tenerlo a su disposición en todo momento por estar sujetos a disponibilidad permanente, ya que, si bien resulta un medio idóneo para supervisar su labor, en modo alguno resulta necesario a este fin[37]. Ejemplo paradigmático puede encontrarse también en una sentencia que ha considerado factor de riesgo la instalación de un dispositivo denominado «acelerómetro» en cada uno

[35] SSTSJ de Madrid de 29 de septiembre de 2014 (rec. 1993/2013) o de Castilla-La Mancha de 17 de junio de 2014 (rec. 1162/2013).

[36] STSJ de Andalucía de 19 de octubre de 2017 (rec. 1149/2017).

[37] STSJ del País Vasco de 2 de julio de 2007 (rec. 1175/2007).

de los teléfonos móviles de los trabajadores con un componente microelectromecánico cuya función es captar los movimientos bajo el pretexto de servir a un protocolo de actuación ante un posible accidente[38].

No faltan, sin embargo, interpretaciones más permisivas de conformidad con las cuales se admite la instalación de un GPS en el vehículo de la empresa utilizado por el trabajador en sus desplazamientos, pues no existe otro mecanismo eficaz para verificar el cumplimiento de la prestación laboral al realizarse esta fuera del lugar de trabajo, máxime si se tiene en cuenta que mediante un dispositivo de esta naturaleza se obtiene exclusivamente información sobre la localización del vehículo y no se graban imágenes ni sonido[39]. Queda acogida, así, una preocupante doctrina que ya había sido utilizada con relativa frecuencia en el control del empleado fuera del puesto a través de medios tradicionales, como solía ser mediante la contratación de un detective privado encargado de vigilar al operario, admitiéndose, como ya consta, cuando existe una sospecha fundada de incumplimiento, no haya posibilidad de acudir a otro medio de control más adecuado, se desarrolle en lugares observables por el ojo humano desde sitios públicos y sea ponderada o equilibrada, es decir, la vigilancia no sea permanente o continua, sino que se limite a algunos días o a un breve espacio de tiempo evitando un conocimiento permanente[40].

En todo caso, de lo que no cabe duda es de que queda excluido el seguimiento intensivo o ilimitado, debiendo existir algún cauce que permita desactivar el sistema fuera de las horas de trabajo, pues la geolocalización no debe servir para prolongar la subordinación del trabajador más allá del límite temporal determinado por la prestación pactada y tampoco repercutir los datos obtenidos fuera del tiempo de trabajo en el ámbito contractual.

4.5. VERACIDAD, EXACTITUD, ACTUALIZACIÓN Y RECTIFICACIÓN: OPOSICIÓN, CANCELACIÓN Y DESCONTEXTUALIZACIÓN

Exigiendo el párrafo d) del artículo 5 del RGPD que los datos sean «exactos y, si fuera necesario, actualizados», consigue que respondan a la situación real del afectado, creando la correlativa obligación para el responsable del tratamiento (el empresario) de cancelar de oficio aquellos apuntes total o parcialmente inexactos o incompletos y sustituirlos por otros rectificados o inte-

38 STSJ de Cataluña de 23 de mayo de 2013 (rec. 6212/2012).

39 Sentencia del Juzgado de lo Social núm. 32 de Madrid de 1 de octubre de 2003. En el mismo sentido, STSJ de Castilla-La Mancha de 5 de marzo de 2012 (rec. 5194/2011).

40 STS de 21 de junio de 2012 (rec. 2194/2011); asimismo, SSTSJ de Navarra de 3 de octubre de 2008 (rec. 238/2008), de Cataluña de 5 de marzo de 2012 (rec. 5194/2011) y de Andalucía/Granada de 24 de mayo de 2012 (rec. 738/2012).

grados, procediendo también a su actualización, habida cuenta de que una información que no esté al día puede ser considerada –al menos en principio– inexacta.

Como correlato lógico a la obligación de exactitud, actualidad y veracidad en los datos que el artículo 5.1 d) del RGPD hace descansar sobre los responsables del tratamiento, surgen con entidad propia los derechos autónomos de acceso, rectificación sin dilación indebida, supresión y bloqueo (arts. 16 y ss. RGPD y 13 y ss. PLOPD), a ejercitar por el trabajador.

Aun cuando no cabe imponer restricciones indirectas que desincentiven el ejercicio del derecho de acceso como circunscribir su práctica a la terminación de la jornada de trabajo o considerar el tiempo invertido como no trabajado, lo cierto es que el párrafo tercero del artículo 14 del PLOPD impone una fuerte limitación, de difícil encaje en el ámbito laboral, al establecer que el acceso a las informaciones no podrá ejercerse en intervalos inferiores a seis meses salvo causa legítima para ello, teniendo en cuenta la frecuencia de contratos de trabajo de duración inferior a un año. Procede entender, al igual que sucedía en la Ley 15/1999, que podrá ejercitarse el derecho de acceso en periodos inferiores si existe un interés legítimo del afectado teniendo en cuenta la naturaleza de los datos almacenados, su finalidad, el tiempo previsto de almacenamiento, la naturaleza de la actividad de procesamiento a la que se someten, o la repercusión de dichos datos en la adopción de decisiones empresariales (Poquet, 2013, p. 191).

Íntimamente vinculados a las facultades de acceso aparecen los parámetros que gobiernan el almacenamiento de datos informáticos, a saber, oposición, cancelación, olvido y descontextualización (arts. 17 y 21 RGPD y 15 PLOPD), cuyo incumplimiento puede generar la imposición de cuantiosas multas a la entidad mercantil[41]. El principio de congruencia despliega su eficacia durante todo el tiempo en el que los datos recabados permanecen conservados, por lo que deben suprimirse una vez que cesa la finalidad para la que fueron recogidos y registrados. La finalidad esgrimida determina el periodo máximo durante el cual serán almacenados, esto es, solo el estrictamente imprescindible. En el caso de la cibervigilancia, deben borrarse las grabaciones obtenidas por el empleador una vez visualizadas, al igual que los resultados de las auditorías informáticas o de los accesos al centro de trabajo, y solo podrán conservarse si se detecta a través de estos controles alguna irregularidad. En este último supuesto, los registros podrán mantenerse por lo menos hasta el momento de prescripción de las faltas, y en el caso de que fuesen utilizados como prueba para imponer sanciones disciplinarias, durante el tiempo que sea jurídicamente relevante (Desdentado y Muñoz, 2012, p. 69). Parece claro, pues, que en el supuesto de que el trabajador cambie de empresa (por propia voluntad o habiendo sido despedido), o cuando, concluido el proceso de selección el solicitante de empleo no haya sido aceptado (y, por consiguiente, no haya formalizado un vínculo de trabajo con el empresario responsable del fichero), desaparecerá el fin para el cual fueron recabados los datos y, en consecuencia, carecerá de sentido mante-

[41] Tal y como sucede en el caso de una empresa dedicada a la explotación electrónica de datos por cuenta de terceros, que incumple la obligación de inmovilizar un fichero con datos personales. SAN (Sala de lo Contencioso-Administrativo) de 14 de abril de 2014 (rec. 667/2011).

ner tales informaciones en poder de la parte fuerte del contrato. Distinta interpretación supondría una intolerable «apropiación perpetua de amplias facetas de la vida personal» del aspirante a ser contratado o del antiguo trabajador.

Cualquier conservación por más tiempo del estrictamente necesario para «liquidar» los posibles efectos pendientes del contrato de trabajo deberá ser considerada excesiva y, por tanto, ilícita. Elementos distintos confluyen en el supuesto de candidatos que hayan superado las pruebas de selección y, en consecuencia, hayan llegado a formalizar un contrato de trabajo con quien es responsable del fichero. Como observa la doctrina, y en línea de principio –habida cuenta de que la ley no contempla expresamente la posibilidad de destinar los datos inicialmente recogidos con una finalidad determinada a otra igualmente lícita–, la solución debería buscarse en la aplicación de la regla general y, en consecuencia, procedería entender que, si el fin originario de la recogida de datos no era otro sino el de determinar la aptitud profesional del trabajador y esta ya había sido comprobada, tales datos deberían ser cancelados. Como fácilmente procede colegir, es imposible ignorar, sin embargo, el interés empresarial en conservar los datos obtenidos en el proceso de reclutamiento del candidato seleccionado para, con ellos, organizar y dirigir posteriormente su prestación como trabajador en el seno de su unidad productiva.

Por tal razón, y en línea con la Recomendación número 89 (2), sobre el uso de datos personales en el contrato de trabajo, adoptada por el Consejo de Europa el 18 de enero de 1989, es preciso entender que si los datos recabados con ocasión del proceso de selección siguen siendo útiles al empresario para la dirección y organización de la prestación laboral del seleccionado en el seno de la empresa (fin indudablemente legítimo) y, por tanto, adecuados, pertinentes y no excesivos, deberá ser admitido su tratamiento informático con el objeto de:

> No obstaculizar con garantías excesivamente formalistas la actividad de dirección del empresario, hoy cada vez más abocada al uso de sistemas informáticos en la línea del *scientific management*, [pues] sería un requisito absurdo exigir al empleador que cancele unos datos que ya posee y que necesita para un nuevo fin. Ello supondría obligarle a realizar la recogida dos veces, sin que redunde en una mayor garantía de los derechos del trabajador.

En fin, un supuesto especial se plantea también cuando el empresario quiera conservar los datos recabados de un trabajador para fines legítimos a desarrollar en el futuro, como, por ejemplo, la posibilidad de concertar nuevos vínculos contractuales con el mismo (lo cual muchas empresas hacen mediante la incorporación a una bolsa de trabajo de aquellos que no superaran un determinado proceso de selección o que, habiendo suscrito un contrato de duración determinada, han finalizado su vinculación con la empresa pero sin descartar concertar una nueva en el futuro), circunstancia esta que legitima la conservación de los datos, pero, con seguridad, requiere el consentimiento del trabajador (Tascón, 2005, p. 94).

Recientemente, el Tribunal de Justicia de la Unión Europea ha resuelto una cuestión prejudicial planteada por la Sala de lo Contencioso de la Audiencia Nacional española en relación con

determinados preceptos de la Directiva 95/46/CE configurando una detallada doctrina del «derecho al olvido», es decir, del derecho que tienen determinadas personas cuyos datos están alojados en los buscadores de internet a que tales extremos desaparezcan de dichos soportes con el fin de que no sea posible localizar informaciones antiguas o no actualizadas que, mucho tiempo después de su ingreso, siguen apareciendo. Implica el derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye la potestad de limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información) (Martínez, 2016, p. 69). Reconoce, por tanto, la prevalencia de la voluntad del titular sin necesidad de acreditar perjuicio, salvo la concurrencia de circunstancias de interés público. A resultas de este pronunciamiento, la Audiencia Nacional ha establecido los criterios «para reconocer el derecho al olvido», resumidos en el sentido siguiente:

> Quien ejercite el derecho de oposición ha de indicar ante el responsable del tratamiento o ante la Agencia de Protección de Datos que la búsqueda se ha realizado a partir de su nombre, como persona física; los resultados o enlaces obtenidos a través del buscador; así como el contenido de esa información que le afecta y que constituye un tratamiento de sus datos personales a la que se accede a través de dichos enlaces[42].

Por otra parte, los artículos 18 del RGPD y 15.2 del PLOPD reconocen también el derecho al bloqueo, esto es, a la limitación del tratamiento cuando el interesado impugne la exactitud de los datos personales durante un plazo que permita al responsable verificar la corrección de los mismos, cuando el tratamiento sea lícito y el interesado solicite la limitación de su uso, cuando el responsable ya no necesite los datos personales para los fines del tratamiento pero el interesado los reclame para la formulación, ejercicio y defensa de reclamaciones, o cuando el afectado se haya opuesto al tratamiento mientras se verifica si los motivos alegados por el responsable prevalecen sobre los del interesado. En la práctica, este derecho va a funcionar como medida cautelar en el ejercicio de los derechos de rectificación y supresión y su aplicación en el marco del contrato de trabajo es incuestionable.

Todo ello sin olvidar que los artículos 22 del RGPD y 18 del PLOPD reconocen al interesado el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente; regulación que introduce garantías importantes a la hora de aportar medios de prueba justificativos de la imposición de medidas disciplinarias o despidos.

[42] SAN (Sala de lo Contencioso-Administrativo) de 29 de diciembre de 2014 (FJ 13.º).

4.6. PORTABILIDAD DE LOS DATOS Y CONTROL DE LA CESIÓN A TERCEROS

Los artículos 20 del RGPD y 17 del PLOPD reconocen al interesado, de un lado, el derecho a recibir copia de sus extremos personales en un formato electrónico estructurado y de uso común y, de otro, el derecho a solicitar que se transmitan los datos a otro responsable del tratamiento sin que lo impida el primero, permitiendo que las referencias pasen, a instancia del afectado, de uno a otro cuando fuera posible. Este derecho no viola el derecho de preservar la intimidad de las circunstancias informatizadas[43], pues la regla general parte, como no podía ser menos, de la imposibilidad de ceder tales datos a terceros sin consentimiento del afectado[44], admitiendo únicamente excepciones relacionadas con el cumplimiento de obligaciones legales.

La importancia de toda esta regulación en el ámbito laboral es indudable, entendiendo justificadas, dentro de las excepciones previstas, las transmisiones de datos sin consentimiento de los trabajadores a Hacienda y a la Seguridad Social, al igual que a compañías de seguros o gestoras cuando se instrumentan mejoras voluntarias a través de pólizas y planes de pensiones y, cómo no, a la autoridad judicial[45]. No lo es menos la exigencia de su estricta observancia, dado el incremento actual de la circulación de los trabajadores en el mercado y la correlativa necesidad de transmitir la información sobre los mismos, tanto entre los propios empresarios como entre los intermediarios en el proceso de colocación –públicos y privados– en forma de referencias o –por su supuesto– de las denominadas «listas negras» que, si bien han existido siempre, presentan una radical novedad-gravedad en los últimos tiempos dada la extensa difusión –prácticamente ilimitada– de esos datos a través de la informática, máxime cuando la «solidaridad empresarial» tiende a que la información facilitada sea lo más exhaustiva posible en una situación agravada de forma acusada en las grandes organizaciones productivas de los países desarrollados, organizadas en consorcios con gestión centralizada del personal y acumulación de detalles en importantes bancos de datos, de forma tal que ya ni siquiera será necesario solicitar información dentro de cada sector económico sobre un trabajador que hubiera desempeñado funciones con anterioridad en otra empresa del ramo, pues tales referencias obrarán en el banco de datos del consorcio, dando pie al peligro añadido y evidente de transferencia incontrolada de circunstancias, cuyo contenido no será necesariamente político-sindical, sino comprensivo de razones sociales, familiares, de salud y todo el largo etcétera que imaginarse pudiera (consiguiendo un auténtico *block modeling* a partir del cual quedarían clasificados en bloques –«tribus»– los sujetos-candidatos a través de los datos recogidos). De ahí el interés de lo previsto en el artículo 88.2 del RGPD, que exige prestar especial atención a la «transferencia de datos personales dentro de un grupo empresarial».

[43] SSTSJ del País Vasco de 28 de junio de 2005 (rec. 136/2005) y de Madrid de 26 de septiembre de 2006 (rec. 2576/2006).

[44] STC 466/2000, de 30 de noviembre.

[45] Para este último supuesto, SAN (Sala de lo Contencioso-Administrativo) de 15 de octubre de 2013 (rec. 153/2012).

Al mismo tiempo, la desvinculación permitida entre el contenido de la información y las circunstancias en las cuales fue recabada posibilita que determinadas referencias –positivas o negativas–, veraces desde un punto de vista concreto, dejen de serlo cuando son objeto de cruces o cesiones con otras de signo diverso o cuando los datos solicitados para un fin hayan sido utilizados para otros absolutamente distintos. Las agencias privadas de colocación, de recolocación y las empresas de trabajo temporal son, a estos efectos y casi por definición, sujetos para y entre los cuales puede resultar sumamente difícil trazar la frontera entre lo lícito y lo ilícito en el tratamiento y circulación de datos personales informatizados de los trabajadores; ello por no aludir a la existencia de empresas cuyo objeto social es precisamente la recogida y venta de información sobre quienes van a ser objeto de un próximo proceso de selección, las cuales tendrían que –o deberían ser obligadas a– observar rigurosamente las previsiones establecidas en la LOPD, pues un manejo de la información no acorde con la ley permitiría constituir auténticos «documentos volantes de potenciales trabajadores».

No obstante, sería legítima la cesión de datos de los trabajadores por parte de empresas de trabajo temporal, pues, existiendo una verdadera vinculación contractual laboral entre trabajador y empresario temporal, esta presenta la importante peculiaridad de que necesariamente requiere, para el cumplimiento de los fines legítimos de todas las partes de esta particular «relación triangular», la cesión de los datos del asalariado a un tercero –la empresa usuaria–, quedando tal transmisión amparada, en tanto no desborde los límites de lo debido por razón del desarrollo de la prestación laboral –pues también estas entidades han de someterse a la normativa de protección de datos–, por la excepción al consentimiento derivada del desarrollo de una relación jurídica que implica necesariamente la conexión con ficheros de terceros (Cardona, 1999, p. 264). Igualmente quedaría amparada, haciendo referencia a un ejemplo concreto, la cesión por la Tesorería General de la Seguridad Social de los datos sobre cotización de los trabajadores a la Fundación Laboral de la Construcción, con la finalidad de que esta pueda practicar una liquidación frente a la empresa por las contribuciones adeudadas a tenor de lo previsto en convenio colectivo[46].

Dudoso resulta, sin embargo, que puedan quedar salvaguardadas las operaciones de transferencia de datos llevadas a cabo con ocasión de una escisión de sociedades, por cuanto en realidad se produce una duplicación de los «tratamientos de datos» que parece que requeriría el consentimiento del afectado para mayor seguridad de sus intereses. Igualmente complicado resulta el supuesto dado por las empresas en red, en las cuales, una pluralidad de organizaciones productivas son gestionadas como si fueran una sola, lo cual permite presumir que los datos recabados por alguna de ellas van a ser indistintamente utilizados por las otras, algo que resulta difícil que pueda quedar amparado por la excepción al consentimiento de los trabajadores afectados ahora comentada. La misma respuesta merecen los casos de externalización de actividades, pues en el contrato de obra o arrendamiento de servicios ha de constar la finalidad de la prestación y que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable, sin posibilidad de comunicación a otras personas.

[46] STSJ de Asturias de 6 de febrero de 2009 (rec. 2518/2008).

También parece difícil determinar el supuesto de tratamiento y cesión de datos por parte de las agencias privadas de colocación, las de selección de personal o, de nuevo, de las empresas de trabajo temporal cuando estas últimas actúan como agencias de empleo. Estas peculiares entidades aparecen caracterizadas, al margen de sus diferencias, por manejar grandes cantidades de información en su misión de intermediación entre trabajador y empresario, las cuales van a ser registradas en ficheros de datos; dichas informaciones (facilitadas por los propios demandantes de ocupación) serán utilizadas legítimamente en aras de valorar la aptitud profesional de los candidatos en el intento por encontrar al óptimo, de entre los distintos posibles, para ocupar un determinado puesto de trabajo; en ocasiones, dichos datos van a ser comunicados a terceros (principalmente, los empresarios oferentes de empleo). Desde luego, la recogida inicial de datos por parte del sujeto intermediario va a requerir el consentimiento del interesado, así como la debida información por parte del responsable del tratamiento, sin que puedan incorporarse asientos distintos a los necesarios para valorar la aptitud laboral de los candidatos, porque entonces serían excesivos e impertinentes (cuestión esta de especial relevancia, como consta, en un momento en el que la debilidad de quien busca un empleo puede llevarle a estar a disposición de revelar cuantos extremos le sean requeridos) y sin que puedan ser conservados por más tiempo del imprescindible. Pueden ocurrir dos alternativas no por conocidas menos dignas de reiteración: o bien el trabajador es contratado, razón por la cual, cumplida la finalidad de la intermediación, debería procederse a la cancelación de los datos; o bien, pasado un tiempo considerable, el trabajador continúa sin encontrar empleo, motivo por el cual podría justificarse entender revocado su consentimiento si la agencia privada de colocación o la empresa de trabajo temporal no exigiera su renovación. Cosa distinta es que, en la mayoría de los supuestos, no se actúe siguiendo estas pautas en claro perjuicio de los demandantes de ocupación.

Puede traerse a colación un supuesto en el que la AEPD impone una sanción a una empresa que había recibido por fax el currículum de un trabajador enviado por otra empresa, procediendo a llamarle por teléfono para ofrecerle un puesto de trabajo. Posteriormente, la Audiencia Nacional anula la sanción por entender que los datos nunca fueron incorporados a un fichero y la simple recepción por fax del currículum y la llamada telefónica no pueden tener la consideración de tratamiento[47].

La Sala de lo Penal del Tribunal Supremo ha condenado a un funcionario de la Tesorería General de la Seguridad Social por revelación de datos personales de trabajadores y de empresas, referidos a la vida laboral, prestaciones y certificados sobre la situación de cotización, a distintas mutuas y a conocidos[48].

En fin, estas reflexiones pueden llevar a considerar que tan solo una adecuada valoración de los intereses en juego y la aplicación de las reglas de la buena fe, sobre todo en los estadios precontractuales, podrá evitar una ilícita circulación de datos personales automatizados, que tan

[47] SAN (Sala de lo Contencioso-Administrativo) de 18 de diciembre de 2006 (rec. 241/2005).

[48] STS (Sala de lo Penal) de 17 de junio de 2014 (rec. 136/2014).

gravemente podría afectar al futuro profesional del trabajador, cuando no servir para hacer «pública» una información perteneciente a su vida privada, a su esfera íntima.

5. GARANTÍAS: LA OBLIGACIÓN EMPRESARIAL DE ASUMIR DETERMINADAS OBLIGACIONES

Además de los derechos de defensa legalmente reconocidos a los afectados, existen una serie de medidas tuitivas específicas para asegurar su respeto, cuyo incumplimiento desatará los mecanismos de tutela previstos (reclamación ante la AEPD u organismo competente de la comunidad autónoma correspondiente y acceso directo a la vía judicial o después de no haber visto satisfechas todas sus expectativas por los citados órganos administrativos). Estas garantías constituyen otros tantos deberes que pesan sobre la persona del empresario, responsable del fichero automatizado, muchas veces reducidos al mínimo al ser interpretados como meros gastos añadidos al proceso de producción; a saber:

1. Deber de seguridad y principio de *accountability*. El responsable de la base de datos (el empleador) está obligado a velar por la conservación de la información en el ámbito para el cual ha sido creada con la finalidad de evitar su alteración, pérdida, tratamiento o acceso no autorizado (arts. 32 RGPD y 4 PLOPD)[49]. Es más, los responsables de los ficheros no solo deben adoptar medidas de protección de los datos, sino demostrar la eficiencia de las mismas a lo largo de todo el proceso de tratamiento. A estos efectos, deberán configurar las medidas técnico-organizativas necesarias para evitar cualquier «ciberataque», «hackeo», «crakeo», «*phishing*», «visita no deseada» o «fuga» en la información almacenada, singularmente mediante la elaboración del llamado «protocolo de seguridad», debiendo notificar a la autoridad de control y al propio interesado las violaciones de la integridad de los datos (arts. 33 y 34 RGPD). Asimismo, el RGPD promueve el establecimiento de un «sistema de control de los riesgos» asociados al tratamiento de los datos personales que, de manera preventiva, considere la necesidad de tener en cuenta la privacidad y la protección de los datos personales en todo el ciclo de vida de la tecnología, desde la fase de diseño hasta su fin, tanto de los sistemas de información como de las arquitecturas y redes de comunicación, así como los procesos productivos y de negocio, de tal manera que se entienda siempre la privacidad como una opción por defecto (*privacy design*) (García-Perrote y Mercader, 2017b, p. 2).

   Un ejemplo claro de vulneración del cumplimiento de las medidas de seguridad se produce con la transmisión a tiempo real de imágenes del interior de una oficina a través de una página web. El visionado de la cámara era de libre acceso para

[49] STSJ de Canarias/Santa Cruz de Tenerife de 15 de julio de 2005 (rec. 456/2005).

cualquier usuario con la simple selección de la dirección de internet en el navegador. Indica la AEPD y ratifica la Audiencia Nacional que la empresa estaba obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas en la normativa y, entre ellas, las dirigidas a impedir el acceso a los datos personales por parte de terceros no autorizados[50].

Es más, de nada sirve que la empresa haya proporcionado instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos si aparecen en la vía pública escritos que contienen datos de carácter personal de uso empresarial interno (nóminas, recibos de liquidación o de cotización a la Seguridad Social), pues la entidad tendría que haber exigido a los empleados el cumplimiento de dichas instrucciones[51]. Igualmente, la Audiencia Nacional ha considerado que una empresa de trabajo temporal ha incumplido el deber de seguridad al aparecer en la vía pública currículos, fotocopias de DNI, cartillas de la Seguridad Social y de libretas de ahorros y fotografías de aspirantes y de trabajadores de las empresas usuarias[52].

El RGPD y el PLOPD promueven la elaboración de códigos de conducta como mecanismos o instrumentos de autorregulación previendo expresamente que establezcan procedimientos extrajudiciales de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados. Estos instrumentos de *soft law* han de tener presente y ajustarse al principio de *accountabilitity* (AEPD-ISMS Forum, 2017, pp. 25-26), basado en el reconocimiento, asunción de responsabilidad y actitud transparente sobre los impactos de las políticas, decisiones, acciones, productos y desempeño asociados a una empresa, que ha de establecer procedimientos internos previos a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación, dotación de recursos para la gestión de la privacidad, cauces de resoluciones de quejas, auditorías, etc.).

2. Registro de actividades. En las empresas de más de 250 trabajadores y en las de menor volumen de plantilla en las que se realicen tratamientos que puedan entrañar un riesgo para los derechos y libertades de los interesados, que no sea ocasional, o incluyan categorías especiales de datos personales, incluidos los relativos a condenas e infracciones penales, cada responsable y cada encargado del tratamiento llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad (arts. 30 RGPD y 31 PLOPD). No es necesario, por tanto, a partir de ahora proceder a dar de alta el fichero ante la AEPD.

3. Deber de confidencialidad y de secreto profesional. Responden a la misma finalidad analizada de evitar que la información salga del círculo de personas a quienes está destinada, habida cuenta de que sobre los ficheros pesa una «presunción de secreto»

[50] SAN (Sala de lo Contencioso-Administrativo) de 27 de mayo de 2010 (rec. 621/2009).

[51] SAN (Sala de lo Contencioso-Administrativo) de 29 de octubre de 2008 (rec. 508/2007).

[52] SAN (Sala de lo Contencioso-Administrativo) de 12 de julio de 2006 (rec. 8/2005).

(arts. 5.1 f) RGPD y 5 PLOPD). Es exigible tanto al responsable del soporte informático como a los encargados del tratamiento, a los delegados de protección de datos y a quienes tengan acceso a la información existente en cualquier momento de la recepción o tratamiento de los datos personales informatizados (en su caso –lógicamente–, a aquellos en nombre de quienes haya sido realizada la petición), los cuales, en consecuencia, quedan estrictamente limitados en su posibilidad de comunicar la información conocida aun después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo (Monzón, 2017, p. 44)[53].

La Agencia de Protección de Datos ha considerado incorrecta la remisión de un correo electrónico por parte de un servicio de un organismo público dirigido a diversas dependencias de esa entidad en el que figuraban anexos con datos personales de empleados en situación de baja médica para su citación a un reconocimiento, apareciendo el nombre, apellidos y destino, fecha de baja, diagnóstico y observaciones[54]. Se viola también el secreto cuando en los tablones de anuncios de la empresa aparecen los nombres de los trabajadores con la expresión de las causas de sus faltas de asistencia (enfermedad, fecha de baja, permiso sindical, vacaciones y ausencia no justificada) sin contar con el consentimiento de los trabajadores y sin ajustarse a la finalidad de la recogida, que era el control de la presencia y el pago de las nóminas[55].

4. Evaluación de impacto (*privacy impact assessments* o PIA) y consulta previa. El RGPD introduce la obligación del responsable del tratamiento de realizar, con carácter previo, una evaluación del impacto de las operaciones que se van a desarrollar en la protección de datos personales cuando sea probable que un tipo de tratamiento, en particular si se utilizan nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas (art. 35). Debe aplicarse, en síntesis, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales en el ámbito regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado un nuevo mecanismo digital. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas (García-Perrote y Mercader, 2017b, p. 3).

[53] STSJ del País Vasco de 28 de junio de 2005 (rec. 1228/2005).

[54] Resolución AEPD 01007/2007.

[55] Resolución AEPD 20/2010.

El contenido mínimo de dicha evaluación incorporará: una descripción sistemática de las operaciones de tratamiento previstas y de los fines de dicho tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable; una consideración de la necesidad y la proporcionalidad de las operaciones de tratamiento en relación con sus finalidades; una ponderación de los riesgos para los derechos y libertades de los interesados; así como las medidas previstas para hacer frente a los riesgos, incluidas las garantías, los dispositivos de seguridad y los mecanismos para garantizar la protección de los datos personales y para demostrar el cumplimiento de la normativa, teniendo en cuenta los derechos e intereses legítimos de los interesados.

5. Sistema interno de denuncias (*whistleblowing*). La puesta de manifiesto por los empleados de cualquier irregularidad que redunde en beneficio del interés público conlleva, en la mayoría de los casos, un tratamiento de datos personales, de modo que se debe garantizar que la información recogida y tratada se transmita exclusivamente a las personas responsables de la investigación de los hechos denunciados. Además, los sujetos que reciban esta información han de asegurarse de que se maneja de forma confidencial y se adoptan las medidas de seguridad, preservando la identidad del denunciante y los derechos del denunciado en cuanto a información, acceso, rectificación, cancelación y oposición (Mercader, 2018b, p. 161).

6. Sanciones. El RGPD adopta como premisa la reparación integral de los daños y perjuicios causados con la operación de tratamiento, atribuyendo responsabilidad solidaria al responsable y encargado (art. 82.1), sin dejar de imponer sanciones administrativas, cuya cuantía se eleva sustancialmente, distinguiendo dos escalones: el primero, que cuantifica hasta 10 millones de euros o una cantidad equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior; y el segundo, de hasta 20 millones de euros o de un montante equivalente al 4% como máximo del volumen de negocio total del ejercicio financiero anterior (art. 83).

6. ANÁLISIS PARTICULAR DE ALGUNAS CATEGORÍAS ESPECIALES DE DATOS PERSONALES: LOS DATOS BIOMÉTRICOS

La garantía de la intimidad informática del trabajador o demandante de empleo permite distinguir, además, dos niveles de protección en función del bien jurídico tutelado: de un lado, los datos personales que cabría calificar como «ordinarios»; de otro, los datos «sensibles», «especialmente protegidos» (también denominados «superpersonales»), esto es, aquellos estrechamente vinculados a la dignidad y personalidad humana (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de las personas), los cuales, aun cuando están ya garantizados por otros derechos fundamentales, reciben del artículo 9 del RGPD una atención especial, al establecer, como regla general, la prohibición de su tratamiento, que solo puede ser levantada bien cuando exista consentimiento explícito del afectado, bien

cuando el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral y de la seguridad y protección social, bien para proteger intereses vitales del interesado o de otra persona física, bien implique actividades legítimas y con las debidas garantías de una fundación, asociación o cualquier otro organismo sin ánimo de lucro, bien se refiera a datos personales que el interesado ha hecho manifiestamente públicos, bien suponga actuaciones en el ámbito judicial, bien concurran razones de interés público esencial o de interés público en el ámbito de la salud como fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico o prestación de asistencia sanitaria o social, bien con miras al archivo, o bien, para determinadas categorías de este subgrupo de datos –y como excepción–, cuando medie autorización legal en función de su interés general.

El PLOPD distingue, a su vez, dentro del género de datos especialmente protegidos, dos especies diferentes: por una parte, los relativos a la ideología, afiliación sindical, orientación sexual, creencias, religión y origen racial o étnico, en los cuales el mero consentimiento no puede levantar la prohibición del tratamiento (art. 9.1); por otra, el resto, es decir, datos genéticos, datos biométricos o relativos a la salud, en los cuales el consentimiento tiene que ser explícito y no solo sobre el tratamiento, sino también sobre su recogida, pudiendo ser recabados también cuando, por razones de interés general, una ley así lo disponga, sin olvidar lógicamente el elenco de supuestos excepcionales que recoge el RGPD[56].

Por su parte, los datos relativos a infracciones penales no pueden ser objeto de tratamiento salvo que lo permita una norma de derecho de la Unión, la propia LOPD u otras normas de rango legal, no pudiendo ser incluidos en otros ficheros distintos de los de las Administraciones públicas competentes (arts. 10 RGPD y 10 PLOPD). Por su parte, el tratamiento de los datos relacionados con infracciones y sanciones administrativas requerirá que los responsables sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones y que el tratamiento se limite a los extremos estrictamente necesarios para la finalidad perseguida por aquel, o bien que una ley autorice su tratamiento (arts. 86 RGPD y 27 PLOPD).

De todo este catálogo, mención especial merecen los datos biométricos, teniendo en cuenta también su repercusión en las relaciones laborales.

Como ha reconocido el Tribunal de Justicia de la Unión Europea, el control del tiempo de trabajo entra dentro del concepto ordinario de datos personales[57]. Y así la supervisión del acceso y localización del trabajador en la entidad empresarial, a través de sistemas de fichas, tarjetas electrónicas identificativas, huellas o, incluso, mediante infrarrojos, es considerado lícito cuando obede-

[56] STSJ de la Comunidad Valenciana de 7 de junio de 2006 (rec. 1149/2006).

[57] SSTJUE de 30 de mayo de 2013, asunto Worten; 20 de mayo de 2003, asunto Osterreichischer Rundfunk, y 16 de diciembre de 2006, asunto Huber.

ce a motivos de seguridad –bien por el tipo de actividad desarrollada por la empresa o bien por el valor de los elementos utilizados en ella– o «contribuye a comprobar el efectivo cumplimiento de las obligaciones de los trabajadores, obligaciones que se inician en el momento de la puntual incorporación a sus puestos de trabajo y en una estricta observancia de los tiempos de la prestación»[58].

De este modo, por ejemplo, las tarjetas identificativas permiten al empleado, tras conectarlas o acercarlas a un lector, acceder a ciertas salas, operar con el ordenador, poner en marcha máquinas de trabajo..., facilitando al tiempo el trazo de los movimientos realizados y de su ubicación concreta en cada momento. Por su parte, las etiquetas de identificación por radiofrecuencia facilitan el procesamiento de datos sin contacto físico ni interacción visible entre el lector o grabador y la etiqueta. No puede extrañar, por tanto, que la Recomendación de la Comisión de las Comunidades Europeas de 12 de mayo de 2009, en su apartado 7.º, aconseje que los Estados velen por que los operadores (las empresas) elaboren y publiquen una política de información precisa, concisa, exacta y fácil de comprender del uso de estos sofisticados instrumentos, incluyendo la identidad y el domicilio de los operadores, su finalidad, los extremos procesados y un resumen de la evaluación del impacto sobre la intimidad y las medidas para reducirlo. Es más, la AEPD recomienda, en su «Guía sobre seguridad y privacidad de la tecnología RFID», informar a los trabajadores sobre la existencia del tratamiento de forma clara y accesible, indicando la localización de las etiquetas, la existencia de lectores, su posible monitorización y el modo de desactivación.

Ahora bien, las nuevas tecnologías habilitan, incluso, para que el control del acceso a las dependencias empresariales y del horario de trabajo se realice a través de sistemas biométricos, que pueden ser de dos tipos: por una parte, los que permiten el análisis de aspectos físicos y morfológicos de la persona, a través de la comprobación de las huellas dactilares, la verificación de los patrones de la mano, el reconocimiento facial, la geometría del iris, los rasgos de la voz, las estructuras venosas, las pulsaciones o las características de la retina; por otra, los que facilitan la valoración de los comportamientos de una persona, mediante la comprobación de su escritura, su firma o la presión de las teclas del ordenador. La principal ventaja de estos mecanismos radica en que no permiten la suplantación del sujeto sometido a la vigilancia, a diferencia de las tarjetas de identificación tradicionales, que admitían la transferibilidad (Poquet, 2013, p. 282). El RGPD incorpora los datos biométricos entre las categorías especiales, quedando prohibido su tratamiento (art. 9.1). No obstante, como ya consta, el artículo 9.2 b) excepciona la anterior regla cuando:

> El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado (García-Perrote y Mercader, 2017a, p. 1).

[58] STSJ (Sala de lo Contencioso-Administrativo) de Cantabria de 21 de febrero de 2003 (rec. 763/2002).

En el entorno laboral, estos sistemas biométricos de reconocimiento resultan muy útiles para el control del acceso físico a instalaciones; en particular, lugares críticos como centrales energéticas o sensibles o de estancia restringida. Sirven también para ejercer un control horario y de presencia de los trabajadores, ya sea para evaluar los momentos de entrada y salida, ya sea para calcular el tiempo dedicado por los trabajadores a la actividad profesional, lo que se revela particularmente útil en empresas con horario flexible o con jornadas irregulares. Y son, asimismo, una solución idónea para garantizar el acceso a los equipos técnicos, a través de lectores de huellas o detectores de la mirada como alternativa más segura que las claves de acceso (Goñi, 2009, p. 51).

Con mayor detalle, en todo proceso de reconocimiento biométrico se pueden diferenciar dos fases: una, la de inscripción o alistamiento de muestras biológicas, que consiste en la captación por medio de un sensor específico para cada tipo de técnica biométrica de una serie de rasgos específicos del usuario, y en la transformación de esos datos en una secuencia numérica conformándose una plantilla que queda registrada en una base de datos; otra, la de comparación, en la que se vuelve a recoger una muestra biométrica y la huella así obtenida se compara con la plantilla almacenada, al objeto de comprobar la equivalencia (Poquet, 2013, p. 79).

Precisamente, la primera fase de recogida y tratamiento de los datos biométricos puede poner en peligro los derechos fundamentales de los trabajadores al suponer riesgos para la vida privada; no en vano –y como mero ejemplo–, el iris puede revelar el consumo de drogas y de alcohol o el padecimiento de enfermedades como hipertensión o diabetes. De ahí que la doctrina judicial venga aplicando el juicio de proporcionalidad para valorar la licitud de la decisión empresarial de instalación de estas técnicas. En consecuencia, cabe entender permitido su uso si es el único medio que puede cumplir con la finalidad asignada, es decir, no existe otro menos gravoso con el que cubrir las necesidades empresariales, y se trata de un cauce imprescindible[59]. Todo ello sin olvidar aplicar todos los principios de tutela del ordenamiento de protección de datos[60].

En este contexto, quizá los pronunciamientos judiciales más llamativos son los referidos al citado control biométrico de la mano que permite identificar al trabajador mediante un reconocimiento tridimensional: largo, ancho y espesor. Cuestionada la licitud de semejante método utilizado en una Administración regional como fichaje horario del personal, el tribunal considera, en primer lugar, que resulta idóneo para conseguir el objetivo propuesto, cual es «lograr un mayor nivel de eficacia en la Administración pública controlando el efectivo cumplimiento de sus obligaciones por parte de los empleados públicos». Reconoce el órgano judicial que «la existencia de otros posibles sistemas igualmente idóneos para conseguir la referida finalidad no convierte el medio enjuiciado en ilícito, siendo legítimo que la Administración opte, dentro de la legalidad, por aquel cauce que considere más conveniente». En segundo término, la medida se entiende necesaria debido al «notorio carácter imperfecto de los sistemas de control más comúnmente

[59] STSJ de Murcia de 25 de enero de 2010 (rec. 1071/2009).

[60] STS (Sala de lo Contencioso-Administrativo) de 2 de julio de 2007 (rec. 5017/2003).

usados», que no impiden «la sustituibilidad en su cumplimiento». Finalmente, se concluye que la implantación supone más ventajas para el interés general que perjuicios sobre otros valores en conflicto, porque de esta forma se garantiza que el empleado público cumplirá debidamente sus obligaciones y ello redundará en una mayor eficiencia de la Administración para la consecución de los intereses generales[61].

Atendiendo a este razonamiento, muy cuestionable resulta, sin embargo, la implantación de chips subcutáneos entre el dedo índice y el pulgar por la que han optado algunas compañías belgas, pues no solo puede atentar frente a la privacidad del trabajador, sino también causar efectos nocivos para la salud física.

7. LA PROTECCIÓN DE DATOS COMO NUEVO YACIMIENTO DE EMPLEO

La progresiva y vertiginosa irrupción de la tecnología digital, telemática, robótica, plataformas, algoritmos, internet de las cosas, comunicaciones máquina a máquina, realidad aumentada e inteligencia artificial en la actividad productiva bajo la denominación de industria 4.0 ocasiona cuatro cambios importantes en la industria tradicional: la irrelevancia de la ubicación geográfica, el papel clave de las plataformas, la importancia de los efectos de red y, como ya consta, el uso de grandes bancos de datos. Cierto es que todas estas innovaciones provocan una amenaza constante de destrucción de empleos ante el desempeño por robots de gran parte de las tareas, el posible acceso a bienes y servicios sin intermediación de empresa alguna o la pérdida de cualificación de los trabajadores ante la automatización de las cometidos («desempleo tecnológico»). No menos verdad resulta, sin embargo, que las nuevas tecnologías pueden contribuir también a la generación de ocupaciones laborales (entre otras, analistas de datos; *data miners*; *data arquitects*; expertos en *software* y aplicaciones; *social media*; especialistas en *networking*, inteligencia artificial, internet de las cosas y *cloud computing*; diseñadores y creadores de máquinas de nueva inteligencia, robots e impresoras 3D; expertos en negocios digitales y especialistas en *e-commerce*) (Álvarez, 2017, p. 82).

La propia normativa de protección de datos recoge una nueva ocupación laboral, que se añade a las ya existentes de encargado de seguridad o encargado del tratamiento (muchas veces, personas físicas que actúan como asalariados del empresario responsable; en otras ocasiones, personas jurídicas que intervienen como gestorías especializadas): el delegado de protección de datos (DPD) o *data protection officer* (DPO), regulado en los artículos 37 a 39 del RGPD y 34 y siguientes del PLOPD, capaz de proporcionar abundantes expectativas de empleo, esperando que se convierta en una de las profesiones cualificadas más demandadas a lo largo de los años venideros.

[61] SSTSJ (Sala de lo Contencioso-Administrativo) de Cantabria de 10 de enero de 2003 (recs. 760/2002 y 517/2002) y 14 y 28 de marzo de 2003 (recs. 893/2002 y 739/2002).

La designación de esta figura, que puede estar en la plantilla de la empresa o puede ser externa vinculándose a través de un contrato de prestación de servicios, es obligatoria en tres supuestos (Ortega, 2018, p. 5): 1) cuando el tratamiento es llevado a cabo por una autoridad u organismo público; 2) cuando las actividades principales del responsable o del encargado del tratamiento consisten en operaciones que requieren el seguimiento regular y sistemático de los interesados a gran escala; 3) cuando las actividades principales del responsable o del encargado del tratamiento impliquen el manejo a gran escala de categorías especiales de datos o referencias personales relacionados con condenas y delitos penales. Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y los fines de dicho tratamiento. Se ocupará, pues, de supervisar, coordinar, gestionar, llevar la implantación continua y las auditorías internas en materia de protección de datos, con el fin de prevenir y evitar conductas o praxis que pueden desembocar en sanciones administrativas (Plaza, 2017, p. 20). Es, en definitiva, una suerte de «delegado de cumplimiento» de la normativa de protección de datos, que presta ayuda o colaboración necesaria con el responsable o encargado del tratamiento.

Algunas de las empresas que necesitan contar con un DPD son, entre otras, colegios profesionales, centros docentes, entidades de seguridad privada, centros sanitarios, compañías de seguros, empresas de prestación de servicios de comunicaciones electrónicas y de la sociedad de la información, entidades financieras, empresas de inversión, distribuidores y comercialización de suministros energéticos (Sierra, 2018, p. 241).

El DPO tiene una posición especial en el organigrama empresarial: actúa como interlocutor ante la AEPD; cuando sea trabajador por cuenta ajena responsable o encargado del tratamiento, no podrá ser despedido ni sancionado por el ejercicio de sus funciones, debiendo considerar tales decisiones empresariales nulas en parecidos términos a lo que sucede con la garantía de la que gozan los representantes de los trabajadores por el ejercicio de sus tareas como tales representantes; si es un sujeto externo a la organización empresarial, actuará con plena independencia y autonomía y, en todo caso, comunicará a los órganos de la Administración la existencia de cualquier vulneración relevante en materia de protección de datos (Martos, 2017, p. 7). En el desempeño de sus quehaceres estará obligado a mantener el secreto o la confidencialidad.

La AEPD ha diseñado un esquema de certificación de la capacitación de dichos profesionales basado en la norma ISO 17024.

8. CONCLUSIÓN

Pese al fortalecimiento de la exigencia del consentimiento o, al menos, del ineludible derecho de información, la tutela reforzada de los datos integrantes de categorías especiales, el agravamiento de las sanciones administrativas, el diseño de la figura del DPD y la garantía del derecho al olvido por los que apuesta el nuevo RGPD, lo cierto es que muchas de sus previsiones genéricas son difíciles de trasladar al marco de las relaciones laborales. Es más, la práctica se encarga de

demostrar que la protección de datos es una de las asignaturas pendientes en los procesos actuales de dinámica de la gestión empresarial. Siendo indubitada hoy en día la aplicación de la normativa de protección de datos en los centros de trabajo, lo cierto es que su observancia no es, en este campo, todo lo satisfactoria que cabría esperar; circunstancia preocupante por sí sola, capaz de suscitar las más inquietantes dudas acerca de cómo y por qué los derechos del ciudadano (léase –por lo que a este estudio interesa– trabajador) están siendo sistemática y reiteradamente conculcados.

Dos pueden ser las razones principales que propician una situación de ilegalidad (e inconstitucionalidad) tan manifiesta. En primer lugar, cabe aludir, sin lugar a dudas, a la gran complejidad técnica que, de suyo, supone cualquier intento por dar cumplimiento a la normativa sobre protección de datos sobre todo en las empresas de reducidas dimensiones. En segundo término, es menester dar cuenta de una perspectiva, por desgracia, de hondo calado en la estructura empresarial española –manifiesta también, sobre todo, en las pequeñas y medianas empresas–, de conformidad con la cual cualquier exigencia de tutela de algún derecho fundamental de los trabajadores suele ser vista por parte de quien dirige la organización productiva como puro y simple coste empresarial, que habrá que evitar o, al menos, reducir en cuanto sea posible a su mínima expresión a riesgo de suponer un freno evidente al libre desarrollo de la competitividad y del beneficio (Tascón, 2008, p. 465). Al tiempo, son flagrantes los atentados al derecho de protección de datos derivados del ejercicio del poder de control empresarial, pues muchas veces se confunde la finalidad, en sí misma legítima de supervisión y a resultas de ello de poder ejercer –cuando proceda– el poder disciplinario, con la licitud del medio digital de supervisión empleado, que no siempre es el menos invasivo.

Frente a este desolador panorama de inobservancia generalizada, tan solo cabe efectuar una invitación decidida hacia la sensibilización frente a una realidad que está llamada a terminar por imponerse en los próximos años, recordando las gravísimas consecuencias que para el responsable de la utilización (la empresa) se pueden –y deben– derivar de la transgresión de las normas encargadas de regular el tratamiento de los datos personales, tanto bajo la forma de las abundantes infracciones y cuantiosas sanciones administrativas que deberá imponer la AEPD, como a través de las pertinentes indemnizaciones por los daños y perjuicios causados, lo cual puede encontrar respuesta específica en el orden laboral, bien a través del procedimiento de tutela de los derechos fundamentales (arts. 177 y ss. Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social), obteniendo en este caso, además de la compensación económica pertinente, la cesación de la conducta empresarial, bien, y cuando la gravedad del incumplimiento empresarial así lo permitiera, la resolución del contrato de trabajo a instancia del trabajador con la pertinente indemnización de 33 días de salario por año de servicio con el máximo de 24 mensualidades (art. 50 ET).

En fin, aun cuando la eficacia de la tutela reparadora es indudable, la promulgación de una nueva ley de protección de datos personales no debe hacer olvidar la necesidad de introducir normas específicas de derecho del trabajo que sigan las indicaciones del Tribunal Europeo de Derechos Humanos, introduciendo un nuevo título en el ET, para regular los derechos fundamentales de los trabajadores en las relaciones laborales, despejando las incertidumbres del ejercicio de dichos derechos fundamentales en igualdad y sin discriminaciones y en relación con las tecnologías de la información y comunicación, con el entorno tecnológico digital, que es una realidad insoslayable,

virtualmente ausente en la actualidad (Casas, 2018, p. 119; Conclusiones FIDE, 2016, p. 3). Tratar de dar respuesta a los interrogantes generados por la protección de los datos personales de los trabajadores exige, pues, la difícil tarea de partir de las reglas jurídicas que ordenan con carácter general el tratamiento automatizado, ahora singularmente abanderadas por el Reglamento (UE) n.º 2016/679, para, a partir de tales pilares, construir pautas especiales que atiendan a las características propias del trabajo asalariado.

Referencias bibliográficas

AEPD-ISMS Forum. (2017). Código de buenas prácticas en protección de datos para proyectos big data. Recuperado de <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf> (consultado el 11 de abril de 2018).

Alemán Páez, F. (2017). El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la «Loi Travail N.º 2016-1088». *Trabajo y Derecho*, *30*, 12-33.

Álvarez Cuesta, H. (2017). *El futuro del trabajo vs. el trabajo del futuro. Implicaciones laborales de la industria 4.0*. Madrid: Colex.

Cardona Rubert, M. B. (1999). *Informática y contrato de trabajo*. Valencia: Tirant Lo Blanch.

Carrillo, M. (2016). El uso de internet en la empresa: a propósito de la STEDH de 12 de enero de 2016. Caso Bărbulescu c/ Rumanía. *Iuslabor*, *1*, 1-16.

Casas Baamonde, M. E. (2018). Informar antes de vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital? La necesaria intervención del legislador laboral. *Derecho de las Relaciones Laborales*, *2*, 103-121.

Conclusiones FIDE (2016). Recuperado de <https://www.fidefundacion.es/attachment/764963/> (consultado el 11 de abril de 2018).

Cuadros Garrido, M. E. (2017). La mensajería instantánea y la STEDH de 5 de septiembre de 2017. *Aranzadi Doctrinal*, *11*, 129-146.

Desdentado Bonete, A. y Muñoz Ruiz, A. B. (2012). *Control informático, videovigilancia y protección de datos en el trabajo*. Valladolid: Lex Nova.

Gallardo Moya, R. (2017). Un límite a los límites de la vida privada y de la correspondencia en los lugares de trabajo. Comentario a la sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de septiembre de 2017 en el caso Bărbulescu II c. Rumanía. *Revista de Derecho Social*, *79*, 141-156.

García-Perrote Escartín, I. y Mercader Uguina, J. R. (2017a). El control biométrico de los trabajadores. *Información Laboral*, *3*.

García-Perrote Escartín, I. y Mercader Uguina, J. R. (2017b). El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo al tratamiento de datos personales, un primer acercamiento. *Información Laboral*, *2*.

Goñi Sein, J. L. (2004a). Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos. En M. R. Alarcón Caracuel y R. Esteban Legarreta (Coords.), *Nuevas tecnologías de la información y la comunicación y derecho del trabajo* (pp. 49-87). Albacete: Bomarzo.

Goñi Sein, J. L. (2004b). Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos. *Justicia Laboral*, *17*, 13-54.

Goñi Sein, J. L. (2009). Controles empresariales: geolocalización, correo electrónico, internet, videovigilancia y controles biométricos. *Justicia Laboral*, *39*, 11-58.

Goñi Sein, J. L. (2017). Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento europeo de protección de datos de 2016. *Revista de Derecho Social*, *78*, 15-42.

Martínez López-Sáez, M. (2017). La vigilancia electrónica en el contexto laboral europeo y estadounidense: perfilando el derecho a la protección de datos en el trabajo. *Revista General de Derecho del Trabajo y de la Seguridad Social*, *47*.

Martínez Rojas, A. (2016). Principales aspectos del consentimiento en el Reglamento general de protección de datos de la Unión Europea. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, *42*, 59-82.

Martos Díaz, N. (2017). El delegado de protección de datos: ¿figura interna, externa o mixta? *Actualidad Jurídica Aranzadi*, *936*, 7-7.

Mercader Uguina, J. R. (2017). *El futuro del trabajo en la era de la digitalización y la robótica*. Valencia: Tirant Lo Blanch.

Mercader Uguina, J. R. (2018a). La protección de datos personales del trabajador. La obligación del empresario de informar al trabajador sobre sus condiciones de trabajo. En M. E. Casas Baamonde y R. Gil Alburquerque (Dirs.), *Derecho social de la Unión Europea. Aplicación por el Tribunal de Justicia* (pp. 745-784). Madrid: Francis Lefebvre.

Mercader Uguina, J. R. (2018b). *Protección de datos en las relaciones laborales*. Madrid: Francis Lefebvre.

Miguel, J. de (2018). La obligación de informar de los encargados de tratamiento en el RGPD. *Actualidad Jurídica Aranzadi*, *938*, 11-11.

Miñarro Yanini, M. (2004). Límites a las facultades empresariales de vigilancia y control. *Tribuna Social*, *158*, 7-14.

Molina Navarrete, C. (2017). El poder empresarial de control digital: ¿nueva doctrina del TEDH o mayor rigor aplicativo de la precedente? A propósito de la STEDH de 5 de septiembre de 2017, caso Bărbulescu c. Rumanía. *Iuslabor*, *3*, 287-297.

Molina Navarrete, C. (2018a). De «Bărbulescu II» a «López Ribalda»: ¿qué hay de nuevo en la protección de datos de los trabajadores? *RTSS.CEF*, *419*, 125-135.

Molina Navarrete, C. (2018b). ¿Saber es poder?: conectividad empresarial, geolocalización (GPS) y autodeterminación digital del trabajador. Comentario a la Sentencia del Tribunal Superior de Justicia de Andalucía/Granada 1937/2017, de 18 de septiembre. *RTSS.CEF*, *419*, 136-146.

Monzón Pérez, H. (2017). El «deber de protección de datos personales» de los trabajadores y su transgresión. *Información Laboral*, *2*, 37-55.

Ortega Giménez, A. (2018). El Reglamento general de protección de datos en la UE en la empresa: novedades prácticas. Recuperado de <http://diariolaley.laley.es> (consultado el 11 de abril de 2018).

Plaza Penadés, J. (2017). Implementando el nuevo Reglamento general europeo de protección de datos. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, *43*, 19-21.

Poquet Catalá, R. (2013). *El actual poder de dirección y control del empresario*. Pamplona: Aranzadi.

Preciado Domènech, C. H. (2017). La vídeo vigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal. ¿Es acorde la doctrina del TC y del TS con el derecho de la UE? *Revista de Derecho Social*, *77*, 175-194.

Rodríguez Escanciano, S. (2009). *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*. Albacete: Bomarzo.

Rojo Torrecilla, E. (2018). Derecho del trabajador a la privacidad en la empresa y límites a su control por cámaras de vigilancia. Estudio del caso López Ribalda y otras contra España (a propósito de la Sentencia del Tribunal Europeo de Derechos Humanos de 9 de enero de 2018). *Revista Derecho de las Relaciones Laborales*, *2*, 135-152.

San Martín Mazzucconi, C. (2014). El derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos. En C. San Martín Mazzucconi (Dir.) y A. V. Sempere Navarro (Coord.), *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico* (pp. 205-327). León: Eolas.

Sancho López, M. (2017). Nuevas amenazas para la protección de datos en el contexto del big data. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, *43*, 123-142.

Sierra Benítez, E. M. (2018). El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico. *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, *6*(1), 236-260.

Tascón López, R. (2005). *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*. Madrid: Civitas.

Tascón López, R. (2008). La protección de datos personales de los trabajadores. *Revista Jurídica de Castilla y León*, *16*, 447-502.

Thibault Aranda, J. (2006). *Control multimedia de la actividad laboral*. Valencia: Tirant Lo Blanch.

Thibault Aranda, J. (2009). La vigilancia del uso de internet en la empresa y la protección de datos personales. *Relaciones Laborales*, *1*, 215-226.

Valdés Dal-Ré, F. (2017). Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa. *Revista de Derecho Social*, *79*, 15-35.